

КОНТРОЛИРУЕМЫЙ ВЗЛОМ

2-е издание

БИБЛИЯ
СОЦИАЛЬНОЙ
ИНЖЕНЕРИИ



Юрий Другач

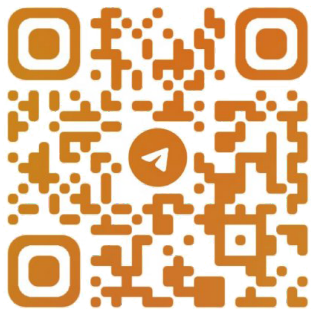
bhv®

Юрий Другач

КОНТРОЛИРУЕМЫЙ ВЗЛОМ

БИБЛИЯ
СОЦИАЛЬНОЙ
ИНЖЕНЕРИИ

2-е издание



@CODELIBRARY_IT

Санкт-Петербург
«БХВ-Петербург»

2024

УДК 004.415.538
ББК 32.973.26-018.2
Д76

Другач Ю. С.

Д76 Контролируемый взлом. Библия социальной инженерии. —
2-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2024. — 208 с.: ил.
ISBN 978-5-9775-1990-8

Книга рассматривает используемые современными киберпреступниками методы социальной инженерии и способы защиты от нее — как организационные, так и технические. Приведено 130 практических примеров атак, даны примеры фишинговых писем, раскрыты применяемые мошенниками психологические приемы и трюки, позволяющие вводить пользователей в заблуждение, подробно разобран используемый злоумышленниками программный инструментарий. Описаны различные векторы атак: по электронной почте, в мессенджерах, в социальных сетях и в реальной жизни. Предложена методика создания 10 000 сценариев учебных атак, а также дана пошаговая инструкция их проведения от этапа подготовки до составления отчета. Во втором издании особое внимание уделено использованию в социальной инженерии и фишинге современных технологий искусственного интеллекта.

Для специалистов по информационной безопасности

УДК 004.415.538
ББК 32.973.26-018.2

Группа подготовки издания:

Руководитель проекта	<i>Павел Шалин</i>
Зав. редакцией	<i>Людмила Гауль</i>
Редактор	<i>Григорий Добин</i>
Компьютерная верстка	<i>Ольги Сергиенко</i>
Дизайн обложки	<i>Зои Канторович</i>

Подписано в печать 03.07.24.
Формат 70×100^{1/16}. Печать офсетная. Усл. печ. л. 16,77.
Тираж 1200 экз. Заказ № 10119.
"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.
Отпечатано с готового оригинал-макета
ООО "Принт-М", 142300, М.О., г. Чехов, ул. Полиграфистов, д. 1

ISBN 978-5-9775-1990-8

© Другач Ю. С., 2024
© Оформление. ООО "БХВ-Петербург", ООО "БХВ", 2024

Оглавление

https://t.me/it_books/2

Предисловие	11
Об этом издании	11
От автора	12
Кому и как можно использовать эту книгу?	14
Для представителей служб ИБ, СБ и ИТ-служб.....	16
Для пентестеров.....	17
Для хакеров.....	17
Что такое социальная инженерия?.....	17
Опасность социальной инженерии.....	18
Цитаты.....	19
Ущерб от СИ.....	19
Глава 1. Онлайн-атаки	23
Подготовка	23
Пентестеру	24
OSINT для СИ	24
Разведка боем	25
Проверка антиспама	28
Переходим на личности	28
Какую фишинговую форму создавать?	29
Несуществующий адрес.....	29
Пробиваем MX-записи.....	30
Неведение.....	30
От чьего имени писать?.....	31
ВЕС-атака.....	32
Таблица персонализации	33
Пример email-MITM.....	34
Какой фишинговый домен купить?.....	35
Безопаснику	35
Готовим атаки	36
Атаки по email	36
Идеи по составлению темы письма.....	36
Какую подпись и оформление использовать?.....	37

Выбираем контекст	37
Векторы и сценарии	38
Контекст: событийные атаки (Event attacks)	38
Событийные атаки: чрезвычайная ситуация	38
Событийные атаки: праздники	39
Событийные атаки: политика	39
Контекст: причина	40
Якобы взлом	40
Внеплановая проверка от СРО	41
Неудачные попытки авторизации	42
Уведомление	42
Что вы делаете в Бразилии?	42
Контекст: запросы	43
Контекст: вопросы	43
Вопрос с вложением	43
А что это вы мне отправили?	43
Контекст: отправка	44
Контекст: изменения	44
Контекст: желание	45
Контекст: «непонятки»	46
Переписка-ссылка	46
Одинокий файл	46
Усиление контекста	46
Усиление контекста: эмоции	47
Усиление контекста: давление	48
Адресаты в копии	48
Письма от госорганов	49
Срочно обновитесь	50
Усиление контекста: ложь	50
Фейковая переписка	51
Фейковая пересылка	51
Усиление контекста: совпадение	52
Источники фишинговых писем	52
Файлы	53
Некорректное отображение	53
Подарочный сертификат	53
Пустой файл	54
Документ с «мыльцой»	56
Имитация Excel-таблицы в Word-документе	60
Небезопасный PDF-файл	60
Файл как прокладка перед нагрузкой	62
Отсутствующий сертификат	64
Разрешите и заполните	65
Файл ICS	66
Социальные сети	67
Подготовка	68
О поиске сотрудников в соцсетях	72
Клонирование аккаунтов	73

Медленно, но верно	73
Многоходовка в соцсети	73
Терпеливо ждем	74
Поддельный рекрутер	74
Мессенджеры	75
Telegram-каналы	76
Сотрудник — физлицо	76
Онлайн-консультанты	76
Веб-сайты	77
Поддельное окно для ввода логина и пароля	77
Скачайте на нашем сайте	78
Корпоративные порталы	78
Разрешите уточнить	79
Новостные ресурсы	79
Туда, да не туда	80
Фейковая капча и предупреждение о cookie	80
Всплывающее окно	81
Персонализированный сайт	83
Покажи себя	84
Реклама	85
Таргет по MAC-адресу	85
Таргет по геолокации	86
Адвёртинг	86
Фиктивный APK-файл	87
Лидеры мнений	87
Видео-deerfake	87
Видео без видео	88
Аудио-deerfake	88
Find trap сценарии	89
Find trap с помощью рекомендаций	90
Выдуманная компания	91
Find trap с помощью звонков	91
Продажа фиктивного сертификата	91
Комментарии	92
Легализованная СИ	92
Отправили к вам	93
Фишинг	94
Проверка на утечку	94
Data-phishing	94
Многоходовки	96
Фейковое интервью	97
Отложенная отправка	97
Цепочки писем	98
Цепочки писем: неправильная кодировка как повод	98
Цепочки писем: простите, не туда	98
Цепочки писем: нас взломали	98
Цепочки писем: использование для data-фишинга	99
Фейковые посетители	99

Глава 2. Технологические трюки введения в заблуждение.....	101
Маскировка ссылок	101
Символ @.....	101
Слеш в Unicode.....	102
Домены в Punycode	102
Зашумление юникодом	102
Обфускация ссылок.....	102
QR-коды	103
Некорректный протокол	104
Ссылки в виде картинок	104
Ссылка в документах	104
Очень длинная ссылка	105
Ссылка виде цифр	106
Невидимая при наведении мыши.....	106
Редиректы	107
Неактивные ссылки.....	108
Похожие на официальные	109
Ссылки в поддоменах	110
Сращивание с поддоменом.....	110
Сращивание с протоколом	110
Домен после слеша.....	110
В дополнение	110
Капча от ботов защитного ПО.....	110
Одноразовые ссылки	111
Подделка отправителя.....	111
Email с официального ресурса.....	112
Вложения и файлы.....	113
Файлы Microsoft Office	113
Рушим шаблоны поведения через печать	114
PDF-файлы	115
HTML-файлы.....	116
Маскировка расширения <i>html</i>	117
Архивы с паролем	117
Архивы без пароля	118
Редко используемые форматы архивов.....	119
Онлайн-документы	119
Excel-файл, размещенный онлайн	119
Глава 3. Атаки в офлайне.....	123
Проникновение на физические объекты.....	123
Предмет в руках	123
Подслушанная легенда	124
Проведение интервью	125
Давайте помогу.....	125
Корпоративная столовая.....	125
Небезопасные парковки.....	126
Паровозик.....	126
Мусорный дайвинг	127
Отделение банка.....	127

Отвлекающий маневр	128
Потенциальный клиент	128
Собеседование	128
Гостевой пропуск	128
Подделка карты-пропуска	129
Черный ход	129
Плечевая атака	129
Piggybacking	129
USB-устройства	130
Таргетированная флешка	131
Флешка с легендой	131
«За букет роз»	131
Juice jacking	132
Смишинг	132
Вишинг	133
Подделка номера	133
Многоходовый звонок	133
Вернитесь на работу	133
Забыл кодовое слово	134
Отсылка к отпускинику	134
Синхронный ввод	134
Телефон + find trap	135
Любой добавочный	135
Китовые атаки	135
Усиление звонком	136
Квид про кво	136
Callback phishing	137
Нас взломали, помогите восстановить	138
Бумага не во благо	138
Подбрасывание корпоративных документов	138
Визуальный пропуск	138
Реклама на бумаге	139
QR-коды на бумажных носителях	139
Справка	139
Общественный транспорт	141
Wi-Fi	141
Мероприятия	141
Двухдневное мероприятие	142
Организовал себе на голову	142
Конференции, выставки и форумы	142
Пришел к одним, пошел к другим	142
Корпоратив	142
Комбинирование	143
Истории для вдохновения	143
Обход системы	143
Пентест тюрьмы	145
Случай в отеле	146
Неприступная крепость	148

Глава 4. Проведение онлайн-атак по email	151
Какой софт использовать?	151
Список email-пользователей	152
Как создавать сообщения для атак?	152
Чек-лист применения электронной СИ.....	154
Как повысить киберграмотность сотрудников?	154
Технические аспекты обучения.....	156
Глава 5. Технические меры противодействия СИ	159
Софт	159
Корпоративный браузер	159
Сегментация сети и Zero Trust	160
Невозможность залогиниться в почте с недоверенных IP-адресов	160
Обнаружение повторного использования пароля	160
Фиды о фишинге	161
Антифишинговый шрифт	161
Настройка DKIM, SPF и DMARC	162
Предотвращение выполнения исходного кода	163
SSO	164
Sandbox.....	165
Технические аспекты защиты от СИ	165
Способы применения чек-листа	165
Выбирайте методы фильтрации вредоносного содержимого в зависимости от вашей тактики.....	165
Настройте защиту от фишинговых ссылок	166
Ссылки, похожие на официальные сайты	167
Настройте защиту от вредоносных вложений.....	167
Возможные к запрету расширения, используемые в фишинге.....	167
Настройте проверку заголовков email на подозрительные признаки	167
Настройте защиту по содержимому письма.....	168
Hardware	168
Межсетевые экраны	168
FIDO	169
Различия между UAF, U2F и FIDO2	169
Недостатки этого способа защиты	170
OTP-токены.....	170
Глава 6. Организационные меры противодействия СИ	173
Модель зрелости осведомленности о безопасности	173
Одобрение процесса повышения осведомленности у руководителей.....	175
Обучение: памятки, курсы, форматы обучения.....	176
Регламенты	177
Регламент обучения персонала.....	178
Некоторые аспекты для учета в регламентах	178
Контроль реквизитов	179
Дополнительная проверка перед оплатой	179
Как вести себя с гостями?	179
Общение с коллегами	180
72 минуты до начала конца.....	180
Сотни регламентов по информационной безопасности	180

Послесловие	183
Приложение 1. Генератор онлайн-СИ	185
Приложение 3. Классификатор СИ	186
Электронная социальная инженерия <i>v0.81</i>	186
Офлайн социальная инженерия <i>v0.2</i>	192
Приложение 3. Таблица персонализации.....	194
Приложение 4. Бесплатное в помощь службе ИБ и ИТ.....	195
Приложение 5. Критерии выбора платформы по повышению осведомленности	196
Приложение 6. Словарь терминов.....	202

Предисловие

Об этом издании

Во второе издание этой книги добавлено более 7 тысяч слов, и немалый вклад в такое ее обновление сделали читатели предыдущего издания. Вообще, большое спасибо всем, кто оставил отзывы о книге на маркетплейсах и в личных письмах. Это действительно мотивирует продолжать исследование социальной инженерии.

Хотелось бы конкретно поблагодарить некоторых читателей первого издания книги за их отзывы и пожелания. Читательнице с ником Toyota Mark2 — за наводку на раскрытие темы с ИИ, теперь в книге появилась отдельная глава, освещающая некоторые аспекты этой темы. Григорию Лебедеву — за вопросы о безопасности операционных систем macOS и Linux. Хотя эта тема и для другой книги, будет о чем подумать в разрезе технических уловок и социальной инженерии применительно к этим операционным системам. А пока, раз книга посвящена социальной инженерии, в это ее издание добавлено описание случая с журналистом НВО, который работал на macOS. Оно приведено в конце главы 3 — в разделе «Истории для вдохновения». Благодарю также Григория Емельянова. Спасибо ему за идею по раскрытию темы ложных вакансий и резюме. В этой книге мы не рассматриваем атаки на физических лиц, но для пентеста компаний было добавлено несколько сценариев на тему рекрутинга.

Итак, в этом издании книги появились следующие обновления.

□ В главе 1:

- в раздел «Усиление контекста: давление» добавлен трюк «Адресаты в копии»;
- в раздел «Социальные сети» добавлен сценарий «Поддельный рекрутер»;
- в разделе «Многоходовки» описан новый пример «Отложенная отправка»;
- добавлен раздел «Фейковые посетители» с примером нестандартной атаки на маркетологов.

- В раздел «Неактивные ссылки» главы 2 добавлено описание маскировки ссылки с помощью букв и курсива.
- В главе 3:
 - в раздел «Паровозик» добавлено описание похожей техники Tailgating и приведена ссылка на пять примеров ее использования;
 - добавлен раздел с описанием техники Piggybacking;
 - в разделе «USB-устройства» приведен пример того, как работает вредоносное ПО, сохраненное на флешке и имитирующее устройство ввода;
 - в раздел «Визуальный пропуск» добавлен пример использования спец-одежды при проникновении на объект;
 - добавлен раздел «Истории для вдохновения» с описанием нескольких примеров социальной инженерии офлайн;
- В главе 5:
 - в раздел «Софт» добавлено описание метода SSO;
 - добавлен раздел «Технические аспекты защиты от СИ» с чек-листом, которого ранее не было в открытом доступе.
- Добавлена глава 7 — про искусственный интеллект, эксперименты с ним и его роль в атаках.
- В раздел «Ущерб от СИ» предисловия добавлены свежие примеры атак в РФ с использованием фишинга.
- В приложение 4 добавлено упоминание антифишингового плагина для Chromium-браузеров.
- В «Словарь терминов» (приложение б) добавлены новые определения.

От автора

Перейдем теперь к основной части предисловия — приятного чтения!

Можно сказать, что информационная безопасность (ИБ) была для меня хобби. Началось всё, когда я, еще живя в Воркуте, первый раз увидел журнал «Хакер». У меня не было Интернета, но между домами нашего района проводами организовали локальную сеть. Когда мне впервые в 2004 году показали «Яндекс», я вообще не понял, что там происходит.

Проработав три года в воркутинской шахте, я переехал в Москву, и тут, наконец, мои «навыки», почерпнутые из именитого журнала, пригодились. Я познакомился с одной женщиной, она жила в Германии и списалась с неким парнем из России. Он сообщил ей, что болен раком и не может быстро приехать к ней. Уж и не помню почему, но я попросил ее переслать мне любой из email, которые он ей отправлял. Простое изучение заголовков выявило, что письмо отправлялось днем, и IP-адрес принадлежал одному из вузов. Я сказал ей, что, возможно, он

студент и выдает себя за другого. Она устроила ему допрос с пристрастием, и реально выяснилось, что он ее «разводит» (даже не предполагаю, с какой целью), так что она с ним порвала. Обломал парню кайф, ну да ладно, врать нехорошо...

Потом я поучаствовал в Bug Bounty¹, где можно легально что-то взломать, и тебе за это ничего не будет (в большинстве случаев). К сожалению, я не разбираюсь в программировании и не напишу даже страничку на HTML без заглядывания в Google — мне проще дается обход системы.

Я попытал счастья при поиске ошибок в «Яндексе». К их чести, они два раза заплатили вознаграждение, когда я показал им, как можно бесконечно, без капчи, парсить выдачу и отправлять фишинговые письма с любой ссылкой от имени **support@yandex.ru**. Подобные уязвимости не ликвидировал Google, и в 2019 году мы получали много спама от **analytics@google.com** и еще бог весть каких Google-сервисов.

Еще помнится (это уже вне рамок Bug Bounty), у меня, как у заслуженного энкэйщика², получалось находить XSS-уязвимости³ на сайтах нескольких банков. Делал я это из праздного любопытства и с обязательным последующим уведомлением банков, что у них случился XSS. При этом я был настолько наивен, что отправлял письма в банки на их info@ в один конец.

Потом я промышлял обзвоном. Нет, не тем, которым сейчас обзванивают граждан РФ от имени служб безопасности банков. Звонил я в организации по разным поводам. Например, однажды знакомый сообщил мне, что у него что-то не так с сайтом, — будто там про турецких хакеров написано, и часть страниц перезаписана этим сообщением. Проблему знакомого решили с помощью фрилансера, после чего я решил погуглить фразу этих турецких хакеров в «Яндексе» («погуглить в “Яндексе”» — дожили) и обнаружил еще несколько десятков взломанных сайтов. Дай-ка, думаю, им позвоню и предупрежу, что их взломали. В итоге сделал около полусотни звонков и наслушался, конечно, разного. Кто-то благодарил, а кто-то начинал расспрашивать подробности в контексте: «А не вы ли нас взломали?»

Кстати, начинающие свою практику в ИБ ребята, студенты профильных факультетов и просто фрилансеры в сфере ИБ, могут таким образом искать клиентов.

¹ Bug Bounty — программа, предлагаемая некоторыми веб-сайтами и разработчиками программного обеспечения. С ее помощью люди могут получить признание и вознаграждение за нахождение ошибок, особенно тех, которые касаются эксплойтов и уязвимостей.

² Энкэйщик — шуточное название работника, обязанностью которого является техническая поддержка пользователей компьютера внутри компании. Название произошло от надписи: «Press any key» («Нажмите любую клавишу») — когда-то эта надпись могла пугать пользователей, и они звали энкэйщика, чтобы он всё починил.

³ XSS (Cross-Site Scripting, межсайтовый скриптинг) — подтип атаки на веб-системы, заключающийся во внедрении в выдаваемую веб-системой страницу вредоносного кода (который будет выполнен на компьютере пользователя при открытии им этой страницы) и взаимодействии этого кода с веб-сервером злоумышленника.

Когда я звонил пострадавшим, у меня спрашивали, могу ли я решить их проблему. Я, конечно, отказывался, поскольку это не мой профиль, и, вообще, я просто добавлял в мир чуть-чуть добра своими звонками, но если ты соображаешь, как почистить базу сайта от «лишних» записей, то сможешь заработать на ИБ первые деньги. Лучше меньше, но законно получить немного рублей за свои навыки.

Можно закончить это житие рассказом о том, как мое хобби стало делом жизни. Когда-то я написал в конференции bis-expert.ru свой первый пост о методе социальной инженерии (СИ) find trap (поиск ловушек) и отхватил негатива от одного из комментаторов. Но когда потом в одном из теневого каналов Telegram я увидел ссылку на этот пост с пометкой «интересная техника», а моя первая статья в «Хакере» набрала самое большое количество просмотров по теме СИ, и службы ИБ начали использовать ее фрагменты в брифингах, я понял, что если делиться практической информацией, а не перепечатывать Википедию, то в эту область-таки можно привнести немного упорядоченности и безопасности.

Кому и как можно использовать эту книгу?

Сразу хотелось бы объяснить, почему в названии книги используется слово «библия». В переносном смысле «библия» — это некий труд с основами в какой-либо области, в каком-либо сообществе. основополагающим документом эта книга станет, если сообщество информационной безопасности будет вносить свой вклад в сферу защиты от социальной инженерии.

Мы не пожалеем ресурсов, чтобы переиздавать эту книгу со все более полезной информацией, — просто пишите отзывы и дополнения на icast@bk.ru. Пусть это будет бумажная Википедия по социальной инженерии, а потом мы дополним и электронную, а то даже там идут споры о том, что такое социальная инженерия ;-).

А теперь вернемся к теме.

С момента выпуска в 2007 году книги Максима Кузнецова и Игоря Симдянова «Социальная инженерия и социальные хакеры»¹ утекло много воды, но на постсоветском пространстве от авторов из СНГ не появилось более известных книг по социальной инженерии в контексте информационной безопасности. В книге коллег упоминались такие вещи, как дискеты с ключами электронно-цифровой подписи (ЭЦП) — про которые теперь знают лишь те, у кого голова украшена седыми волосами или отсвечивает залысынами (без обид, у меня присутствуют оба эти признака).

Иконой СИ заслуженно является Кевин Митник, по его книгам даже пишутся дипломные работы студентами российских вузов. Ну а как же наша знаменитая смекалка (рис. П1)?

¹ См. <https://bhv.ru/product/sotsialnaya-inzheneriya-i-sotsialnye-hakery/>.



Рис. П1. Мы выживали как умели

Пора сделать известным опыт русскоговорящих коллег и рассмотреть современную социальную инженерию, хоть и считается, что ее методы не устаревают. Машинное обучение, сдаваемые в аренду кол-центры с операторами-мошенниками, фишинговые SaaS-сервисы с подпиской, подделка голоса и видео — это лишь некоторые современные инструменты злоумышленников, взламывающих не машину, а человека.

По роду деятельности мы регулярно тестировали сотрудников разных организаций на знание правил информационной безопасности с помощью проведения учебных кибератак. Мне хотелось создать не просто книгу, а предложить инструмент в первую очередь для коллег, чтобы они не думали каждый раз, какую бы атаку провести сегодня. Требовалась база конкретных примеров атак, без «воды»: скопировал, вставил, отправил. Я попытался создать такую базу в форме этой книги, и надеюсь, она станет вашим рабочим инструментом при проверке знаний правил ИБ сотрудников.

И, наверное, самое главное — хотелось систематизировать все известные знания о СИ в одном месте, хотя моя книга и не претендует на статус научного исследования.

Почему возникла такая идея? Зайдите в поисковик и погуглите: социальная инженерия это. Что вы найдете? Википедию, бесконечный копипаст из нее и очень много интерпретаций одних и тех же терминов и методов.

Коллега из известной организации, занимающейся ИБ, рассказывал, что они с другими экспертами полчаса дискутировали на тему, что такое социальная инженерия в информационной безопасности. Но ведь не получится долго дискутировать, например, по поводу стола или стула. Все их знают, и легко объяснить, нарисовать и показать, что собой эти предметы представляют. На тему же СИ каждый высказывает свою трактовку термина (и я не исключение). Много

людей расскажут, что это такое по-своему, и часто легче объяснить СИ примерами, чем дать определение.

В общем, не хватало системного подхода, чтобы любой новичок мог в одном месте почерпнуть достаточный объем знаний и после этого сказать: «Теперь я знаю основы социальной инженерии».

После проведения учебных атак мы обычно обучаем сотрудников, которые провалили проверку, поэтому книгу можно использовать и как проверочный список для составления по нему учебных материалов, которые стоит изучить персоналу, чтобы не попасться на уловки киберпреступников.

Для наведения некоторого порядка каждый термин, приведенный в книге, многократно вычитан, чтобы он согласовывался с другими частями книги и методами атак, а также составлен «Классификатор СИ» (см. *приложение 2*). В результате собранные материалы хотя и не претендуют на научный трактат, но от них точно должно пахнуть систематизацией знаний.

Еще раз хочу подчеркнуть: эта книга — лишь скромная попытка систематизировать некоторые знания из области СИ. Любой пентестер накидает столько примеров, как он применял СИ, что можно будет снять фильм не хуже «Миссия невыполнима». Поэтому, коллеги, буду рад, если материал книги дополнит ваш багаж знаний о методах СИ, и буду крайне признателен, если вы поделитесь своими примерами из практики или пожелаете дополнить «Классификатор» неучтенными векторами.

Если сообщество потребует следующего переиздания этой книги с дополнениями и нововведениями, с радостью упомяну всех участвовавших в этом процессе на странице благодарностей с указанием вклада, который был внесен ими в расширение материалов книги.

Так вот, для кого и как эта книга может стать рабочим инструментом?

Для представителей служб ИБ, СБ и ИТ-служб

Последней категории (ИТ) я сочувствую — если в вашей организации нет отдельной службы ИБ, и обязанности по повышению осведомленности сотрудников возложили на вас (хотя по-разному бывает, может, вы и справляетесь). По поводу СБ — часто в них работают бывшие представители силовых ведомств, а т. к. «бывших» не бывает, в этом разделе я буду обращаться к вам на «вы», от греха подальше. Итак:

- в каждой главе есть конкретные сценарии атак, вы можете брать их по отдельности и сравнивать с правилами своей организации, чтобы понять, от всех ли сценариев у вас есть регламенты поведения сотрудников, и настроены ли технологические преграды для злоумышленников;
- на основе материалов книги можно составлять обучающие материалы как для новых сотрудников, так и для «старослужащих»;

□ если вам не хватает фантазии, но проверить сотрудников на правила информационной безопасности очень хочется, откройте *раздел «Атаки по email» главы 1*, выберите вектор атаки и воспроизведите один из способов на своих пользователях. Также изучите «Генератор онлайн-СИ» (см. *приложение 1*), чтобы быстро сочинить собственный текст для атаки конкретного сотрудника или подразделения.

Впрочем, безопасники сами кого хочешь научат, как фишить сотрудников. Иногда предлагают такие векторы, что думаешь: «Боже, как же повезло планете, что вы на светлой стороне». Поэтому учить эта книга вас точно ничему не будет, а только лишь подскажет, как еще более изощренно применить фантазию. К тому же некоторые векторы в книге получены от ваших коллег — обмениваемся опытом, так сказать...

Для пентестеров

Произвольно открывай любую страницу из *глав 1 и 3*, и да поможет тебе Бог! Ты ведь на светлой стороне, правда, Илья? — он работает в известной пентестерской компании и взламывает не только клиентов ;-)

Для хакеров

Да-да, я знаю, что ты тоже читаешь эту книгу, несмотря на то, что были приняты меры, чтобы ты ее заюзал со значительным временным лагом (без обид, иначе меня бы заподозрили, что я на твоей стороне). Так вот, тебе тоже может пригодиться эта книга.

Если ты «мамкин хакер», то можешь слить книгу на серых форумах. Читатели все равно сделают все неправильно, а ты заработаешь рейтинг. Ну а если серьезно, то надеюсь, ты перейдешь на светлую сторону, ведь зарабатывать деньги с твоими навыками можно, не волнуясь при звонке в дверь в 5 утра.

Что такое социальная инженерия?

Часто мы слышим путаницу в определениях, когда фишингом называется любое письмо от злоумышленника. Давайте введем определение, в контексте которого будет рассматриваться СИ в этой книге.

Социальная инженерия (в ИБ) — совокупность методов обмана человека с целью побуждения к действиям, направленным на получение выгоды за счет несанкционированного доступа к защищаемой информации и/или инфраструктуре, как организации, так и частных лиц. В «Словаре терминов» (см. *приложение б*) ты найдешь более емкое определение.

Ключевыми способами проникновения злоумышленников в инфраструктуру организации остаются социальная инженерия и фишинг. Злоумышленники вводят человека в заблуждение, после чего он дает им доступ к компьютерам организации или пропускает в закрытый периметр.

В отношении частных лиц — это также один из распространенных способов хищения средств или иных мошеннических действий.

В частности, различают три вида электронной СИ: массовая, таргетированная и смешанная.

- Массовая — не обращается в тексте к определенному получателю. Чаще это похоже на обычный спам, рассылаемый миллионам. Кто-то да попадется.
- Таргетированная — та, которая относится к вам и ни к кому другому, вы не спутаете, кому адресовано это сообщение.

Если брать векторы, направленные на организацию, то в сообщении упоминается эта организация и конкретная должность сотрудника в ней (единственная, а не когда в организации много программистов и сообщение адресуется просто программисту) — т. е. компания + Ф.И.О. Таргетированная СИ атакует конкретного человека или конкретную должность для достижения эффекта, который можно получить именно от этого человека.

- Смешанная — таргетируется на конкретную организацию, но без разницы, кто в ней получит письмо.

Например, делается рассылка по большой базе. Если сообщение адресуется бухгалтеру, а в компании их несколько — это смешанная СИ, если адресуется конкретному бухгалтеру (например, главному или с Ф.И.О.) — это таргетированная СИ. Если пишут «документы во вложении», без названия компании и должности, — массовая.

Это помогает классифицировать атаку и соответствующим образом реагировать. При смешанной — предупреждаем остальных бухгалтеров, при таргетированной — оповещаем всю организацию. Массовую отправляем в спам + организуем обновление фильтров антиспама, если письмо его обошло.

Более подробно узнать, какие бывают векторы и сценарии СИ, вы можете, посмотрев «Классификатор СИ» (*приложение 2*).






Опасность социальной инженерии

Когда-то для меня было загадкой (да и сейчас вопрос не потерял актуальности), почему социальная инженерия считается такой опасной и такой распространенной, но при этом бюджеты в организациях выделяются в основном на софт и железо. Хорошо еще, если при заказе пентеста включают опцию с СИ.

Разбираясь с этим, мы стали собирать информацию, состоящую из двух разделов: высказывания о СИ экспертов по ИБ и кейсы взломов, основанных на человеческом факторе.

Я не уверен, что могу упоминать имена и фамилии экспертов, не получив их согласие на обработку персональных данных, тем более что один из них сейчас находится в СИЗО, а вещь он сказал важную. Но по правилам цитирования ссылки на высказывания оставляю, там же упоминаются и авторы.


Цитаты

- «Ключевыми способами проникновения злоумышленников в инфраструктуру остаются фишинг и социальная инженерия, т. е. человеческий фактор» («Ростелеком-Solar»). 
- «Чаще всего киберпреступники проводят целевые атаки с использованием рассылок вредоносного программного обеспечения» (банк «Открытие»). 
- «...Какие бы ни были технологии, все становится бессмысленно, если сотрудники открывают подозрительные файлы и кликают на фишинговые ссылки...» (Group-IB). 
- «...“Врожденной” защиты от фишинга нет ни у одной платформы — это по-настоящему универсальная угроза» («Лаборатория Касперского»). 
- «Сейчас социальная инженерия определенно является самым эффективным способом первичного проникновения в компании» («Инфосистемы Джет»). 


И завершающая большая цитата:

«Практика расследования целевых атак показывает, что именно рассылка фишинговых писем — наиболее частый и при этом эффективный начальный вектор атак, позволяющий злоумышленникам проникнуть во внутреннюю сеть компании.

Когда сотрудник скачивает файл из письма и запускает его, происходит заражение системы, и киберпреступник получает контроль над компьютером.

Семь из девяти рассматриваемых хакерских группировок проникают в инфраструктуру компаний путем рассылки фишинговых писем» (Positive Technologies). 

Ущерб от СИ

Общая статистика, например, за 2019 год, гласит: «В 2019 году ущерб российских компаний от методов социальной инженерии в кибербезопасности составил 1,26 млрд руб.» 

У физлиц, конечно, украли больше: «Почти 290 тыс. россиян стали жертвами кибермошенников за 9 месяцев 2020 года, ущерб составил 68 млрд рублей» (ИА ПРАЙМ).

Почему у физлиц украли больше? Предположу, потому что в этом случае никому не интересно скрывать такие цифры, — в отличие от реального ущерба в организациях. И это, конечно, плохо. Знай руководители реальный ущерб при кибератаках на другие организации, выделяли бы больше бюджетов на информа-

ционную безопасность. Но стоит учесть и то, что порог входа для преступников при взломе физлица ниже, чем при взломе организации.

А вот что об этом пишет «Интерфакс» со ссылкой на зампреда правления Сбербанка: «...сейчас в России больше 30% офисных работников имеют склонность открывать фишинговые письма. Этот тренд сохраняется с ростом 1–2% примерно за квартал. В целом потери российской экономики в 2019 г. от действий кибератак оцениваются в 2,5 трлн рублей».

Теперь давайте рассмотрим конкретные случаи взломов с помощью СИ в СНГ, которые я слышал от коллег.

□ Компанию из строительной отрасли взломали и зашифровали ее рабочие компьютеры. На восстановление ИТ-инфраструктуры потребовалось около недели. Все началось нетривиально — с письма и вируса-шифровальщика. Потери составили около 10 млн рублей. Да, не очень много. Но зато про этот случай, как и про многие другие, мы не узнаем из СМИ, — мне о нем рассказал друг из этой компании. Широкой огласке такие случаи предавать никто не хочет по понятным причинам.

□ И еще пара попате-инцидентов от коллег (об этом не напишут в СМИ, но знакомые в компаниях расскажут):

- в группу компаний входило сметное бюро. Сделав email-рассылку с фишинговой ссылкой, злоумышленник получил доступ к email-переписке четырех сотрудников.

В результате была получена инсайдерская информация о предстоящем тендере, которую передали конкуренту. Он выиграл тендер, предоставив более выгодные условия организатору;

- поставщик одной из компаний был взломан. В нужное время от его имени в компанию было отправлено письмо со счетом, но с «обновленными» реквизитами. Сотрудник бухгалтерии не знал, как различить письмо злоумышленника, и компания потеряла отправленные деньги.

Далее идет то, что удалось найти на просторах Сети:

□ Северокорейские хакеры атаковали российские оборонные предприятия, включая Ростех. Хакеры осуществляли рассылку вредоносных сообщений.



□ АО «Государственный ракетный центр имени академика В. П. Маеева» атаковано с помощью целевого фишинга.






□ Хакер с помощью фишинга взламывал сотрудников авиакомпаний и туроператоров и создал авиабилетов на 2 млн долларов.





□ Китайские хакеры атаковали ЦКБ МТ «Рубин», проектирующее подводные лодки для ВМФ России, отправив его гендиректору изображения подводной лодки с вредоносным кодом.






- Атака хакеров на военно-промышленный комплекс России произошла через email-рассылку зараженных документов. 
- Испанская государственная железнодорожная компания Adif подверглась атаке вымогателя REvil также с использованием фишинга в начале атаки. 
- Программа-вымогатель поражает транспортную систему Сан-Франциско. Предполагаемый вектор заражения — социальная инженерия. 
- В конце 2017 года в России впервые была осуществлена успешная атака на банк «Глобэкс» с выводом денег за рубеж через международную систему передачи финансовой информации SWIFT. Преступники похитили около миллиона долларов.
- Фишинговую кампанию, связанную с группировкой Cobalt, обнаружили исследователи NetScout Systems (ранее Arbor Networks). Отправляемые email содержали сразу два типа URL: одни ссылки вели к загрузке файла Word, содержащего вредоносное содержимое, другие приводили к загрузке файла, замаскированного под файл JPG.
- Аналитики «Лаборатории Касперского» обнаружили шпионский инструмент, с помощью которого велась атака на высокопоставленных и известных военных и дипломатических работников, военных подрядчиков и государственные учреждения в 40 странах мира. Как и многие аналогичные атаки, эта началась с простого фишинг-письма, использовавшего пару известных уязвимостей Microsoft.
- Банк жилищного финансирования: «Как стало известно “Ъ”, хакеры вывели из БЖФ около \$100 000 через шлюзы платежных систем. Вредонос попал в банк с помощью фишингового письма».
- Банк «Юнистрим» взломали. Заражение было произведено через сделанную от имени крупного банка фишинговую рассылку, с помощью которой хакерам удалось похитить средства (сумма не называется, но оценивается как «существенная»).
- Хакерская группа RedCurl взламывала компании по всему миру и похищала корпоративные документы. Ущерб от ее деятельности может составлять десятки миллионов долларов.

RedCurl, которая занималась корпоративным шпионажем, совершила по меньшей мере 26 целевых кибератак на коммерческие организации в разных странах, включая Россию и Украину. Это строительные, финансовые, консалтинговые компании, ретейлеры, банки, страховые, юридические и туристические организации. Прежде всего, RedCurl интересовали деловая переписка, представляющие коммерческую тайну документы, персональные данные и пароли сотрудников.

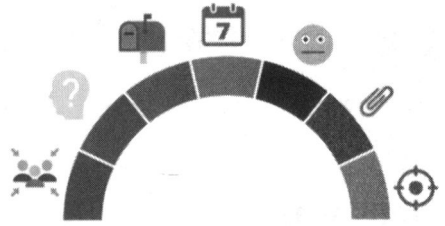
- ❑ При открытии вложенных в письма документов о премировании на компьютере жертвы запускался троян, который контролировался через легитимные облачные хранилища. 
- ❑ Северокорейские хакеры атакуют ИБ-исследователей, используя социальную инженерию. К специалистам применяли социальную инженерию и пытались втереться к ним в доверие, чтобы в итоге заманить на вредоносные сайты и заразить их системы малварью. 
- ❑ Эксперты компании Check Point опубликовали историю хакера, который смог осуществить атаку в отношении китайского венчурного фонда, используя приемы СИ.

Изначально хакеру стало доступно начало переписки о предстоящих инвестициях между венчурным фондом и израильским стартапом. После этого хакер с помощью двух вновь зарегистрированных доменов, схожих по написанию с доменами сторон, стал посредником в их переписке. Он подменил банковские реквизиты стартапа своими, похитив таким образом \$1 млн. Обе стороны отправили друг другу около 30 писем, но не заметили подвоха.

- ❑ Norsk Hydro пришлось приостановить работу нескольких цехов и переключить оставшиеся подразделения на ручное управление после того, как хакеры заблокировали компьютерные системы предприятия и потребовали выкуп за разблокировку. Потери компании составили около \$40 млн. По мнению экспертов, атака началась с фишингового сообщения.
- ❑ Хак-группа LazyScripter атакует авиакомпании. Атаки обычно начинаются с фишинга. Хакеры используют малварь, которая доставляется жертвам посредством вредоносных документов и ZIP-архивов, содержащих встроенные объекты VBScript или пакетные файлы.
- ❑ В апреле 2024 г. масштабной кибератаке с использованием вируса-шифровальщика подвергся Агрокомплекс им. Н. И. Ткачева. Компания еще устраняет последствия инцидента. Ей пришлось столкнуться не только с трудностями в работе, но и с вымогательством 500 млн руб. Одна из обсуждаемых причин взлома — фишинг. 
- ❑ В феврале 2024 г. группировка LockBit, которая использует фишинг в начале своих атак, взломала крупную российскую компанию. Часть похищенных данных хакеры выставили на продажу на нескольких ресурсах. 
- ❑ Хакеры одной фишинговой атакой взломали 400 компаний в РФ. 

Тут должен был приведен нашумевший случай с распознанным нами исполнителем, но — от греха подальше (и международного скандала) — цензуру он не прошел, так что переходим непосредственно к материалу книги.

Глава 1



Онлайн-атаки

https://t.me/it_books/2

Эта глава пригодится тебе, чтобы почерпнуть идеи для учебных атак или полностью копировать приведенные в ней сообщения и использовать их «как есть».

Чтобы социальная инженерия была применима, между жертвой и пентестером должно произойти общение. Общение — это когда ты создаешь информацию и делаешь ее доступной одному или нескольким лицам. Те, в свою очередь, воспринимают ее и передают тебе информацию в ответ (или делают то, что ты попросил сделать).

Для того чтобы жертва смогла увидеть твоё сообщение, существует несколько распространенных каналов его передачи и, собственно, его форматов. Кстати, давай сразу договоримся, что «жертва» в контексте книги — это пользователь организации, которого ты тестируешь на легитимных условиях. Причем не факт, что пользователь станет жертвой, он пока еще только потенциальная жертва, но писать будем сокращенно.

Далее мы рассмотрим наиболее распространенные каналы и способы донесения информации, применимые в социальной инженерии. Но сначала давай немного поговорим о подготовке к атакам.

Подготовка

Социальная инженерия сама по себе является подготовительным этапом к получению несанкционированного доступа к информации, т. е. СИ — это бесполезная вещь, если полученную информацию не используют во вред (или для получения выгоды, смотря с какой стороны смотреть). Всё это очевидно, но упомянул я об этом только потому, что некоторые считают, что СИ — вид атаки на информационные системы, хотя это лишь промежуточный этап перед совершением вредоносного действия.

Если не говорить о взломе организации, а рассматривать ситуацию, например, когда хакер с помощью СИ просто получает какую-то закрытую информацию,

но никак ее не использует и никому ее не сообщает, то организации это вреда не наносит.

Итак, раз СИ подразумевает работу с человеком по каналам связи, то нам как минимум потребуется email жертвы, или телефон, или ее страница в соцсети.

Пентестеру

Когда мы проводим учебную атаку по принципу «черного ящика», нужно выбрать метод подготовки:

- в лоб. Письмо рассылается наугад по доступным email — например, то, которое давало результат в прошлых атаках и более или менее подходит для всех организаций;
- с использованием OSINT — собираем данные о пользователях и организации.

OSINT для СИ

По определению в Википедии OSINT¹ — это разведывательная дисциплина, включающая в себя поиск, выбор и сбор разведывательной информации из общедоступных источников, а также её анализ.

Эта дисциплина незаменима при пентесте организации по принципу «черного ящика».

В Интернете есть много статей по сбору сведений о потенциальной жертве, так что здесь я не буду расписывать каждый инструмент, — информацию о них можно найти в Google. Приведу только некоторые известные инструменты с разной степенью сложности их реализации и применения.

- Специализированные сервисы: **hunter.io** и **findthatlead.com** (и еще несколько подобных: **<https://sales.reply.io/#/email-finders>**) — позволяют осуществлять онлайн-поиск email по домену и дают возможность узнать формат написания личных email-адресов в организации (об этом подробнее написано далее).
- Сервисы **<https://searchdns.netcraft.com>** и **<https://pentest-tools.com>** помогут в поиске поддоменов, на которых размещен корпоративный портал, — тебе ведь нужно имитировать какую-то форму для входа.
- Набор полезных сервисов **<https://viewdns.info>** — иногда интересно деанонить тех, о ком пишут в зарубежной прессе, просто изучив IP History :-)
- Софт: SpiderFoot, Maltego, theHarvester, FOCA, SubBrute.
- Социальные сети: Facebook, VK, Ok, LinkedIn, Instagram. Сразу примечание: если аккаунт пользователя закрыт от посторонних, нужно заранее «набиться» к нему в друзья. Прежде чем набиваться в друзья, погугли его интересы и

¹ OSINT расшифровывается как Open-source intelligence, разведка по открытым источникам.

укажи у себя такие же, в том числе на «стене». Если видны его друзья, то сначала можно добавиться к ним, а потом отправить заявку в друзья цели.

❑ Вот еще подборка по OSINT от компании «Интернет-Розыск»:

<https://t.me/irozysk/6217>.

Разумеется, нельзя обходить стороной и обычные поисковики. Просто отдельно отмечу: если ищешь текстовую информацию, не забудь проверять и выдачу по картинкам. Нередко там попадает информация, которой нет в обычной выдаче.

С помощью приведенных здесь ресурсов и инструментов можно собрать не только email-адреса и информацию об организации, но и информацию о конкретных сотрудниках. Всё это помогает персонализировать атаку, чтобы она отличалась от обычного спама.

Хотел бы также добавить, что моем списке нет 100 500 программ и сервисов, которыми пользуются все хакеры мира. Могу высказать по этому поводу два соображения:

❑ нам пока хватает и этого;

❑ мы не закрыты для обучения и рады узнать от тебя что-то новое. Например, у нас уже получалось написать фишинговое письмо так, что 100% открывших сообщение попались на фишинговую ссылку. Но мы будем учиться до тех пор, пока абсолютно все сотрудники, уже из списка рассылки, не перейдут по фишинговой ссылке. А когда это произойдет, мы будем учиться подбрасывать флешки со 100%-ной конверсией. А вдобавок мы насчитали около 10 тыс. сценариев только онлайн социальной инженерии, так что еще учиться и учиться.

Если ты не понял предыдущий абзац, извини, просто есть такие, что им сколько ни напиши, всё равно будет не так, а напишешь энциклопедию, скажут «это баян».

Разведка боем

Рассмотрим несколько способов узнать контакты сотрудников, которые не доступны в открытых источниках.

Делаем рассылку с любым содержимым — подойдет даже пустое письмо — по всем имеющимся в открытом доступе адресам, в ответ может прийти сообщение автоответчика (рис. 1.1).

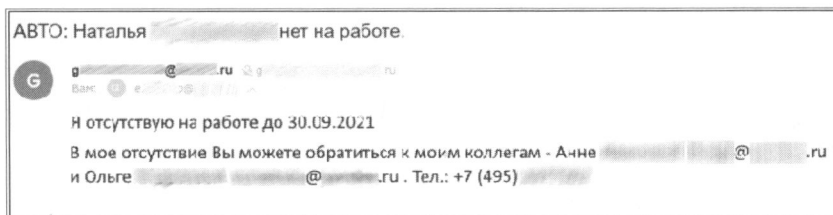


Рис. 1.1. Пример письма, которое пришло при рассылке по email из открытых источников

Исходя из приведенных на картинке данных, прямо-таки напрашивается текст для дальнейшей атаки:

Анна, добрый день, Наталья сказала, что она в отпуске и документы можно передать Вам (*прикрепил*).

Еще способ. Запрашиваем на обычном **info@domain.ru** почту ответственного за наём сотрудников. Приходит сообщение от такого сотрудника. Смотрим формат: **e.guseva@domen.ru**. Тем самым узнаем формат построения корпоративной почты — на основании имени и фамилии. Через соцсети узнаем других сотрудников компании и их должности.

Например, в «ВК». Ссылку специально даю полную, потому что сам каждый раз ищу страницу, где нужно указать именно поиск по работе (кто не захочет набирать такой длинный адрес, может воспользоваться QR-кодом):

https://vk.com/search?c%5Bcompany%5D=%D0%90%D0%9E%20%D0%A0%D0%BE%D0%B3%D0%B0%20%D0%B8%20%D0%BA%D0%BE%D0%BF%D1%8B%D1%82%D0%B0&c%5Bname%5D=1&c%5Bper_page%5D=40&c%5Bsection%5D=people



В поле **Работа** вводим нужную организацию и смотрим, кто указал это место работы (рис. 1.2).

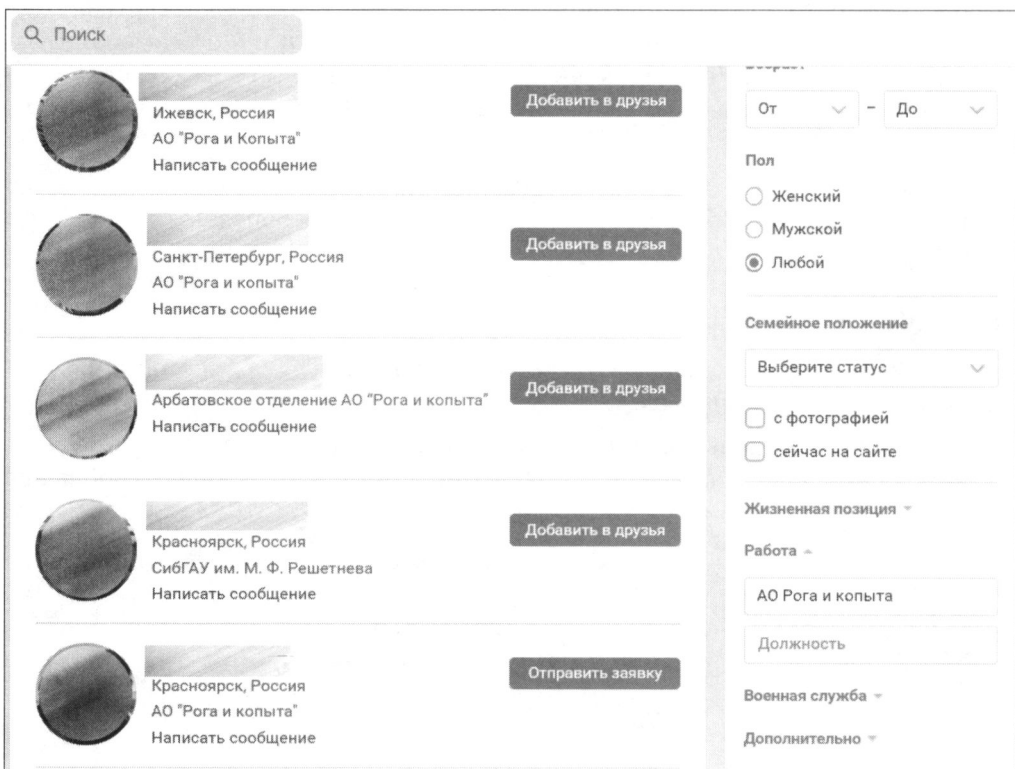


Рис. 1.2. Пример результатов поиска

Сотрудник может прислать ответ на письмо, в котором порекомендует, к кому лучше всего обратиться с этим вопросом. Это, конечно, дело случая, но можно его подтолкнуть, спросив в письме:

Не могли бы Вы подсказать, к кому обратиться по вопросу...

В результате ты с большой вероятностью получишь email, которого нет в открытом доступе.

Отдельно рассмотрим упомянутый ранее сервис **hunter.io**. С его помощью узнаём, как в организации пишутся личные email сотрудников (рис. 1.3).



Рис. 1.3. Пример поиска в hunter.io

Если оказалось, что на целевом домене — например, в зоне **.ru**, нашлась всего одна почта **info@domain.ru**, зайти на сайт и посмотреть в разделе **Контакты** — возможно, почты сотрудников привязаны к домену в другой зоне — например, в **.com**.

Далее, ищем сотрудников целевой организации в соцсетях (рис. 1.4), самостоятельно генерируем потенциально рабочие email и получаем email на основе найденных Ф.И.О.: **afiget@bankromashka.ru**.

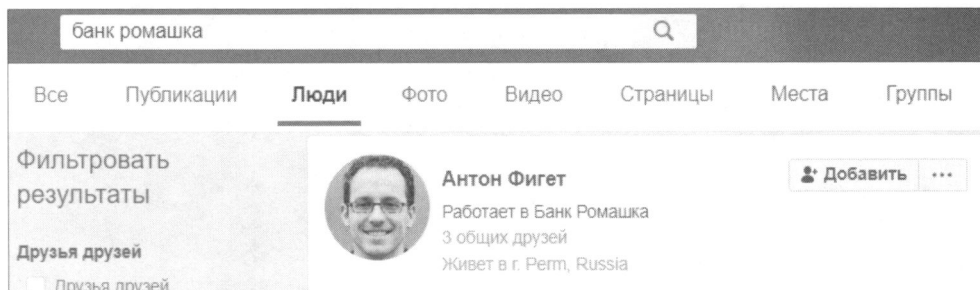


Рис. 1.4. Результаты поиска сотрудников по названию компании

Если на сайте стоит «Яндекс.Метрика», то email, на который оформлен счетчик, можно узнать через саппорт «Яндекса» — через спец. форму (ищи ее тут: <https://yandex.ru/support/metrica>). Просто говоришь, что забыл почту, на которую регистрировал счетчик, и называешь идентификатор, который находится в открытом виде.

Технические аспекты социальной инженерии мы рассматриваем в меньшей степени, всё же книга про обман, а не вредоносную нагрузку, но, как пентестеру-новичку, тебе пригодится изучение email-заголовков, полученных в ответ из организации.

Например, по заголовку можно узнать, какое защитное ПО использует целевая организация:

```
X-KSMG-AntiVirus: Kaspersky Secure Mail Gateway, version 2.0.1.6960,  
bases: 2023/10/03 04:05:00 #22028123
```

Проверка антиспама

Хочешь узнать, пройдет ли твое боевое письмо через фильтры? Сделай тестовую отправку одного из писем.

Просто задай вопрос:

Здравствуйтесь. Вы еще работаете в АО «...»?

Если на письмо ответил большой процент сотрудников, значит, антиспам пропускает массовую рассылку.

Либо отправь письмо со ссылкой, имитируя обычный спам:

Пройдите опрос и получите выигрыш!

Так мы не вспугнем службу ИБ, но узнаем, проходят ли ссылки через антиспам.

Переходим на личности

Этот способ разведки, скорее всего, не подойдет для пентеста, т. к. тут мы переходим за грань между сотрудником организации и его личной жизнью. Поэтому он больше применим для организаций, где у сотрудников техподдержки и всевозможных консультантов на аватарке стоит настоящая фотография (рис. 1.5).

Открыв картинку в новой вкладке, мы увидим ее в большом размере, а можно и сразу поискать ее в «Яндексе» через контекстное меню браузера (рис. 1.6).

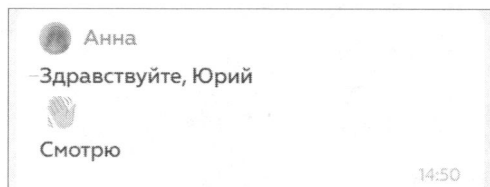


Рис. 1.5. Пример сообщения в чате банка от сотрудника с аватаркой

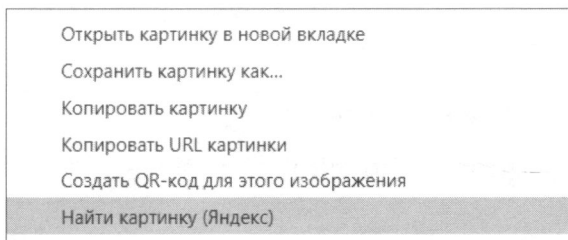


Рис. 1.6. Контекстное меню браузера Chrome с кнопкой поиска по картинкам

Дальше всё просто: из полученных фотографий находим профили жертвы в социальных сетях и на других сайтах (рис. 1.7).

В этом конкретном случае у сотрудника был найден профиль в VK, а вместе с ним телефон, фамилия (и соответственно рабочий email, основанный на данных из **hunter.io** по способу, описанному ранее), а также данные более 200 коллег, по которым злоумышленник мог бы отправлять персонализированные фишинговые письма или сначала попробовать добраться до личного ПК.

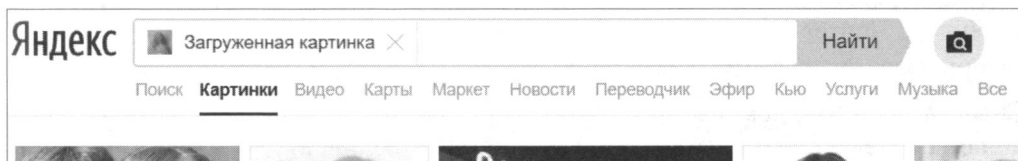


Рис. 1.7. Результаты поиска по картинкам в «Яндексе»

Ну и раз уж мы находимся на белой стороне, давайте что-нибудь порекомендуем владельцу бизнеса, который использует в аватарках настоящие фото сотрудников: если используете маленькую картинку, она не должна открываться полно-размерно — так ее будет сложно найти через поисковики.

Какую фишинговую форму создавать?

Для «угона» учетных данных чаще всего применяется именно фишинг. Рассмотрим пару случаев, показывающих, как можно узнать, какую все-таки форму авторизации нужно создать, чтобы сотрудник увидел знакомую картину.

Несуществующий адрес

Вот так, отправив письмо на несуществующий адрес, мы «случайно» узнали, что компания пользуется Office 365 (рис. 1.8).

Теперь становится понятно, какую форму для ввода учетных записей нужно подделывать при фишинге.

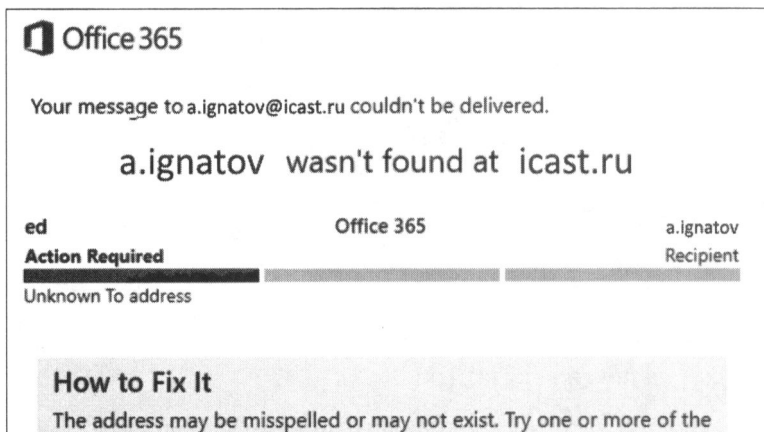


Рис. 1.8. Пример «отбойника» от почтовой службы

Пробиваем MX-записи

Иногда оказывается, что даже крупные компании создают корпоративную почту на популярных почтовых системах. То есть они привязывают домен, например, к «Яндекс.Почте» или Gmail. В таком случае ты будешь знать, на какую форму авторизации будет вести твоя фишинговая ссылка ;-)

Сначала прочекай домены организации и узнай, какой домен к какому сервису привязан. Делается это, например, в Windows, командой в CMD (рис. 1.9):

```
nslookup -type=mx primer.ru
```

Или с помощью сервиса [mailtester.com](https://www.mailtester.com).

```
icast.ru      MX preference = 20, mail exchanger = mail.icast.ru
icast.ru      MX preference = 10, mail exchanger = mx.yandex.net
```

Рис. 1.9. Результат выполнения команды nslookup

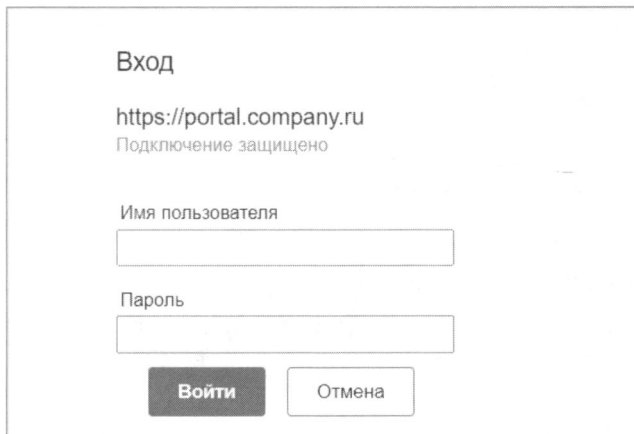
Если ты не выпался и не понял, о чем речь: узнав, что домен **icast.ru** имеет запись **mx.yandex.ru**, тебе нужно создать фейковую форму авторизации «Яндекса» и отправить ссылку на нее жертве.

Неведение

Если ты никак не можешь узнать, какую именно форму используют в организации, имитируй классическую базовую аутентификацию (basic access authentication) или что-то похожее на нее (рис. 1.10), — пользователи вводят свои учетки где угодно, нужно их просто попросить.

Как еще можно собирать дополнительную информацию о жертве, используя Google и логику, ты можешь узнать из следующей статьи: <https://fapicsfacts.blogspot.com/2017/02/google.html>.





Вход

https://portal.company.ru
Подключение защищено

Имя пользователя

Пароль

Войти Отмена

Рис. 1.10. Пример нейтральной формы для ввода учетных данных

От чьего имени писать?

Для начала я бы разделил направления — т. е. определился, от кого кому уходят сообщения:

- внешнее от сотрудника (пишет из отпуска, командировки, из филиала или головного офиса);
- внешнее от организации (подрядчик, партнер, госорган);
- внешнее от физлиц (потенциальные/действующие клиенты);
- внешнее с подделкой отправителя email (изменяются заголовки email, и в почтовом клиенте виден легитимный отправитель);
- внешнее с пересылкой внутри (клиентская поддержка пересылает письмо клиента в техподдержку или ИТ-отдел);
- внутреннее с подделкой отправителя email (сотрудник пишет сотруднику);
- внутреннее при взломе инфраструктуры (рассылка идет из инфраструктуры организации со вновь созданного email, похожего на оригинальный email);
- внутреннее при взломе email сотрудника (реальный или фиктивный взлом);
- легализованное внутри (начальник попался и отдает приказ сотрудникам совершить вредоносное действие). Вынесено в отдельное направление, т. к. может начинаться как внутри, так и извне.

Все эти направления можно использовать в своих рассылках при пентесте. А службе ИБ имеет смысл делать «прогон» по всем этим направлениям во время учебных атак.

Соответственно, выбирая вектор атаки, ты можешь начать с решения, кого будешь имитировать из приведенного списка, а потом сочинять сам текст сообщения. Конечно, большинство направлений из этого списка подойдут только для

email-писем (ведь не у всех организаций есть внутренний мессенджер или соц-сеть).

Как этим пользоваться для придумывания отправителя сообщения?

Имеем вводные:

- домен организации: **company.com**;
- email бухгалтера: **ivanova.a.m@company.com**;
- Ф.И.О. бухгалтера: Иванова Анна Михайловна;
- подходящее нам направление: внутреннее при взломе инфраструктуры (расылка из инфраструктуры организации со вновь созданного email, похожего на оригинальный email).

Получаем отправителя: **ivanova.a.m@c0mpany.com**.

Другой пример:

Имеем вводные — подходящее нам направление: внешнее от организации (подрядчик, партнер, госорган).

Получаем отправителя:

ИФНС 1264 г. Санкт-Петербурга <**request-nalog1264@naiog.ru**>.

Кстати, проясни для себя ситуацию по поводу имитации госорганов — возможно, тебе за это может прилететь, так что оформляй все пентесты по закону.

Помимо «человеческих» отправителей есть отдельный тип писем — разного рода системные уведомления. В таком случае отправителя можно писать такого: **noreply@domain.ru**.

Есть еще направления у частных лиц, но тут мы специально их не рассматриваем: в корпоративном секторе они не пригодятся, а когда книга попадет не в те руки... зачем давать почву для идей.

ВЕС-атака

В этом разделе, относящемся к отправителям, мы можем рассмотреть популярный вредоносный метод ВЕС — расшифровывается как Business Email Compromise, компрометация корпоративной переписки.

Незнание некоторыми уважаемыми вендорами и иностранными государственными органами значения слова «компрометация» приводит к неверному толкованию этого метода.

В ВЕС-атаке злоумышленник получает доступ к почтовому аккаунту жертвы и переписывается от ее имени или «наблюдает» за ее перепиской с коллегами, партнерами, контрагентами.

В программировании всё четко: «это будет этим, работает вот так». В социальной инженерии каждый сам себе художник. Отсюда мы получаем определение фишинга: «это когда флешку с вирусом подбрасывают». Или фишинговым инцидентом называют «открытие фишингового письма».

Ну да ладно, возвращаемся к ВЕС-атакам. Если тебе одобрен пентест, когда ты угоняешь почту работника и продвигаешься во взломе инфраструктуры дальше, то можешь непосредственно взломать сотрудника и писать от его имени или заниматься data-phishing (сбором данных)¹.

Если же пентест или проверка осведомленности (если ты ибэшник) оканчивается на том, что ты похитил учетные данные, то можешь имитировать ВЕС.

Например, писать сотруднику якобы от имени клиента (другого сотрудника, партнера и т. п.). Практически все упомянутые ранее направления писем применимы к имитации ВЕС.

И вот ты имитируешь взлом email председателя правления:

Андрей,
сегодня тебе напишет аудитор, они готовят нас к налоговой проверке.
Все запрашиваемые им документы представь как можно быстрее.
Я пока не на связи, приеду — обсудим.
Андрей Семёнов
Председатель правления ЗАО «Альфа»

Ну а если ты получил учетные данные председателя правления, то, соответственно, ничего не имитируем — пишем прямо с его почты (если рамки оговоренного пентеста позволяют).

Таблица персонализации

Хорошим подспорьем в придумывании отправителя и повода, по которому нужно написать в письме (мессенджере, соцсети и т. п.), может послужить таблица персонализации (рис. 1.11). Когда-то я ее придумал, чтобы можно было создавать таргетированные атаки и тратить меньше времени на их придумывание.

Еще больше пользы она принесет службе ИБ, когда они будут организовывать учебные атаки внутри организации, т. к. у них изначально есть больше информации, чем у пентестера.

	Бухгалтер	Продавец	IT-специалист	Топ-менеджер
Гос. органы	*			*
Клиенты	*	*		
Руководитель	*	*	*	
СМИ				*

Рис. 1.11. Пример таблицы персонализации

¹ Подробнее о data-phishing рассказано в «Словаре терминов» (см. приложение 6).

Можно сказать, что мы при этом задействуем один из вариантов претекстинга (способа вхождения в доверие, подразумевающего использование ранее полученных данных о пользователе). Для разных организаций таблица персонализации будет иметь свои различия.

Итак, составляем список департаментов (отделов или даже отдельных людей) в верхней строке. В левой колонке пишем возможных отправителей — т. е. тех, кто может, в принципе, писать письма в эту организацию.

Потом проставляем «звездочки» по каждому подразделению, подразумевая, кто из левой колонки может написать сотруднику того или иного подразделения. Например, продавцам могут писать клиенты и руководитель.

Вот и готов отправитель для нашего фейкового письма по целому подразделению (или отдельному сотруднику этого подразделения).

Пишем от имени «клиента» и думаем, о чем может писать клиент продавцу? Ну, например, клиент что-то купил и хочет купить еще, или жалуется, или благодарит и т. п.

Так и пишем в письме:

Здравствуйте.

Прикладываю заявку, прошу прислать смету.

ЗАО «Бета»

Пример email-MITM

Всё думал, в какой раздел добавить этот пример. Пусть он будет в этом разделе — с направлениями коммуникации.

Email-MITM (Man In The Middle, человек посередине) — вид атаки, когда злоумышленник создает два поддельных email-адреса и отправляет с них сообщения двум жертвам, имитируя для них легитимную переписку. Пример взят из статьи: <https://rb.ru/story/hacker-letter-vc>:

«Хакер из Китая похитил \$1 млн, подделав переписку между китайской венчурной компанией и израильским стартапом.

Хакер создал два домена, похожих на адреса венчурной фирмы и стартапа. После этого он отправил сторонам по одному письму, указав ту же тему, что и в исходном сообщении. Компании начали посылать письма хакеру, а он пересылал их настоящему адресату, меняя детали. Таким образом он отправил фонду свои банковские данные вместо реквизитов стартапа».

Во время работ по повышению киберграмотности в одной организации мы делали периодическую рассылку от имени начальника отдела кадров. В адресе email **ekaterlna@company.ru** была подменена одна буква (i поменяли на l). Служба безопасности сообщила, что некоторые сотрудники добавили эту фейковую почту в адресную книгу. Если злоумышленник получит контроль над системой создания email в организации, он будет читать корреспонденцию, которую отправляют начальнику отдела кадров на такой поддельный email, и пересылать прочитанные сообщения уже на настоящую почту начальника.

Но можно попробовать и другой способ — без проникновения в сеть.

Проверив, что твоя рассылка проходит спам-фильтр, можно сделать email «начальника» на похожем домене (или вообще на gmail.com) и сообщить сотруднику: «По техническим причинам моя почта временно изменилась (не работает), пока что общаться будем через этот email, я сообщу, когда что-то поменяется».

Не все, но часть сотрудников будут писать тебе, а ты будешь пересылать сообщения на оригинальную почту начальника, подменив email сотрудника похожим фейковым. Таким образом переписка будет проходить через тебя.

Какой фишинговый домен купить?

Если нужны идеи:

1. Перейди на <https://dnstwister.report> или <https://dnstwist.it/> (они несколько различаются, поэтому посмотри оба).
2. Впиши официальный домен организации и нажми кнопку **Искать**.
3. На вкладке **Available** будут показаны похожие свободные для регистрации домены.

Безопаснику

Помимо только что приведенного совета про покупку фишингового домена, по большей части для тестирования сотрудников и привития им навыков кибербезопасности, вам будет достаточно списка email. Но он уже у вас есть, так что ваша подготовка на этом закончена :-)

Да, можно пойти дальше: написать парсер соцсетей и собрать профили сотрудников, смотреть, что они постят, или настроить поиск определенных ключевых слов в их постах.

Можно также писать им с фейкового аккаунта и пытаться купить конфиденциальную информацию или заводить ботов, которые будут с ними общаться. Но если они еще не научились проверять ссылки и файлы в email — это будет несвоевременная работа и пустая трата времени. Поэтому перейдем к следующему шагу.

Имитируя отправителя писем, вам не обязательно покупать много доменов и создавать поддельные почтовые аккаунты — подделанного отправителя вы можете просто добавить в белый список. Что же касается фишинговых доменов для вставки в письма, то вы можете купить несколько (от одного до трех вполне достаточно) доменов и маскировать ссылки разными способами (см. *разд. «Маскировка ссылок» главы 2*).

Это же относится и к социотехническим пентестерам, которые с вами работают. Когда мы сотрудничаем по принципу «белого ящика», нас добавляют в white-list, т. к. мы тестируем не защитное ПО, а реакцию людей.

Готовим атаки

В этом разделе и его подразделах мы рассмотрим различные типы атак по разным каналам коммуникации.

ВАЖНОЕ ПРИМЕЧАНИЕ!

В *разд. «Атаки по email»* предложены разные способы введения человека в заблуждение, применимые и к другим каналам коммуникации. Эти поводы также отмечены в «Классификаторе СИ» (см. *приложение 2*). То есть на примере атак по email мы будем учиться придумывать векторы на основе этого классификатора.

Например, рассматривая в атаке по email повод, когда жертве нужно открыть вложение, мы не станем в *разд. «Файлы»* еще раз рассказывать, что написать в письме, чтобы человек открыл файл, а поясним, что нужно писать в самих файлах, чтобы запустить нагрузку.

Если ничего не понял, просто читай дальше :-)

Атаки по email

Этот раздел с примерами атак будет самым объемным — по причине распространенности использования email для доставки вредоносного содержимого. Но принципы составления векторов подойдут и для других каналов связи — например, соцсетей и мессенджеров.

Как уже отмечалось ранее, существуют три типа атак электронной СИ, если различать их по степени массовости:

- А) массовая — когда не принципиально, какой из сотрудников в какой компании получит письмо;
- Б) таргетированная — персонализированная атака под компанию, отдел, человека;
- В) смешанная — используется небольшая персонализация, например под бухгалтеров, но письмо рассылается по тысячам компаний или заточено под конкретную организацию, но не принципиально, кто лично получит вредонос.

Когда мы тестируем сотрудников, то стараемся осуществить все три вектора. Например, в векторы «Б» и «В» попадаетея от 30 до 80% сотрудников просто из-за того, что пользователи доверяют отправителю, т. к. в email используется реальный домен организации.

По большей части в этом разделе мы будем рассматривать атаки типа «А», но некоторые тексты этих атак пригодятся и в «Б», и в «В» векторах, — тип «А» всегда можно превратить в «Б» и «В».

Идеи по составлению темы письма

Добавлять Re: и Fwd:.

Пример: Re: регламент.

- Упомянуть организацию.

Пример: для АО «Ромашка».

- Упомянуть полностью или частично Ф.И.О. пользователя.

Пример: Получатель Иванов А. И.

- Эмоциональные рабочие аспекты: увольнение, премия (лишение, надбавка).

Пример: Новогодние премии.

- Комбо-бруталити:

Fwd: Список на увольнение АО «Ромашка». Адресат – Иванов А. И.

Адекватная причина не открыть письмо с такой темой — не увидеть его.

И еще. Если ты не имитируешь массовый спам, не используй смайлики и кучу символов в теме. В корпоративной среде так общаются редко.

Какую подпись и оформление использовать?

Подписи в письмах в одной организации бывают одинаково оформленные или самопальные — каждый сам выбирает, что написать о себе.

Ты можешь использовать разное оформление писем в зависимости от того, кого ты имитируешь:

- во внешних письмах лучше вставлять логотип (для вымышленных организаций можно использовать онлайн-генераторы логотипов вроде logoza.ru);
- если имитируешь внутреннего сотрудника, который пишет коллеге, старайся использовать единый стиль организации. Узнать его можно, отправив письмо на info@ и спросив коммерческий отдел. В результате кто-то вам да ответит (с info@ или продавец);
- для безопасников: помимо корпоративного оформления, попробуйте тестировать сотрудников, отправляя письма с нестандартным оформлением писем.

Выбираем контекст

Под «контекстом» я понимаю повод, по которому мы пишем пользователю. Приведенный здесь перечень взят из «Генератора онлайн-СИ», который ты можешь найти в *приложении 1*. Генератор поможет тебе составлять собственные векторы и тексты писем. Далее мы также рассмотрим примеры контекста подробнее.

Итак, по какому поводу мы пишем пользователям:

- событийные атаки;
- причина;
- запросы;
- вопросы;

- отправка чего-то;
- изменения в чем-то;
- желание.

Что ж, повод есть, теперь его можно усилить. Усилить его мы будем разными эмоциями и человеческими реакциями, которые станем вызывать у получателя, — так вероятность обмана увеличится.

Далее приведен перечень усилителей, а затем мы рассмотрим их подробнее и с примерами (см. *разд. «Усиление контекста»*).

- Эмоции: сочувствие, страх, гнев, консерватизм, интерес, радость.
- Давление: авторитет, просьба о помощи, срочность, угроза.
- Желание: секс, халява, экономия, деньги.
- Ложь: поддельная переписка, несуществующий разговор, подделка переписки, подтасовка фактов.
- Совпадение: когда у жертвы часть идентности совпадает со злоумышленником.

Векторы и сценарии

Итак, с вводной частью закончили, теперь рассмотрим разные тексты и поводы, по которым мы будем писать пользователям.

Контекст: событийные атаки (Event attacks)

Рассмотрим разные примеры таких атак — в зависимости от события.

Событийные атаки: чрезвычайная ситуация

Пару лет назад в мире бушевала пандемия одного известного вируса. Точнее, бушевали СМИ, т. к. обычный грипп нанес человечеству больше вреда. Но сейчас не об этом. То, что широко освещается в СМИ, становится отличным инфоповодом для атак. Пандемия сошла на нет, но еще долго эту тему будут использовать мошенники, а потом станет мусолиться еще какой-нибудь вирус (надеюсь, не зомби-апокалипсис), и приведенные здесь тексты помогут проверить сотрудников на бдительность.

ПРИМЕР 1

Скачайте приложение, чтобы отслеживать зараженных вирусом людей рядом с вами.

ПРИМЕР 2

Корпоративная поддержка во время пандемии. Для получения отсрочки по кредитным платежам, включая ипотеку, подайте заявление, и вам будет предоставлена такая возможность.

Во вложении бланк заявления. Распечатайте его, заполните и отправьте ответным письмом.

ПРИМЕР 3

Коллеги, для обеспечения шифрованной связи с удаленными сотрудниками просьба сегодня скачать программу по ссылке ... (ссылка ведет на файлообменник или напрямую на файл на удаленном сервере). С завтрашнего дня коммуникация будет проходить через нее.

ПРИМЕР 4

Для нашей организации обслуживающий банк предоставляет беспроцентный кредит на 1 год, кредитная история не будет учитываться. В случае ухудшения финансовой ситуации (а это, по всем прогнозам, произойдет) кредит будет списан за счет работодателя. Образец заявления во вложении.

ПРИМЕР 5

В связи с обновлением правил поведения жителей г. Москвы (*твой целевой город*) на время карантина введена система пропусков. В случае, если вам нужно покинуть квартиру по любому поводу, для получения пропуска перейдите по ссылке на сайт госуслуг и заполните анкету.

ПРИМЕР 6

Просьба заполнить данные по ссылке для начисления доплат за удаленную работу.

Событийные атаки: праздники

Намечается государственный праздник с последующими выходными? Вот темы, которые можно использовать:

- график работы в праздничные дни;
- тройная компенсация за работу в праздники в рамках мероприятий по повышению лояльности работников;
- праздничные дни отменяются, будем работать без выходных.

Событийные атаки: политика

Политически взбудораженные люди с удовольствием открывают ссылки в письмах на темы, соответствующие или не соответствующие их взглядам.

Есть спокойные люди, имеющие свое мнение о политике, а есть те, кто яростно убеждает других, какое мнение они должны иметь. Их легко определить — они любят писать капслоком, ставят много восклицательных знаков в конце и оскорбляют оппонентов за инакомыслие. Вот такие будут нажимать на твои ссылки аж двойным кликом.

Дабы не будоражить умы соотечественников, приведу пример зарубежного фишинга на политическую тему (рис. 1.12).

Если у тебя, как и у меня, с английским плохо, то суть новости в том, что шесть арабских стран, включая Саудовскую Аравию и Египет, разорвали дипломатические отношения с Катаром, обвинив его в дестабилизации региона.



Рис. 1.12. Пример фишинга на политическую тему

Контекст: причина

Что-то произошло (или не произошло), и я вам пишу. Некто сказал, что по этому поводу следует писать вам.

Например:

Так и не дождался от вас ответа, может, письмо не дошло. Дублирую пакет документов.

Или:

В техподдержке сказали по этому вопросу обратиться к вам.

Якобы взлом

Приведу пример из Сети, когда злодеи отправляют электронное письмо, в котором прикладывают используемые жертвой логины и пароли, утечка которых, скорее всего, произошла ранее. Авторы сообщения утверждают, что взломали веб-камеру компьютера и засняли, как человек смотрит порнографические ролики и что делает в это время. Затем мошенники требуют выкуп в биткоинах за то, чтобы они не рассылали видео, которое якобы есть у них.

В корпоративной среде можно сделать свою версию «якобы взлома»:

Дорогой коллега.

Вчера был обнаружен взлом корпоративной сети. Несколько сотрудников были взломаны, и их логины и пароли оказались у злоумышленников.

В связи с этим срочно нужно выполнить следующие действия:

- Проверьте в списке ниже, есть ли ваш email среди скомпрометированных.
- Если он есть в списке, срочно смените пароль по ссылке (*фишинговая ссылка*).

Список скомпрометированных email:

- abc@yx.com

- abd@yx.com

(и так около 10 email, примерно на 8-м месте автоподстановкой вставляем адрес жертвы).

Всё, ждем улова. Если вы делаете атаку с обратной связью (когда общаетесь с жертвой, а не просто отправляете письмо в один конец), то в конце письма можно попросить, чтобы ответным сообщением вас оповестили, что смена пароля произведена.

ЗАМЕТКА

Узнать, попал ли в общий доступ пароль от корпоративной почты вашей компании, можно здесь: <https://haveibeenpwned.com/DomainSearch>. Вписываете свой домен, подтверждаете право владения и получаете уведомления, когда в Сеть утечет связка email:password.

Внеплановая проверка от СРО

Предприятиям, состоящим в каких-либо саморегулируемых организациях, могут приходить специфические письма. Пользуйся этим при проверке сотрудников.

Вот пример такого письма с вредоносной ссылкой:

Добрый день.

Согласно последним жалобам потребителей микрофинансовых услуг на вашу МФО, а также в соответствии с Базовыми правилами защиты прав и интересов малого и среднего бизнеса, получателей финансовых услуг СРО Союз «Микрофинансовый альянс» назначили вам внеплановую выездную проверку на 03.07.2020. Этим письмом направляем вам Запрос № 222-120 от 23.06.2021 на представление документов (информации). Просьба довести до сведения руководства и быть готовым представить все необходимые документы к 03.07.2021.

Проверка проводится в соответствии со ст. 4, 5 Федерального закона от 13 июля 2015 года № 223-ФЗ «О саморегулируемых организациях в сфере финансового рынка», Федеральным законом от 2 июля 2010 года № 151-ФЗ «О микрофинансовой деятельности и микрофинансовых организациях», Указанием Банка России от 3 февраля 2016 года № 4278-У «О требованиях к содержанию базового стандарта защиты прав и интересов физических и юридических лиц — получателей финансовых услуг, оказываемых членами саморегулируемых организаций в сфере финансового рынка, объединяющих микрофинансовые организации».

С уважением,

Руководитель рабочей группы Контрольного комитета

Союза «Микрофинансовый альянс "Институты развития малого и среднего бизнеса"»

Коленская Мария Юрьевна

Рассылалось такое письмо с email info@alliance-mfo.pw, а настоящий адрес этого союза: info@alliance-mfo.ru.

И еще один, немного измененный пример:

Здравствуйте.

СРО «МиР» получила несколько жалоб потребителей микрофинансовых услуг на вашу МФО, поэтому мы назначили вам внеплановую проверку на 15.07.2020.

Этим письмом направляем вам Запрос №526-1\007 от 02.06.2020 на представление документов (информации).

Просьба к 15.07 быть готовым представить все необходимые документы через личный кабинет СРО.

Проверка проводится в соответствии со ст. 4, 5 Федерального закона от 13 июля 2015 года № 223-ФЗ «О саморегулируемых организациях в сфере финансового рынка», Федеральным законом от 2 июля 2010 года № 151-ФЗ «О микрофинансовой деятельности и микрофинансовых организациях», Указанием Банка России от 3 февраля 2016 года № 4278-У «О требованиях к содержанию базового стандарта защиты прав и интересов физических и юридических лиц — получателей финансовых услуг, оказываемых членами саморегулируемых организаций в сфере финансового рынка, объединяющих микрофинансовые организации».

С уважением,
Председатель Комитета СРО «МиР»
Элла Керимова

Неудачные попытки авторизации

По аналогии со скриптами мошеннических кол-центров, звонящих и сообщающих, что у нас пытаются снять деньги, сочиняем свой скрипт для проверки пользователей в организации:

Уважаемый пользователь!

Нами зафиксирован вход в вашу учетную запись.

Место: Швеция

IP: 165.231.143.161

Если это были не вы, срочно смените пароль

<https://portal.company.ru/email@company.com>

Внимание: письмо создано системой предотвращения вторжений, отвечать на него не нужно.

Уведомление

Пример письма с уведомлением (рис. 1.13). Этот сценарий актуален для банковской сферы.

Что вы делаете в Бразилии?

Пишем сообщение:

Мы заметили, что вы зашли с необычного места в почту — местоположение Бразилия. Если вы не входили в свой аккаунт, отмените вход по ссылке.

Далее пользователь попадает на страницу, где ему сообщается, что якобы всё Ок, и «давайте теперь сменим пароль, т. к. похоже, что вас взломали».

Одно из полей — старый пароль, и поле для нового пароля. Для имитации легитимности можно написать мини-инструкцию по составлению пароля (короткую, в одно предложение).

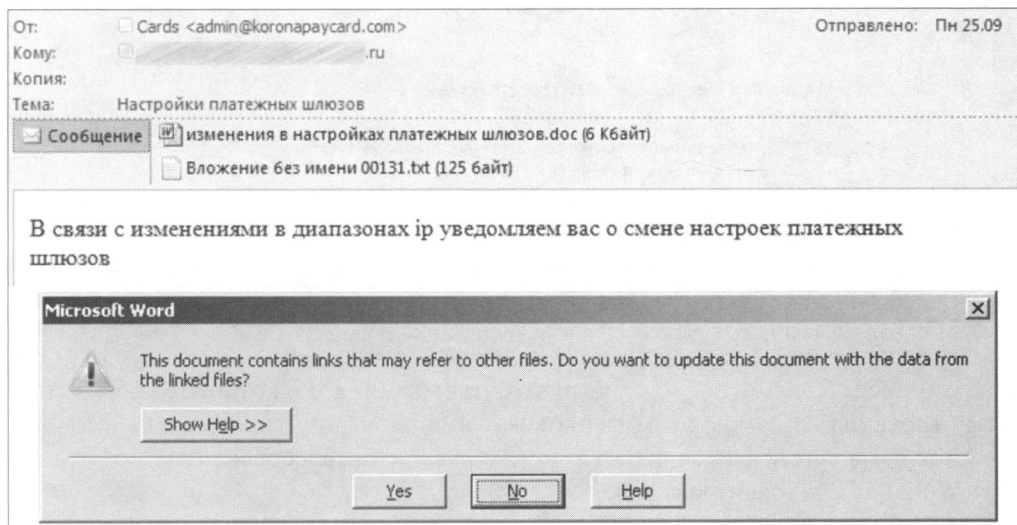


Рис. 1.13. Пример письма с уведомлением

Контекст: запросы

...КП, сметы, счета, декларации, оплаты, документы, неконфиденциальная или конфиденциальная информация.

Например:

Вышлите, пожалуйста, КП. Смету прилагаю.

Просьба выслать акт сверки с ООО "...". Ранее оплаченные вами счета во вложении.

Контекст: вопросы

Отлично подходит для многоходовок, когда нужно начать общение, или для разведки, проходят ли письма первичный антиспам. К тому же после ответа твой адрес еще и в адресную книгу жертвы попадет, что усилит траст у антиспама.

Вопросы можно задавать такие:

Эта почта работает?

Вы на связи?

По такому-то вопросу — это к вам?

Вопрос с вложением

Естественно, вопросы можно задавать не только для этого, а в рамках атаки уже в первом письме (рис. 1.14).

А что это вы мне отправили?

Пишем:

А что это за ссылку вы мне отправили?

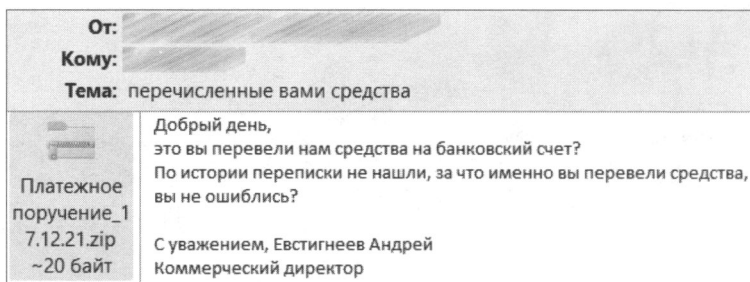


Рис. 1.14. Пример письма с вопросом и вложением

Письмо представляем так, как будто это ответ на письмо, которое якобы жертва нам отправила. В самом этом фейковом сообщении идет призыв к действию и имеется сама ссылка. Расчет на то, что жертва, заинтересовавшись, что это она там отправила, кликает на ссылке.

Контекст: отправка

Отправлять информацию можно в самом теле сообщения или вложением.

Отправляю вам: ТЗ, КП, акты, счета, анкеты, опросы, требование, регламенты (введение новых, изменение старых), приказ, правила, документ, приглашение, благодарность (за работу, за какое-то действие), уведомление, рекомендации.

Как всё это выглядит во вложении, понятно, а что имеется в виду под «отправлять информацию можно в самом теле сообщения», ведь нам же нужно отправить какую-то нагрузку?

Сам задал вопрос, сам отвечу :-). Ссылаемся на всё те же анкеты, опросы, требования, регламенты и т. д., но якобы отправляем ссылку на них. Например, даем ссылку на документ на корпоративном портале.

Кстати, ссылаться на корпоративный портал можно, даже если пользователь не знает о его существовании или его не существует вовсе. Всё равно кликают на ссылки и вводят учетные данные от почты, проверено.

Контекст: изменения

В организации могут меняться регламенты, расписание, правила, корпоративный портал может обзавестись новыми разделами.

Например:

В связи с изменением регламента работы удаленных сотрудников просьба сегодня ознакомиться с приказом во вложении.

А вот еще один пример (рис. 1.15).

По ссылке перешли 100% работников, открывших письмо, из них 30% заполнили фишинговую форму.

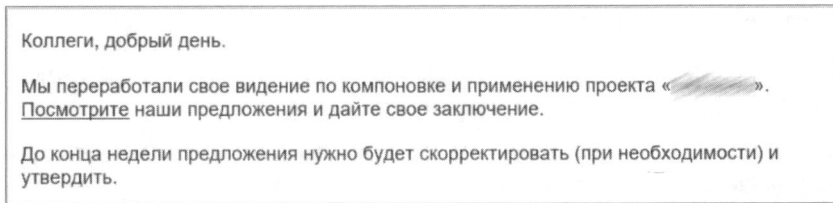


Рис. 1.15. Пример письма с изменениями и упоминанием проекта, который адресатам знаком

Контекст: желание

Само собой, желание получить что-то как можно с меньшим трением нам при-
суще.

Пишем пользователю про экономию (скидки, акции, замена чего-либо альтерна-
тивным, лучшим вариантом), про что-то бесплатное и, конечно, про деньги (по-
вышение, премия, надбавка).

ПРИМЕР ПИСЬМА

Коллеги. В связи со сменой ассортимента продукция со склада будет распродана
среди работников предприятия по 1 руб. Дешевле продать не можем в связи с тре-
бованиями законодательства.

Обновлены списки премированных сотрудников в третьем квартале.

На рис. 1.16 приведен еще один пример из практики.

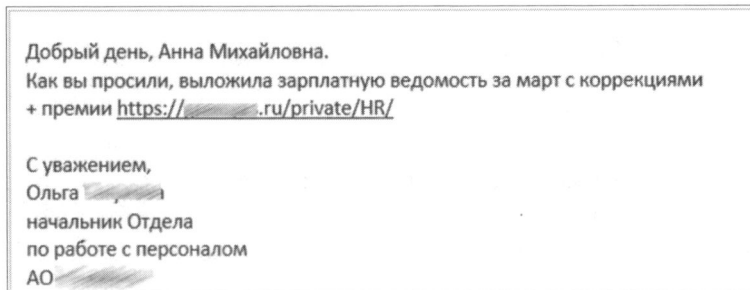


Рис 1.16. Пример письма с вызовом желания узнать зарплату коллег

Анна Николаевна здесь — это действительно главный бухгалтер. Мы пишем от
имени начальника отдела по работе с персоналом, но по всем сотрудникам. Про-
сто делаем вид, что ошиблись адресатом.

Этот вектор мы осуществляли в одном из банков. Что интересно, нам дали
100 пользователей, причем 50 из них месяцем ранее обучались правилам ИБ
в учебном центре, а 50 не обучались. Разослали мы им это письмо якобы
с ошибкой в адресате и зарплатной ведомостью.

В результате попались 60% в обеих группах с разницей в 2%.

Контекст: «непонятки»

Ранее я не упоминал эту категорию поводов, потому что следующие примеры отправляются без повода. Но обо всем по порядку.

Люблю письма, когда в них нет призыва к вредоносному действию, и пользователь сам догадывается, что ему нужно сделать.

Переписка-ссылка

В этом случае просто пишем ему: «Хорошо!» — и ниже ссылка, по которой ему нужно кликнуть. Примерно так это выглядит в Яндекс-интерфейсе (рис. 1.17).

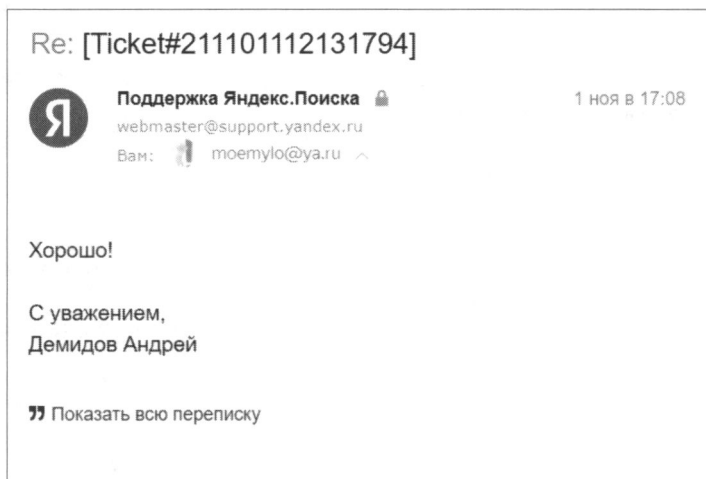


Рис. 1.17. Пример письма со ссылкой для раскрытия подробностей

После клика на ссылке можно просто проверять, что у него за устройство, а можно имитировать разлогин системы, чтобы он заново ввел логин и пароль, но только теперь на твоём сайте.

Одинокий файл

Аналогично способу, показанному в предыдущем разделе, отправляем файл во вложении, не указывая в теле письма вообще ничего. Только тема письма и файл. В теме тоже пишем нейтрально, но чтобы было понятно, что это не совсем спам. Например, название организации пользователя или «В ... (название подразделения)».

Усиление контекста

Покажем, что может являться усилителями контекста. Часто это просто добавка в виде одного предложения или упоминание усилителя в теме письма. Мы придумали повод, по которому пишем пользователю, а теперь нужно «дожать» его.

Усиление контекста: эмоции

Какую эмоцию мы вызываем своим сообщением или с какой эмоцией пишем:

- **сочувствие** (к чему-либо/кому-либо) — например, подбираем сотрудника, который в отпуске, и пишем:

Отправляю оставшиеся документы. Меня уволили, в отпуск пошла, и сказали с последующим увольнением. Но всё нормально. Почта сегодня будет заблокирована, так что отвечать уже не нужно. Желаю успехов и достижений.

- **страх** (штраф, увольнение, лишение, потеря ценностей) — самые нелюбимые векторы. Вообще не люблю обманывать. Но раз хакер может такое написать, значит, и нам нужно протестировать работников.

Пишем:

В связи с реорганизацией опубликован предварительный список сотрудников на сокращение.

Более простой пример усиления контекста страхом:

Андрей Николаевич злой, надо срочно всё заполнить.

Представителям службы ИБ рекомендуется не часто практиковать усиление страхом. Лояльность сотрудников падает, и как минимум полдня у бизнеса вылетит после такой рассылки, все только и будут обсуждать предстоящую реорганизацию. Вообще, про повышение культуры ИБ, если будет проявлен интерес, напишу в следующей книге, посвященной защите от СИ. Двигаемся дальше;

- **гнев** (от начальника, клиента, партнера, близкого).

Пишем:

Быстро всё заполнить, и чтобы я больше такого не видел!!!

Кстати, низкие эмоции в рамках регулярных работ по повышению осведомленности лучше использовать не чаще 1 раза в год. Да, хакер церемониться не будет и напишет что угодно, но лучше не перебарщивать, если лояльность сотрудников для организации важна;

- **консерватизм** — тут всё просто, в сообщениях про раздачу криптовалюты можешь безумствовать, а в деловой переписке придерживайся официального тона сообщения :-)

Копию на sales@...ru (или support@) также отправил. Прошу впредь таких ошибок не допускать (далее вставляем фишинговую ссылку).

Способ подходит для сотрудников, которые любят переправлять письма в другие отделы, когда в любой непонятной ситуации сотрудник решает, что письмо относится примерно к такому-то отделу, и отправляет ваше письмо туда. А этим способом мы делаем вид, что уже отправили туда информацию, и теперь он лично должен провзаимодействовать с нашим письмом;

- **интерес** — тут работает старое доброе любопытство. Если в теме письма было про премии персоналу, то в тексте можно просто вставить ссылку якобы на корпоративный портал и больше вообще ничего не писать — ни приветствия, ни подписи, ничего;
- **радость** — якобы дарим какой-то подарок или по-другому повышаем лояльность работников.

Например:

В связи с успешным закрытием года работники, добирающиеся до места работы более 20 минут, в первом квартале будут обеспечены поездками на такси за счет организации, нужно только заполнить анкету.

- **секс** — я еще не знаю, какой возрастной рейтинг получится у книги, но не будем его вот так вот сразу завышать. Просто знай, что если в сообщении добавлен флирт или намек — это уносит воображение жертвы. Естественно, на примерных семьянинах такое не сработает.

На откуп твоей фантазии — как это использовать в корпоративных email-сообщениях, но в соцсетях и мессенджерах это работает. Не обязательно писать про это в тексте, достаточно симпатичной аватарки в профиле и в разделе фото.

Усиление контекста: давление

Давление, наряду с эмоциями, работает хорошо, ведь оно тоже вызывает эмоции. Итак, рассмотрим виды давления.

- Упоминаем в письме авторитета — например, начальника, госорган. Или пишем от их имени.
- Просим о помощи. Добавляем в сообщение, например, такое:

Не могли бы вы помочь, мне необходимо...

В другой ситуации человек бы точно отказался, но тут додавливают и просят помощи.

- Давим на срочность — например:

Изучить приказ нужно сегодня до конца рабочего дня.

- Угрожаем негативными последствиями — например:

Всех, кто не заполнит анкету, обещали лишить ежегодной премии.

Следующий пример хорошо иллюстрирует усиление контекста с помощью давления за счет добавления email директора в копию письма.

Адресаты в копии

В копию email-письма можно поставить вымышленные email с настоящими именами сотрудников организации жертвы. Домены у таких email исполь-

зуем легитимные. Например, настоящее имя контакта и email <Джон Доу> **dir@domain.com**, а мы используем в письме <Джон Доу> **director@domain.com**.

При этом сотрудник увидит авторитетных коллег в копии и решит, что они уже в курсе этой просьбы (хакера), и с большей вероятностью сделает то, что написано в письме. Разумеется, вымышленные email-адреса в копии не должны совпасть с реальными, иначе настоящий директор быстро прекратит атаку.

Чтобы не ошибиться, можешь вставить кириллические или punycode-символы в легитимном email. Outlook прекрасно отображает их, даже если они идут вперемишку с латинскими символами.

Письма от госорганов

Часто такими письмами пугают физлиц, но способы атак на них — это тема для отдельной книги.

Тебе же нужно имитировать госорганы, представляясь ими, например, так:

В рамках плановой проверки на предмет легализации средств, полученных преступным путем, уведомляем, что вам нужно подготовить документы по представленному во вложении списку.

Срок предоставления информации 2 рабочих дня.

Росфинмониторинг

Поначалу я хотел вставить сюда список всех органов власти, но ты и сам их сможешь загуглить. Принцип составления писем от госорганов простой:

1. Думаешь, с каким из госорганов в списке может взаимодействовать организация.

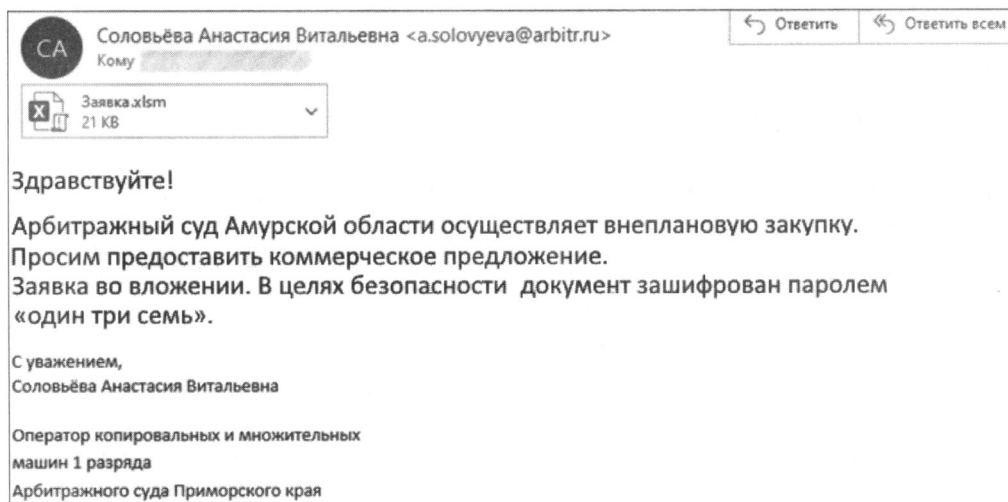


Рис. 1.18. Пример письма с запросом коммерческих предложений

2. Смотришь, чем занимается этот госорган, чтобы выбрать повод для сообщения.
3. Пишешь письмо с этим поводом и прикрепляешь нагрузку — ссылку или файл.

Не забываем, что госорганы могут не только пугать, но и предложить заработать (рис. 1.18).

Срочно обновитесь

Пример письма со «сделайте это сразу» приведен на рис. 1.19.

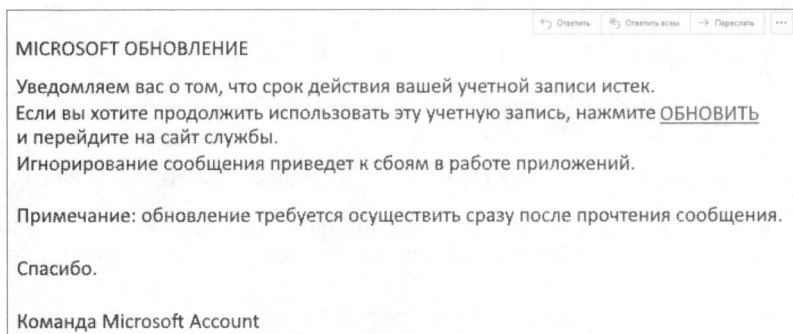


Рис. 1.19. Письмо с контекстом срочности

Усиление контекста: ложь

Тут всё просто: используем обман. Вся социальная инженерия — это, по сути, обман. Но тут мы дополнительно усиливаем сообщение фейками.

- Якобы состоявшееся общение. Ссылаемся, например, на руководителя, что с ним вопрос обсудили, и он якобы отправил по этому вопросу к нашей жертве.
- Упоминание фейкового сотрудника — например, помощник заведующего производством (но такой должности даже не существует) переправил наш запрос к жертве.
- Вставка фейковой переписки ниже в письме в виде скриншота или переписки со знакомыми жертве людьми.
- Подтасовка фактов.

ПРИМЕР 1

В связи с тем, что у нас будет ежегодный корпоратив, посвященный празднованию Дня независимости нашего офиса, необходимо заполнить опрос.

ПРИМЕР 2

В связи с происходящим слиянием/поглощением с ОАО «...», нужно сделать следующее...

Фейковая переписка

В письмо вставляем переписку с сотрудником, которой не было, и просим что-то сделать.

От кого: Начальник КБ
Почта: v.n.babanov@company.gov.ru
Тема: Fwd: NDA сотрудникам

Добрый день.
Просьба ознакомиться.
С уважением,
Бабанов В.В.

АО «Альфа»
<https://company.gov.ru>
+7 495 777-44-11
г. Москва, Средний Овчинниковский переулок, 21

-- Пересылаемое сообщение-- -

From: Игорь Перлов [mailto:igor.perlov@company.gov.ru]
Sent: Thursday, July 22, 2021 2:45 PM
To: Babanov V.<v.Babanov@company.gov.ru>
Subject: Re: NDA
Отправляю NDA, нужно сегодня довести до сотрудников.

С уважением,
Виктор Перлов

Фейковая пересылка

По аналогии с примером из *разд. «Фейковая переписка»* пишем от имени одного из начальников: «Сделать сегодня», а ниже якобы приказ от гендиректора, который говорит, что нужно сделать (перейти по ссылке или скачать файл).

Просто в этом случае мы не комментируем приказ гендиректора и пересылаем сообщение как есть.

И еще один пример пересылки, теперь якобы от клиента.

В письме сотруднику пишем просьбу посмотреть, что там хочет человек, и ниже якобы просьба клиента с упоминанием жертвы. Соответственно этому сотруднику-жертве отправляем сообщение от имени другого сотрудника (из другого отдела).

Например, имитируем якобы пересылку сообщения от службы поддержки или руководства: «Это, похоже, для тебя». И ниже просьба клиента или жалоба, в которой подставляется email или Ф.И.О. жертвы + нагрузка (ссылка или файл).

Усиление контекста: совпадение

Когда у жертвы часть идентности совпадает с твоей вымышленной — лояльность растет. Часть идентности — это то, по чему человека отличают от других. Например, Андрей Иванов, водолаз, который ездит на красной Ferrari и живет в Воркуте.

Вот, например, части идентности, которые можно использовать: тезки, однофамильцы, профпринадлежность, политические взгляды, землячество, увлечения, учебные заведения, воинская служба. На этом делается или не делается акцент в сообщении, профиле, на «стене» в соцсетях.

Другими словами, если пользователя зовут Андрей Иванов и он юрист, можно тоже представиться Андреем Петровым или юристом Сергеем Жуковым.

Источники фишинговых писем

Если ты спокойно читаешь на английском, вот еще база с более чем 200 примерами социотехнических email: <https://cofense.com/real-phishing-examples-and-threats>. Они отсортированы по видам нагрузок и темам.



А вот сайт <https://app.any.run>, где могут отсыпать еще немного образцов ссылок и файлов, основанных на социальной инженерии (~38 500 шт.). Помимо всего, там можно скачать вложения, которые злоумышленники отправляли жертвам (рис. 1.20).

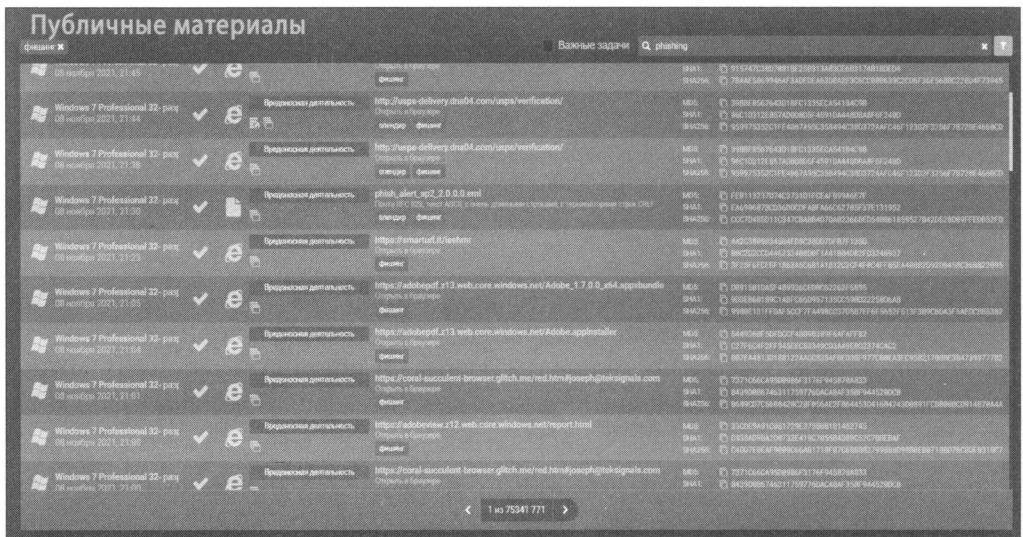


Рис. 1.20. Результаты поиска на сайте app.any.run по запросу фишинг

Файлы

Файлы входят в топ по распространенности нагрузок, используемых при взломе информационных систем.

Файлы можно:

- непосредственно отправить по каналам коммуникации (email, соцсети, мессенджеры и т. д.);
- побудить запросить их у тебя;
- побудить скачать с твоего сайта.

Давайте рассмотрим примеры атак, когда под каким-то предлогом нужно, чтобы сотрудник разрешил запуск макросов в офисных документах или небезопасное содержимое в PDF-файле, ну или запустил EXE-файл в архиве.

Некорректное отображение

Составляем файл, в котором якобы имеются проблемы с кодировкой, и написана инструкция, что с этим можно сделать (рис. 1.21).

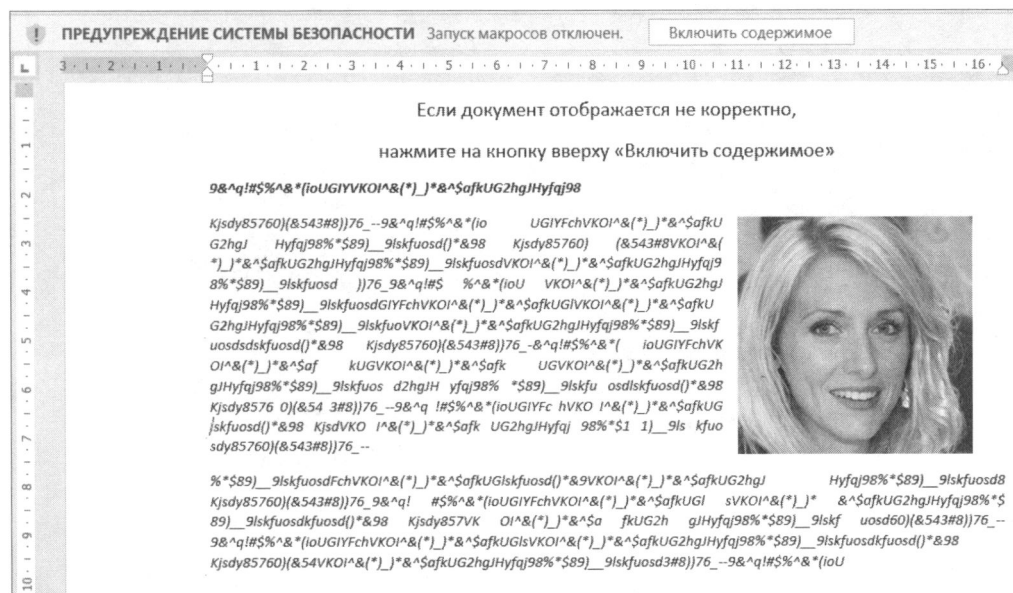


Рис. 1.21. Имитация текста в файле с некорректной кодировкой

Подарочный сертификат

Еще один пример с якобы техническими проблемами (рис. 1.22).

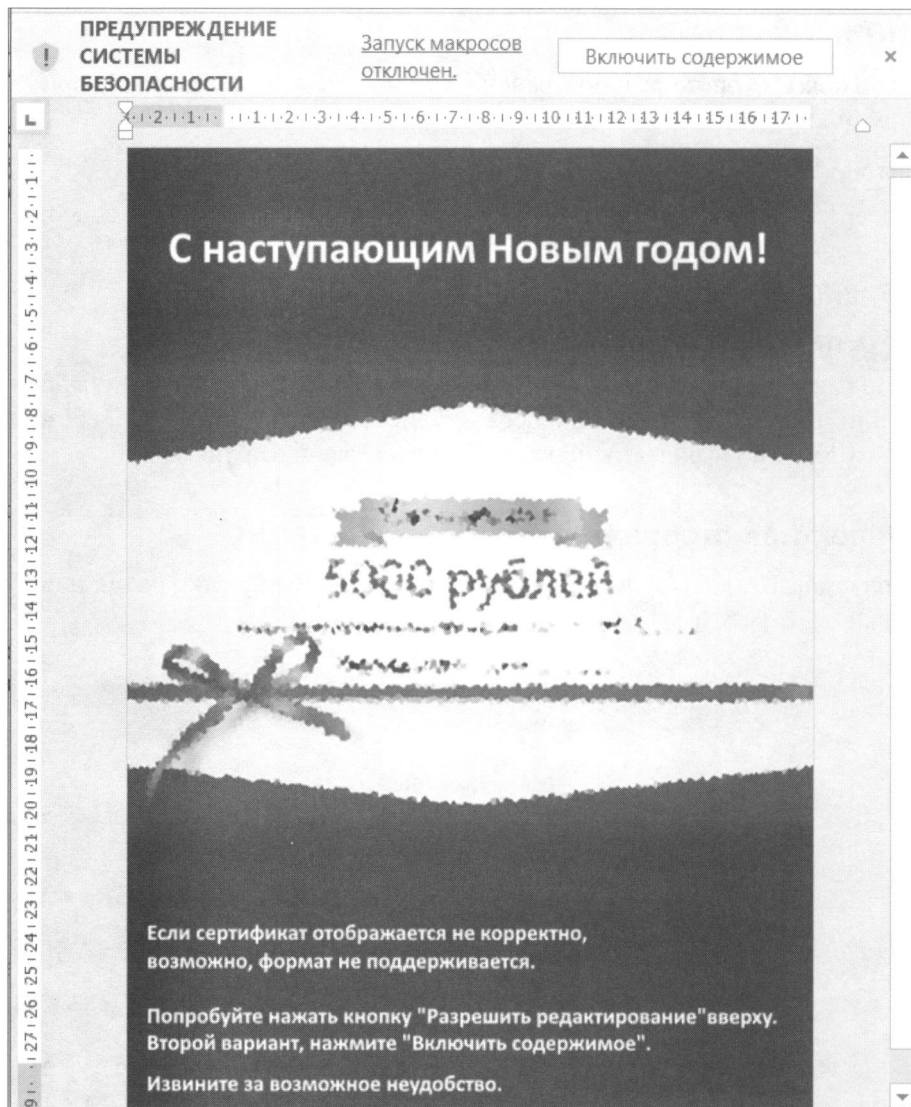


Рис. 1.22. Пример фейкового сертификата в Word-файле

Пустой файл

Отлично работающий способ, когда документ пуст. Мы достаточно часто его используем — 20–30% получателей разрешают макросы, чтобы увидеть все содержимое, которого, разумеется, нет (рис. 1.23).

Еще один пример пустого файла — просто теперь пишем не про дополнительные настройки, а про макросы (рис. 1.24).

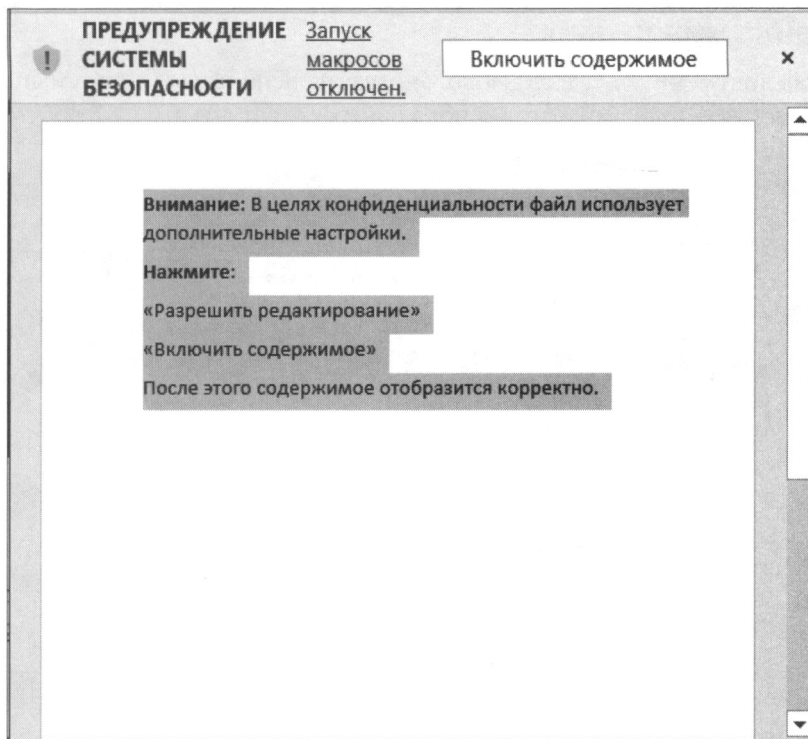


Рис. 1.23. Имитация отсутствия содержимого «в целях конфиденциальности»

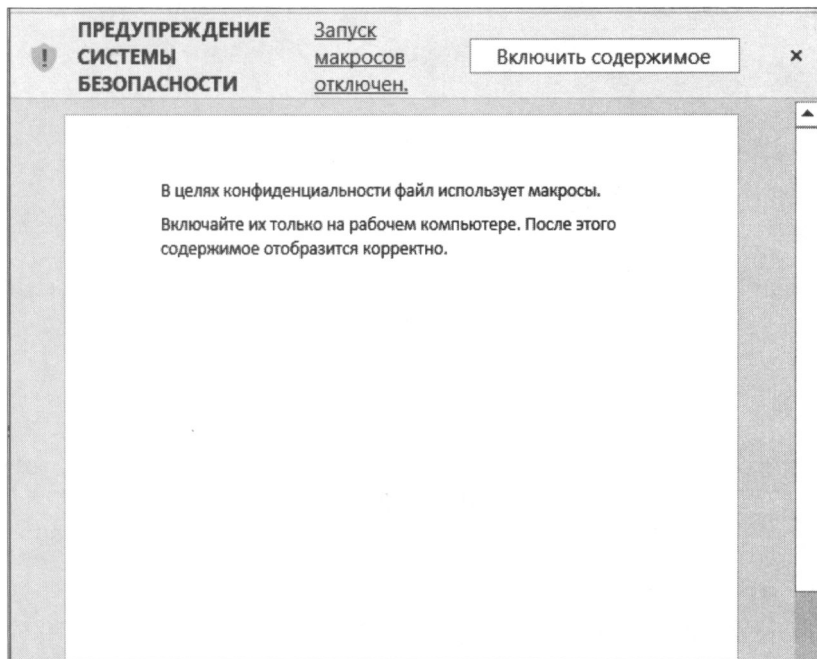


Рис. 1.24. Текст в файле с упоминанием необходимости включить макрос

Документ с «мыльцой»

Размытый документ (рис. 1.25) довольно часто используется злоумышленниками, а используется потому, что это пока еще работает :-)

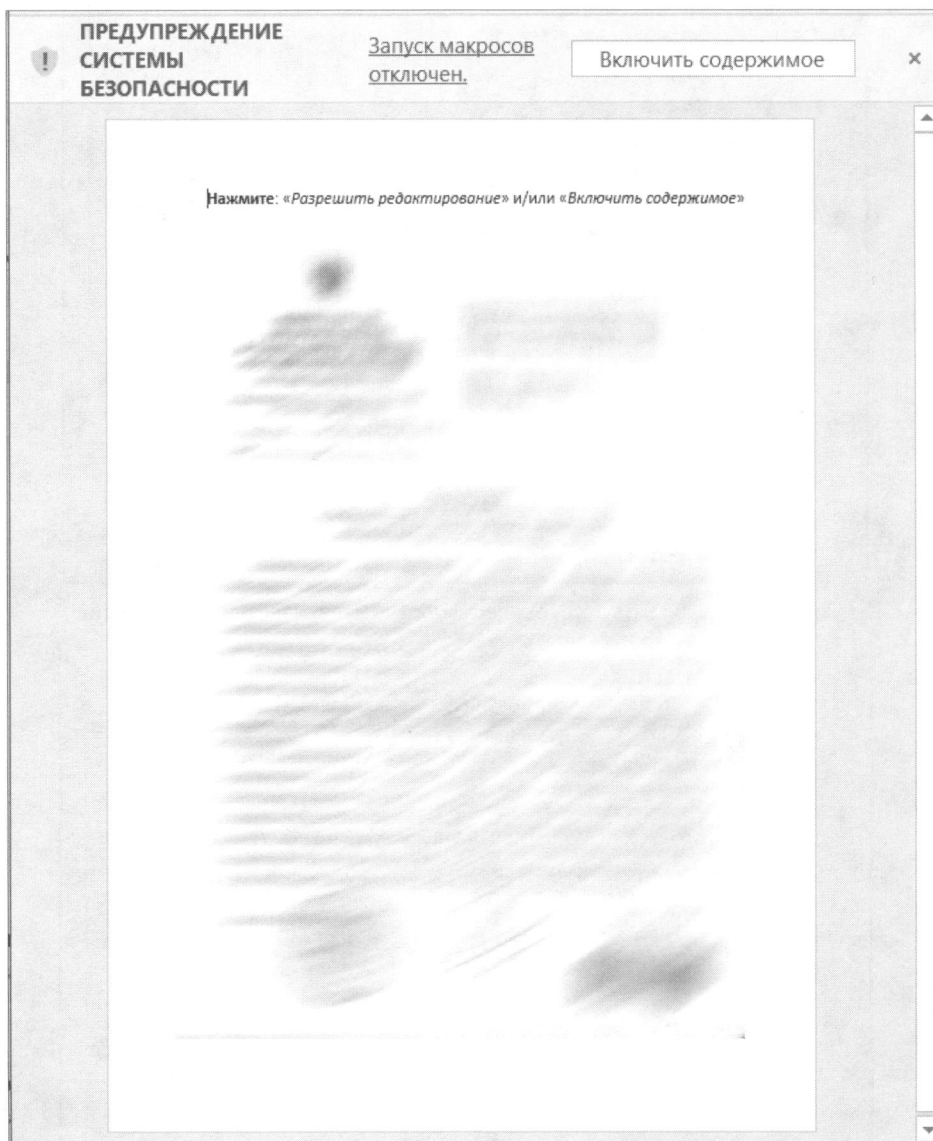


Рис. 1.25. Пример файла с замыленным содержимым

Еще один вариант с «мыльцой» (рис. 1.26).

И еще один расширенный вариант (рис. 1.27).

А вот пример, имитирующий официальный приказ (рис. 1.28).

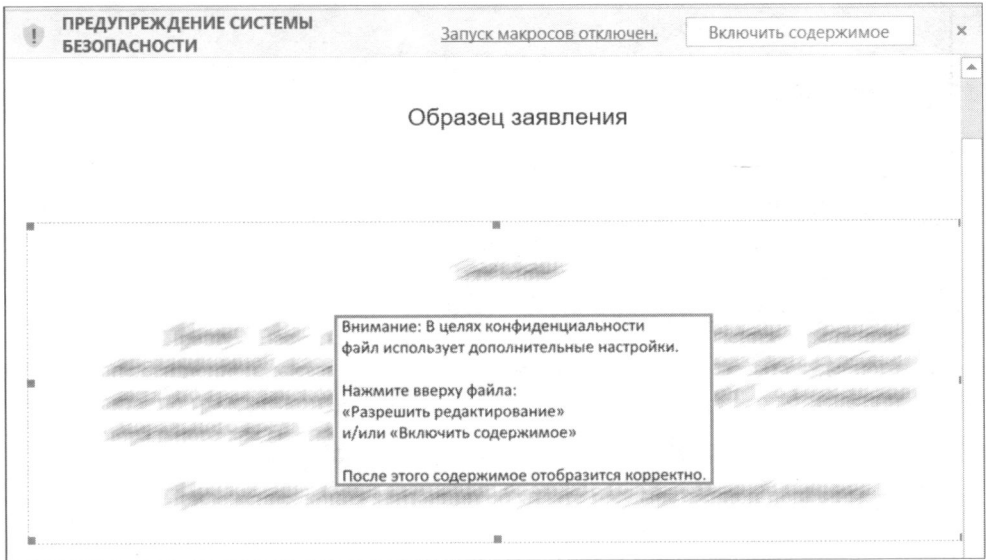


Рис. 1.26. Пример письма с замыленным содержимым и «объяснением»



Рис. 1.27. Замыленное содержимое в файле с частично скрытым текстом

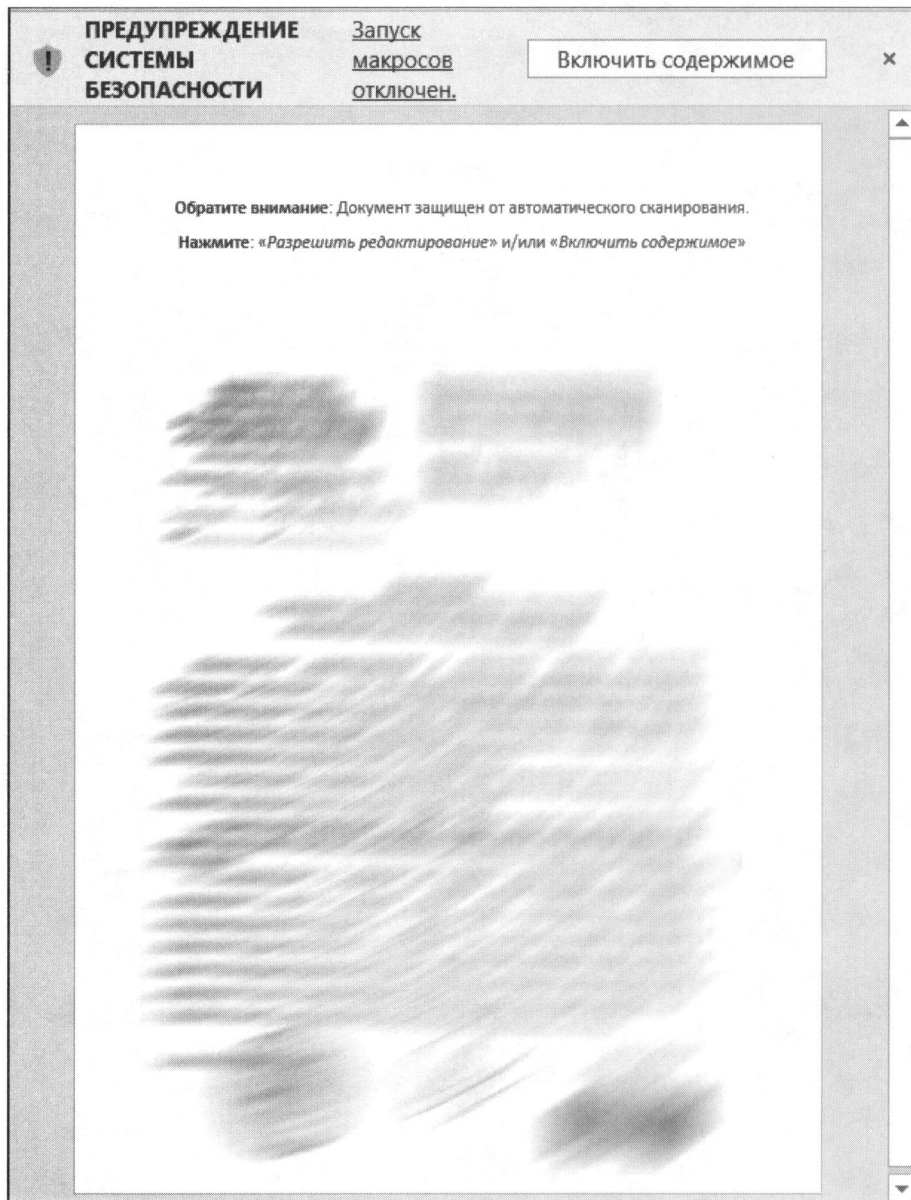


Рис. 1.28. Пример файла с замыленным «приказом»

Помимо приказа можно писать о некоем соглашении, а «инструкцию» использовать из других примеров (рис. 1.29).

Вот такой «мультивход» (рис. 1.30) ты можешь предлагать, когда не знаешь, что за почтовая служба у пользователя.

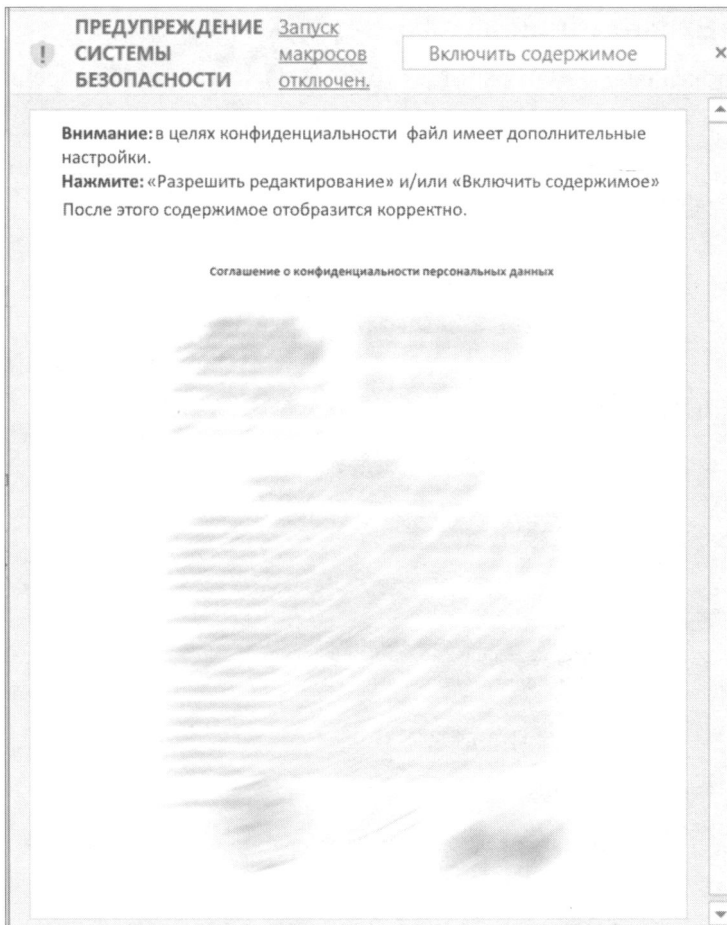


Рис. 1.29. Пример замыленного текста с инструкцией и якобы официальным документом

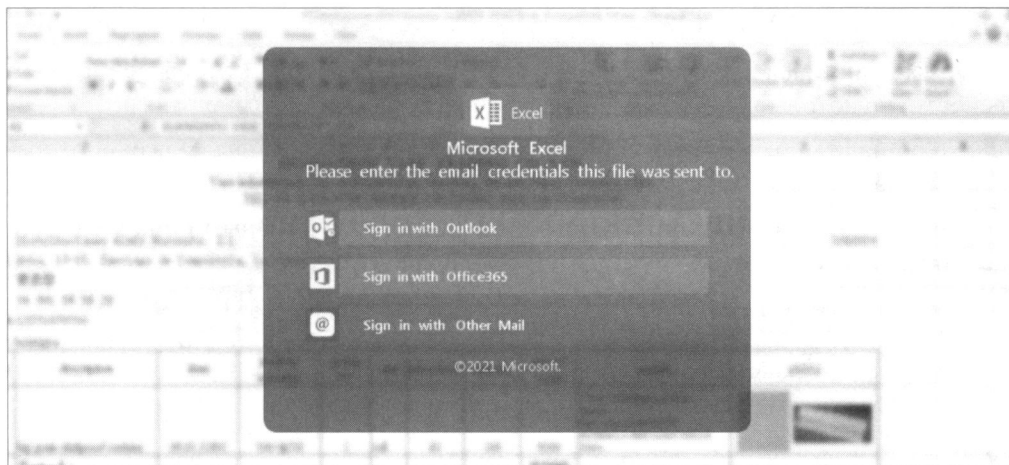


Рис. 1.30. Пример уведомления, где пользователь выбирает сервис для ввода учетных записей

Имитация Excel-таблицы в Word-документе

Как ни парадоксально — это работает (рис. 1.31), хотя и противоречит здравому смыслу :-).

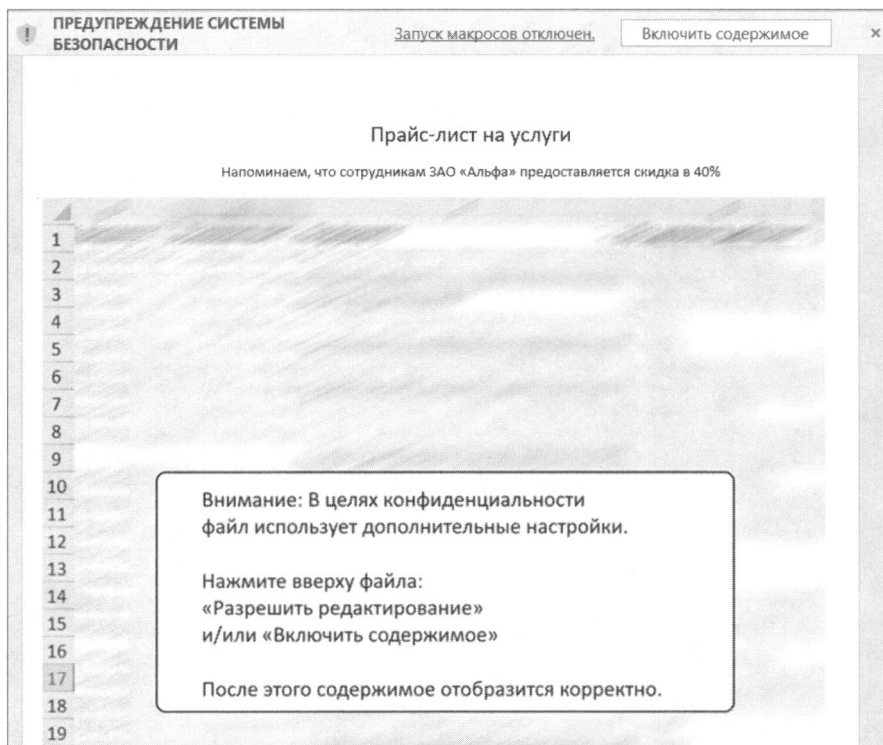


Рис. 1.31. Имитация Excel-таблицы в Word-файле

Небезопасный PDF-файл

В PDF-файлах никаких макросов нет, но там есть другие предупреждения безопасности, на которые нам нужно, чтобы нажал пользователь (рис. 1.32).

Если тебе надо проверить реакцию сотрудника на такие файлы, можешь отправить ему файл с текстом, как показано на рис. 1.33.

Или используй «инструкции» в файле — по аналогии с офисными документами, рассмотренными ранее.

Сам Adobe пишет о таких предупреждениях следующее:

«Предупреждение появляется, поскольку содержимое PDF может потенциально навредить вашему компьютеру. Например, предупреждение появляется для PDF-файлов, которые могут передавать или выполнять программы и макросы».

Ну а раз PDF-файлы не всегда безопасны, то проверять, как поведет себя сотрудник с запуском небезопасного содержимого, таки нужно.

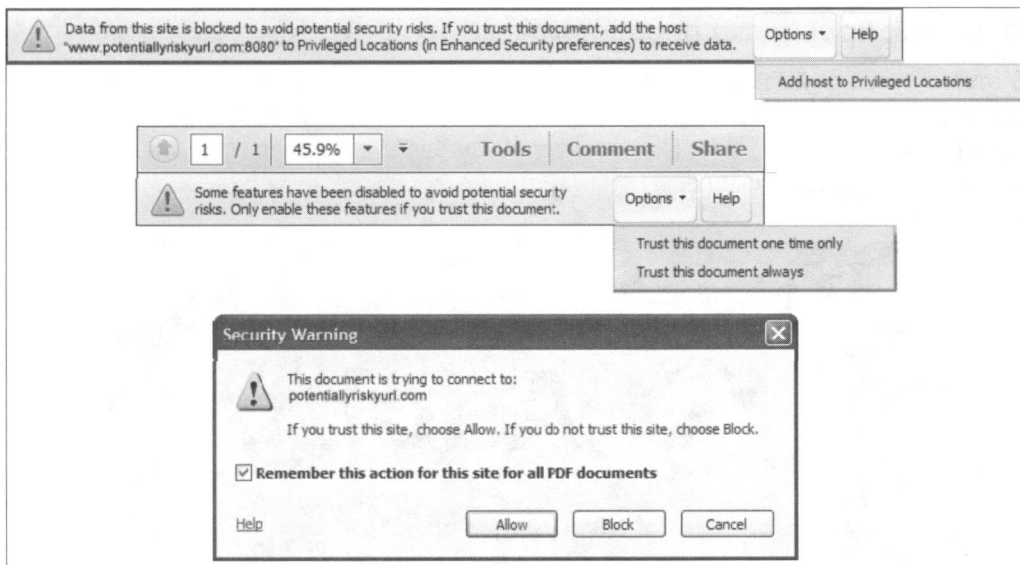


Рис. 1.32. Всплывающее окно с предупреждением в PDF-файле

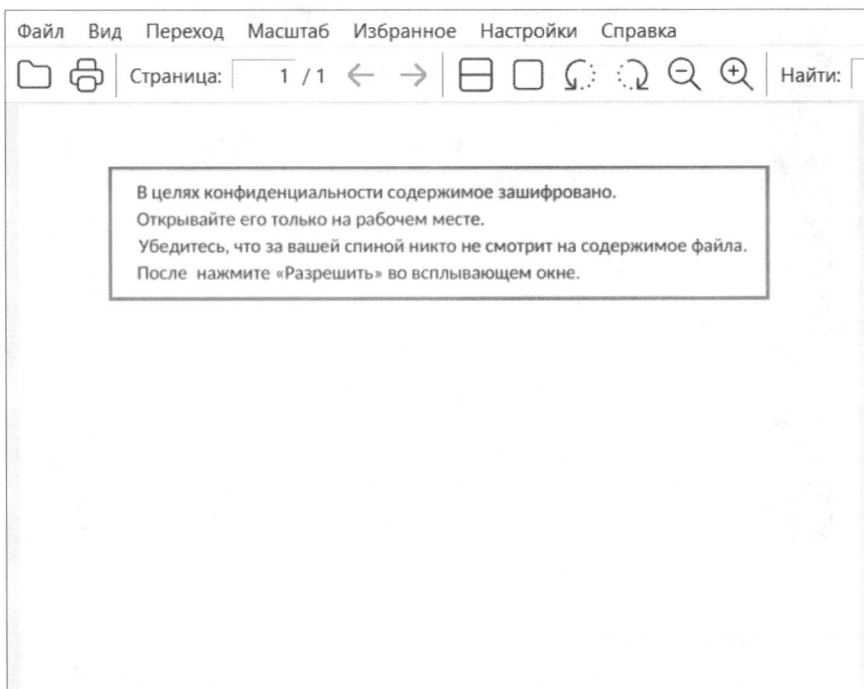


Рис. 1.33. Пример текста с «инструкцией» в PDF-файле

Файл как прокладка перед нагрузкой

В этом случае файл из вложения или скачанный файл сами по себе не являются вредоносными. Но в них будет отсылка к вредоносу, который необходимо скачать по ссылке (рис. 1.34). Пользователь скачивает твою нагрузку либо переходит по фишинговой ссылке.

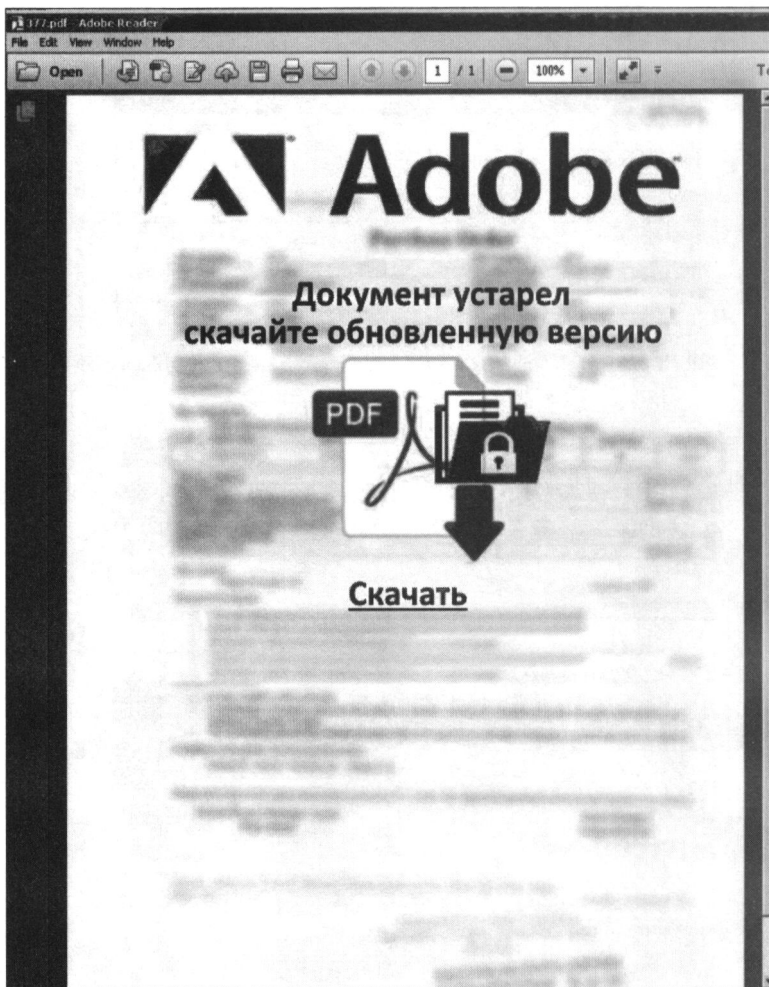


Рис. 1.34. Ссылка в тексте файла с замыленным содержимым

Вот и еще подобный вариант (рис. 1.35).

И еще один пример с другим визуальным оформлением (рис. 1.36).

А это вариант, когда мы напрямую отправляем пользователя на сайт (рис. 1.37).

Для разнообразия используем не только PDF-формат, но и TXT и другие (рис. 1.38).

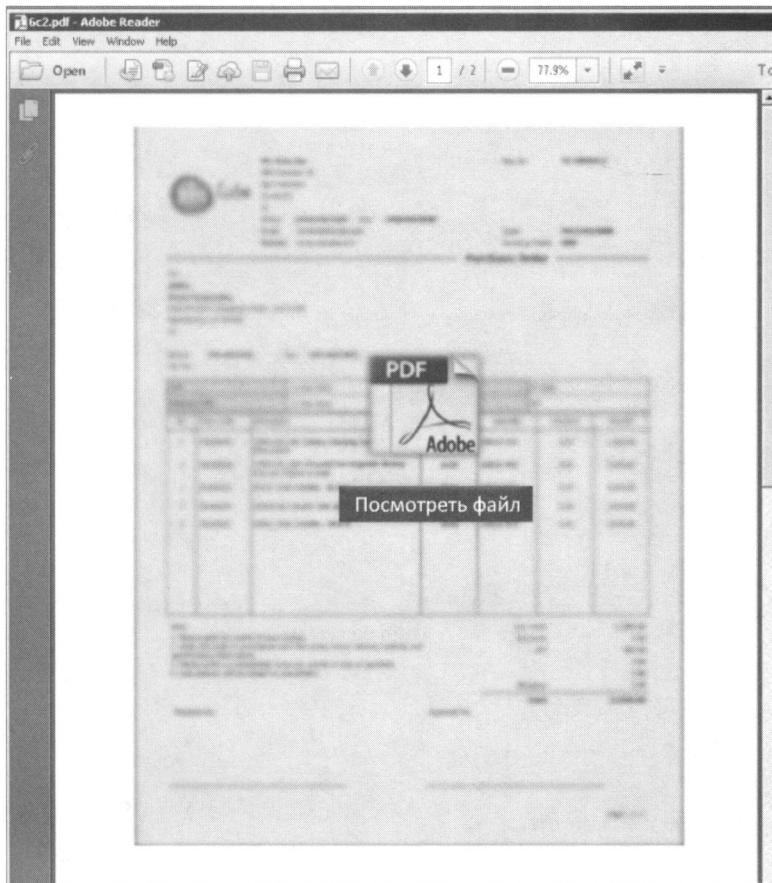


Рис. 1.35. Пример PDF-файла с замыленным содержимым и кнопкой для скачивания вредноса или перехода на фишинговый сайт

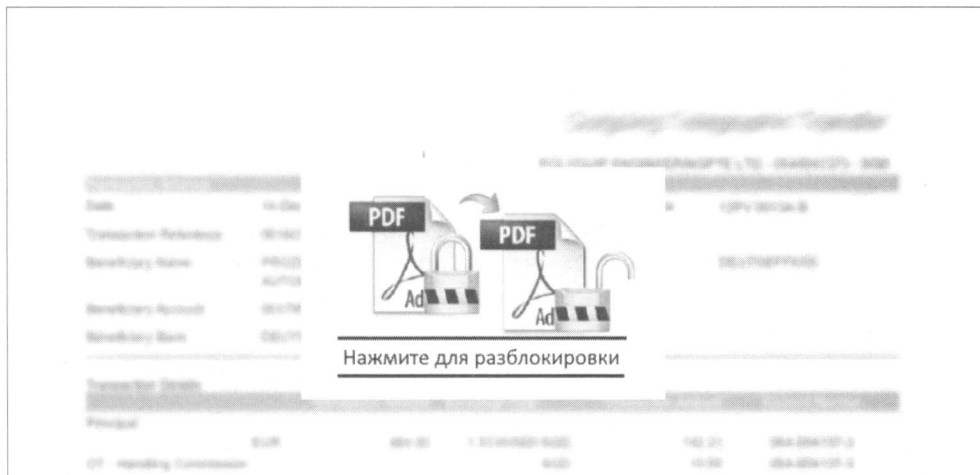


Рис. 1.36. Пример визуального оформления PDF-файла прокладки

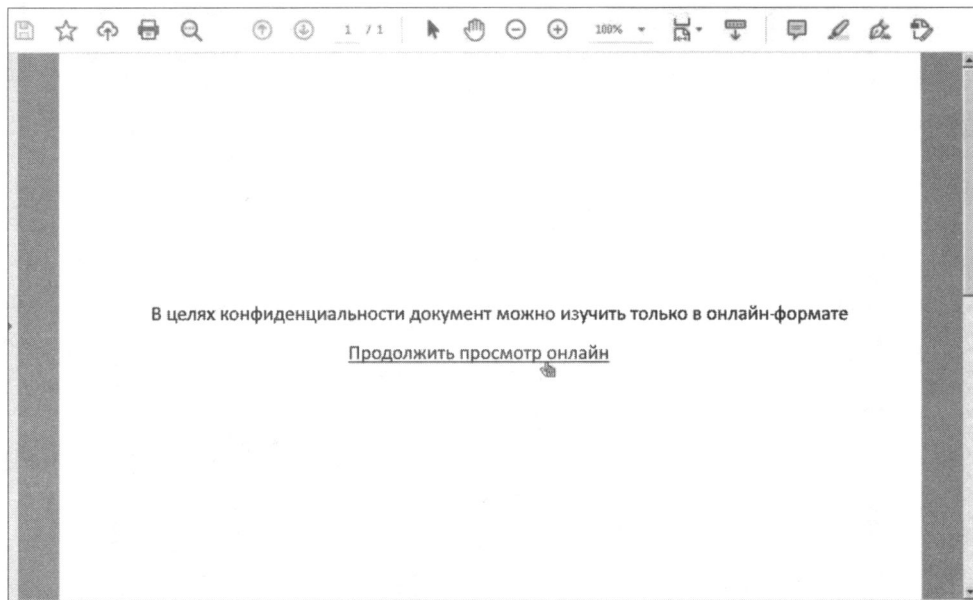


Рис. 1.37. Файл со ссылкой

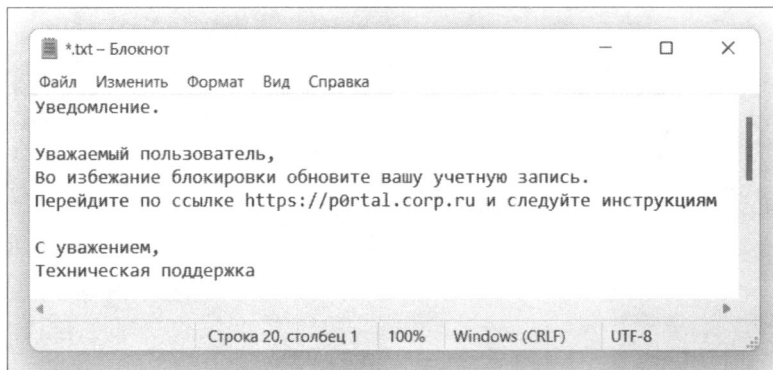


Рис. 1.38. Текстовый файл с фишинговой ссылкой

Отсутствующий сертификат

Мы с тобой знаем, что EXE-файл может запускаться не сразу, а предупреждать пользователя об опасности, поэтому нужно «помочь» получателю файла запустить твою нагрузку. Например, в Windows 10 предупреждение выглядит так, как показано на рис. 1.39.

В письме с файлом можно «предупредить» получателя примерно так:

Уважаемый коллега. Во вложении обновленный VPN-клиент. Мы еще не получили цифровой сертификат на него, но им можно и нужно пользоваться уже с сегодняшнего дня, т. к. без него не будет работать большинство приложений на удаленных рабочих компьютерах.

Что необходимо сделать:

Запустите файл в архиве.

У вас появится синее окошко, где нужно нажать ссылку «Подробнее», и появится кнопка «Выполнить в любом случае».

Нажмите на нее, и после этого VPN-клиент заработает.

Напишите, если у Вас возникнут трудности с запуском.

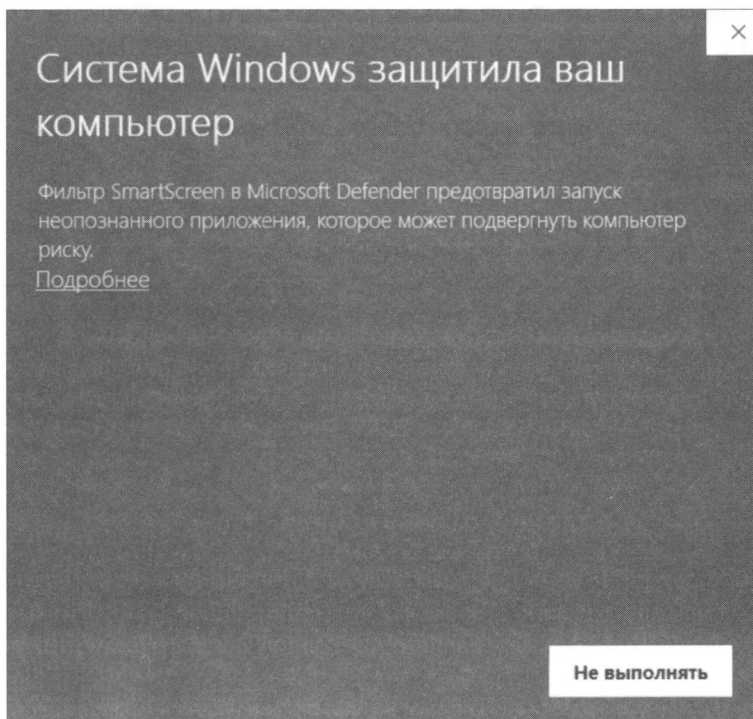


Рис. 1.39. Уведомление безопасности в Windows при запуске файла с отсутствующим сертификатом

Разрешите и заполните


Обычно мы просим пользователя разрешить редактирование офисного документа — якобы для того, чтобы содержимое корректно отобразилось. Но можно подтолкнуть его на это интуитивно.

Если прислать документ, в котором надо заполнить много информации и отправить файл обратно, то он не сможет этого сделать, пока не «догадается» нажать кнопку «Разрешить редактирование», что нам и нужно.

Так, например, действовали хакеры в 2021 году, атакуя военно-промышленный комплекс России.



Содержимое вложения приведено на рис. 1.40.



© Акционерное общество
«Государственный ракетный центр имени академика В.П. Макеева»
Отдел кадров (по вопросам трудоустройства)
Адрес: 456300, г. Миасс, Челябинская область, Тургорякское шоссе,1
Факс: 8 (3513) 55-51-91, 24-12-33
тел. 8 (3513) 28-63-33, 28-63-70
E-mail: src@makeyev.ru

Проверка Сотрудников (2021.9.16.)

В период с 16 по 21 сентября 2021 года отдел кадров проведет проверку данных сотрудников для обновления списка сотрудников в компании.

Пожалуйста, заполните форму.

<u>Имя</u>	
<u>День Рождения</u>	
<u>Отделение</u>	
<u>Название Работы</u>	
<u>Эл. адрес</u>	
<u>Номер телефона</u>	
<u>Номер мобильного</u>	
<u>Женатый</u>	<u>Да / Нет</u>
<u>Количество Детей</u>	
<u>Дата Приема На Работу</u>	

После заполнения формы отправьте ее в отдел кадров по электронной почте или ответьте на это письмо.

Рис. 1.40. Содержимое файла, который предлагается заполнить

Файл ICS

Формат ICS (первая буква — заглавная «i») — формат файлов, используемый для календарей и email-клиентов (Google Calendar, Apple iCal, Microsoft Outlook). В iPhone, например, такой файл отображается так, как показано на рис. 1.41.

Здесь кнопки **Сохранить** в свой календарь нет, но это не беда. Такой вариант подходит для срочных векторов:

Коллеги, напоминаем, что онлайн-встреча сотрудников с генеральным директором уже началась. Повторно прикрепляю файл с напоминанием для календаря.

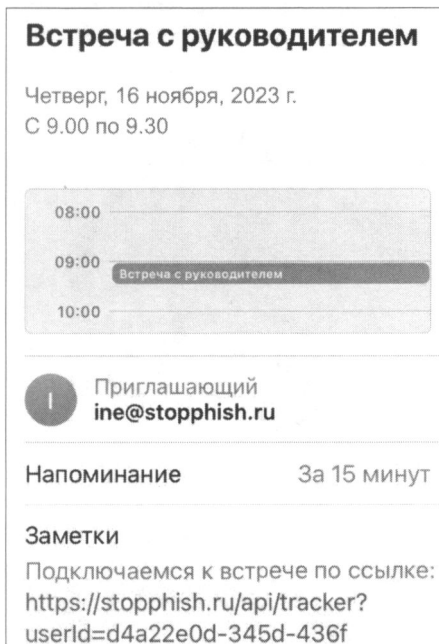


Рис. 1.41. Пример отображения файла ICS на iPhone

Отправляем в 9.05. Сотрудник подумает, что уже опаздывает, и будет меньше размышлять, стоит ли переходить по ссылке.

Социальные сети

При пентестах и проверке осведомленности социальные сети часто обходятся стороной. В принципе, причины понятны — это личное пространство пользователя, и соцсети часто запрещено запускать на корпоративном ПК.

Но в тот момент, когда сотрудник на своей странице указал, где работает, он становится целью. Поэтому выборочно можно проверять сотрудников на то, как они поведут себя с теми же самыми файлами и ссылками, полученными в соцсети. Помимо отправки нагрузки, можно также заниматься data-фишингом или просто разведкой.

Зачем злоумышленнику атаковать сотрудника в социальной сети?

- Сотрудник может отправить «коллегам» конфиденциальную информацию.
- Злоумышленник может получить доступ к личному телефону или ПК сотрудника. Если на его устройстве есть VPN, который подключается к сети организации, считайте, что злоумышленник уже «гуляет» по корпоративному серверу или рассылает фишинговые письма другим сотрудникам.
- Если у вас слабая парольная политика, то сотрудник будет использовать одинаковый или схожий пароль как к соцсети, так и к ресурсам организации.

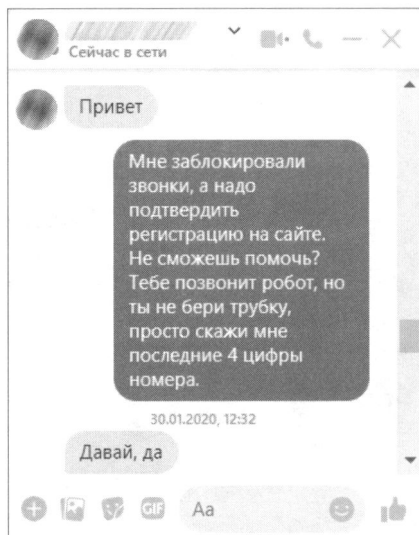


Рис. 1.42. Пример сообщения от злоумышленника в социальной сети для прохождения им двухфакторной аутентификации, где используется второй фактор как автоматический звонок

Пример, показанный на рис. 1.42, конечно, не для корпоративного мира, а для простых граждан, но вдруг пригодится, когда нужно пройти такой вид аутентификации от корпоративного ПО.

Подготовка

Перед тем как проверять осведомленность сотрудника в соцсети, нам, конечно, понадобится аккаунт (скорее даже несколько). Аккаунт можно создать или купить (пишешь в поисковике: купить аккаунт в ...). Только не покупай «лом» — за угнанные аккаунты по голове не поглядят.

Нам потребуются женские аккаунты — причем неважно, какого пола наша цель. В большинстве случаев подготавливаемому нами боту должно быть около 35–45 лет. Эротических фото размещать не надо. Обычная женщина.

Фотографию на аватарку генерируем с помощью нейронных сетей тут: <https://thispersondoesnotexist.com> — так соцсеть тебя автоматически не забанит за воровство фото с других аккаунтов. Результат генерации получается довольно реалистичным (рис. 1.43).

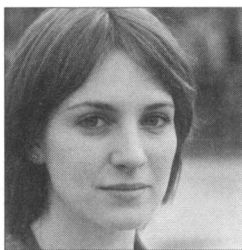


Рис 1.43. Пример сгенерированной «фотографии»

Остальные фотографии берем с людьми, но без лиц. 3–5 фото вполне достаточно. Для получения уникальных фото отлично подойдут скриншоты из видео.

Подписывать фото важно «по-человечески», эмоционально, чтобы создавалось впечатление, что они не фейковые. Непрофессиональные фотографии природы тоже подойдут, но не забываем о подписях — например: «Зима в разгаре» (рис. 1.44).



Рис. 1.44. Пример бытовой непрофессиональной фотографии

Заполняем остальные поля в профиле по настроению: школа, вуз и т. д. Место работы не пишем (впрочем, можно написать, что ты HR, если собираешься общаться с жертвами в его роли). Когда будешь писать одному конкретному человеку, то в аккаунте можно использовать вектор *«Усиление контекста: совпадение»* из разд. *«Атаки по email»* этой главы.

Если ты создал аккаунт с нуля, надо добавить ему «историю». На «стене» должны присутствовать какие-то записи в прошедшем времени, а не так, что сегодня создали аккаунт и давай писать сотрудникам. Создать себе аккаунт десятилетней давности легче всего на FB.

Для этого размещаем пост с настройкой видимости **Только я** (рис. 1.45), после чего жмем на меню сверху справа и меняем дату на 3–4 года назад (рис. 1.46). Создаем таким способом 8–10 постов.

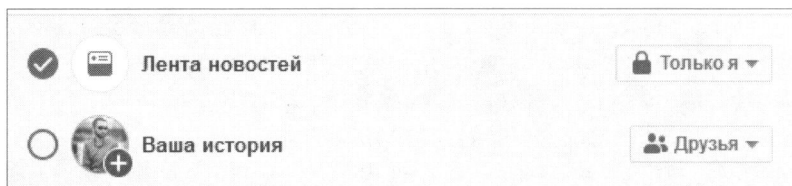


Рис. 1.45. Пример настройки видимости поста

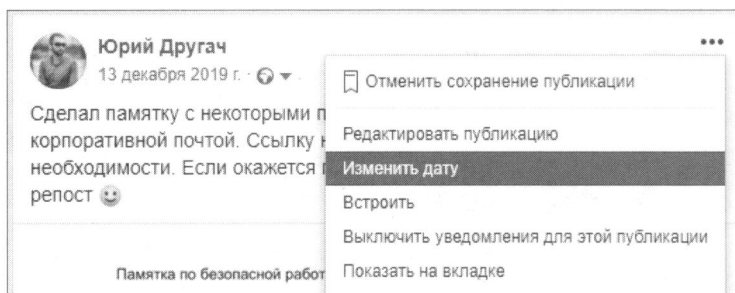


Рис. 1.46. Изменение даты публикации поста

Теперь нужно «набить» друзей в аккаунт. Кто у нас любит знакомиться с новыми людьми, даже если не знает их? Правильно, так и пишем в поиске по группам, как показано на рис. 1.47.

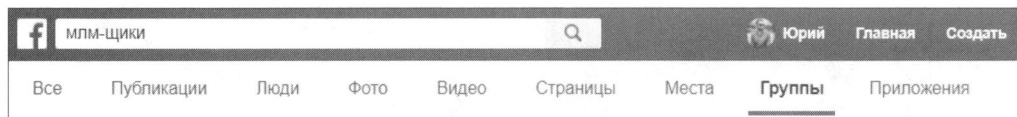


Рис. 1.47. Поиск тематических групп

Добавляемся в первую попавшуюся группу и в разделе **Участники** видим десятки тысяч наших потенциальных друзей. Открываем их профили и добавляемся в друзья к 20–30 участникам. Как только вас добавит несколько человек, идем к ним в профили в раздел **Друзья** и отправляем заявки в друзья их друзьям (как много слов «друзья» в одном предложении, но что поделать...).

Люди, которым будут приходить наши заявки, увидят, что у нас есть общий друг, и с большей вероятностью добавят нас к себе в круг. За час таких добавлений заявки я уже отправлял потенциальным френдам с общим пересечением в 5–7 человек и набирал по 500–600 человек в «близкий круг». Но для наших целей достаточно и 100–200 человек.

Теперь нужно добавлять целевых друзей. Ищем людей по названию организации (рис. 1.48).

Добавляем человек 10, не больше, и ждем, когда нас примут в друзья. Теперь отправляем заявки всем остальным, кого мы смогли найти, — как ты понимаешь, доверия будет больше, если у нас в друзьях уже числится коллега из орга-

низации жертвы. Если сотрудников таким способом нашлось не много, придется идти в другие соцсети (например, в LinkedIn) и искать там (рис. 1.49). На странице организации видим список сотрудников и пытаемся найти их в FB, чтобы добавить в друзья.



Рис. 1.48. Пример поиска сотрудников какой-либо организации

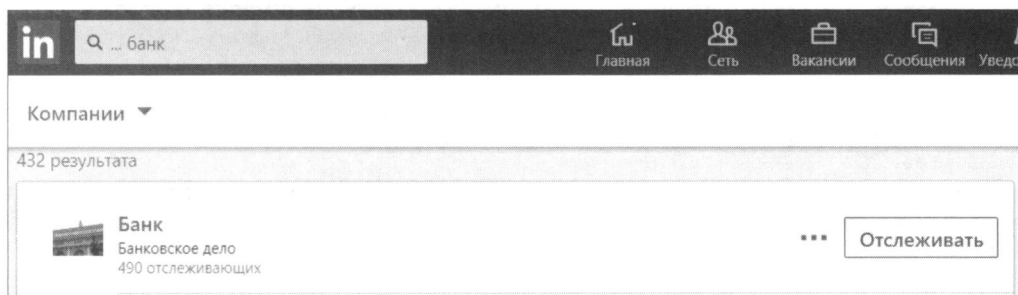


Рис. 1.49. Пример поиска организации в LinkedIn

Ну а совсем нехороший человек может стать SMM-рейдером — т. е. присвоить себе группу в LinkedIn, у которой еще нет владельца (рис. 1.50), но сейчас не об этом ;-)

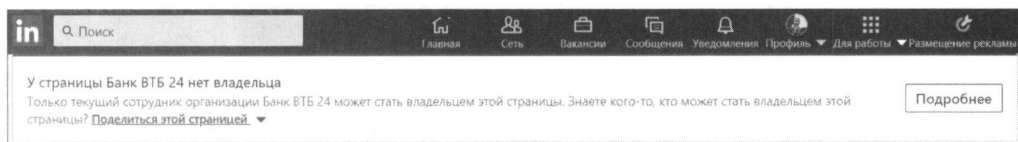


Рис. 1.50. Пример сообщения на странице организации, у которой нет владельца

Итак, мы «подружились» с сотрудниками организации, которая заказала у нас пентест.

Приступим к написанию сообщений. Если вы не уверены, что человек работает в целевой организации, — это отличный повод начать общение (на самом деле, даже если он там работает).

Делаем «многоходовку» и пишем простое именованное сообщение:

..., добрый день. Вы еще работаете в ...?

В ответ придет одно из трех: «да/нет/а что?».

Если ответ утвердительный, пишем:

Жаль, конечно, в хорошем смысле, но ладно, успехов Вам!

Жертве станет любопытно, и она опять же спросит: «А что?»

Пишем:

Так как речь идет о работе, я не хочу, чтобы меня обвиняли в переманивании, поэтому вы можете ознакомиться с информацией в открытом доступе самостоятельно (*тут ссылка на фишинговую форму авторизации в соцсети*). Только если что, Вы нашли ее случайно.

Если целимся на завладение телефоном жертвы или домашним ПК, то предлагаем отправить файл. Пишем:

Так как речь идет о работе, я не хочу, чтобы меня обвиняли в каком-то там переманивании. Но если Вам интересна работа по специальности, с более высокой зарплатой и действительно адекватным руководителем, я могу отправить файл на Вашу личную почту.

Или делаем другое окончание:

...и действительно адекватным руководителем, то прикрепляю файл.

Ну и после этого отправляем жертве анкету с макросом или фишинговую ссылку со всеми вытекающими.

Если на первоначальный вопрос жертва пишет «Нет», вычеркиваем человека из нашего рабочего списка, т. к. нам за таких не платят.

НА ЗАМЕТКУ

- Название файла или ссылки может включать «120000р» или «120kRub» — так мы дадим понять, что деньги предлагаются хорошие.
- Начинать сообщение с «Добрый день» (утро, вечер) лучше, чем со «Здравствуйте» — конверсия в ответы выше.
- В рабочее время сотрудник, скорее всего, будет заходить в соцсеть со смартфона, учти это при планировании атаки.
- В зависимости от копирайтинга сообщения можно отправить сотруднику не просто ссылку или файл с макросом, но и APK-файл (*.apk) — якобы специально созданное для соискателей закрытое приложение, в котором нужно разрешить геолокацию, авторизоваться в gmail, дать доступ к СМС и т. п.

О поиске сотрудников в соцсетях

Помимо стандартного поиска в соцсети, можно искать сотрудников через страницы компании. Например, в FB посмотреть, кто лайкает посты на этой странице, — если один человек лайкнул несколько постов (особенно, когда лайков под постами 2–3), с большой долей вероятности можно сказать, что это сотрудник организации. Но при таргетированной СИ имеет смысл уточнить эту информацию по другим источникам (соцсетям, поисковикам), поскольку этот лайкающий, может быть, просто хочет устроиться в компанию работать.

Как искать сотрудников в VK, мы уже рассматривали ранее, в *разд. «Подготовка»*. Не грех и повториться — идем на страницу:

https://vk.com/search?c%5Bcompany%5D=%D0%90%D0%9E%20%D0%A0%D0%BE%D0%B3%D0%B0%20%D0%B8%20%D0%BA%D0%BE%D0%BF%D1%8B%D1%82%D0%B0&c%5Bname%5D=1&c%5Bper_page%5D=40&c%5Bsection%5D=people



и вбиваем название работодателя в поиск.

Ну а LinkedIn создан для поиска сотрудников в определенных компаниях. Он заблокирован в РФ, но, странно, люди как-то продолжают им пользоваться.

Клонирование аккаунтов

Вновь созданный аккаунт будет пользоваться бóльшим доверием, если это фейковый профиль коллеги, друга, знакомого потенциальной жертвы.

Создавая фейковую копию аккаунта коллеги, используй подмену символов. Как мошенники в Telegram создают копии известных групп, так и ты можешь пользоваться этим приемом при указании имени аккаунта в благих целях. Например, в Instagram мошенники так и рекомендуют делать — вместо точки использовать нижнее подчеркивание и наоборот: `yu.ra` ↔ `yu_ra`.

Не забывай и про обычный тайпсквоттинг, когда символы меняются на похожие или добавляются лишние.

Если пользователь вдруг заметит подвох и спросит, почему ты пишешь с нового аккаунта, скажи, что ты потерял доступ к старому аккаунту, а восстановить не получается.

Медленно, но верно

Почаще лайкай и комментируй посты на странице или в группе организации. Постарайся примелькаться — пусть тебя заметят 5–10 сотрудников (поймешь по лайкам и комментариям твоих комментариев).

Дождись момента, пока тебя не попросят о помощи или не зададут вопрос. Ответишь, что можешь скинуть на почту (естественно, в идеале корпоративную), и отправляешь вредонос.

Лучшие векторы — когда пользователь сам инициирует отправку ему нагрузки.

Многоходовка в соцсети

Порой удивляешься фантастическим сценариям социальных инженеров.

Вот пример многоходовки, когда иранские хакеры маскировались под инструктора по аэробике. Более 18 месяцев они работали через сеть ботов в FB и по email (рис. 1.51), общаясь с работниками воздушно-космической обороны США. Особенно хакеров интересовали те, кто участвует в операциях на Ближнем Востоке.

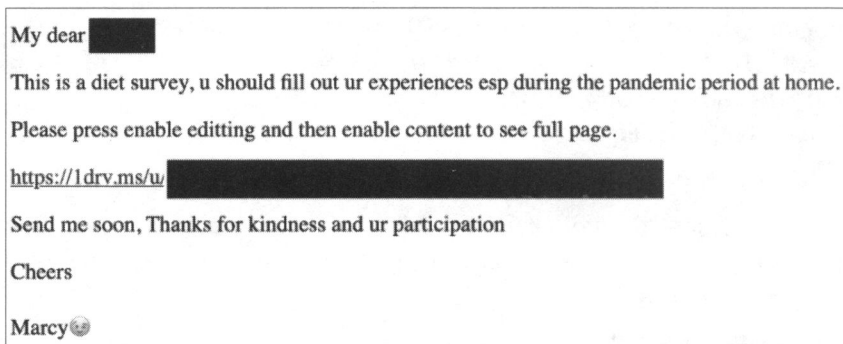


Рис. 1.51. Пример письма от иранского хакера с опросом для жертвы о ее питании

Полную статью можно почитать тут:
<https://xakep.ru/2021/07/28/marcella-flores/>.



Терпеливо ждем

У тебя может не быть нескольких месяцев на тесты, но не всегда нужно торопиться, — ведь если сотрудники привыкают к «быстрым» методам атак, то сложную многоходовку им разгадать намного сложнее.

Нельзя не упомянуть тактику выжидания. Познакомившись с тобой в соцсети, рано или поздно жертва сама напишет в своем посте просьбу (или уже написала, посмотри ее ленту), что ей что-то необходимо.

Воспользовавшись поводом, можно отправить не только «вредоносный» архив, но и фишинговую ссылку на сайт, где якобы раскрывается ответ на ее вопрос. Сайтом может быть и социальная сеть, в которой ты общаешься с жертвой.

Поддельный рекрутер

Если в рамках пентеста ты решил начать атаку через HR или отдел кадров, то для тебя открывается целый веер способов и поводов для первоначального проникновения в организацию. Помимо того, что можно отправить что-то для HR, якобы устраиваясь на работу, или проникать в периметр компании для «собеседования», можно атаковать и сотрудников заказчика, самому представившись рекрутером.

Один из поводов написать сотруднику целевой компании — это предложение о работе.

Например, как это делала хак-группа Lazarus:
<https://xakep.ru/2023/10/03/lazarus-lightlesscan>.



Злоумышленники вышли на связь с сотрудником компании-жертвы, представляясь рекрутером известной ИТ-компании, и вынудили его установить бэкдор.

Используя этот сценарий в пентесте, можно написать что-то вроде:

«Добрый день. Я вижу, что вы работаете в компании ... Не рассматриваете ли вы предложения о работе?»

Ссылку или файл можно отправить сразу, но лучше после некоторого общения, как в многоходовках.

Разумеется, предложения о работе можно писать не только в соцсетях, но и по другим каналам связи.

Аналогично описанному сценарию, в 2024 году хакеры проводили фальшивые собеседования, нацеленные на разработчиков, чтобы склонить их к установке Python-трояна удаленного доступа:

<https://xakep.ru/2024/04/27/dev-popper/>.



Хакеры использовали их доверие к процессу приема на работу, где отказ от выполнения тестовых заданий интервьюера может поставить под угрозу возможность трудоустройства.

В этом случае злоумышленники точно таргетировали атаку под род деятельности жертвы. Подобные задания можно придумать для любой профессии.

Мессенджеры

В мессенджерах лучше применять не массовую, а таргетированную СИ, — так тебе понадобится меньше ресурсов на подготовку и реализацию мероприятий по поиску неосведомленного сотрудника. К тому же найти базу мобильных номеров большинства сотрудников организации не так-то просто (но если нашел, технически такая рассылка делается через сервисы рассылок, — погугли).

В случае, когда атаку инициирует безопасник, все мобильные телефоны у него в наличии есть, просто нужно обсудить возможность таких тестов с юристом.

Мы же рассмотрим ситуацию, когда ты потом и кровью добыл несколько номеров мобильных телефонов и тебе одобрен таргетированный тест нескольких сотрудников.

В зависимости от мессенджера, тебе потребуется либо номер мобильного телефона (например, для WhatsApp), либо никнейм (в Telegram).

Для тестов можно купить готовый аккаунт. Напиши в поисковике: купить аккаунт Телеграм, и найдешь немало предложений, включая инструкции по установке portable-версий клиента для мультиаккаунтовости.

Для регистрации WhatsApp-аккаунта используем сервисы активации SMS. Рекламирывать тут никого не стану — гуглить в «Яндексе» все умеем :-)

Собственно по «Классификатору СИ» (см. приложение 2) составляем сценарий, который от email будет отличаться лишь краткостью сообщений. В качестве нагрузки проще использовать ссылку. Кстати, учти, что WhatsApp «ходит» по ссылкам, которые ты отправляешь. А то подумаешь, что пользователь попался и перешел по ней.

Представляться в таких сообщениях можно коллегой, который узнал номер и пишет в мессенджер, т. к. дело не терпит отлагательств. Пишем после работы или на выходных.

Telegram-каналы

Раз злоумышленники их используют, значит, и тебе они могут пригодиться.

Распространенный способ подделки Telegram-аккаунтов — с помощью большой И (I) вместо маленькой Л (l).

В корпоративном мире всё чаще используют Telegram-группы для общения и оповещения сотрудников. Ссылки на них бывают размещены в общедоступных местах. Например, в одной организации, в которой чуть что случись — приезжает ФСБ, QR-код с приглашением в корпоративную группу в Telegram был размещен возле лифта.

Тебе ничего не мешает прикинуться сотрудником и почитать, о чем пишут в таких группах, — а может, и разместить что-то или, подделав аккаунт сотрудника, написать коллеге.

Сотрудник — физлицо

Если юридически проверка осведомленности сотрудника по номеру мобильного телефона одобрена, то вектор для него можно создать не только корпоративный. Вот, например, такое сообщение пришло коллеге (рис. 1.52):

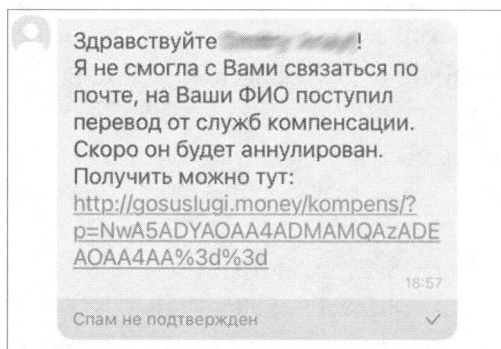


Рис. 1.52. Пример фишингового сообщения

Онлайн-консультанты

С онлайн-консультантами всё просто — тестируем службу поддержки, используя способы маскировки ссылок, как и в email (рис. 1.53). В этом эксперименте использовались Unicode-разделитель «/» (U+0B75) и символ @. Для эксперимента домен **talog.ru** выбран случайный, куда и попадал посетитель, переходя по ссылке.

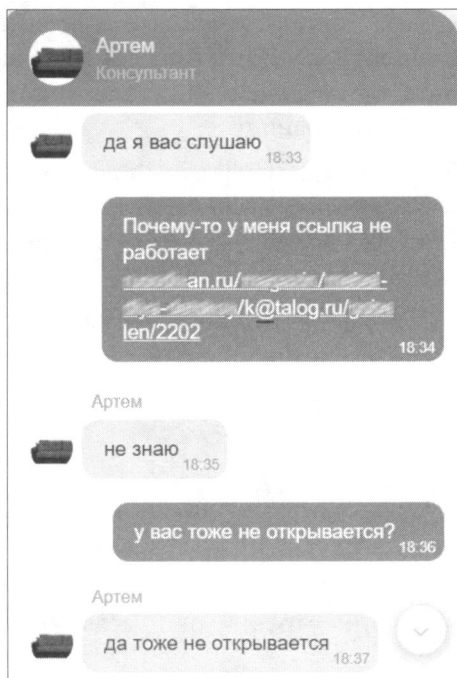


Рис. 1.53. Пример отправки вредоносной ссылки в онлайн-консультанте на сайте

Веб-сайты

Сайты были и будут оставаться одними из самых востребованных и одними из самых опасных элементов Интернета. Попадая на страничку, посетитель даже не задумывается, что уже находится «под колпаком», если, например, он давно не обновлял свой браузер.

Но в этой книге мы не будем говорить о уязвимостях zero day, т. к. я вообще не разбираюсь в техническом взломе, а конкурсы Bug Bounty выигрывал только в «номинациях» — нецелевое использование инфраструктуры. Да и книга у нас не об этом :-)

Итак, как же можно использовать сайты при эксплуатации социальной инженерии?

Поддельное окно для ввода логина и пароля

По аналогии с тем, как у геймеров утягивают аккаунты к Steam, в том числе защищенные двухфакторной аутентификацией (<https://hacker.ru/2019/10/30/steam-phishing-2>), ты можешь использовать такие окна для учебного фишинга.



Интересны эти сценарии тем, что в таких всплывающих окнах можно написать любой адрес в адресной строке, т. к. по факту ее просто нет. То есть там ты можешь нарисовать что угодно.

Эта атака — когда в браузере жертвы отображается всплывающее окно — называется Browser-in-the-Browser (BitB). Есть также и ее модификация — Browser-in-the-Middle (BitM), когда злоумышленник создает экземпляр сервера, принимающего соединения через веб-страницу.

В статье <https://ptresearch.media/articles/slozhnee-chem-kazhetsya-soczialnaya-inzheneriya-2023> рассказывается подробнее об этих атаках, но ты можешь просто их погуглить, — есть и более подробные статьи, с вариантами эксплуатации.



Применимо это в тестах пользователей в корпоративном сегменте — ты можешь имитировать официальный сайт компании, при клике на любой из ссылок которого будет появляться окно для ввода учетных данных.

Скачайте на нашем сайте

В одном из кейсов мы побуждали сотрудников качать нагрузку с нашего поддельного сайта, а не прикладывали ее к письму, но обо всем по порядку.

К нам обратилась организация, которая попросила реализовать сложный сценарий проверки осведомленности сотрудников (выглядит всё легко, но организационных мер было немало).

Сценарий был такой:

Сотрудникам отправляется письмо, где есть ссылка на поддельный сайт банка (не портал, а обычный сайт). Поводом было предложение посмотреть начисленные зарплаты с премиями. Ситуация осложнялась тем, что в банке использовался терминальный Интернет — т. е. сотрудник не просто кликал на ссылке, он копировал ее и вставлял в отдельное окно.

На фишинговом сайте были размещены небольшой текст и ссылка с надписью **Скачать файл**.

Тогда мы еще не могли отслеживать, кто конкретно скачал и пытался запустить файл, поэтому служба ИБ проверяла это по логам.

В результате выяснилось, что файл скачало и запустило около 60% сотрудников — т. е. они не проверяли ни ссылку в письме, ни сайт, на который попали.

Корпоративные порталы

Начнем с классики. Если на корпоративном портале используется форма авторизации (например, как показано на рис. 1.54), смело копируем форму и вставляем на свой поддельный сайт.

Если повод, под которым ты отправил сотрудника на «портал», убедительный, жди логинов и паролей. Кстати, если портал использует базовую аутентификацию (basic access authentication), то скопировать такую форму тем же Gophish не получится. Для таких случаев мы с нуля верстаем HTML-форму, похожую на оригинальную.

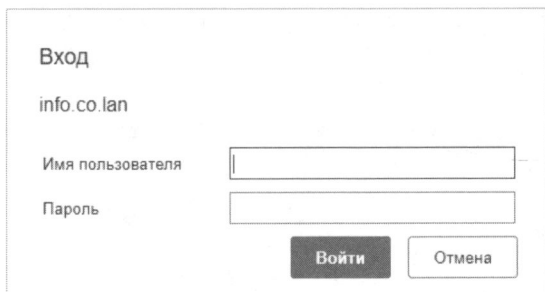


Рис. 1.54. Пример простой формы авторизации

Но не беспокойся обо всех деталях страницы авторизации — по опыту, 20–40% сотрудников оставляют свои учетки после убедительной легенды в сообщении со ссылкой.

Разрешите уточнить

Такое окошко (рис. 1.55) должно быть тебе знакомо.

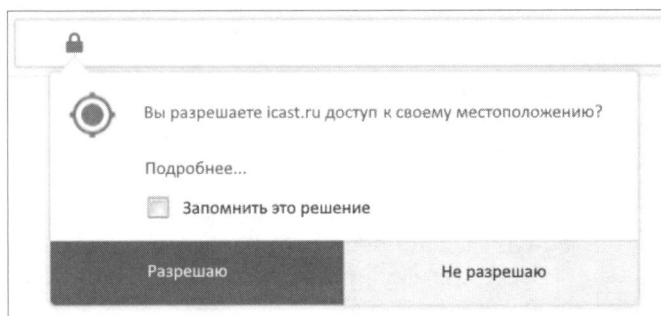


Рис. 1.55. Пример сообщения браузера с запросом разрешения доступа к местоположению

Если на веб-странице написать что-то вроде:

Внимание, контент на этом ресурсе доступен только для жителей стран СНГ.
Подтвердите, что вы находитесь в одной из этих стран, нажав **Разрешаю**.

то ты сможешь убедиться, что сотрудник открыл твой сайт на своем рабочем месте, а не дома (или наоборот), — если тебе для чего-то понадобилось узнать, где он находится.

Новостные ресурсы

Копируем новостной ресурс и пишем «статью», что сотрудникам такой-то организации пора искать работу в связи со сложившейся ситуацией (снижение прибыли и т. п.). В статье указываем, что организация на своем сайте уже разместила список подразделений и филиалов, которые будут сокращены в первую очередь, и даем ссылку.

На поддельном сайте организации даем ссылку на скачивание файла или показываем форму логина и пароля для ввода учетных данных.

Метод жесткий, поэтому повод для новости в СМИ можешь придумать свой. Главная суть сценария — использование фейкового сайта СМИ как стартовой площадки для атаки.

Туда, да не туда...

Если навести мышь на ссылку, то увидим **ya.ru** (рис. 1.56).

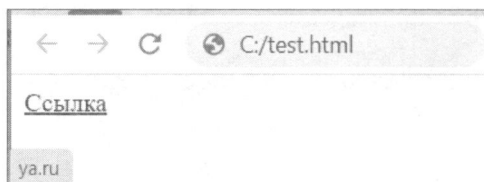


Рис. 1.56. Пример отображения ссылки в браузере при наведении указателя мыши

Но на самом деле после клика на ней мы попадем на **https://stopphish.ru**. Вот почему пользователям нужно проверять интернет-адрес (URL) не только перед переходом по ссылке, но и после того, как уже попали на страницу.

HTML-код для подмены отображения ссылки

```
<a onclick="window.location.href='http://stopphish.ru';return false"  
href="http://ya.ru" >Ссылка</a>
```

Помимо того, что этот метод маскировки целевой страницы можно использовать непосредственно на веб-сайтах, попробуй отправить HTML-файл как вложение в письме, если тебе требуется замаскировать ссылки в открывшемся в браузере окне.

Фейковая капча и предупреждение о cookie

Всякое случается, вдруг пригодится...

Побудить пользователя сделать клик на сайте можно с помощью фейковой капчи (рис. 1.57) — например, для активации эксплойта или события java-скрипта (я слышал от маминой подружки, что это нужно для утилиты VeEF).

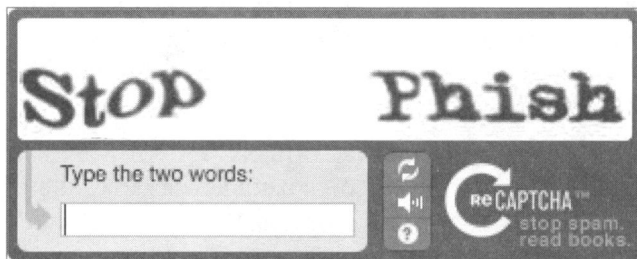


Рис. 1.57. Капча

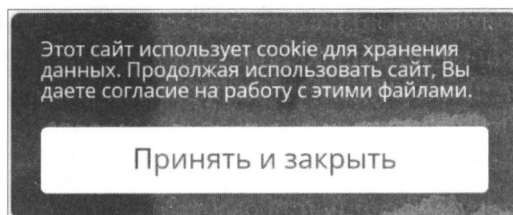


Рис. 1.58. Всплывающее сообщение с предупреждением об использовании cookie

Этой же цели поможет добиться фейковое окно с предупреждением об использовании cookie-файлов (рис. 1.58).

Всплывающее окно

Полноразмерное всплывающее окно браузера, перекрывающее интерфейс браузера, на котором пользователь совершает действие (нажимает клавишу на клавиатуре или кликает кнопкой мыши), может сбить с толку. Создается оно с помощью Fullscreen API в HTML5. Тут описано, как это сделать: <https://habr.com/ru/post/184926>.

Что показывать пользователю во всплывающем окне? Например, окно авторизации в ОС (рис. 1.59), желательно с персонализацией в виде email или логина, который идет до символа @ в корпоративной почте. Такое можно реализовать не только при таргетированной атаке на конкретного человека, но и массово, используя ссылки в письмах с идентификаторами, соответствующими email получателя (подробности способа приведены далее — в *разд. «Персонализированный сайт»*).



Рис. 1.59. Всплывающее окно, имитирующее окно входа в Windows

Вот еще один пример того, что может всплывать в таком окне. Описание технической реализации всплывающего окна во весь экран можно посмотреть тут:



<https://xakep.ru/2013/11/26/html5-fullscreen-api>.

Впрочем, может использоваться всплывающее окно и не на весь экран. Например, имитированное всплывающее окно для авторизации в Outlook (рис. 1.60). Или вариант более старой версии Outlook (рис. 1.61).

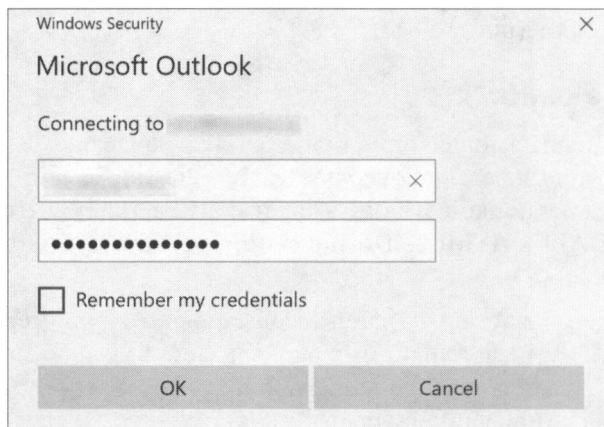


Рис. 1.60. Всплывающее окно для авторизации в Outlook

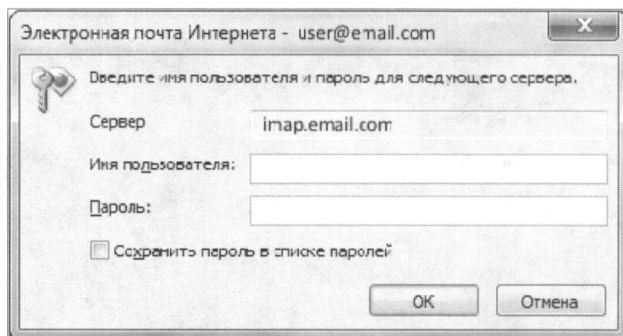


Рис. 1.61. Пример устаревшего окна авторизации в Outlook

Можно сделать всплывание такого окна с задержкой, чтобы пользователь не ассоциировал клик (или другое действие на сайте) со всплыванием окна. Еще лучше, если в письме пользователю придет вложение HTML, откроется браузер, и в окне надо будет что-то кликнуть, — юзер получает, что хотел (читает информацию), а через 5–10 секунд всплывает окно авторизации.

Персонализированный сайт

В этом способе берем на вооружение метод, который используют маркетологи, персонализируя один и тот же сайт в зависимости от меток в ссылке.

Самый простой способ реализации этого — использовать email получателя как идентификатор.

Рассмотрим способ по порядку:

1. Пишется письмо, в него вставляется ссылка, а в ссылку — идентификатор в виде email-адреса получателя:

Василий Семенович, добрый день.

Выложил документы в облачное хранилище, архив оказался слишком большим.

Ссылка для скачивания

https://yadi.sk/1_wkB@zlo.com/?id=vasiliy.s@company.com

С уважением, Андрей В.

2. Скрипт на странице, куда попадает жертва, обрабатывает ссылку и берет из нее email.
3. Затем на веб-странице этот email подставляется в необходимое место.
4. Данные из сформированной таблицы (рис. 1.62) подставляются в ссылку, и теперь она будет содержать больше данных:

https://yadi.sk/1_wkB@zlo.com/?id=vasiliy.s@company.com&OOO%20«Рога»&Директор&Иванов%20Андрей&Строительство.

Email	Компания	Должность	Ф. И. О	Род деятельности
1@ya.ru	ООО «Рога»	Директор	Иванов Андрей	Строительство
2@ya.ru	ООО «Копыта»	Бухгалтер	Иванова Анна	ИТ

Рис. 1.62. Таблица с данными, используемыми при персонализации ссылок

Но рекомендую потратить время и использовать в письме такую ссылку:
https://yadi.sk-1_wkB@zlo.com/?id=12768652376.

5. На сервер с фейковым сайтом загружаем базу данных, в которой ней определенные Id имеют соответствующие данные в ячейках.
6. И если у тебя есть заготовка сграбленного новостного сайта, в результате получается достаточно персонализированный сайт (рис. 1.63).

Как ты понимаешь, с такой персонализацией человек запустит и небезопасное содержимое в файле, и макрос и, при твоей должной сноровке, введет данные от требуемого кабинета.



Рис. 1.63. Пример персонализированного сайта

Покажи себя

Согласись, что Microsoft достаточно убедительно описывает, зачем ей нужен доступ к твоим устройствам (рис. 1.64)?

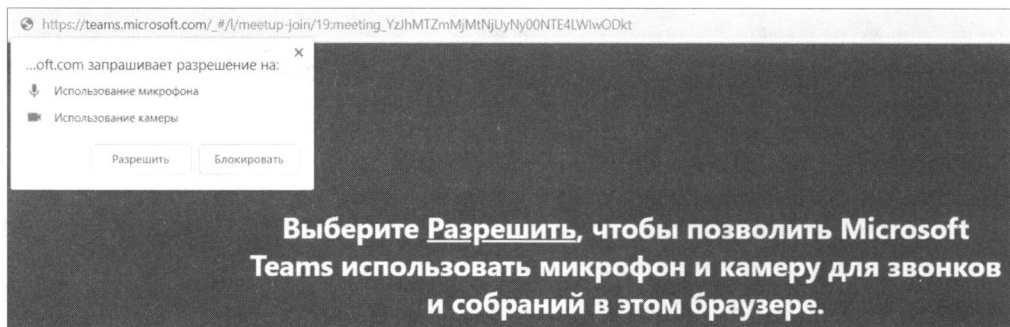


Рис. 1.64. Объяснение, зачем необходимо разрешить использование микрофона браузером на сайте Microsoft

Почему бы нам тоже не попросить человека включить доступ к камере и микрофону?

Например, так:

Нажмите **Разрешить**, чтобы просматривать видео со звуком на нашем сайте.

Реклама

Таргетировать рекламу на сотрудников конкретной организации не так просто — на ум приходит только таргетинг по геолокации или MAC-адресам.

Таргет по MAC-адресу

Снифаем MAC-адреса сотрудников, стоя возле входа в офис с рюкзачком (сидя в машине на въезде на корпоративную парковку), в котором лежит ноутбук с запущенным сниффером. Потом догоняем их рекламой, вроде: «Для сотрудников ...».

Тут описана история, как проворачивалась эта процедура для рекламных целей:

<https://vc.ru/marketing/127713-kak-ya-sobirala-mac-adresa-i-pochemu-stargetirovat-po-nim-reklamu-okazalos-ne-tak-prosto>.



В результате необходимая для запуска рекламы тысяча пользователей из одного бизнес-центра была собрана.

На самом деле, если ты соберешь только 100 полезных MAC-адресов, а остальные окажутся даже не из этого бизнес-центра, — не беда, рекламу ведь ты персонализируешь под конкретную организацию, и в заголовке объявления будет ее название (рис. 1.65), что побудит кликать нужных сотрудников. А залетных, кто использует твою нагрузку, фильтруй, за них тебе не платят, да и проблемы с законом не нужны.

Кстати, не знаю, в какой стране ты читаешь эту книгу, но имей в виду, что сбор и хранение MAC-адресов не везде разрешены законодательно.



Рис. 1.65. Пример персонализированной рекламы под определенную организацию

Таргет по геолокации

Таргетировать рекламу можно по геолокации и по работодателю. И показывать сотрудникам рекламу, которая относится к их работе, — например картинку с новостью об их компании.

В «Яндекс.Аудитории» с помощью «полигонов» это делается примерно так, как показано на рис. 1.66 и 1.67.



Рис. 1.66. Настройка геолокации в «Яндекс.Аудитории»

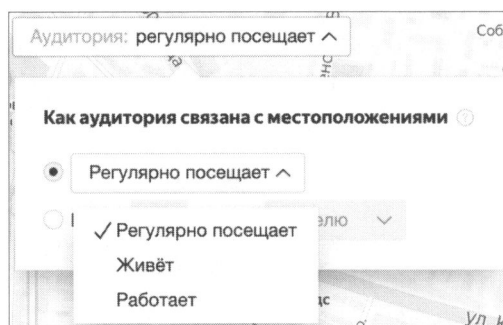


Рис. 1.67. Настройка связи пользователей с местоположением в «Яндекс.Аудитории»

Адвёртинг

Вектор, чаще используемый для физлиц или малого бизнеса, но для полноты классификации социальной инженерии упомянем и его.

Суть в том, что блогеру или другому лидеру мнений предлагают рекламную интеграцию. Для этого ему нужно скачать наш рекламируемый софт и потестить, а уже потом прорекламировать его по своим каналам.

Жертва качает ПО и заражает свой ПК.

Фиктивный APK-файл

Ты, конечно, такое повторять не станешь, но не секрет, что существует вид обмана, когда в «Яндекс.Директ» и Google AdSense в результатах выдачи на первом месте появляется рекламное объявление, оплаченное злоумышленником.

Сотрудник рекламной сети, получив созданное и отправленное на модерацию злоумышленником объявление, может проверить ссылку в объявлении только на ПК, но при этом он не увидит вредоносного приложения.

А если по ссылке зайдет пользователь со смартфона, то ему будет отдан на скачивание вредоносный APK-файл — т. к. вредоносный ресурс сам определяет, с какого устройства зашел посетитель.

Так обычному пользователю могут подсунуть, например, поддельное приложение банка.

А ты, если сумел таргетировать рекламу на определенных сотрудников тестируемой организации (например, по геолокации определенного бизнес-центра или через «Яндекс.Аудитории» с помощью «полигонов»), сможешь отправить его на свой ресурс.

Лидеры мнений

Это такие люди, к которым прислушиваются и которые имеют свою аудиторию. Если он что-то скажет — это вызовет у потенциальной жертвы большее доверие.

В этом векторе мы не подделываем сообщение якобы от лидера мнений — мы побуждаем его разместить наше сообщение. Например, админ группы в соцсети рассказал о сайте или софте (платно или нет), а после модерации админом он был подменен вредоносным.

При целевом пентесте такой вектор займет значительное время, и не факт, что жертва увидит сообщение лидера мнений, так что это подойдет только для недоступных жертв или если тебе нужно осуществить «вау-сценарий», о котором потом будут писать в СМИ.

На крайний случай ты всегда можешь имитировать лидера мнений и написать жертве якобы от его имени.

Видео-deepfake

На момент подготовки книги (окончание 2024 г.) публичных инцидентов с применением подделки видео для атаки компании зафиксировано не было, или они были известны лишь узкому кругу лиц.

Но физических лиц уже обманывают с помощью таких видео — например, 07.09.2021 на «Хабре» описывалась ситуация с Олегом Тиньковым:

«Мошенники используют deepfake¹ с лицом Олега Тинькова для сбора данных»: <https://habr.com/ru/news/t/576650/>.



В отличие от других подобных видео, Олег моргал, что несвойственно подделкам :-).

По части таких векторов можно только прогнозировать, что в ближайшем будущем видео-deepfake переключается из мошенничества с физлицами в корпоративную среду.

При желании поиграйся в создание видео-deepfake с проектом: <https://github.com/iperov/DeepFaceLab>.



Вангую манипуляции с акциями компаний, торгующихся на фондовом рынке, указанием бухгалтеру в мессенджере с просьбой перевести деньги на определенные реквизиты, снижением лояльности сотрудников из-за видео топ-менеджера «со скрытой камерой», где он плохо отзывается о сотрудниках.

Прогнозировать — не мешки ворочать, но на дворе ночь, и я, пожалуй, пойду спать ;-). Да и пищу для размышлений злоумышленникам лучше не давать.

Видео без видео

Можешь попробовать сделать такой вектор: рассылка письма по сотрудникам с превью видео от службы ИБ (в виде картинка) и поясняющим текстом, что якобы «подготовили для вас инструкцию из-за невозможности сделать настройки на каждом отдельном компьютере». При переходе по превью человек попадает на видео, в котором уже нет лица безопасника, но он объясняет (голосом или текстовыми подсказками), как изменить нужные тебе настройки на компьютере (в учетной записи и т. п.).

Аудио-deepfake

Я долго размышлял (15 минут), к онлайн- или офлайн-атакам отнести этот вектор, поскольку вредоносная нагрузка будет доставляться человеку либо с помощью соцсетей и мессенджеров, либо через телефонный разговор. Поэтому рассмотрим этот вид атак в отдельной категории.

В отличие от видео-deepfake, подделка аудио уже имеет несколько примеров применения в корпоративной среде.

Как пишет «Хакер» (<https://xakep.ru/2019/09/05/voice-deepfake>), мошенники использовали голосовой deepfake, чтобы во время телефонного разговора выдать себя за руководителя компании. По телефону фиктивный глава компании, чей голос был подделан при помощи ИИ,



¹ Методика синтеза изображения или голоса, основанная на искусственном интеллекте.

попросил главу неназванной дочерней фирмы из Британии срочно перевести 220 тыс. евро на счет некоего венгерского поставщика, хотя на самом деле этот счет принадлежал преступникам.

Symantec сообщает, что еще в 2019 г. она засекала как минимум три случая, в которых замена голоса помогла ворам обхитрить компании и заставить их отправить мошенникам деньги.

В мае 2021 г. эксперт из ИБ-фирмы Secure Anchor пишет уже о 17 пострадавших компаниях только за 4 месяца (в среднем каждая потеряла по \$175 тыс., а в одном случае хакеры получили доступ к ИТ-системам предприятия).

Если у тебя есть желание поотправлять жертве в мессенджере голосовые сообщения от имени знакомого человека, почитай статью: <https://proglib.io/p/golosovoy-deepfake-ili-kak-rabotaet-tehnologiya-klonirovaniya-golosa-2019-12-11> — может пригодиться.



Также ты можешь посмотреть *разд. «Подделка голоса» главы 7* — там мы обсуждаем аудио-deepfake с использованием ИИ. Подделка голоса в реальном времени — это не то же самое, что отправка заготовленных аудиофайлов ;-)

Find trap сценарии

На мой взгляд, в числе трендов будущего в СИ — find trap, одним из видов которого является распространение тем или иным способом слова или комбинации слов, которые люди не знают и которые они ищут в Интернете.

Злоумышленники этим пользуются, но метод не был классифицирован как самостоятельный. Условно его можно определить как «самостоятельный поиск ловушки».

Этот вид атаки требует от злоумышленника определенной подготовки, но он отличается от других видов атаки тем, что пользователю не отправляют никаких вредоносных нагрузок (ссылки, вложения). Он сам начинает искать вредоносный ресурс в поисковых системах.

Давайте рассмотрим этот алгоритм подробнее.

Жертве отправляется письмо (например, вызывающего характера):

Если Вы не отправите закрывающие документы сегодня, то мы подаем в суд.

В подписи отправителя пишется что-то наподобие:

ООО «ОблСнабСервисМонтаж»

Необходимо уникальное, но реально не существующее название.

Жертве интересно, что это за отправитель, и она начинает его искать в поисковой системе, а на первом месте результатов выдачи размещен вредоносный сайт злоумышленника, на который и переходит жертва.

Очевидно, что злоумышленнику нужно заранее подготовиться и создать страницу в Интернете этой самой несуществующей компании. Чтобы загнать сайт

в топ-1 поисковика, добавьте его в <https://webmaster.yandex.ru/> и в <https://www.google.ru/intl/ru/>. В поисковых системах на первом месте он появится быстро, т. к. конкуренции по такому запросу не будет.

В зависимости от текста письма можно сделать так, чтобы ваше письмо получили определенные лица в компании (бухгалтер, специалист по безопасности, директор, менеджер и т. д.) — первоначальный получатель уже сам перешлет письмо нужному сотруднику.

Убедитесь, что на главной странице в теге <title> прописано ваше «необычное» слово, и в контенте на странице оно встречается в теге <h1>.

Как-то в рамках эксперимента мы загнали сайт несуществующего «Профессора Рисабо» в топ (рис. 1.68).

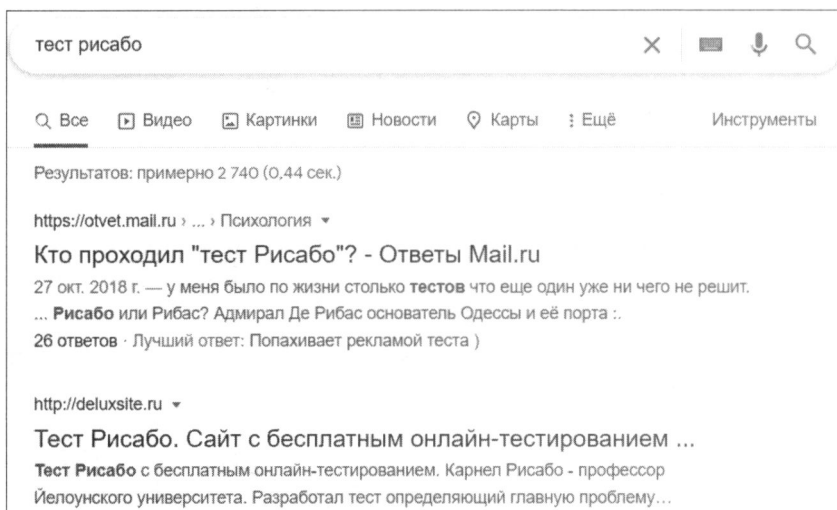


Рис. 1.68. Результаты поисковой выдачи по уникальному запросу

Сейчас в Google он на втором месте, но на первом месте находится наша приписка на otvet.mail.ru. Сайт не вредоносный — это просто эксперимент. На otvet.mail.ru был размещен вопрос, и за 50 руб. он был поднят в категории **Психология**. Люди читали вопрос и гуглили, что это за профессор, а на сайт шел трафик.

Теперь давай рассмотрим еще несколько примеров этого метода.

Find trap с помощью рекомендаций

На форуме или в соцсетях (у себя, или у активно обсуждаемых авторов, или в группах) задается вопрос, а другой пользователь на него отвечает и не дает ссылок (что-то типа «погугли сам»). Найденный ресурс ожидаемо будет вредоносным. Также можно использовать уникальный хештег, подготовив посты в соцсети с отзывами и сам рекламный пост.

Выдуманная компания

Можно создать якобы дочернюю компанию известной организации — например «Сбербанк Коучинг». Мы проводили исследование, просто поздравив с Новым годом некоторое количество юрищ. На сайт выдуманной компании перешло несколько тысяч человек. Тут главным поводом искать нашу выдуманную организацию выступал текст поздравления — он был написан «от души» ;-)

Find trap с помощью звонков

Не буду расписывать техническую составляющую, но последовательность этого метода такова: делается массовый прозвон и сброс на разные телефоны (например, по слитой базе номеров мобильных телефонов сотрудников организации), люди ищут в Интернете, кому принадлежит этот номер, находят наш сайт, и дальше всё как обычно, — на сайте им предлагают «ловушку».

Не смог быстро найти скриншот, но не так давно читал о применении такого метода. Там человеку позвонили с зарубежного номера, он его загуглил и попал якобы в личный кабинет сайта (если не ошибаюсь, связанного с криптовалютой). На балансе лежала круглая сумма, и для ее вывода нужно было сделать какие-то манипуляции вроде пополнения баланса для достижения минимального порога для вывода средств.

Продажа фиктивного сертификата

Приведу пару proof of concept для тех уважаемых экспертов, которые считают find trap сценарии нереальными.



В этих примерах злоумышленники побуждали искать выдуманные названия сертификатов, которые якобы нужны для участия в тендере.

И кстати, подобный find trap используется и при обмане физлиц.

Эту модификацию можно назвать «Струфальтово перо». Слышал о таком? Можешь почитать:

<https://shopmagi.nethouse.ru/products/23867452>



Если кратко, то суть в том, что жертве требуется купить несуществующие товары для совершения магического обряда, и, конечно, эти товары можно купить только в интернет-магазинах мошенников.

Давай вернемся к теме сертификатов. Как ты понимаешь, жертве нужно не просто дать название несуществующего сертификата, но и предложить изучить «образец» на сайте, который она найдет в поисковике. А уже сам образец будет малварью, которую человек в предвкушении выгодного контракта скачает и запустит. Поэтому не стоит недооценивать этот метод — ему не подвержен лишь тот, кто не знает, что такое поисковые системы.

Комментарии

Комментарии относятся как к социальным сетям, так и к разным платформам (форумы, блоги и т. д.), поэтому вынесены в отдельную категорию.

Тут всё просто: находим комментарии жертвы в соцсетях (рис. 1.69), на форумах или других сайтах, пишем что-то цепляющее самолюбие (или возьми другое чувство, на котором можно сыграть, или как бесчувственный манипулятор напиши просто что-нибудь плохое) и упоминаем нечто, что цель должна начать гуглить (применяем сценарий find trap, заранее заготовив сайт, а на нем — вредоносный файл). Если жертва пытается разводить демагогию, приводим довод, что он даже Google не умеет пользоваться.

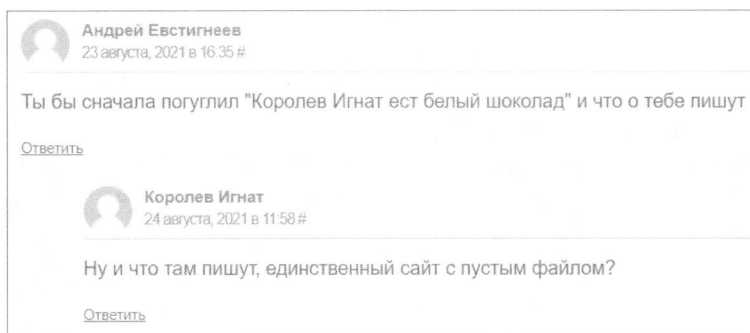


Рис. 1.69. Пример предоставления нужного нам запроса в комментариях и ответа «попавшегося» человека

Легализованная СИ

Легализованная социальная инженерия остается вредоносной, просто она случайно или целенаправленно обеляется в глазах жертвы (полностью или частично).

Пример случайного обеления: начальник попался на нашу уловку и отдает приказ сотрудникам совершить вредоносное действие (рис. 1.70).

Такое вот письмо мы рассылали при проверке осведомленности одной из организаций.

Один из руководителей переслал этот запрос подчиненным, чем легализовал его и расширил площадь атаки еще на 15 сотрудников, которых не было в списке рассылки. Все до единого сотрудники, получив указание от руководителя, ввели свои учетки на фишинговом портале.

Можно сказать, что случайно легализованная СИ пентестеров интересует меньше, т. к. мы не контролируем этот процесс. Поэтому давай рассмотрим пример, когда легализации можно поспособствовать.

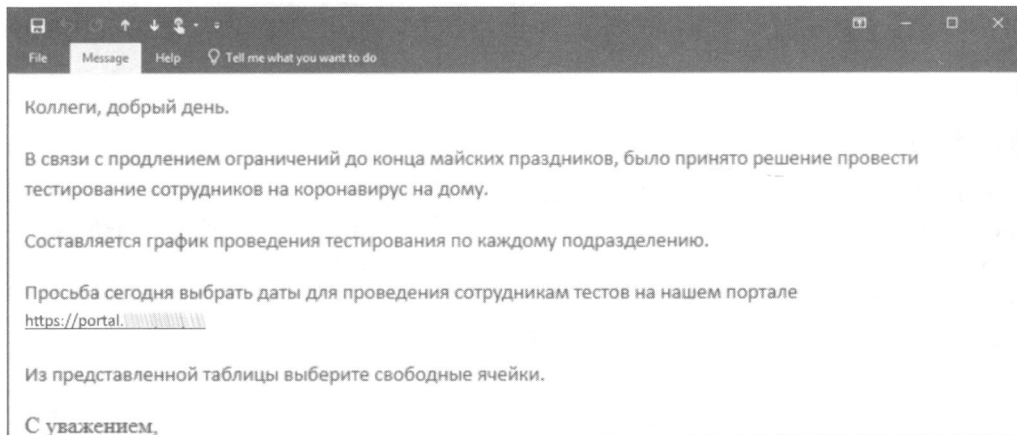


Рис. 1.70. Письмо, которое начальник переслал подчиненным с приказом заполнить

Отправили к вам

Вот такое письмо мы рассылали по некоторым сотрудникам одного из хостингов:

Анастасия, здравствуйте.

Тех. поддержка сказала, что вы можете помочь, хотя я не понимаю, почему отправили к вам.

Проблема с сервером. Панель не отображается (*URL*)

Похоже, нужно докупить мощности.

Что делать?

С уважением, Борис Стороненко

В этом случае идет обеление, поскольку мы упоминаем службу поддержки — якобы с ней уже пообщались и поэтому пришли к пользователю.

Еще один пример, когда мы ссылались на кого-то другого в организации:

(Имя), добрый день.

Если Вы утверждаете, то мы готовы начать работу.

Документы по проекту во вложении.

С уважением, Зуева Анастасия

ЗАО «ПроЗероЗис»

Копия пересылаемого сообщения:

From: Зуева Анастасия <zueva.anastasiya@{phishdomain}.ru> **Sent:** Tuesday, December, 2020 11:07 AM **Subject:** Утверждение последовательности

Здравствуйе.

Пусть (*Фамилия и Имя*) утвердит.

Борисов А. И.

Заместитель руководителя

АО «(Компания жертвы)»

Здесь мы упоминали руководство в фейковой переписке для придания веса письму.

ФИШИНГ

Фишинг (от *англ.* fishing — рыбная ловля, выуживание) в информационной безопасности — это процесс выманивания конфиденциальной информации у человека. Чтобы не путаться с определением фишинга и разными его видами, отталкиваемся от изначального его предназначения: ловля, как в рыбалке.

Сам удивился, когда обнаружил, что этот раздел — один из самых маленьких. В книге про СИ раздел с фишингом маленький! Что?! 0_o

Дело в том, что все аспекты фишинга разбросаны по разным разделам книги. Что написать в письме, как замаскировать ссылку, какой домен выбрать, какую форму сделать, с помощью чего рассылать фишинговые ссылки и т. д. Всё это есть в книге.

Но если ты открыл книгу именно с этой страницы, давай-таки рассмотрим еще один любопытный пример.

Проверка на утечку

Отправляем пользователю ссылку на сайт по проверке пароля на утечку. Что-то вроде <https://haveibeenpwned.com>, только с оформлением под организацию пользователя, и вписывать в поле нужно не email, а пароль. А логин ты и так знаешь (если логином является корпоративная почта получателя).

В письме пишем:

Участились попытки взлома организации, и был создан корпоративный сервис для проверки на утечки.

Прямо сейчас нужно проверить, не попал ли ваш пароль в руки злоумышленников.

В случае, если результат проверки покажет наличие утечки, требуется сообщить об этом, тогда никаких санкций к работнику применяться не будет.

Сайт соответственно будет выдавать, что всё нормально, а ты будешь получать введенные пароли.

Data-phishing

Фишинг данных — этим термином мы назвали выманивание не логинов и паролей, как в классическом фишинге, а информации, которая может помочь хакеру раскрутить атаку дальше или сразу же навредить организации.

Выманивать могут критические данные и косвенные:

- критические — это такие, которые могут нанести непосредственный вред организации, финансовый или репутационный;
- косвенные — это данные, которые пригодятся злоумышленнику для раскручивания атаки дальше.

От OSINT (поиск информации по открытым источникам) data-phishing отличается тем, что полученные данные не содержатся в открытом доступе, и добывают их непосредственно при общении с людьми.

Рассмотрим примеры.

- ❑ **Критические** — база клиентов с персональными данными, документы с коммерческой или государственной тайной.

Например, раскрытие базы клиентов может привести к потере репутации организации или привлечению внимания, которого организация не хотела. Конечно, в странах СНГ пока еще не очень страшно для организации, когда из банка или интернет-магазина «утекает» такая база. Но в развитых иностранных государствах на организацию за такую утечку накладывают штраф, происходит отток клиентов, падают акции компании, увольняют ответственных лиц и т. д.

- ❑ **Косвенные** — печать организации, полная или часть базы контактов сотрудников, часть структуры компании.

Далее идет раскручивание атаки. Например, печать компании может использоваться для заверения фиктивных документов, которые потом отправляются другим сотрудникам или подрядчикам для усиления обмана.

Полученная база контактов сотрудников используется для распространения атаки на всю организацию или на конкретных работников, данных о которых нет в открытых источниках.

А получив некоторое представление о структуре организации: кто кому подчиняется или каким образом взаимодействует — можно персонализировать атаку.

Еще один пример дата-фишинга. После рассылки любого письма по списку email из открытых источников может прийти автоответчик, в котором сотрудник указывает, до какого числа он в отпуске (часто указывает и контакты коллег вместе с Ф.И.О.).

Теперь злоумышленник может представиться отпускником и обратиться к коллеге с легендой, что он не имеет доступа к рабочему ПК:

Вот этот документ во вложении очень важно распечатать и отдать начальнику.

Такая персонализация атаки имеет большой шанс на успех. Мы проверяли — это работает :-)

Кроме того, вступив с сотрудником в переписку, можно узнать следующие данные: версию используемого ПО, наличие антивируса на ПК, email и телефоны других сотрудников, номер мобильного телефона самого сотрудника или коллег, способ официального оформления письма и подписи в нем.

Многоходовки

Один из любимых векторов в электронной СИ: если сначала переписываться с человеком, а потом давать вредонос, вероятность срабатывания атаки выше.

Это достигается благодаря двум составляющим:

- жертва больше приучена подозрительно относиться к первому, а не к последующим письмам;
- системы защиты в организации легче обходятся, если в первоначальном сообщении нет ссылок и файлов.

Чаще всего достаточно написать 2–3 письма — и вероятность открытия файла (ссылки) удваивается.

Например:

Здравствуйте. Жду ответа уже больше недели. Мое письмо вообще пришло к вам?

Нам отвечают, что нет.

Следующее письмо пишем уже с нагрузкой:

Наверное, что-то с почтой произошло. Я по поручению руководителя назначен ответственным за согласование регламента взаимодействия между нашими организациями. Просьба сегодня посмотреть проект регламента (*прикрепил*) и дать комментарии.

Еще несколько вариантов первых писем для двухходовок:

Здравствуйте. Эта почта еще работает?

Здравствуйте. Вы еще работаете в ОАО «...»?

Здравствуйте. Я правильно понимаю, что вы отвечаете за бухгалтерию в АО «...»?

Для проработки топ-менеджмента можно начать с приглашения поучаствовать в конференции, напечататься в СМИ, через фейковую секретаршу руководителя крупной компании выйти на секретаршу жертвы и начать «организовывать встречу и переговоры» с целью data-phishing или завладения ИТ-ресурсами секретаря (а там много чего есть про топ-менеджера ;-)).

До полноценной переписки с долгими диалогами о жизни или обсуждением политической повестки доходило редко. Просто в рамках тестирования сотрудников у нас такой задачи не стояло — сотрудники уже попадались и на коротких вариантах переписок, чаще с двумя письмами с нашей стороны.

Но где бы вы ни переписывались (email, соцсети, мессенджеры и т. д.), помните правило многоходовки: сначала общение, потом нагрузка.

Автоматизируя многоходовки, можно создать цепочки писем и в зависимости от открытия письма (или неоткрытия) и от шаблонных ответов пользователей отправлять то или иное следующее сообщение хоть с помощью сервиса Getresponse, даже без подключения нейронки, как это будет реализовано в нашем софте :-).

Фейковое интервью

Как в атаках, произошедших в 2020 году, ты можешь имитировать сообщения якобы от журналистов с просьбой прокомментировать какую-либо ситуацию.



Приведу выдержку из статьи РБК:

«Хакеры написали поддельное письмо, отправленное якобы с корпоративной почты РБК, которое также содержало логотип компании. В нем одному из сотрудников калининградского банка злоумышленники представились журналистом издания и предложили получателю пройти интервью в рамках «всероссийского исследования банковского и финансового сектора во время пандемии коронавируса».

Злоумышленник сообщает, что добавил его в Calendly (открытый планировочный сервис. — РБК), на самом же деле для проведения атаки хакеры создали аналогичный календарь, в котором и назначали встречу жертве. После предложения об интервью злоумышленники написали повторное письмо жертве: в нем журналист сообщает, что написал вопросы для интервью, выгрузил их в облако и ждет ответов на них. Повторное письмо хакеры направляют, чтобы удостовериться, что получатель на крючке: он заинтересован, прочитал письмо и перешел по ссылке. Для большей убедительности в каждом письме фигурирует имя известного вендора в сфере кибербезопасности, которым якобы проверено письмо. Так злоумышленник окончательно усыпляет внимание атакуемого».

Интервью обычно берут не у рядовых сотрудников, а у руководителей разного уровня, поэтому используйте сценарий соответственно.

Отложенная отправка

Недавно в патенте Cofense я обнаружил интересную последовательность атаки: <https://patents.google.com/patent/US8615807B1/en>.



Сначала жертве отправляется одно сообщение, потом второе с вредоносом, по смыслу они связаны.

Например:

«Коллега сказал, что файл можно отправить вам, но, к сожалению, я сейчас не у ПК. Чуть позже отправлю».

Второе письмо будет содержать файл, а в сообщении текст:

«Как и обещал, отправляю файл».

Или другой вариант:

«Коллеги, проводятся плановые технические работы. ИТ-системы могут работать со сбоями. Мы сообщим о завершении работ».

Через 2 часа:

«Коллеги. Технические работы завершены. Активные сессии на корпоративном портале были сброшены. Просьба перезайти в свои кабинеты в течение часа [URL] и удостовериться, что всё работает».

То есть жертву сначала «прогревают», никакой вредоносной нагрузки не предлагается. А на втором письме у нее в голове должна возникнуть мысль: «А-а, как раз про это мне и писали до этого».

Цепочки писем

Мы будем поступать по аналогии с тем, как маркетологи «маринуют» потенциальных покупателей разными сообщениями по email, а потом что-то продают.

Метод похож на многоходовки, с тем лишь различием, что тут мы втираемся в доверие без общения, отправляя сообщения в один конец.

Цепочки писем: неправильная кодировка как повод

Сценарий, когда сотрудникам рассылается письмо с иероглифами и абракадаброй, а потом — уведомление от сотрудника ИБ:

В течение получаса не открывайте писем, особенно с иероглифами, нас атаковали. Алексеич злой, Алла открыла письмо, через час вся бухгалтерия полетела. Мы уведомим об отражении атаки.

Потом отправляем:

Всё нормально, атака отражена. Просьба в течение 5–10 минут сменить аутентификационные данные по ссылке.

Цепочки писем: простите, не туда

Отправляем первое письмо, якобы с интересной информацией:

Ольга Борисовна, добрый день. Прикладываю квартальный расчет премий ОАО «Ро-машка».

И через минуту отправляем еще одно:

Простите, не туда отправила (*случала адресата | перепутала email*).

Как ты понимаешь, ситуация похожа на часто встречающуюся в повседневной работе, но редко используется для отправки «нагрузки», поэтому не надо ею пренебрегать :-)

Цепочки писем: нас взломали

Сначала пишем от имени несуществующего сотрудника службы ИБ или ТП:

Организацию взломали, мы разбираемся, никому пока не рассказывайте (не надо привлекать к себе негативное внимание), я чуть позже вам напишусь.

Вторым письмом через 20–30 минут пишем:

Так, похоже, разобрались, пытались украсть конфиденциалку, в том числе с вашего ПК (*или что-то еще*). Сейчас в первую очередь вам нужно сменить пароль от учетной записи. Перейдите по ссылке и смените пароль.

Цепочки писем: использование для data-фишинга

Цепочка писем может быть направлена и для сбора дополнительной информации — например, дополнительных контактов сотрудников.

Продолжая предыдущий сценарий, дописываем во второе письмо:

Сегодня уже пятница, напишите, по какому мессенджеру можно связаться с вами в выходные, т. к. дело критичное, и мы будем работать на выходных и оповестим вас о результатах.

Опасность для организации в этом случае заключается в том, что в выходные сотруднику сложнее оповестить службу ИБ, или мозг уже не работает так, как в защищенном периметре. Соответственно по другому каналу связи с сотрудником можно общаться и отправлять нагрузку.

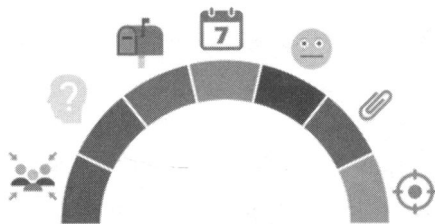
Фейковые посетители

Маркетолог компании может увидеть в системе аналитики всплеск переходов с какого-то сайта на ресурс, который ему подконтролен (корпоративный, YouTube-канал и т. п.). Перейдя на сайт, который дает удивительно много переходов, он попадает на твой фишинговый ресурс.

Всё дело в том, что можно искусственно создать всплеск таких переходов на сайт или ресурс жертвы, что должно заинтересовать хорошего маркетолога. Посетителей на сайт с определенного ресурса можно накрутить с помощью инструмента Beef (beefproject.com).

Предварительно проверь в исходном коде сайта, какая система аналитики там стоит, под нее ты и создашь фишинговую форму. Ну а YouTube-канал можно не проверять, он и так ведет статистику переходов.

Глава 2



Технологические трюки введения в заблуждение

https://t.me/it_boooks/2

В этой главе мы рассмотрим, как можно «обманывать» пользователя с помощью различных технических приемов.

Маскировка ссылок

Мы смогли собрать в одном месте около 20 способов маскировки ссылок: с символом @, слеш в юникоде, домены в юникоде, зашумление юникодом, обфускация, QR-коды, некорректный протокол, в виде картинок, в документах, очень длинные, в виде цифр, невидимые при наведении мыши, редиректы, неактивные, похожие на официальные, в поддоменах, сращивание поддомена, домен после слеша.

Если ты знаешь еще какие-то, буду и я рад узнать о них и в будущем дополнить книгу. И вообще, любые коррекции и дополнения к книге приветствуются. Пусть это будет настоящий справочник по социотехническому тестированию.

Итак, вернемся к способам маскировки ссылок.

Символ @

Для тех, кто привык смотреть, что идет сразу после **https://**, и думать, что URL безопасен, ссылка: **https://bank.ru@zloysite.ru** — не приведет ни к чему хорошему.

Почему так происходит? Допустимые в URL символы описаны в стандарте RFC 1738. Символ @ используется в URL как спецразделитель, когда нужно прямо в URL дать права для доступа к странице. В конструкции вида **http://<логин>:<пароль>@<хост>** до @ можно указывать практически что угодно — браузер все равно отправит пользователя на хост, указанный после @.

Ну а такой вариант: **https://@ya.ru** — подойдет для проверки антифишингового ПО.

Слеш в Unicode

Используется чаще всего с символом @, другое применение отдается на откуп твоей фантазии. Пример:

<https://www.facebook.com?aqweqwewwqdeq:wdeqwedqdwqwed@ya.ru>.

До «собаки» можно использовать символ U+0B75 (/ — дробь одна шестнадцатая языка ория), и человек подумает, что это легитимная ссылка, если он привык считать доменом то, что идет до первого слеша. Кстати, так удавалось обмануть не только человека, но и защитное ПО.

Домены в Punycode

Если сделать ссылку в письме неактивной (некликабельной), можно побудить получателя скопировать адрес вида **<https://кто.рф/company.ru>** и вставить в браузер. А из-за того, что кириллические домены можно представить в виде Punycode, мы получаем еще один способ маскировки ссылок — например, такой:

<https://xn--j1ail.xn--plai/company.ru>.

Зашумление юникодом

Отличие от предыдущего способа заключается в том, что там ты регистрировал домен с unicode-символами, а тут ты просто добавляешь их в любую часть домена.

Ты можешь отправить такую ссылку: **<https://prom^o.ru>**, и браузер решит, что это «о» в конце, и перейдет на **<https://promo.ru>**. Так же работают символы ¹, ² и буквы — напишу их в Unicode: U+2102, U+210D, U+212F, U+211D и другие. Тестировалось и работало в Google Chrome версия 116.

Также для обхода систем фильтрации ссылок тебе может пригодиться сервис Domain Obfuscator (**<https://splitline.github.io/domain-obfuscator>**). Он преобразует символы домена в нечитательный набор букв.

Обфускация ссылок

Делая ссылку в письме неактивной, мы также получаем еще один способ маскировки ссылок с помощью обфускации:

❑ **<https://0xd9.0x45.0x8b.0xca/company.ru>**;

❑ **<https://0331.0105.0213.0312/company.ru>**;

❑ **<https://3645213642/company.ru>**.

Еще пару примеров можно посмотреть на «Хабре»:

<https://habr.com/ru/post/69587>

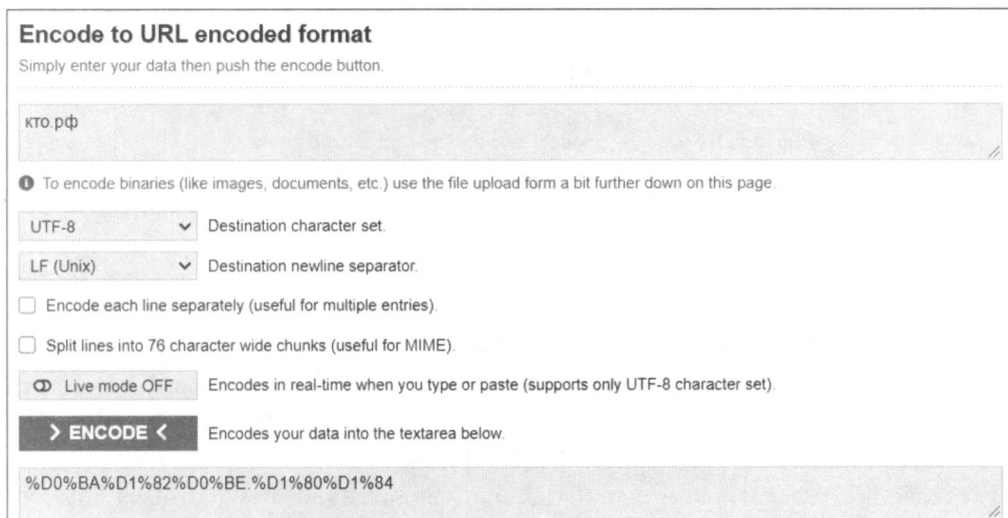
и тут: **<https://bo0om.ru/domain-and-ip-checker-bypass>**.



В приведенных примерах мы маскировали IP-адрес, а вот так можно представить сайт **кто.рф** с помощью Urlencode:

http://%D0%BA%D1%82%D0%BE.%D1%80%D1%84.

Сделать это ты сможешь с помощью сервиса **urlencoder.org** (рис. 2.1) или подобных.



The screenshot shows the 'Encode to URL encoded format' interface. At the top, it says 'Simply enter your data then push the encode button.' Below this is a text input field containing 'кто.рф'. A note below the input field states: 'To encode binaries (like images, documents, etc.) use the file upload form a bit further down on this page.' There are two dropdown menus: 'Destination character set' set to 'UTF-8' and 'Destination newline separator' set to 'LF (Unix)'. There are three checkboxes: 'Encode each line separately (useful for multiple entries)', 'Split lines into 76 character wide chunks (useful for MIME)', and 'Live mode OFF' (which is checked). Below these is a large button labeled '> ENCODE <' with the text 'Encodes your data into the textarea below.' At the bottom, a text area displays the encoded result: '%D0%BA%D1%82%D0%BE.%D1%80%D1%84'.

Рис. 2.1. Интерфейс сервиса urlencoder.org и результат обфускации ссылки

QR-коды

QR-коды используются как для онлайн, так и для офлайн-атак.

Например, можно прислать QR-код в письме:

Коллеги, в связи с обновлением ассортимента продукция будет распродана среди сотрудников с 95%-ной скидкой. На нашем портале в специальном разделе есть список оставшейся продукции.

Отсканируйте QR-код с помощью смартфона:



То, что Вы решите выкупить, пометьте в таблице знаком «+».

Это мероприятие действует до конца недели.

Также QR-коды можно наклеивать в общественных местах или офисных пространствах поверх легитимных кодов (рис. 2.2).



Рис. 2.2. Пример «корпоративного» QR-кода возле точки Wi-Fi

Некорректный протокол

Способ больше подойдет для обхода некоторых систем анализа ссылок и лишь отчасти запутает человека, но о нем стоит упомянуть, т. к. для обмана пользователей могут применяться комбинации разных способов.

Ссылку вида **https:\ya.ru**, **http:///ya.ru**, **https:\\ya.ru** может пропустить анти-спам, но есть вероятность, что человек ее скопирует и вставит в браузер. При этом **https:\\ya.ru** превращается в **https://ya.ru/**.

Ну и раз уж мы заговорили про обход спам-фильтров и «неуместные» символы в URL, не будем обходить и так называемый *корневой домен*. Почитать о нем можно в Википедии, а сейчас нам достаточно лишь знать, что **https://ya.ru/news/** — это то же самое, что и **https://ya.ru/news/**.

Ссылки в виде картинок

В этом случае не просто отправляется ссылка, а все сообщение является картинкой-ссылкой (рис. 2.3). Вариант подойдет для обхода некоторых правил систем защиты, анализирующих текст сообщения.

Ссылка в документах

В *разд. «Файлы» главы 1* мы уже разобрались, что нагрузку можно встраивать в файлы и предлагать пользователю с нею повзаимодействовать.

Просто для порядка нужно упомянуть это и здесь, отдельно выделив этот способ, — чтобы все способы маскировки ссылок были в одном месте.

Во вложении в письме пишем убедительный текст, объясняющий, почему нужно нажать на ссылку. Так мы обходим некоторые фильтры и не используем самый распространенный шаблон фишеров — размещать ссылку в теле письма.

Текст письма может быть примерно таким:

Добрый день. Инструкция по установке программного обеспечения для удаленной работы во вложении.

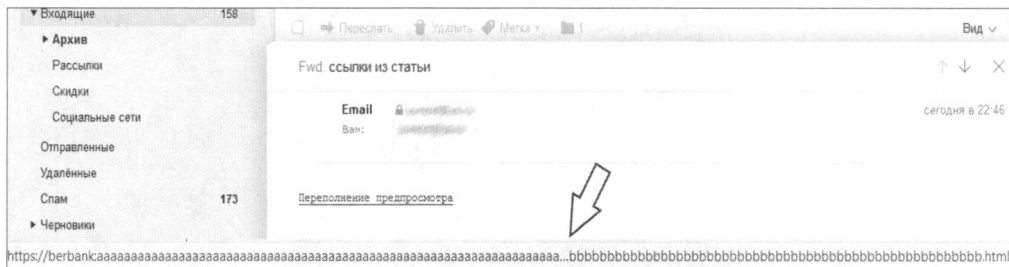


Рис. 2.4. Отображение ссылки в браузере со скрытым конечным URL

Ничто не мешает тебе использовать длинные ссылки, даже не рассчитывая на то, что целевой адрес не виден при наведении мыши.

В длинных ссылках сложно увидеть, куда она ведет:

`https://facebook.coml.ppu-utm-sourcefacebook.information-security.site/utm_medium_campaiggostIwAR1CoVv7auXaheOmv7JsvaCBKwZTyJW=wdhp4PR8THuzZJLzpWDAPi8T=cwh=AT2L2tbBiGEdbMR5ZyCwd98EXfS6bK/46hrlqhWYT=12&_tn_mH=R&c%5b0%5d=ATQm4PN3tEu9tVf9h_DsH1hWwU2Kog_/Ya31zLfiXvfEfJu6s2cKcWC6q05g7O&_coconnected?r=facebook.com/fsgD90MI PmVpyfTL5s4bzKqZ1QXyQfeJEAjVU3knH0bjU=UA2EzVbjcqY8S9mpDtnwMb6U0V=NYdcinCQO/ZMWssOkL7nTw/tQLeZqLl40Pkm50iOkEhUqpn9MDwlt1Sh6L36X19TbjbjV0QB4UdnT19HwkafI3=02qRVIb9zrOdScb4pMS1Ga`

Ссылка виде цифр

Здесь ссылка ведет на IP-адрес подконтрольного тебе сервера, а обычный пользователь не поймет, куда на самом деле она ведет (рис. 2.5).

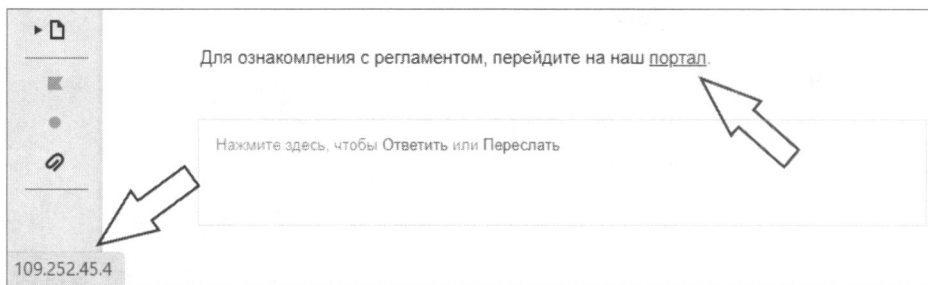


Рис. 2.5. Отображение ссылки в виде IP-адреса

Невидимая при наведении мыши

Как в примере, рассмотренном ранее, когда при наведении мыши мы видим один сайт, а при клике попадаем на другой, тут мы также можем использовать этот код:

```
<a onclick="window.location.href='http://stopphish.ru';return false" href="http:// " >Ссылка</a>
```

Просто теперь вместо URL пишем пробел. Тогда при наведении мыши в браузере ничего не появится, и пользователь не поймет, куда попадет.

По email, конечно, такую ссылку не отправишь, но для вложенных HTML-файлов или на фишинговых сайтах может пригодиться.

Редиректы

Редиректы могут как создаваться с помощью «сокращателей» ссылок типа **bit.ly**, так и с использованием несовершенства систем управления сайтами (SMS), у которых имеется открытый редирект.

Например, вот такая переадресация когда-то работала в одном из банков:

<http://www.moscow-bank.ru/bitrix/redirect.php?goto=http://ne-moscow-bank.ru>

Мы также делали небольшое исследование по Open Redirect на сайтах банков (рис. 2.6).

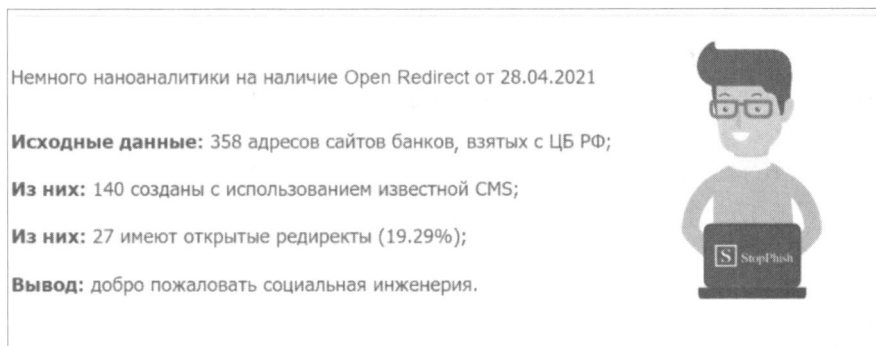


Рис. 2.6. Результаты мини-исследования по открытым редиректам на сайтах банков РФ

Однажды нам пришло письмо от DigitalOcean (у нас там был один из серверов). Это была якобы абюза со ссылкой:

<https://digitalocean.abusehq.net/share/ESPbSCieMIh5kWZw-F>.

«Якобы» — потому, что нам было лень вчитываться, т. к. по виду ссылки становилось понятно, что это спам.

Домен **abusehq.net** редиректил на **abusix.com** — с виду приличную компанию по борьбе с пиратством.

Реальную или вымышленную абюзу мы получили — непринципиально, но это можно использовать в пентестерских целях.

Ссылка может быть фишинговой, а домен — нет. Например, ссылка:

<https://digitalocean.abusehq.net/share/ESPbSCieMIh5kWZw-F>

будет вести на фишинг, а если пользователь начнет «копать» и станет пробивать **digitalocean.abusehq.net** или **abusehq.net**, то попадет на легитимный сайт компании, что вызывает больше доверия. Так и ты — по ссылке делаешь фишинг, а на домен вешаешь вымышленный «легитимный» сайт или редиректишь на авторитетную компанию.

О других методах сокрытия злоумышленниками контента от службы ИБ я писал в статье «Искусство маскировки. Как мошенники прячут свои сайты в Интернете» (<https://xakep.ru/2021/09/09/phishing-domains/>). А ты можешь использовать это в своих благих пентестерских целях.



Неактивные ссылки

В книге уже несколько раз приводились примеры ссылок, которые не работают при клике (написанные в виде текста, без анкера). Так что в этом разделе не станем повторяться и просто отнесем такой вид маскировки ссылок к лайфхакам.

Если тебе требуется замаскировать ссылку, и чтобы при наведении курсором мыши у пользователя ничего не отображалось, нужно побудить его в письме скопировать ссылку и вставить в браузер. Ведь если ты напишешь ссылку:

`https://xn--j1ail.xn--p1ai`

и сделаешь ее активной, то жертва увидит, куда на самом деле она ведет (рис. 2.7).

Поэтому просто пишем ссылку текстом (рис. 2.8).

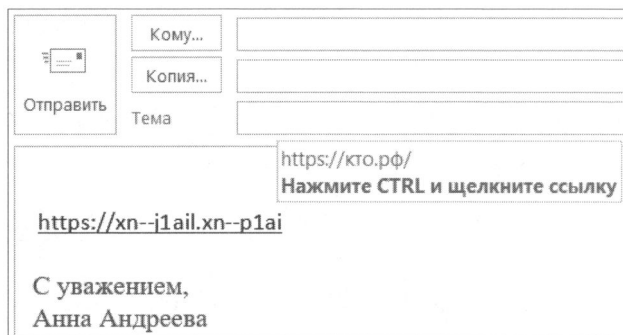


Рис. 2.7. Отображение домена в рипусcode при наведении указателя мыши

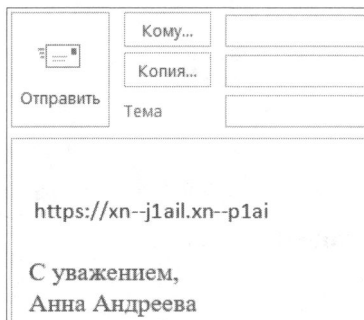


Рис. 2.8. Неактивная ссылка

Еще один способ — это имитация слеша буквой. Пример: bank.ru/action.com — буква I(i) или l(L) делается курсивом, и тогда она выглядит как косая черта. Этот вариант подойдет для писем с HTML-разметкой, иначе нельзя будет указать стиль буквы под наклоном. Стиль шрифта в письме используй без засечек, тогда фейковый слеш будет выглядеть как настоящий.

В случае, если почтовый клиент автоматически превращает такую ссылку в активную, попробуй писать без протокола: **stopphish.ru/forma**.

Или использовать редкие доменные зоны: **stopphish.online/forma.ru**.

Похожие на официальные

В этом случае используются тайпсквоттинг и битсквоттинг. Возможно, ты, как и я, редко пользуешься словарем терминов, приведенным в конце книги (см. *приложение б*), поэтому приведу определения с примерами оттуда:

Тайпсквоттинг (от *англ.* typosquatting, где typo — опечатка + cybersquatting — регистрация доменных имен, содержащих торговую марку, принадлежащую другому лицу) — регистрация доменных имен, близких по написанию к адресам популярных сайтов в расчете на ошибку части пользователей. Пример: вместо оригинального **yandex.com** регистрируем **yandeks.com**.

Битсквоттинг — атака, в рамках которой регистрируется поддельный домен, отличающийся от оригинального одним битом. Например, домен **ya.ru** в двоичном коде выглядит так: 01111001 01100001 00101110 01110010 01110101. Если в сетевом оборудовании произойдет сбой и один из битов будет заменен другим, то в результате пользователь попадет на **ve.com**: 00111001 01100001 00101110 01110010 01110101.

Под цели социальной инженерии больше подойдет тайпсквоттинг, потому как битсквоттинг — это больше про технологии, а тайпсквоттинг относится к человеческому фактору.

Когда мы оказывали услуги по аудиту осведомленности пользователей в одной организации, то зарегистрировали домен, похожий на официальный, но с другой буквой в имени. То есть официальный домен был **company.com**, а зарегистрировали мы домен **kompany.com**.

В течение нескольких месяцев после аудита мы не заходили на этот почтовый сервер, а когда заглянули, оказалось, что более 10 организаций прислали нам письма с разными документами. Просто некоторые дочерние организации ошибались в названии домена управляющей организации и писали письма не туда, а к нам.

Так что регистрируй похожие домены своей организации (или заказчика) и жди улов — ведь можно не просто принимать такие письма, но и переписываться с отправителями, доверие к твоим письмам будет близко к 100%, поскольку жертва сама тебе написала.

Ссылки в поддоменах

Этот способ маскировки не только помогает обмануть человека, но и обходит некоторые технические способы защиты.

По практике: поддомены хорошо работают при проверке осведомленности, — попробуй что-то вроде:

company.com.zlo.online и **portal.company.com.1714documents-online-pdf.site**.

Сращивание с поддоменом

В нескольких организациях при тестировании мы использовали **www** как часть домена. Например, так: **wwwbank.ru** — и около 15–20% сотрудников переходили по таким ссылкам. А если в организации есть свой корпоративный портал, то можно использовать такой домен: **portalbank.ru**.

Сращивание с протоколом

В этом способе протокол является частью фишингового домена, но, конечно же, на самом деле мы получаем совершенно новый домен — например: **httpsbank.ru**.

Домен после слеша

Как оказалось, люди попадаются и на такое: **https://stopphish.ru/company.com**.

То есть, увидев на неофициальном домене официальный сайт в ссылке (лучше работает, когда адрес идет сразу после слеша), «головной файрвол» отключается.

Работает? Используем.

В дополнение

И еще пара примеров. Они больше относятся не к маскировке ссылок, а к маскировке содержимого страницы от отслеживающего софта.

Капча от ботов защитного ПО

Этот трюк также используется «фишерами», поэтому о нем стоит упомянуть хотя бы в какой-то главе книги.

Жертву отправляют на сайт, где ей предлагают разгадать капчу (рис. 2.9) и потом показывают содержимое сайта. Тем самым только человек (ну почти) может попасть на вредоносный сайт.

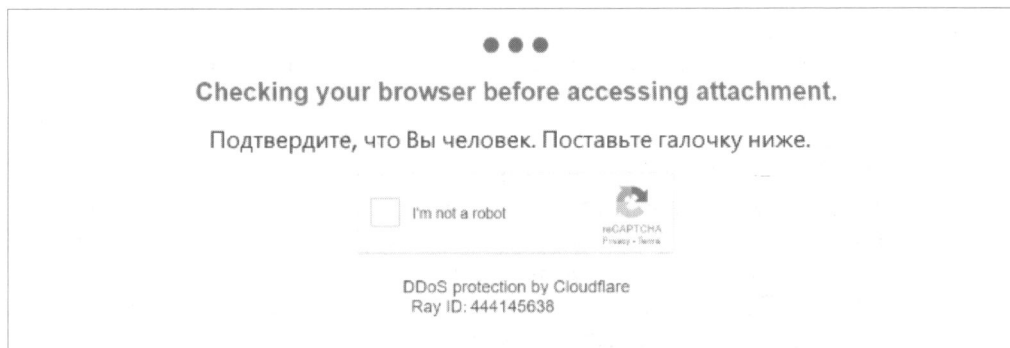


Рис. 2.9. Капча

Одноразовые ссылки

По аналогии с сервисом одноразовых записок <https://privnote.com> ты можешь отправить потенциальной жертве фишинговую ссылку. Если ее перешлют в службу ИБ и снова откроют, то ничего не увидят, что затруднит им расследование инцидента. Можно даже настроить редирект на официальный ресурс — тогда, не заметив переадресации, служба ИБ изучит легитимный ресурс и ослабится.

Учти, что сторонние сервисы и софт могут перейти по ссылке до того, как ее откроет пользователь, так что нужно настроить работоспособность временной ссылки на двукратное и более срабатывание.

Например, когда мы отправляли такие ссылки через соцсети или WhatsApp, по ним происходил автоматический переход сразу после отправки сообщения. А вот, например, когда отправляли ссылку по SMS, она доходила до получателя неактивированной (по крайней мере, до внедрения «Пакета Яровой» :-))

Подделка отправителя

Если в компании не используются SPF-записи, DKIM-подписи и DMARC, применяем классику жанра: подменяем email — и получатель видит в поле **От кого** официальный или знакомый email, а на самом деле отправитель — ты.

Такие компании нужно поискать, но, например, в некоторых госучреждениях до сих пор используется почта не на основе официального домена, а общедоступные **mail.ru** и **rambler.ru**, а это значит, что политика фильтрации почты у них не такая жесткая, как в корпоративных средствах защиты.

А если изучить статью по адресу: <https://habr.com/ru/company/cloud4y/blog/341096/>, то можно узнать, что если компания не использует DMARC, а только SPF и DKIM, то и у нее могут быть проблемы с фишингом.



Проблема в SPF заключается в том, что для проверки подлинности задействуется домен, указанный в поле **Return-Path**, а не в поле **From**, который люди действительно читают.

Хуже того, злоумышленники, занимающиеся фишингом, могут настроить SPF-запись для своих собственных доменов. После чего они смогут отправлять электронные письма, которые, как станет казаться, поступают от компании или бренда, которым доверяют, но домен этой компании будет отображаться в поле **От кого**, а домен мошенника — в **Return-Path**. Такие письма пройдут проверку подлинности SPF. Дополнительное использование DMARC решает эту проблему, позволяя владельцу домена требовать «выравнивания», означающего, что обратные и исходящие адреса должны быть одинаковыми.

Статья написана в 2017 г., но по итогам беглого анализа тех же сайтов банков РФ выяснилось, что далеко не все используют DMARC и в 2021 г.

Потестировать, проходит ли подделка отправителя по email, можно через онлайн-сервис <https://emkei.cz>. Отправляй какой-то вопрос и жди ответ или bounce :-)

Для более серьезных рассылок с подменой отправителя используй софт, упомянутый в *главе 4*.

Email с официального ресурса

Способ, редко применимый для атак на корпоративный сектор, но раз иногда можно, то для полноты картины упомянем.

Суть его в том, что ты используешь возможности легитимных сервисов отправлять уведомления, но только с твоим содержанием (рис. 2.10).

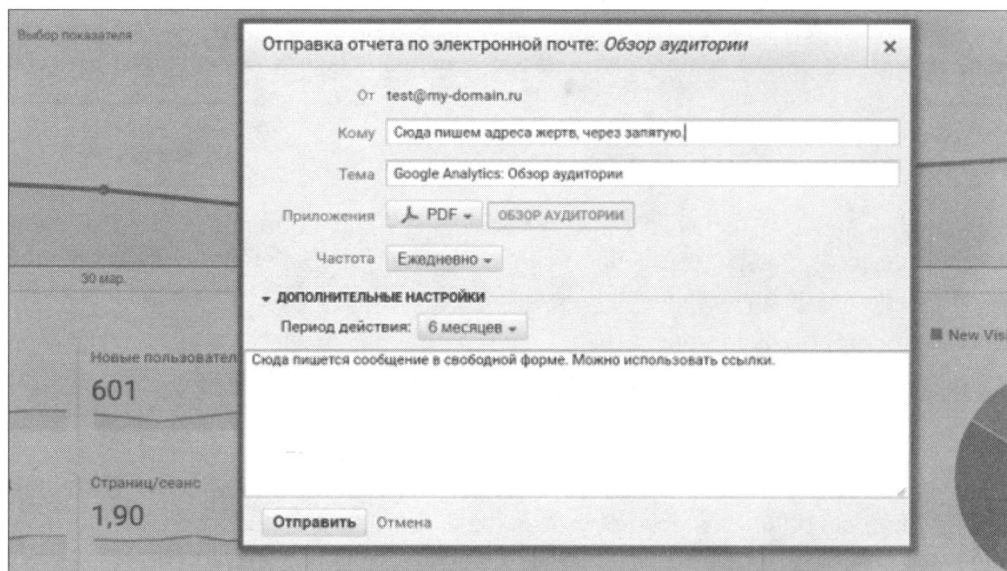


Рис. 2.10. Создание сообщения для рассылки в интерфейсе Google Analytics

Этот способ с Google Analytics я описывал в «Хакере»:

<https://haker.ru/2018/04/05/social-engineering-recipes/#toc01.1>



В «Яндексе» была похожая недоработка: при указании в <https://passport.yandex.ru/profile> дополнительного email можно было вместо **Имени** вставить в соответствующее поле свое сообщение. Жертве приходило письмо с уведомлением, но вместо имени она видела сообщение со ссылкой.

Вложения и файлы

В разд. «Файлы» главы 1 мы рассмотрели атаки с файлами с точки зрения классификации — как их доставляют и что в них пишут, чтобы пользователь попался. Здесь же мы коснемся некоторых технических аспектов, включая маскировку и лайфхаки.

Доставляемые по тем или иным каналам связи файлы можно разделить на:

- файлы Microsoft Office;
- HTML (HTM, SHTML);
- PDF;
- архивы (с паролем и без) с нагрузкой внутри.

Рассмотрим каждый из видов подробнее.

Файлы Microsoft Office

Чаще всего сотрудники обмениваются документами *.doc, *.xls, чуть реже *.ppt.

Самым распространенным вредоносным содержимым в таких документах являются макросы (рис. 2.11).

Когда мы тестировали сотрудников организаций на бдительность, нам достаточно было, чтобы отработал наш трекер при включении макросов. Так мы узнавали, что сотрудник попался на уловки и всё сделал «правильно».

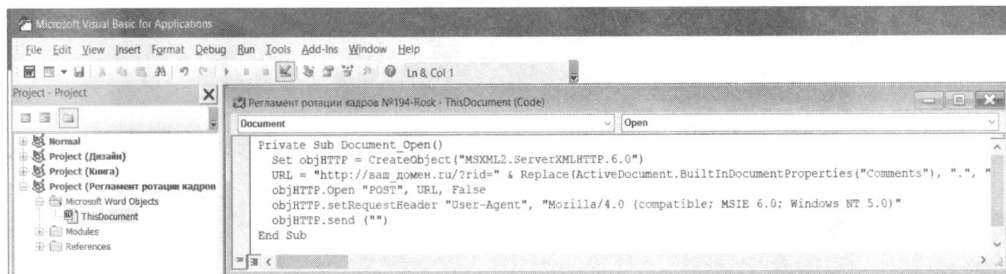


Рис. 2.11. Код макроса

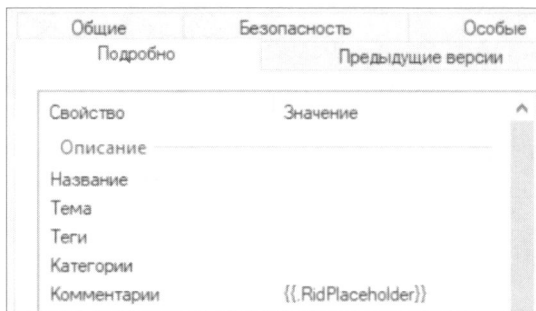


Рис. 2.12. Комментарий в свойствах файла, к которому обращается макрос при запуске

В свойствах файла указывался ID, и так мы узнавали, кто конкретно запустил макрос (рис. 2.12).

Твои же макросы могут запустить что-то другое :-)

Рушим шаблоны поведения через печать

При скачивании файла из Интернета или из вложения в email сотрудник увидит предупреждение (рис. 2.13).

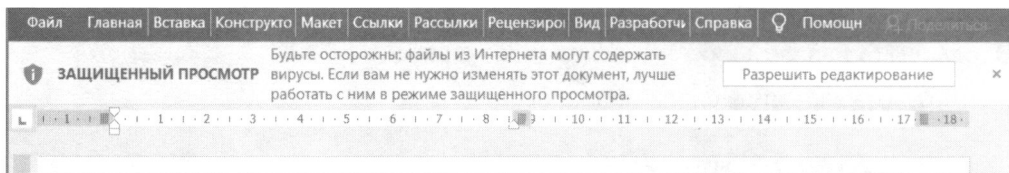


Рис. 2.13. Предупреждение о небезопасном содержимом файла

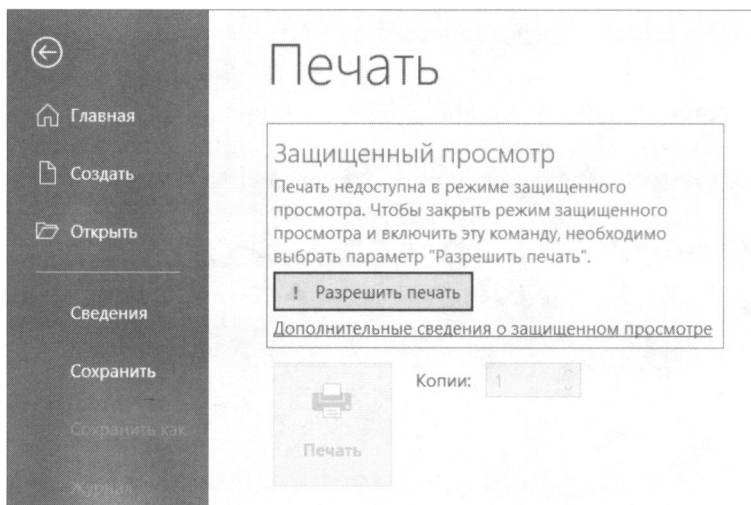


Рис. 2.14. Предупреждение о недоступности печати

Хочешь попросить его выключить защиту необычным способом?

Представься в письме начальником и, например, напиши, что приложенный документ (бланк, таблицу и т. п.) нужно распечатать и подписать, а сегодня в течение дня его заберет сотрудник отдела кадров.

Сотрудник открывает окно с печатью и видит предупреждение (рис. 2.14).

Сотрудник привык, что его просят отключить безопасный просмотр непосредственно в документе, но в этом случае его о таком не просят. Зато сам Word просит отключить защиту, ломая шаблоны осведомленного пользователя.

PDF-файлы

На рис. 2.15 показан пример вредоносной атаки от пользователя «Твиттера» (если что, не серчай на перевод от Google Translate).

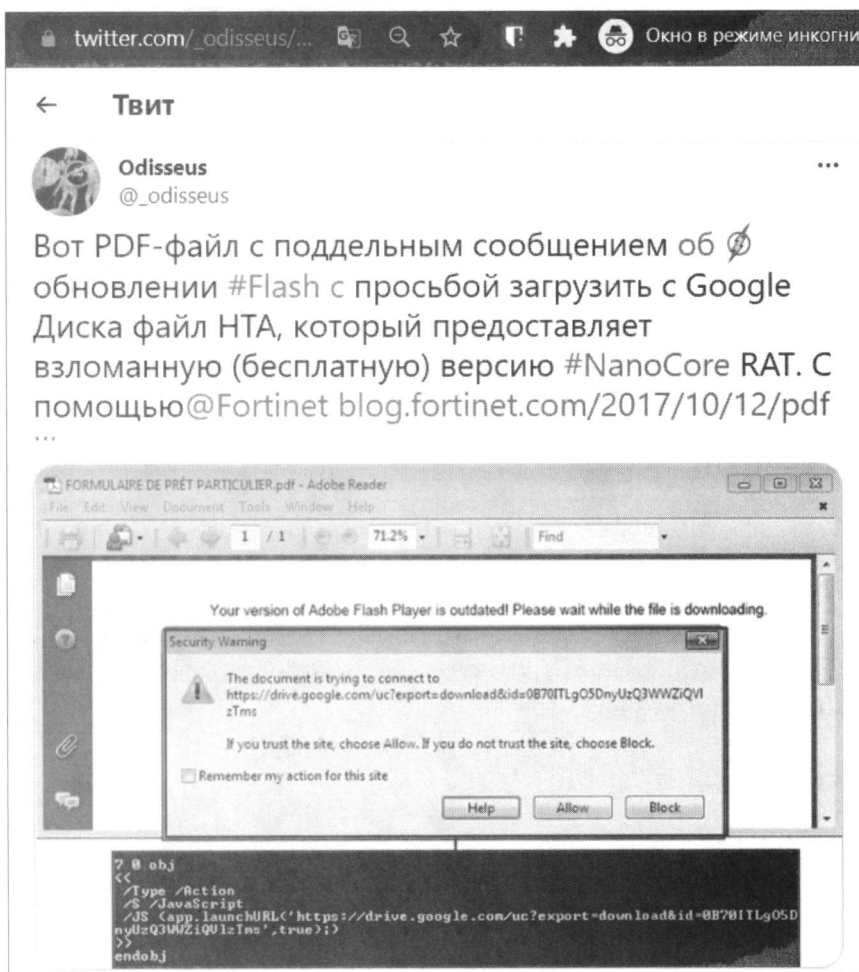


Рис. 2.15. Описание атаки через PDF-файл

Ну а тут ты можешь почитать о подробностях этой атаки:

<https://www.fortinet.com/blog/threat-research/pdf-phishing-leads-to-nanocore-rat-targets-french-nationals>. Быть может, тебе пригодится этот способ доставки нагрузки.



Когда мы делали свои первые социотехнические пентесты в 2017 году, то для трекинга разрешений таких вот загрузок пользовались <http://canarytokens.org> (рис. 2.16).

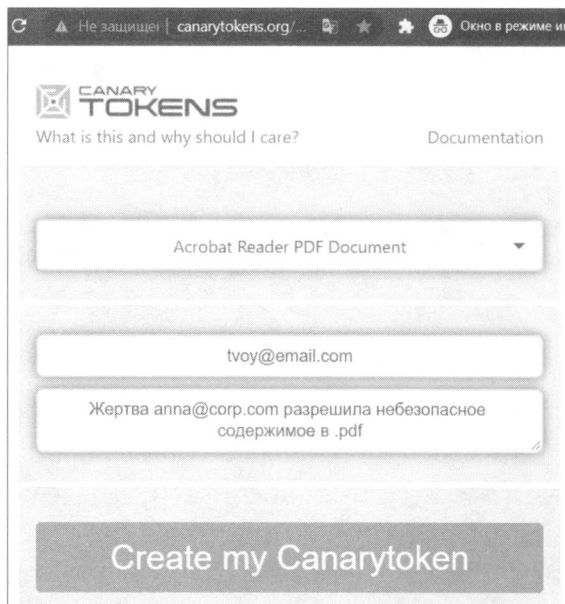


Рис. 2.16. Интерфейс сервиса Canarytokens

Нам и заказчику было достаточно того, что пользователь нажал **Allow** (Разрешить), и это уже считалось инцидентом и показателем того, что пользователь не осведомлен.

В бесплатной версии сервиса StopPhish ты можешь для проверок пользователей использовать этот вектор, что будет чуть легче, чем задействовать Canarytokens для одновременной проверки 100+ пользователей, поскольку тебе не придется готовить под каждого из них отдельный файл :-)

HTML-файлы

Во вложении HTML-файл бывает:

- с редиректом (на страницу злоумышленника в Интернете);
- содержащий вредоносный iframe (кадр внутри кадра), который подтягивает твою страницу из Сети;
- с фишинговым содержанием.

Вот пример фишинга в таком файле:

<https://nakedsecurity.sophos.com/2020/10/02/serious-security-phishing-without-links-when-phishers-bring-along-their-own-web-pages.>



Еще один пример приведен на рис. 2.17.

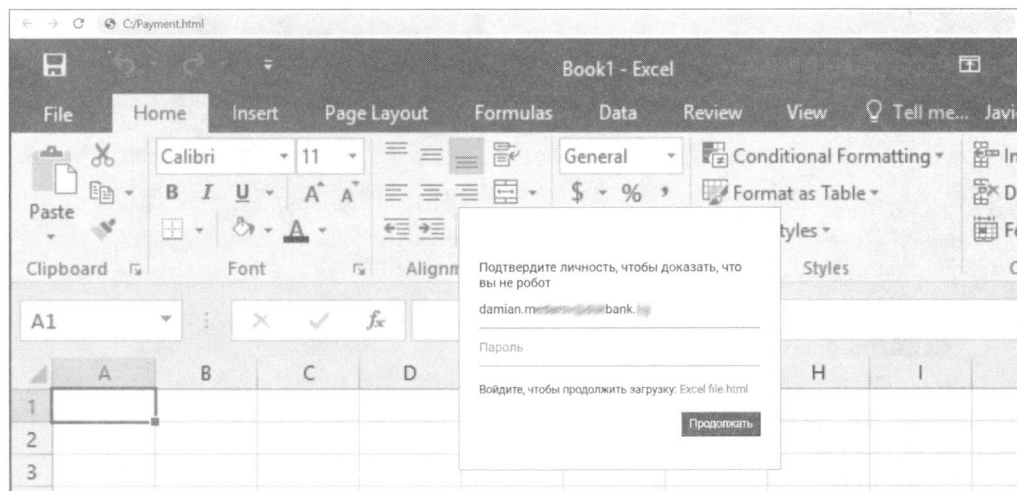


Рис. 2.17. Имитация Excel-файла на веб-странице

Маскировка расширения *html*

От пользователя HTML-вложение можно маскировать так: **WordDocument.docx.html** — или между **docx** и **html** вставить столько неразрывных пробелов (U+00A0), сколько возможно (рис. 2.18).

Да, значок получается не Word'овский, но многих это не интересует :-)

А можешь ничего не маскировать и отправлять как есть (рис. 2.19).



Рис. 2.18. Имитация документа Word в имени HTML-файла с неразрывными пробелами

Архивы с паролем

Для защиты от автоматического сканирования содержимого архива на него можно установить пароль (правда, теперь некоторые системы стали блокировать такие архивы, от греха подальше).

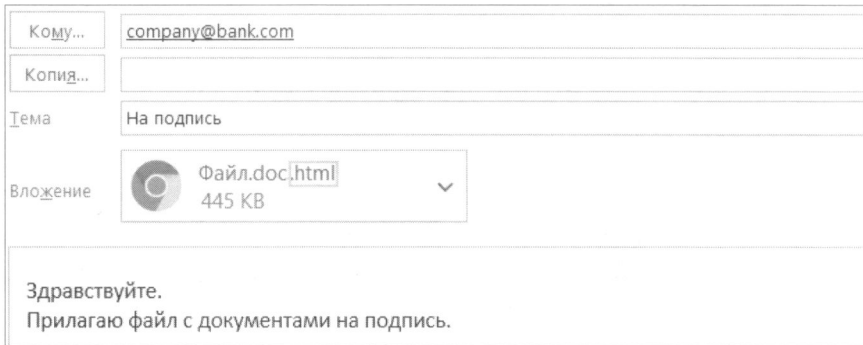


Рис. 2.19. Имитация документа Word в имени HTML-файла

Письмо с запароленным архивом выглядит примерно так:

Добрый день.
 Прикладываю архив с документами.
 В целях безопасности архив защищен паролем.
 Пароль от архива: 12345
 С уважением, Андрей Петров

Архивы без пароля

Вот так мы прятали настоящее расширение файла в архиве. Пользователи реально не понимали, что перед ними *.exe, а не *.pdf (рис. 2.20).

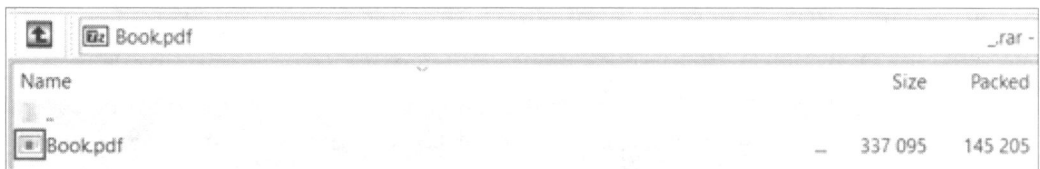


Рис. 2.20. Отображение EXE-файла в архиве, где в имени используется много пробелов

Как это делается? В файле Book.pdf.exe после pdf многократно вставлен «средний математический пробел» (рис. 2.21). Ох, сколько же времени было потрачено, чтобы найти именно этот пробел в Unicode :-)

Количество пробелов, которое удалось вставить в такое имя файла, примерно 280. Так что если у пользователя окно просмотра имени файла раздвинуто вправо (рис. 2.22), то он увидит .exe, но это используют немногие.

Если же вставить много обычных пробелов, то выглядеть это с точки зрения маскировки настоящего расширения файла будет не очень удачно (рис. 2.23).

Техническая информация	Свойства	Кодировка
Название в Юникоде	Medium Mathematical Space	
Номер в Юникоде	U+205F	
HTML-код	 	
CSS-код	\205F	
Разделы Юникода	Основная пунктуация	
Подразделы Юникода	Интервал	
Версия Юникода	3.2 (2002)	

Рис. 2.21. Описание среднего математического пробела

Name	Size
..	
Book.pdf .exe	0

Рис. 2.22. Расширенное отображение поля имени файла в архиве

Name	Size
..	
Book.pdfexe	0

Рис. 2.23. Отображение действительного расширения файла

Редко используемые форматы архивов

Отправляя архивы, используйте — помимо стандартных RAR и ZIP — разные их форматы, пробуйте обойти систему защиты (техническую и человеческую) с помощью форматов архивов CAB, ACE, Z.

Онлайн-документы

Такого рода ловушки чаще всего имитируют офисные документы *.xls, *.doc, *.pdf, но размещенные не во вложении, а онлайн на сайте.

Доступ к ним якобы ограничен и требует от жертвы какого-то взаимодействия — например, ввода данных, установки плагина.

Excel-файл, размещенный онлайн

В этом случае мы видим неперсонализированный вариант фишинга — т. е. жертва сначала вводит email, а в новом окошке пароль (рис. 2.24).

Чтобы больше людей ввело пароль (ведь это он тебе нужен, а почту ты и так уже знаешь), приводи контент страницы в связке с фишинговой ссылкой, которую отправлял. То есть не нужно спрашивать: «Введите email», сразу спрашивай пароль.

Шикарный пример из блога Checkpoint: сначала злоумышленники рассылали письмо (рис. 2.25), после чего пользователь открывал полученный файл (рис. 2.26). Персонализированная страница для сбора учетных данных: красота!

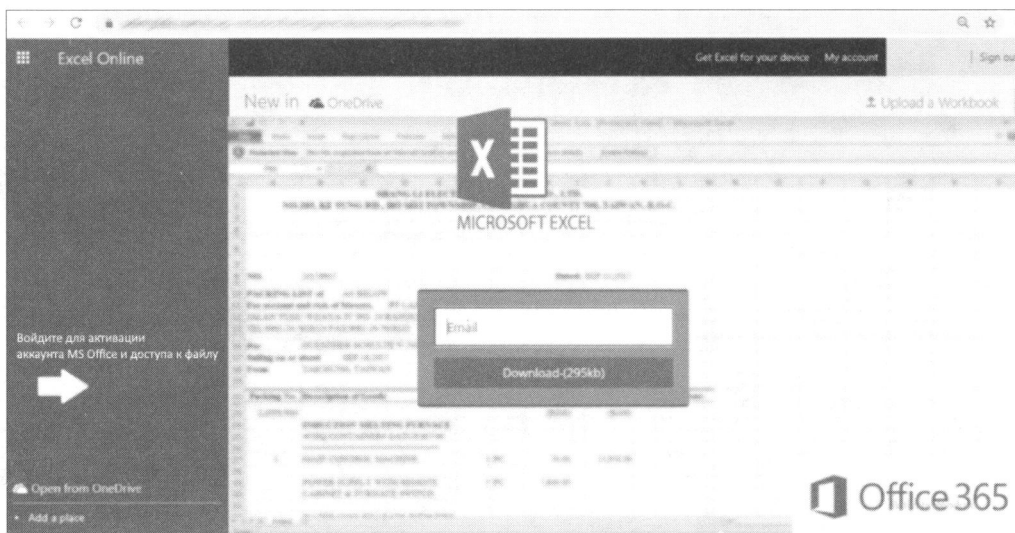


Рис. 2.24. Имитация Excel-файла с формой ввода данных

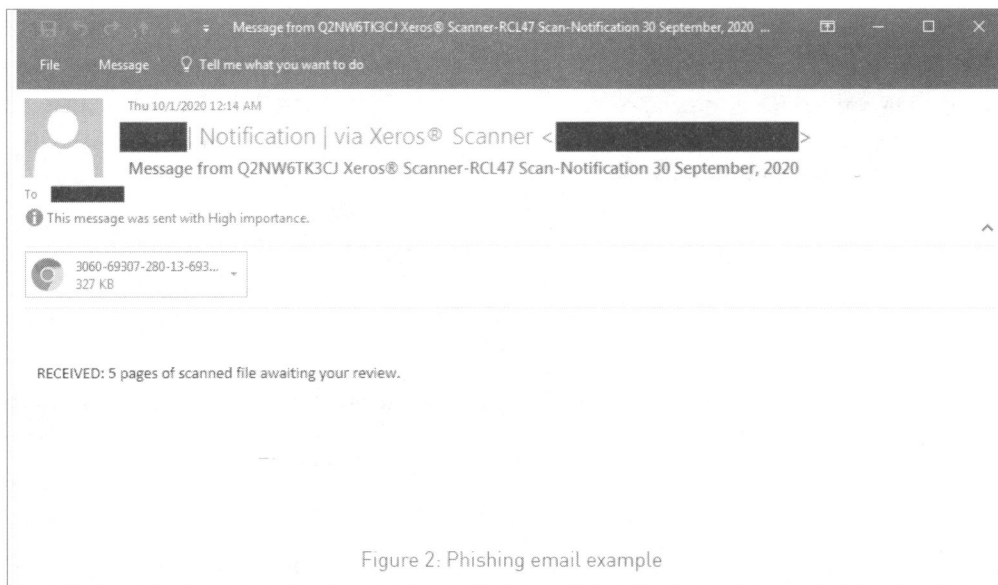


Figure 2: Phishing email example

Рис. 2.25. Письмо с HTML-вложением



Рис. 2.26. Имитация получения доступа к документу с помощью ввода пароля от учетной записи

О технических аспектах этой атаки можно почитать в блоге Checkpoint.



И еще один пример персонализированного фишингового онлайн-документа (рис. 2.27).

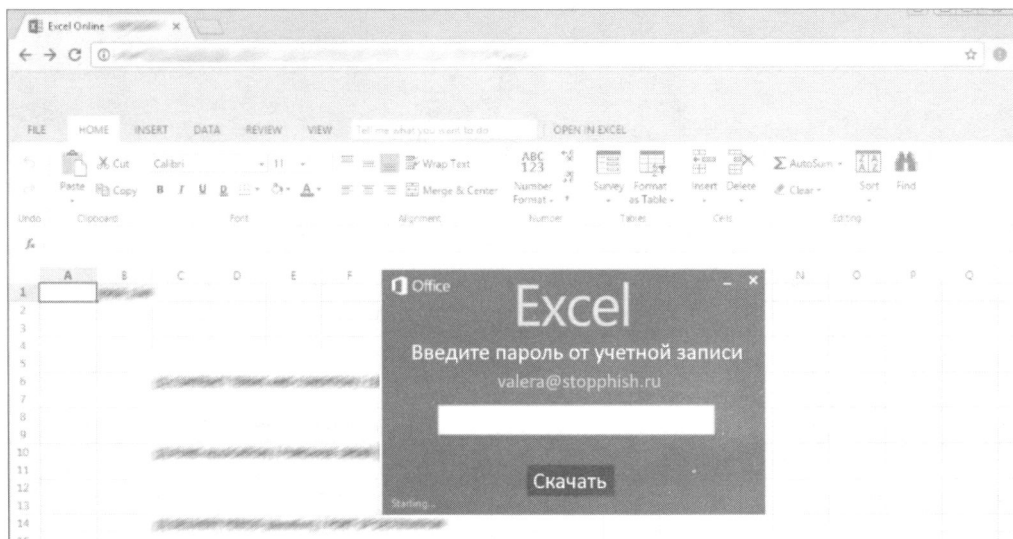
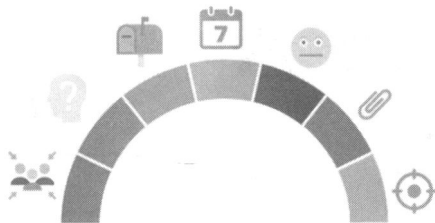


Рис. 2.27. Форма ввода пароля с указанным email жертвы

Глава 3



Атаки в офлайне

Я не люблю иметь дело с физическим контактом — мне больше нравятся способы без обратной связи. Всё потому, что не умею обманывать, глядя людям в глаза :-)

Кроме того, офлайн-атаки гораздо интереснее и более захватывающи в своем исполнении. Эта глава — экспериментальная часть книги. Если ее контент окажется тебе полезным, скажи мне где-нибудь об этом. Мы выпустим переиздание книги с расширением векторов в офлайне или, если материала будет достаточно, издадим отдельную книгу по этой теме.

А пока рассмотрим такие векторы в виде заметок, наших лайфхаков и опыта коллег.

Проникновение на физические объекты

Помимо «обычных» способов проникновения типа потенциального работника, пришедшего на собеседование, или сервисной службы, есть и необычные способы. Рассмотрим некоторые из них.

Предмет в руках

Социальная инженерия + лестница = свободный проход (рис. 3.1).
В нашей группе мы размещали видео, как иностранцы проходили через разные турникеты с лестницей под мышкой:

<https://rutube.ru/video/a43f1c5c8a49e69bb4e57e18100679a6/>.



А на рис. 3.2 приведен пример из Якутии, когда ребята приняли челлендж, на этот раз используя бутылку воды для пропуски в суды, МВД, прокуратуру и т. д.



Рис. 3.1. Проход через турникеты с лестницей в руках

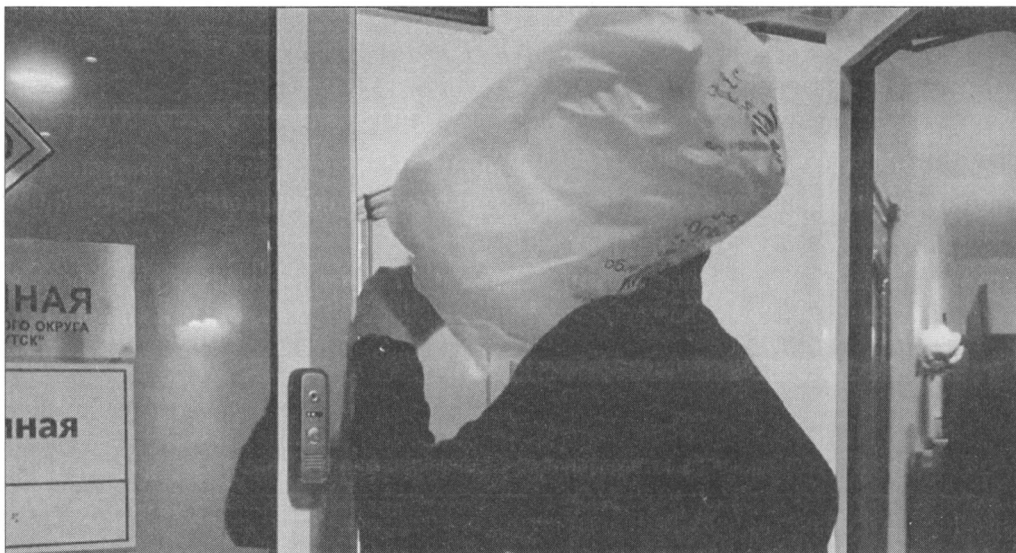


Рис. 3.2. Проход на закрытую территорию с бутылкой в руках

Подслушанная легенда

Этот способ также относится к звонкам по телефону, но на этот раз — звонок не жертве.

Если понадобится, чтобы охранник организации что-то предварительно узнал о тебе, но не напрямую, можно попробовать такой сценарий: становишься рядом с охранником и якобы звонишь сотруднику организации (можно даже типа ее

начальнику, называя его по имени-отчеству), в которую ты пришел, излагая свою проблему (вроде как у тебя нет пропуска, и тебя могут не пустить). Боковым зрением смотришь, наблюдает ли за тобой охранник. Далее ведешь себя так, будто «сотрудник» дает тебе некое решение проблемы, и ты повторяешь его вслух. Теперь если проговорить это решение охраннику, у него создается впечатление, что это придумал не ты, а некто в их организации, и тебе нужно посодействовать.

Так, кстати, делал один паренек, когда пытался проникнуть на конференцию через пост охраны.

Этот же способ поможет, если тебе приходится подолгу околачиваться на проходной, наблюдая за происходящим. Ты можешь имитировать разговор: «Да, я на входе... Хорошо, жду...» Через полчаса: «Так, ну сколько еще ждать?»

Проведение интервью

Берем у топ-менеджера интервью удаленным способом. Потом напрашиваемся на офлайн-встречу под предлогом, что его нужно сфотографировать на рабочем месте для вставки в статью.

Давайте помогу

Перед входом в закрытое помещение стоим с коробкой, покачиваясь от тяжести (можно пустой), делаем вид, что пытаемся что-то найти в карманах (копошимся), и ждем, пока кто-то будет выходить (входить). Расчет на то, что он придержит для тебя дверь.

Корпоративная столовая

Часто бывает, что в здании организации расположена столовая, доступ в которую разрешен для посторонних (капитализм, куда без него). Например, такая столовая есть в налоговой инспекции № 1 в Москве.

Кто питается в таких столовых? Правильно — сотрудники организации. Бывает, даже с бейджиками, на которых написано подразделение.

Такую, например, тему можно эксплуатировать, подсев за столик одного из них: «А вы тоже работаете в ...? Просто я стажировку прохожу и еще не запомнил всех 400 сотрудников» (выдаем что-то типа шутки). У тебя обязательно спросят отдел, где ты стажировешься, скажи: «Помощник HR (или начальника отдела кадров)», и назови институт, в котором учишься (подбери на свой вкус).

Далее ведем непринужденную беседу о радостях корпоративной и студенческой жизни. Завершением разговора может последовать просьба передать прозрачный файл с документом и флешкой от вашего начальника главному бухгалтеру (или другому сотруднику подразделения, которое ты увидел на бейджике собеседника), а тебе якобы нужно бежать в институт. В документе приведено опи-

сание содержимого флешки (бонусы, зарплата, внедрение новой системы мотивации, график сокращения или ротации персонала в текущем году, 4-дневная рабочая неделя и т. д.).

Не забудь приложить шоколадку: одну — главбуху, вторую — твоему помощнику (вторую шоколадку достаем не сразу, а спустя несколько секунд), и добавь: «В институте нас учили, что корпоративные вопросы без шоколадки неразрешимы». Прощаемся и ждем, с какого ПК флешку запустят в первую очередь.

Небезопасные парковки

Проникновение на корпоративную парковку — это не проникновение на объект, но ты уже близок :-)

Парковки бывают общими, но с пометкой, что определенная зона выделена только для сотрудников определенной организации.

Прибыв на парковку с утра, ты сможешь определить сотрудника из определенной организации по месту, где он припарковался. Дальнейший сценарий уже зависит от твоей цели: передашь ты ему какой-нибудь предмет, пакет документов или узнаешь что-то.

Еще немного о парковках. Одному пареньку три раза удавалось проходить в крупные организации через дверь на парковке — открывали ее выходящие сотрудники. А в одной из организаций въехать на парковку можно было, моргнув два раза фарами, как это делали въезжающие сотрудники. В общем, в офлайне главное — наблюдательность.

Паровозик

Метод так назвал Кевин Митник (а ребята, проходящие так через турникет в метро, и не знали). Это работало в те годы — работает и сейчас. В корпоративной курилке стой вместе со всеми, а когда все начнут заходить в здание через черный вход, пристраивайся к группе.

Этот метод также называется Tailgating. Название этого типа атаки можно перевести как «упасть на хвост» или «паровозик». Она предполагает физическое следование за уполномоченным лицом для получения доступа в запрещенную зону или здание.

В этом видео ты можешь посмотреть пять примеров реализации этой атаки: <https://www.youtube.com/watch?v=jksOir0WGM8&t=15s>.



Второй пример из видео, где показывается проникновение на объект через открытую дверь, я реально наблюдал в одной из организаций со строгими мужчинами на проходной. Все бы хорошо, но запасной вход был открыт нараспашку.

Вообще, стоит отметить, что один из главных навыков социального инженера — это не психология или, боже упаси, НЛП, а наблюдательность. С ее помощью

собирается информация о цели, что уже составляет примерно половину работы. Ну а при реализации офлайн-сценария важным навыком будет хладнокровие, ведь не так просто сдерживать эмоции, когда ты пытаешься пройти мимо охраны по поддельному пропуску.

Мусорный дайвинг

Думаешь, только в кино десятилетней давности хакеры копались в мусорке в поисках полезной информации? Почитай книгу от практика СИ Джонни Лонга No «Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing»¹. Отдельная глава в ней посвящена чисто копанию в мусоре :-)

И опять же, если понимаешь, когда говорят на английском языке, можешь посмотреть видео, как ребята используют копание в мусоре перед тем, как проникнуть в автосалон с дорогами авто:

https://www.youtube.com/watch?v=MdQas_We_kI&t=1259s.



Отделение банка

Опишу случай из жизни. Специально не пытался применить СИ, но внезапно это превратилось в один из способов проникновения в кабинет начальника отделения банка.

На аппаратах, которые выдают талончики с номерами очереди, есть пункт с чем-то похожим на «Другие вопросы». Взял талончик, сижу, жду своей очереди. На табло появляется мой номер. Иду в кабинет — как оказалось, «другие вопросы» решал начальник филиала банка, а нам и нужен отдельный кабинет, а не общее пространство с другими посетителями. Захожу — в кабинете пусто. Выхожу, стою возле двери, через минуту приходит начальник, и снова захожу с ним, чтобы решать свой вопрос.

А что можно было сделать, если бы у вас заказали тест на проникновение в этот филиал?

За минуту можно было бы положить флешку с вредоносным содержимым на стол и прикрыть чем-нибудь, прилепить стикер с «полезной» информацией, положить официальную бумагу с инструкциями по работе с новой версией портала и т. п. Понятное дело, что начальник чаще находится на месте, чем выходит, и тут просто совпало, но флешку в кабинете (на столе, на полу) можно оставить и при сотруднике, пока он отвлекся на что-то. Или имитируй падение бумажек на пол, когда заходишь в кабинет, — сбрасывание флешки при их поднятии никто не заметит — вас все равно разделяет монитор.

Еще один вариант попадания в кабинет: взять талончик, пропустить свою очередь и сидеть ждать, пока начальник выйдет, после этого войти с указанными целями. Главное — держать талончик обеими руками перед собой, на случай,

¹ См. <https://www.amazon.com/No-Tech-Hacking-Engineering-Dumpster/dp/1597492159>.

если натолкнешься на начальника. Тем самым создается впечатление, что ты ничего не прячешь, руки — вот они, ничего не украл, держишь «официальную бумажку», которую выдает банк.

Не забудь, независимо от того, с какой целью тебе санкционировали такое проникновение, проверить наличие видеокамеры в кабинете сотрудника. Если служба безопасности тестируется не только на ИТ-взлом, но и на возможность проникновения на физический объект, чтобы тебя не обнаружили, смотри по сторонам в поисках глаз «меньшего брата».

Отвлекающий маневр

Два напарника действуют сообща. Один отвлекает, второй проходит. Этот способ применим лишь в редких случаях, но не стоит о нем забывать. Когда охранник всего один, и тебе не страшны камеры, записывающие твое проникновение (поскольку когда их просмотрят, пентест уже будет выполнен), напарник может начать общаться с охранником, а ты, прикрываясь другим сотрудником, проходишь за периметр. Прикрываться сотрудником не всегда получится, но пока охранник занят общением с напарником, конечно же, некоторые из турникетов можно перепрыгнуть.

Потенциальный клиент

Отдел продаж может выписать тебе пропуск, если предварительно ты прикинешься их потенциальным клиентом. Не всегда это может сработать — например, в компанию, от имени которой ты якобы действуешь, могут позвонить и спросить, действительно ли ты у них работаешь. Ну и, конечно, способ не пройдет, если сотрудник будет встречать тебя перед пунктом выдачи пропусков, чтобы проводить для изготовления пропуска. Это стоит сразу прояснить по телефону:

А как мне вас найти: вы встретите меня или выпишете пропуск?

Но даже если тебя встретят, то не обязательно, что будут провожать. После собеседования можно идти выполнять свою задачу миссию.

Собеседование

Аналогично предыдущему способу — напрашиваемся на собеседование с HR. Помимо этого, может так получиться, что собеседование назначается нескольким кандидатам одновременно. Пока стоишь в очереди в кабинет HR, можешь немного «погулять, сходить попить воды».

Гостевой пропуск

Покрутившись немного возле бюро пропусков, «развешиваем уши» и слушаем, выдают ли здесь гостевые пропуска и по какому поводу. Некоторое время спустя повторяем легенду и получаем себе «билет» в охраняемый периметр.

Подделка карты-пропуска

Если удалось добыть номер с карты жертвы, которая работает в целевой организации, то тебе придется статья на «Хабре» (<https://habr.com/ru/post/514408>), где описан способ создания копии карты-пропуска по номеру.



Универсальным способ не назовешь — по мне, так проще со считывателем подойти к человеку и снять копию, но книга ведь не про универсальные способы: сейчас пригодится одно, завтра — другое :-)

Черный ход

Тоже из наблюдений. В одной организации была кабинка с охраной, бюро пропусков, турникеты и все такое, но оказалось, что в 100 метрах от турникета имела еще одна дверь на улицу, причем открытая. Служба безопасности потом сказала, что да, такого быть не должно.

Плечевая атака

Этот вид атаки является классикой жанра в СИ. Ее еще называют «плечевой серфинг».

Суть метода в том, что ты просто подглядываешь со стороны за источником конфиденциальной информации. Например, следишь из-за плеча за вводом человеком пароля на телефоне или читаешь текст внутреннего приказа, который сотрудник изучает на ноутбуке.

То ли привычка, то ли банальное любопытство, но я везде, где это прокатит, использую «плечевую атаку». Когда приходишь на встречу в организацию, невольно начинаешь наблюдать: а могу ли я, встав в определенное место, увидеть, что сейчас отображается на мониторе ПК охраны? А есть ли возможность снять это на мобильный? Я ничего, конечно же, не снимал и не читал, т. к. договоров на пентест не подписывал, — просто смотрю, есть ли такая возможность, и сообщаю СБ.

Например, в одной корпорации, пока коллега ждал на проходной, совершенно спокойно можно было наблюдать за монитором охраны, которая при этом находилась в отдельной кабинке.

Piggybacking

Название этой атаки можно перевести как «катание на спине». Она предполагает использование активной сессии пользователя для получения несанкционированного доступа.

Вообще, некоторые авторы статей нередко смешивают воедино Tailgating (физическое следование за человеком для получения доступа в запрещенную зону)

и Piggybacking, притом зачастую прямо в заголовках одной статьи, — якобы это одно и то же. Всегда напрягало подобное структурирование информации. Либо термин один, либо их два, и тогда они несут разный смысл и контекст. Поэтому я разделил их по смыслу, так что тебе не придется ломать голову над различиями этих атак.

В этом постановочном видео мы можем наблюдать, как «злоумышленник» сначала использует «плечевую атаку», подглядывая за тем, что пользователь вводит на компе, а после этого применяет Piggybacking, используя активную сессию в своих интересах: <https://youtube.com/watch?v=EIdLUOWJNZM>.



Вот для чего нужно блокировать сессию, отходя от устройства, но сейчас не об этом ;-)

USB-устройства

На социально-инженерном сленге такие атаки называются «дорожное яблоко» — это когда мы подбрасываем что-то, а жертва подбирает и использует.

Устройства с вредоносом, GPS-трекером, прослушкой, которые можно подключить: внешний жесткий диск, MP3-плеер, powerbank, провод для зарядки (рис. 3.3), автомобильная зарядка.

USB кабель со встроенной GSM прослушкой для iPhone и Android

Время работы не ограничено

Точность координат
местоположение от 50 метров

1 высокочувствительный микрофон
Дистанционная прослушка
Чувствительность микрофона 5 метров
Рабочая температура -40 +50
Вес 17 г

Чтобы оставаться незамеченным, жучок скрыт под обычный USB-кабель, который не издает никаких сигналов и никак себя не выдает. USB-жучок имеет самую низкую цену, а для начала работы необходимо лишь установить мини-сим-карту и подсоединить прослушку к стандартному USB-входу. После этого вы можете позвонить на номер сим-карты, установленной в жучок, как на обычный мобильный телефон и слушать все, что происходит в радиусе 5 метров

Рис. 3.3. USB-кабель с SIM-картой

Перейдя по QR-коду, ты можешь посмотреть, как работает вредоносное ПО, сохраненное на флешке и имитирующее устройство ввода (мышь или клавиатуру). «Вирус» срабатывает, даже несмотря на то, что на целевом компьютере запрещен запуск исполняемых файлов. Ролик на английском, однако можно использовать широко известный браузер для онлайн-перевода видео — он довольно неплохо справляется со своей задачей.



А теперь давайте рассмотрим способы доставки таких устройств до конечного пользователя.

Таргетированная флешка

На подбрасываемую флешку или внешний жесткий диск закидывается вредоносный файл плюс еще один файл «инструкция.txt». Нашедший флешку сотрудник дома открывает вредоносный файл, но «ничего не происходит». Затем он читает инструкцию, а там написано, что в целях безопасности файл защищен и будет работать только в сети работодателя (подставляем нужное название компании), — нам ведь надо, чтобы он открыл файл не на домашнем компьютере, а на рабочем ПК.

Флешка с легендой

Подбрасывая флешку, не забудь создать ей «легенду»: в корень кидаем пару личных фоток (нейтральные, из чьей-то соцсети) и пару обычных документов. Это успокаивает жертву — у нее создается впечатление, что флешка принадлежала обычному человеку.

А уже в одну из папок (с названием типа «Личное») помещаем вредонос.

«За букет роз»

Перескажу сценарий вручения флешки, когда-то прочитанный в Сети.

Профиль сотрудницы финансового подразделения был найден в соцсетях, там же узнали и ее телефон. Из постов профиля узнали, что она часто использует продукцию определенного бренда.

Позвонили, представились представителем бренда и сказали, что за ее лояльность и частые заказы хотим сделать ей подарок — она вроде как их мини-амбассадор. Уточнили время доставки (естественно, в рабочее).

В назначенное время курьер доставил букет цветов, коробку конфет и флешку с нагрузкой. Не прошло и получаса, как пентестеры уже имели доступ к ее рабочему ПК и всей сети организации.

Juice jacking

Этот термин описывает любую атаку, основанную на подключении устройств к непроверенным портам USB. Такой вид атак эксплуатирует потребность пользователей оставаться на связи или просто посмотреть фильм, чтобы скоротать время. Человек может как подключить зарядный кабель в зловерный USB (рис. 3.4), так и использовать шнур, в который вшит бэкдор.

Воткнув USB-скиммер в общественную зарядку, ждать, что именно сотрудник целевой организации подсоединит к ней шнур, весьма проблематично.

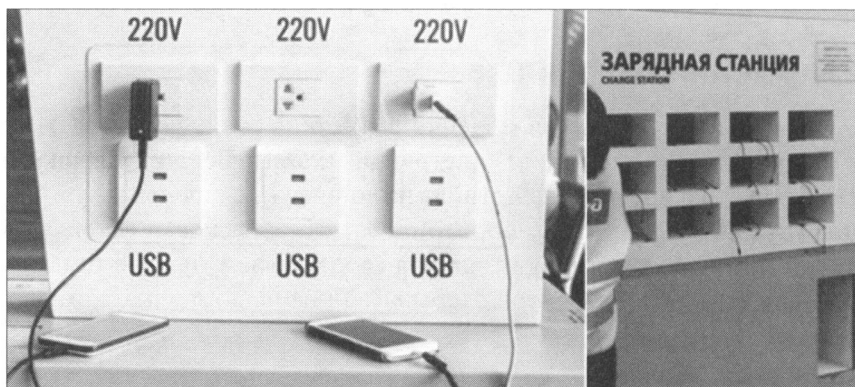


Рис. 3.4. Зарядные станции в общественном месте

Проще адресно доставить вредоносный шнур. Не вдаваясь в подробности, приведу несколько способов такой доставки: домашний почтовый ящик с якобы подарком от обслуживающей организации или местной фирмы (магнитиками от службы по ремонту холодильников уже никого не удивит), раздача через промоутеров, подкидывание в самой организации, курьер с подарком и доставкой на рабочее место.

Смишинг

При классификации этого способа СИ возник спорный момент — отнести его к офлайну или онлайн. Но хотя SMS можно отправить с помощью онлайн-сервисов, принимают его в большинстве случаев в телефоне. Так что смишинг можно определить как способ доставки вредоносного контента с помощью SMS.

С его помощью можно отправить ссылку, ведущую на фишинговый сайт, и похитить информацию:

Добрый день. Благодарим за заказ и оплату. [Zlo.com/payment-7361](https://zlo.com/payment-7361).

Работникам на удаленке можно отправить такое:

Срочно. Рассылка по SMS на личные номера проводится в целях обеспечения безопасности. Работникам ... (организация) требуется сменить пароль от ... (почты, портала) по ссылке corp.ru/email-7361.

А уже на поддельном сайте просим сначала ввести старый пароль, а потом — новый.

Вишинг

Вишинг (vishing, от voice phishing) — использование телефонной связи для обмана пользователя или выманивания у него дополнительной информации.

Рассматривать способы, когда у жертвы блокируется браузер и появляется сообщение, что ей нужно позвонить в техподдержку, не будем, т. к. это больше актуально для физлиц. Рассмотрим корпоративные лайфхаки и методы.

Подделка номера

Многие уже слышали, как мошенники звонят и представляются службой поддержки банка. Номер телефона при этом может подменяться официальным. Стоимость такого сервиса около \$15 за подключение и от \$0,0014 за минуту разговора.

Преступники настолько набрались храбрости, что подделывают не только официальные номера телефонов банков, но и используют в своих схемах номера ФСБ (см. QR-код, чтобы изучить один из кейсов).



При пентесте ты можешь использовать подобные технологии для звонков сотрудникам — ведь знакомый для них номер будет отображаться на экране телефона.

Многоходовый звонок

Сначала звонишь жертве и в лоб говоришь ей, что ты из техподдержки и тебе нужен пароль от ее аккаунта (или еще от чего-либо — даже достаточно отдаленного от ИТ). Жертва тебя отправляет лесом (надеюсь).

После этого звонишь жертве с подменой номера (или без) от имени службы ИБ, объясняешь, что в организации зафиксирована массовая попытка кражи номеров телефонов, и спрашиваешь, звонили ли ей. Она подтверждает и проникается большим доверием.

После этого даешь ей инструкции, как на всякий случай сменить пароль прямо сейчас на твоём фишинговом сайте.

Вернитесь на работу

Вводная: мы знаем, что офис работает до 18.00, и после этого все сотрудники уходят с работы, а проходная закрывается.

В 18.40 звоним сотруднику на мобильный, и происходит такой разговор:

— Анна, добрый день. Это Андрей из техподдержки АО «Стопфиш» (*соответственно тут называем организацию работника*). Вы уже, наверное, далеко ушли от офиса?

— Да.

— Та-а-ак так-так... (Произносим задумчиво и делаем паузу, чтобы нас спросили: «А что случилось?»)

— Дело в том, что нам поручили в вашем отделе после работы перенастроить почтовый сервер, но теперь возникла проблема с доступом у некоторых сотрудников, а Андрей Федорович Копытцев (начальник Анны) сказал, что с утра у работников все уже должно работать. Без вашей учетной записи почтовый сервер не перенастроить.

— Чем помочь?

— Нужно, чтобы вы вернулись и сбросили пароль от учетной записи `anna.ivanova@stopphish.ru`.

— ... (При согласии прийти в офис или «ой, я уже не могу» говорим, что «в принципе, мы с вами можем сделать это удаленно, да и в офис вас на проходной уже не пустят».)

— Хорошо, давайте.

— Мне потребуется текущий пароль. Его уже можно считать устаревшим, т. к. после перезагрузки сервера вам завтра с утра нужно будет придумать новый.

Получаем пароль и благодарим за помощь.

Забыл кодовое слово

Если в банке спрашивают кодовое слово, говоришь «не помню», и тогда есть шанс, что у тебя могут начать спрашивать другие данные. Например, однажды у меня в одном инновационном банке, когда я забыл кодовое слово, спросили данные паспорта и вид деятельности. Судя по всему, в этом банке можно было бы узнать нужную информацию без кодового слова по любому ООО или ИП, знай ты паспортные данные директора и ОГРН организации.

Отсылка к отпускнику

Аналогично тому, как мы делали по email, узнавая, кто сейчас находится в отпуске, и ссылаясь на него в письмах пользователям, — это же можно делать и при телефонном звонке:

Андрей Максимов из отдела закупок сейчас в отпуске и сказал обращаться к вам по этому вопросу.

Синхронный ввод

Позвонив сотруднику по одному из поводов, отмеченных в «Классификаторе СИ» (см. *приложение 2*), попроси его дублировать голосом вводимый пароль для «сверки» с информацией в базе.

Также голосом повторяй за ним вводимые данные для правдоподобности.

Телефон + find trap

В этом случае имеется в виду find trap с использованием телефонных звонков, а не email-рассылок.

Если атакуют физлиц, а не сотрудников организации, делается обзвон клиентов какой-либо слитой базы. Люди ищут, кто звонил, и попадают на сайт фейковой организации.

Например, слита база магазинов «Четверочка» — тогда на сайте злоумышленник укажет «полезную» информацию: якобы «Четверочка» из-за неправильно начисленного НДС делает возврат 20% средств для тех, кто делал покупки в этом году. Нужно лишь ввести данные своей банковской карты, разумеется, включающие дату действия карты и CVV.

Еще, помню, был случай — звонили с какого-то венгерского номера. Трубку не брал, но номер погуглил. На первом или втором месте в результатах поиска оказался сайт, перейдя на который, я обнаружил, что нахожусь в чьем-то личном кабинете какой-то платежной системы. На балансе — криптовалюта.

Расчет здесь на то, что я алчный и попробую вывести средства себе на карту, реквизиты которой и попадут мошеннику.

Но книга эта не рассчитана на защиту физлиц, а имеет более корпоративную направленность. Поэтому сотруднику организации можно 2–3 раза позвонить на мобильный (ожидая по одному гудку), чтобы он погуглил номер. А там — твой сайт и некая информация для сотрудников именно этой организации + нагрузка.

Любой добавочный

Бывает, что нужно попасть в бухгалтерию, — звонишь, но секретарь в приемной говорит, что нужно писать запрос на «info@...». Не знаю, как бы было в корпорациях, но в небольших банках такое получалось. Звонишь и рандомом набираешь любой добавочный (либо сначала его маску, которую ты можешь найти на сайте). Далее примерно такой диалог:

- Алло.
- Здравствуйте. А это бухгалтерия?
- Нет.
- Эх, опять неправильно соединили. Не могли бы вы переключить на бухгалтерию?
- Сейчас попробуем.

Соответственно так мы обходим секретаря и попадаем на целевого пользователя (в нашем случае — бухгалтера).

Китовые атаки

Таким термином обозначают атаки, когда злоумышленник пытается атаковать топ-менеджмент организации.

Я, вообще-то, скептически отношусь к настолько сильному дроблению методов социальной инженерии. Когда ввели термины «вишинг» и «смишинг», они хоть как-то оправдывали дробление, т. к. каналы коммуникации использовались разные. Но когда «китовые атаки» выделяются в отдельный вектор СИ... Да, у уборщицы есть ключи от всех дверей, значит, ее тоже могут атаковать, тогда нужно ввести *cleanshing*, а для методов с кражей PUK-кодов — пукинг...

Тем не менее раз этот термин уже устоялся, упомянем и его.

Если тебе одобрили тест гендиректора :-) (вряд ли, конечно), то можешь представиться журналистом одного крупного журнала о бизнесе, чтобы взять интервью, и после разговора отправить ему ссылку или файл.

Такие ссылки и файлы часто проходят средства защиты, т. к. гендиректор считает, что за ним-то ибэшники «шпионить» не должны.

Усиление звонком

Отправил письмо пользователю и хочешь увеличить доверие к его содержанию?

Позвони ему по рабочему телефону и сообщи, что отправил важное письмо (можешь не вдаваться в подробности), а на половине фразы оборви разговор (имитируя обрыв связи). Главное, что ты привлек внимание к письму — тогда оно с меньшей вероятностью останется незамеченным. А поскольку такой способ редко используется злоумышленниками, к твоей нагрузке будет больше доверия.

Мы в своем софте StopPhish хотим автоматизировать отправку email + автодозвон с таким вот уведомлением — интересно, что получится :-)

Квид про кво

Квид про кво (от *лат.* *quid pro quo* — то за это) — создание условий для пользователя, когда у него появляются проблемы (действительные или вымышленные), а злоумышленник предлагает помощь в их решении.

Аналогично тому, как мошенники сообщают физлицам, что с их карты пытаются списать средства и нужно обезопасить банковский счет, корпоративному пользователю можно помочь решить вымышленную проблему.

Звонок от «службы ИТ»:

— Добрый день, это ИТ-департамент, у вас с компьютером все в порядке, не тормозит?

— Нет.

— Странно, а в Интернет выйти можете? Проверьте.

— Да, открывается.

— Ага, вот-вот!.. Попробуйте перейти еще на какой-то сайт. Перешли?

— Да!

- Так, ну все ясно, вирус подхватили. Ни по каким подозрительным ссылкам не переходили в последнее время?
- Нет!
- Ясно, значит, удаленно загрузили. Придется на пару дней отключить ваш компьютер для очистки от вируса.
- Ой-ой, а что так долго, мне совсем нельзя без компьютера!
- (Задумчиво.) Так... До вас дойти смогу уже только завтра, сейчас тогда компьютер не буду блокировать, можем попробовать удаленно разобраться.
- Да, давайте!

Далее идут несколько сценариев:

- отправка по email «ПО для удаленной техподдержки», которое пользователю нужно установить;
- отправка/диктовка ссылки на это же ПО;
- диктовка фишингового URL якобы технического портала поддержки, по которому пользователю нужно перейти и ввести учетные данные. После логина предлагаем скачать «программу по очистке ПК от вирусов» (на самом деле — пустышка, не наносящая вреда, тебе достаточно и украденных учетных данных).

Либо после логина он попадает на страницу с кнопкой **Перезагрузить текущие сеансы**. Говорим: «Нажать, перезагрузить ПК, и на первое время проблема будет решена».

Принимаем благодарности и прощаемся.

Callback phishing

При таком способе фишинга жертву побуждают позвонить по определенному номеру телефона и уже по этому каналу связи выманивают информацию.

Как вы понимаете, спам-фильтры и другие защитные средства не распознают опасность в письме, где нет ни ссылок, ни файлов.

Все, что нужно сделать для начала атаки, — это отправить письмо на email жертвы:

Добрый день.

Ваша учетная запись заблокирована. Для ее восстановления позвоните ответственному за безопасность, отвечающему за конфиденциальность учетных данных.

Для оперативного решения вопроса звоните по мобильному номеру телефона: *(приводим номер)*.

Отсылку на конкретный номер в письме мы делаем для того, чтобы сотрудник не стал звонить по уже знакомому номеру техподдержки или в отдел ИБ.

Подробности по такому типу атак можно найти тут: <https://xakep.ru/2021/04/01/bazarcall/>. В статье рассказывается, как злоумышленники распространяли вредоносное ПО BazarCall по корпоративным пользователям.



Нас взломали, помогите восстановить

Помимо стандартного звонка сотруднику в пятницу под конец рабочего дня с просьбой задержаться и помочь с восстановлением пароля, поскольку произошел технический сбой, можно попробовать и нестандартный способ:



<https://www.youtube.com/watch?v=wxuYd8XUqmY>.

В этом сценарии «злоумышленник» просит жертву сменить пароль на новый, который он теперь, естественно, знает и которым сможет воспользоваться. Если на портале (или в любом другом сервисе) стоит двухфакторная аутентификация, то пройти ее также поможет пользователь, раз уж он только что помог злоумышленнику сменить свой пароль.

Второй вариант: если человек не знает, что нужно делать, чтобы сменить пароль, можно провести примерно следующий диалог:

Пентестер: «Хорошо, я помогу вам и сменю пароль за вас. Текущий пароль я не знаю, поскольку он уже сброшен, но он сейчас понадобится для восстановления системы».

Жертва: «Хорошо».

Пентестер: «Продиктуйте пароль по символам».

Бумага не во благо

В этом разделе мы рассмотрим примеры атак с использованием бумажных носителей. Ссылка, отправленная в бумажном письме, точно пройдет антиспам-систему, но ее может остановить firewall в лице секретаря :-)

Подбрасывание корпоративных документов

Подбрасывать можно не только флешки с нагрузкой, но и «корпоративные» документы (приказы, списки на увольнение и т. п.). Если ты попал внутрь периметра, иди в уборную, общую кухню :-)) (да, и там удалось побывать), к журнальному столику и положи якобы официальный документ за подписью какого-то начальника организации.

В документе будет ссылка на сайт, собирающий логины и пароли.

Визуальный пропуск

Это СИ реализуется с помощью поддельных пропусков и бейджиков. В тех случаях, когда на пункте охраны пропуск является не техническим, а чисто визуальным атрибутом для проникновения за периметр (понаблюдай, как ведет себя охрана), можно сделать копию такого пропуска. В столовой, кафе, ресторане, где появляются сотрудники, можно без труда сфотографировать образец.

Кстати, если, помимо пропуска, потребуется использовать фирменную одежду целевой организации, в этом видео: <https://www.youtube.com/watch?v=NsAo0HLiWR8> иностранцы подробно рассказывают, как они добывают оригинальную униформу для проникновения на объект.



Реклама на бумаге

С помощью бумажного письма с закосом под рекламу бухгалтеру можно подсушить доступ к якобы новооткрывшемуся сервису ему в помощь. Там он вводит email и пароль, который может подойти и в другом сервисе или к его корпоративной учетке.

Сервис может быть новый (вроде «Гаранта», но только бесплатный) или существующий известный (тот же «Гарант», но якобы у них появился новый сервис).

QR-коды на бумажных носителях

Мы уже упоминали про QR-коды в *разд. «Маскировка ссылок» главы 2*, но там они доставлялись по электронным каналам коммуникации.

Такие коды можно использовать и офлайн — наклеить на чей-то плакат, рекламу, на оповещения для сотрудников в общественных (и не только) помещениях.

Разумеется, можно не только «паразитировать» на чужих плакатах, но и создавать свои :-)

Проник в здание организации? Принимайся раскладывать красиво оформленные, брендированные под организацию-жертву листовки и клеить плакаты — скорее всего, безнаказанно это получится сделать только в туалете :-):

Коллеги, в связи с обновлением ассортимента продукция будет распродана среди сотрудников с 98%-ной скидкой. На нашем портале в специальном разделе (QR-код со ссылкой ниже) есть список оставшейся продукции. То, что Вы решите выкупить, пометьте в таблице знаком «+». Это мероприятие действует до конца недели.

Конечно, для разных организаций листовки будут со своим бонусом — не все ведь продают что-то материальное, или продукция организации нужна не каждому. В таком случае придумай «акцию» от партнеров. Например:

В рамках стратегического сотрудничества для сотрудников ООО «Ромашка» сеть магазинов «Букварь вкуса» предоставила сертификаты номиналом 7500 руб. Для этого...

Справка

Случай из жизни. К знакомым в небольшую организацию пришел «проверяющий» — удостовериться в наличии масок и перчаток у работников (для будущих поколений, читающих эту книгу: в 2020 году в мире был небольшой кипиш по поводу COVID-19). Все бы ничего, но пришел представитель ГБУ Москвы «Мо-

сковский контрольно-мониторинговый центр недвижимости». Справка с места событий прилагается (рис. 3.5).

Что можно почерпнуть для себя как пентестера из этой ситуации: не во все, но в некоторые организации можно попытаться пройти по такой «справке» — главное сделать лицо поувереннее. В рассматриваемом случае реально существующий «Московский контрольно-мониторинговый центр недвижимости» трубку не брал, соответственно проверить, действительно ли пришел их представитель, было невозможно.

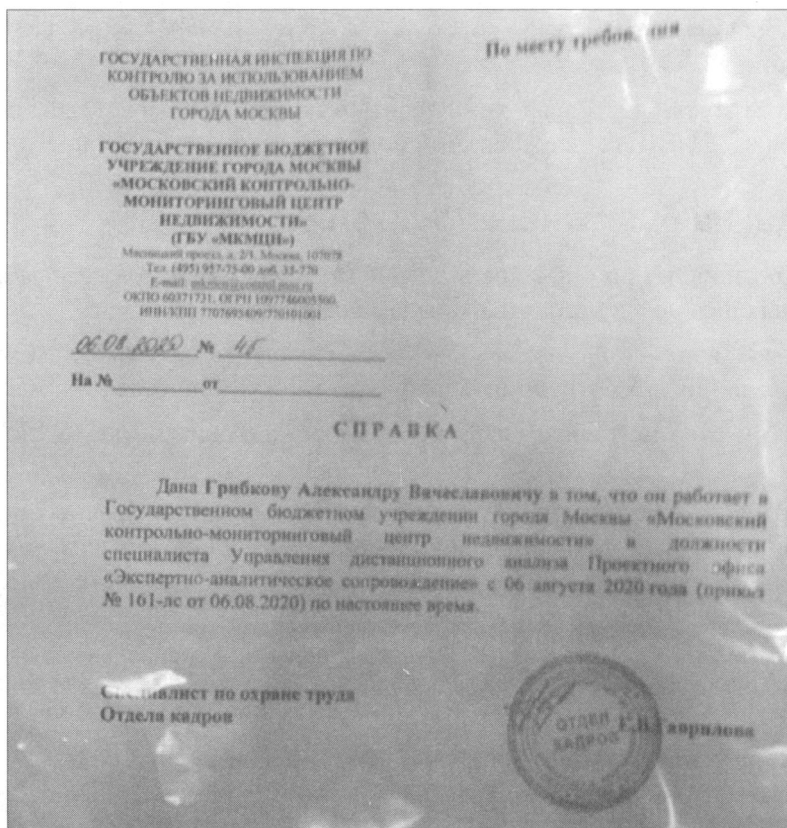


Рис. 3.5. Пример фейковой справки

По сути, можно прийти не только со справкой, но и с «корочкой», и не обязательно от реальной организации. А дальше идти по этажам и разбрасывать флешки, даже если тебя сопровождают.

Я видел много проходных в организациях — с серьезной службой безопасности такое не пройдет, но туда, где в одном бизнес-центре располагается много компаний, и охрана не принадлежит конкретной организации, а в самом офисе целевой организации сидят в основном рядовые сотрудники, можно попробовать пройти со «справкой».

Общественный транспорт

Общественный транспорт удобен тем, что ты сидишь рядом с жертвой, и все, что происходит у тебя, видит и слышит твой сосед, — т. е. ты можешь создать в голове слушателя определенную легенду о себе.

Этот способ можно было бы считать теоретическим и использовать общественный транспорт только для плечевой атаки, если бы в жизни не было примеров его применения.

Несколько лет назад был случай, когда мошенник, охотясь за определенной жертвой, сел рядом с ней в аэропорту и якобы рассказывал кому-то про криптовалюту и выгодное вложение. Жертва была криптоинвестором и сама заговорила с мошенником — ведь у них обнаружили общие интересы. В результате мошенник рассказал о выгодном мероприятии, в которое вложилась жертва и, естественно, лишилась средств.

Wi-Fi

Подключаясь к новой сети, нельзя быть уверенным, что передаваемые по ней данные в безопасности.

Как побудить кого-то подключиться к твоей «зловредной» сети Wi-Fi, которую ты раздаешь, например с ноутбука в рюкзаке?

- Если в целевой организации ты видишь информационный листок с логином и паролем к Wi-Fi — подмени его собственным листком.
- Если доступ на этом листке организован с помощью QR-кода — наклейте поверх него свой или, опять же, замени листок своим.
- Еще один из способов — назвать свою сеть похоже на сеть организации и просто сидеть и ждать, пока к ней кто-то подключится.
- Ну а если тебе повезло, и провод с питанием точки Wi-Fi находится в зоне доступности, назови сеть, как и оригинальную, и выдерни провод, — так к твоей сети подключатся быстрее.

Подробнее о технических аспектах такой атаки можно почитать на «Хабре» в статье «Rogue AP — фальшивые точки доступа» (<https://habr.com/ru/articles/277793/>), где Лука Сафонов делится списком инструментов для атак через Wi-Fi. Напрямую с СИ связаны программы Wifi phisher и Linset.



Мероприятия

Хорошим поводом познакомиться с жертвой или целой группой жертв (например, на корпоративе организации) являются мероприятия.

Рассмотрим некоторые приемы и примеры эксплуатации этого вектора.

Двухдневное мероприятие

Забывтые бейджики с первого дня, являющиеся пропусками при входе, — не редкое явление.

Может получиться, как в моем случае, что верификация входящих на второй день была не такая строгая, как в первый. Просто понаблюдай, что происходит на проходной. Тогда на второй день, назвав свое имя как участника, ты получишь копию «потерянного» бейджика и сможешь пройти внутрь периметра уже как коллега.

Это же можно провернуть и в первый день, подслушав данные о регистрации одного из регистрируемых и потом сказав другому регистратору, что потерял пропуск участника. Или просто, что на перерыве сидел с коллегой в машине, а он уехал с твоим бейджилом.

Организовал себе на голову

Если жертва организывает мероприятие на своей территории, то за периметр можно попасть гораздо проще. Мониторь социальные сети и официальный сайт организации и регистрируйся в списке участников. Ну или не регистрируйся, если это много стоит, и применяй СИ, чтобы попасть внутрь, — заодно проведешь пентест охраны мероприятия. Я знаю, что некоторые безопасники так и делают, когда «забывают билет на мероприятие в машине» :-).

Конференции, выставки и форумы

Если знаешь, что жертва будет на каком-либо мероприятии, — это хороший способ познакомиться с ней вживую или как минимум надеть футболку и кепку, прикинуться промоутером и раздавать USB-устройства. Только не светись перед организатором — ты ведь не оплатил коммерческое участие в мероприятии :-)

Пришел к одним, пошел к другим

Если тебя интересует здание заказчика, а на территории этого здания проводится мероприятие (какой-то другой организацией), то это может сыграть тебе на руку. Ты проходишь через первый кордон охраны, когда идешь на мероприятие, и дальше можешь направляться на территорию заказчика.

Так я гулял по разным этажам организации, тогда как мероприятие проходило на первом.

Корпоратив

Перед новым годом или в рамках локальных праздников организации крупные и не очень компании устраивают корпоративы.

Если обычное место их работы представляет собой Форт-Нокс с биометрией, снайперами по периметру и «неуговариваемой» охраной, то может так полу-

читься, что в арендованном банкетном зале не будет таких мер безопасности, а разгоряченные шампанским сотрудники потеряют бдительность и с радостью с тобой пообщаются. Можешь прикинуться новичком, стажером, сотрудником службы ИБ — да кем угодно, это зависит лишь от выбранной жертвы и сценария.

Комбинирование

Нельзя не отметить комбинацию онлайн- и офлайн-сценариев. Например, как мы делали это в одном из предшествующих разделов, когда писали письмо и сопровождали его звонком с вопросом, получили ли там наше сообщение.

Делать это можно и в обратном порядке — сначала звоним и договариваемся, что отправим письмо. Тогда пришедшее сообщение будет уже не совсем от незнакомого человека.

Да и тот же data-фишинг можно использовать онлайн, а применять полученную информацию офлайн.

Истории для вдохновения

В этом разделе мы рассмотрим разные примеры применения социальной инженерии в физическом мире. Любителям фильмов о мошенниках посвящается ;-)

Обход системы

Социальный инженер — это состояние души.

В любой системе есть изъян, либо технический, либо человеческий.

В этом простом примере, я хотел продемонстрировать, что регламенты и средства защиты — это полумеры, если вы не пригласили пентестера их проверить :)

Однажды я решил проверить, смогу ли я попасть на территорию жилого комплекса, если бы «забыл» код от двери. Что мы видим на фото (рис. 3.6)? Длинную инструкцию о том, что делать, чтобы тебе открыли дверь, ну и, собственно, кодовый замок.

Но немного присмотревшись, мы обнаруживаем, что сама табличка, ее печать, работа дизайнера и мастера по закреплению самой таблички и, естественно, стоимость замка с его установкой, — все эти ресурсы потрачены зря (рис. 3.7).

Этот случай иллюстрирует два момента:

- прочитав предупреждение на табличке, что нужен код для открытия калитки, мы понимаем, что регламенты помогают в идеальных условиях и не всегда работают, как задумано;
- главные навыки социального инженера — наблюдательность и смекалка. Регулярно тренируйте эти навыки в быту, не обязательно работать за деньги ;-)



Рис. 3.6. Кодовый замок на калитке и инструкция для посторонних



Рис. 3.7. Открытие двери в «обход системы»

Еще раз сделаю акцент на том, что нужно тренировать наблюдательность и смекалку, а не нарушать закон, если речь идет не о пентесте ;-)

Пентест тюрьмы

Следующая история иллюстрирует то, что, представляясь кем-то во время теста на проникновение, важно соблюдать детали, чтобы не выглядеть подозрительно. Ну а в идеале, в прошлом иметь опыт работы в профессии, которую ты имитируешь.

На конференции RSA пентестер Джон Стрэнд из Black Hills Information Security рассказал о том, как его мама Рита провела тест на проникновение в тюрьму.

Рита, 58-летняя мать Джона, ранее была ответственной за школьное питание и стала финансовым директором компании сына. Прочитав отчеты о взломах, которые проводил ее сын, она решила попробовать свои силы в тестировании на проникновение.

Целью была выбрана тюрьма. Она отказалась от идеи проникнуть туда под видом курьера и выбрала роль санитарного инспектора, т. к. имела опыт проведения медицинских осмотров.

Подготовившись, она отправилась в тюрьму с поддельным пропуском (рис. 3.8) и настоящими бумажными формами для инспекции. Она просто подошла к главным воротам, сказала, что является медицинским инспектором и пришла для проведения внепланового осмотра помещений.

Джон и его команда ждали в кафе, отслеживая подключение USB-накопителей, которые Рита должна была вставить в компьютеры внутри периметра. После



Рис. 3.8. Фейковый пропуск

получаса ожидания Джон уже начал беспокоиться, но вскоре начали приходить сигналы с флешки. Оказалось, что Рита даже забыла, зачем пришла, и увлеклась проверкой помещений.

Вспомнив о своей цели, она стала возвращаться в помещения, которые проверяла ранее, и устанавливала флешки во встречаемые USB-порты. Когда она почти закончила, директор тюрьмы вызвал ее к себе в кабинет и попросил рассказать о результатах проверки. Она рассказала обо всех проблемах и о том, как их исправить.

В конце директор спрашивает: «Есть ли какой-нибудь способ, с помощью которого мы могли бы подготовиться к подобным проверкам в будущем?».

Рита говорит: «Да. На этом USB-накопителе находится документ с опросником для самопроверки». Джекпот! ;-)

Сорокаминутную презентацию на английском ты можешь посмотреть на Youtube:

<https://www.youtube.com/watch?v=yqOGuXcLdOA>.



Случай в отеле

Еще одна история с физическим пентестом, но на этот раз заказчиком оказалось физическое лицо. Хотя книга посвящена атакам на организации, описанная цепочка событий имеет столько деталей, что возможно, что-то из этого пригодится тебе и при взломе организации. Вдруг, однажды твоей целью будет взлом топа Рэдиссон, проживающего в своем отеле ;-)

Патрик Уордл и Михаил Сосонкин на конференции PHDays в Москве провели успешную кибератаку на Джанну Тобони, продюсера VICE News HBO, чтобы показать уязвимости в безопасности. Она сама попросила их взломать ее, а в завершение они подарили ей флажок России и сказали, что купили его с ее кредитной карты.

Полный сюжет можно прочитать тут (см. QR-код):

https://community.cadence.com/cadence_blogs_8/b/breakfast-bytes/posts/some-real-russian-hacking.



А я далее приведу сокращенный перевод истории.

❑ Фаза 1: Какие устройства у нее есть?

Жертва — популярная фигура. Немного погуглив, Патрик и Михаил обнаружили на ее фотографиях MacBook Pro. Затем, непосредственно наблюдая за ней, они увидели, что она использует iPhone в кафе и на улице.

Вектор с фишингом отметили сразу, т. к. одного конкретного человека поймать сложнее, чем несколько сотрудников в организации. Вместо этого они решили создать мошенническую точку доступа Wi-Fi.

□ Фаза 2: Злая горничная.

Патрик и Михаил решили проникнуть в комнату жертвы. Но они не знали, в каком номере находится жертва. Конференция проходила в Crowne Plaza, поэтому они решили, что она тоже будет в этом отеле.

В РФ действует закон, согласно которому каждый должен пройти аутентификацию под своим именем перед использованием общедоступного Wi-Fi. В отеле это было настроено следующим образом: имя пользователя — это номер комнаты, а пароль — это фамилия гостя, которая была известна исследователям, — Тобони.

Они написали скрипт, проверяющий пары логинов и паролей: «номер: toboni». И в результате нашли комбинацию номера и пароля, которая позволяла им подключиться к Wi-Fi, используя toboni в качестве пароля. Ее номером оказался 2086.

Затем они применили социальную инженерию. Им нужен был женский голос, звучащий по-американски. Жена Патрика Дана воспользовалась функцией Skype для звонков по номеру телефона и позвонила на стойку регистрации чтобы сообщить, что она Джанна Тобони из номера 2086 и что Патрик зайдет, чтобы забрать ключ.

Когда Патрик пришел на ресепшн за ключом, администратор не стал перезванивать в номер, чтобы подтвердить выдачу ключа, т. к. у него лежала записка с просьбой его передать.

Так они проникли в ее комнату.

□ Фаза 3: Несанкционированная точка доступа.

Для организации точки доступа Патрик и Михаил использовали роутер NooToo TravelMate размером с блок питания MacBook. У него две антенны, поскольку он предназначен для соединения двух сетей, и он достаточно дешев, чтобы считаться одноразовым (\$21). Они создали на его основе точку доступа под названием `crowne_plaza_guest`, а затем соединили эту сеть с реальной сетью отеля, чтобы любой, кто ее использует, не заметил ничего необычного.

Они создали также собственную поддельную страницу входа и использовали перенаправление DNS, как это делает общедоступный Wi-Fi, для принудительной аутентификации. Как только жертва прошла аутентификацию, они подключили ее, чтобы она могла нормально просматривать страницы. Теперь они «прослушивали» ее трафик.

В номере жертвы также находился MacBook. Они открыли его в режиме восстановления (предназначенном для устранения неполадок в системе), который дает доступ к жесткому диску. Затем они использовали USB-накопитель для установки вредоносного ПО. Шифрование диска помешало бы этому, но по умолчанию оно не было включено.

Они также установили в номере жертвы скрытую камеру наблюдения, чтобы с ее помощью увидеть и украсть ее пароли.

□ Фаза 4: Кредитные карты.

Итак, теперь у них был доступ к ее MacBook. Но им хотелось большего: ее кредитных карт, ее учетной записи в социальных сетях, возможно, даже видео и записей с микрофона.

Используя вредоносное ПО, они вывели форму на экране жертвы, чтобы вывести ее root-пароль, отобразив диалоговое окно с просьбой этот пароль ввести.

Получив root-права, они могли установить кейлоггер, который передавал каждую нажатую клавишу.

Жертва забронировала поездку на Кубу с помощью своей кредитной карты, и теперь наши «белые» хакеры имели все ее реквизиты. Она написала что-то в «Твиттере», и они узнали ее пароль от аккаунта.

□ Фаза 5: Захват ее видео.

Современные компьютеры Mac имеют светодиодный индикатор, показывающий, когда камера включена, и она управляется прошивкой, которую сложно изменить, не выполнив полную сборку прошивки.

Поэтому исследователи просто включали запись, когда камера использовалась самой жертвой, — например, когда она разговаривала по Skype со своим парнем.

□ Итог.

Встретившись с Джанной, пентестеры сказали:

«Вот тебе российский флаг, Джанна. Извини. Но мы купили его с помощью твоей кредитной карты. После того как ты оплатила нашу поездку в Uber. И мы написали об этом в твоём “Твиттере”».

Неприступная крепость

Однажды коллега позвал меня на встречу в крупную организацию, где он работал, т. е. это был не пентест. Пропуска у меня не было, и по регламенту охрана предложила мне ожидать, пока за мной не придут. Чтобы не терять время зря, я стал смотреть по сторонам. Схема того, что я наблюдал, показана на рис. 3.9 (наконец, пригодился iPad, брал его для рисования схем, но за полгода эта схема оказалась первой).

Справа от входа были расположены диваны, что-то вроде искусственной перегородки, перепрыгивая через которую ты точно привлечешь внимание. А вот знаком вопроса отмечено место, которое я сфотографировал (рис. 3.10).

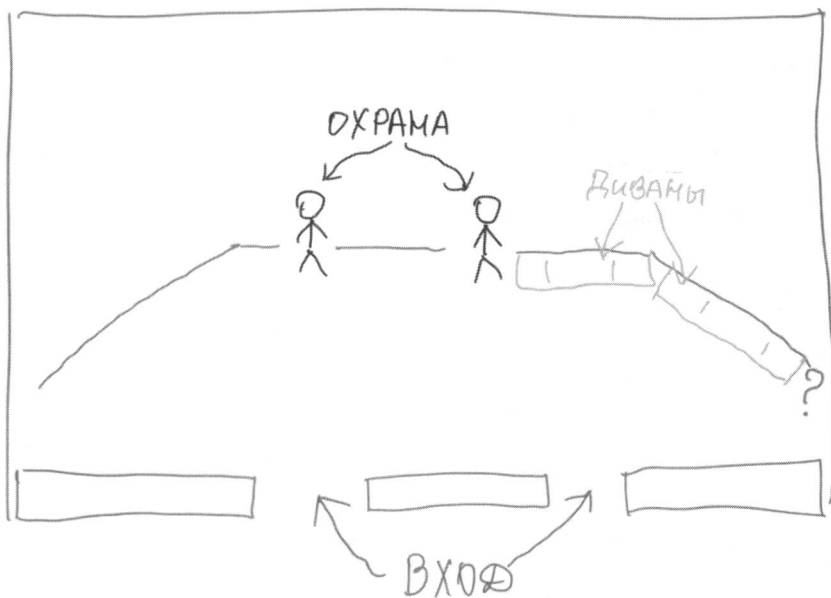


Рис. 3.9. Схема расположения объектов при входе в периметр здания



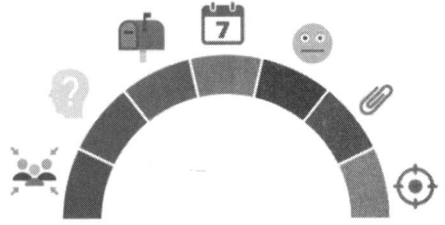
Рис. 3.10. Место обхода — справа от дивана

То есть даже в охраняемом здании с единственной организацией, которая занимает много этажей, можно обойти проходную справа от дивана.

Наблюдают ли за мной, помимо охраны, еще и камеры, я проверять не стал, ведь причина моего нахождения в здании была не в этом. Но для интереса стал смотреть, появится ли в принципе тот момент, когда оба охранника не будут смотреть в мою сторону. И да, было секунд пять, когда один охранник смотрел в пакет проходящего, а второй повернулся ко мне под углом 90° , плюс было обеденное время, и на проходной находилась пара десятков сотрудников.

Пришли вы куда-то для пентеста или нет, просто смотрите по сторонам, ищите уловки, развивайте наблюдательность — это полезно.

Глава 4



Проведение онлайн-атак по email

Независимо от того, безопасник вы или пентестер, — эта глава пригодится всем.

Мы не станем здесь рассматривать способы отправки сообщений в мессенджерах или соцсетях, основной канал межкорпоративного общения — это email. Тем не менее принцип атаки по email тот же, что и по другим электронным каналам.

Что же касается офлайн-векторов, то если представители службы ИБ не планируют одеваться в длинные кожаные плащи, прикрываться зеркальными очками и пытаться проникнуть в свою же организацию, то лучше доверить это профессиональным пентестерам. Но как минимум флешки поразбрасывать можно — например, с записанными на них файлами с трекерами, созданными с помощью сервиса canarytokens.org.

Однако вернемся к онлайн-проверкам осведомленности. Для проведения имитированной атаки по email с использованием электронной СИ нам понадобятся:

- софт;
- список email-пользователей;
- составленные векторы атак для рассылки.

Чтобы результаты были чистыми, о том, что будут проводиться учебные атаки, сотрудников мы не предупреждаем.

Какой софт использовать?

Вот перечень бесплатного ПО:

- Gophish (<https://getgophish.com>) — распространенный фреймворк для рассылки классического фишинга;
- King-phisher (<https://github.com/rsmusllp/king-phisher>) — знаю одного человека, который это использует :-);

- ❑ StopPhish (<https://stopphish.ru/ds>) — наше бесплатное ПО для проверки осведомленности пользователей. Оно несколько функциональнее аналогов, на русском языке, включено в реестр отечественного ПО.

Список email-пользователей

Если вы хотите отправлять именные сообщения (рекомендуется), то загрузите в рассылочную программу таблицу следующего вида (рис. 4.1).

Андрей	Andrey@yandex.ru
Анна	Anna@yandex.ru
Игнат	Ignat@yandex.ru
...	...

Рис. 4.1. Пример таблицы с вводными данными

Вы можете разнообразить письма, используя Ф.И.О. и названия подразделений, — для этого добавьте в таблицу соответствующие поля.

Впрочем, для имитации массовой СИ достаточно будет списка email.

Как создавать сообщения для атак?

Для удобства чтения книги некоторые материалы и инструкции вынесены в приложения, чтобы не дублировать их тут.

Если же взять все возможные комбинации сценариев, которые можно создать на основе того же «Классификатора СИ» (см. *приложение 2*), то получится свыше 100 тыс. вариантов — этого более чем достаточно, чтобы отправить по одному уникальному сценарию каждому жителю Королевства Тонга.

Для создания онлайн-вектора вам пригодятся:

- ❑ «Генератор онлайн-СИ» (см. *приложение 1*);
- ❑ «Таблица персонализации» (см. *приложение 3*);
- ❑ уже упомянутый ранее «Классификатор СИ» (см. *приложение 2*).

На их основе вы сможете составлять письма наподобие представленных далее:

- ❑ **Пример 1:** письмо для кражи учетных данных (рис. 4.2).
- ❑ **Пример 2:** письмо, к которому прикладывается файл с макросом (рис. 4.3).
- ❑ **Пример 3:** письмо с файлом для скачивания на поддельном сайте (рис. 4.4).

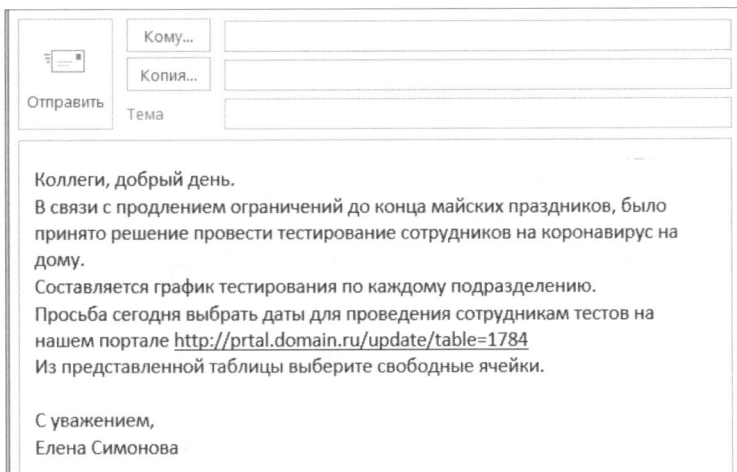


Рис. 4.2. Пример фишингового письма, нацеленного на кражу учетных данных

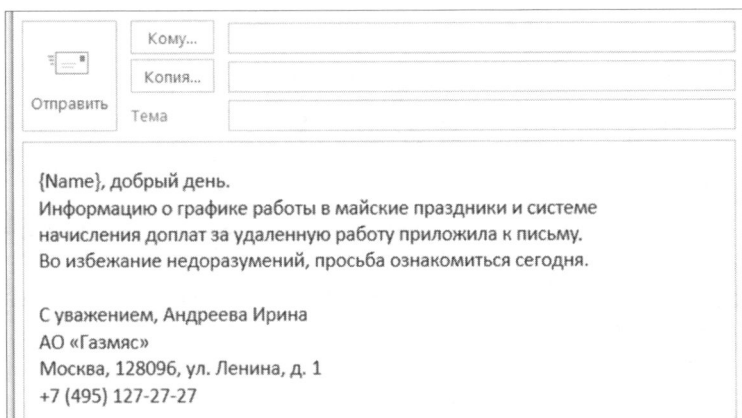


Рис. 4.3. Текст письма, к которому прикладывается файл с «вредоносным» содержимым

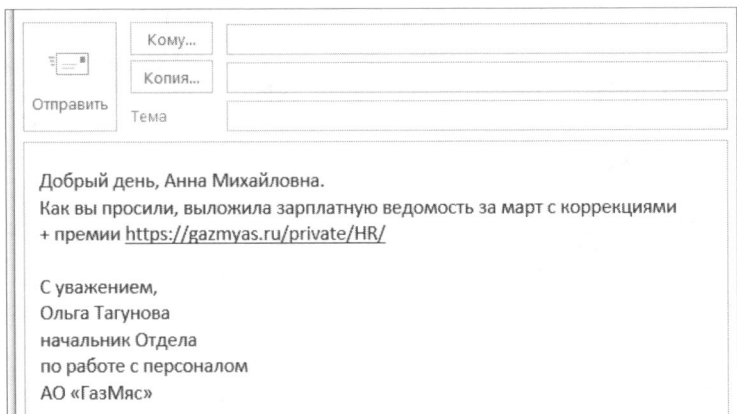


Рис. 4.4. Текст письма, имитирующего ошибочную отправку данных о зарплате, предназначавшегося главному бухгалтеру

Чек-лист применения электронной СИ

Последовательность основных шагов при подготовке атаки на основе электронных средств коммуникации:

1. Подбираем список пользователей.
2. Выбираем тип СИ (массовая, таргетированная, смешанная).
3. Выбираем направление (от кого идет коммуникация).
4. Создаем отправителя сообщения.
5. Готовим нагрузку (ссылка, фишинговая форма, файл).
6. Подбираем контекст (повод для сообщения).
7. Подбираем усилитель контекста (используем эмоции).
8. Пишем текст сообщения.
9. Оформляем сообщение (стиль, подпись).
10. Отправляем сообщения.
11. Для службы ИБ: сводим результаты в отчет.
12. Для пентестера: в зависимости от условий пентеста развиваем атаку дальше, используя полученные данные, или сводим результат в отчет.

Как повысить киберграмотность сотрудников?

Этот раздел больше подойдет для службы ИБ или ИТ (в зависимости от того, на кого возложено обеспечение информационной безопасности), т. к. когда мы узнаем, кто в организации попался на социальную инженерию, то с этими пользователями придется что-то делать, чтобы в случае реальной атаки снизить риск взлома ИТ-инфраструктуры.

Работа пентестера же обычно имеет другие цели — ведь, например, скомпрометированные учетные данные могут быть лишь начальной стадией пентеста.

Итак, когда вы проведете первые три учебные атаки, у вас появится фактура и конкретный процент попавшихся вместе с их Ф.И.О. (рис. 4.5).

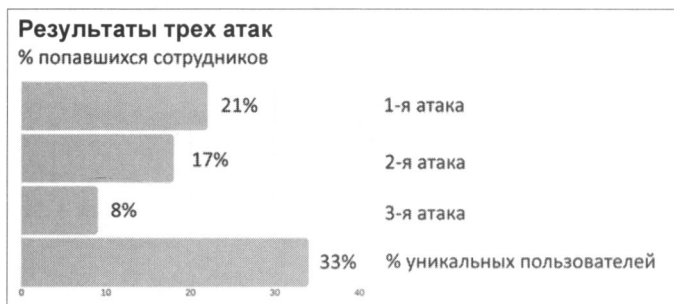


Рис. 4.5. Результаты проведенных учебных атак

Следующий шаг — пойти и отчитаться руководству, получить бюджет на повышение осведомленности, нанять исполнителей на аутсорсе и получать отчеты. Оптимистично? Согласен.

Рассмотрим сценарий, когда вам сказали, что вы молодец, и пожелали удачи в исправлении ситуации, не выделив бюджет.

Нам нужен план. Чтобы снизить количество инцидентов на основе человеческого фактора, мы обычно делаем так:

1. Получаем одобрение от руководства на проведение мероприятий по повышению осведомленности.
2. Пишем 28–56 писем на год вперед (от легких сценариев к сложным).
3. Предупреждаем пользователей об атаках (если нужно будет, напишите, я скину пример такого письма).
4. Делаем доступными обучающие материалы.
5. Если не обучали ранее, рассылаем обучающие курсы по одному в неделю.
6. Рассылаем письма в соответствии с графиком — 2–4 письма в месяц. Если не будет регулярности, результаты окажутся гораздо хуже.
7. Ежемесячно/ежеквартально сводим результаты в отчет о прогрессе мероприятий по повышению осведомленности.

Вот такие графики (рис. 4.6) уже можно показывать руководству. Обратите внимание, что руководителям нужно показывать растущие графики — т. е. называем эту сводку не «Процент инцидентов по векторам атак», а, например, «Процент эффективно обученных пользователей по различным векторам атак».

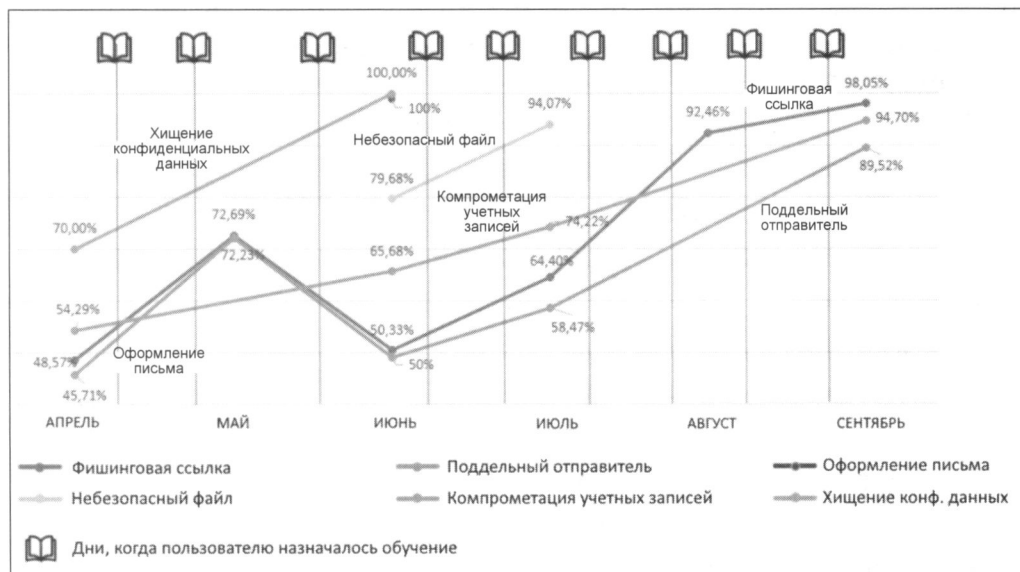


Рис. 4.6. Результаты учебных атак и обучения с течением времени

ПРИМЕЧАНИЕ

Поскольку книга издается не в цветном варианте, названия графиков для ясности продублированы рядом с ними. На реальном отчетном документе это делать не обязательно.

Технические аспекты обучения

Есть два варианта обучения:

- использовать бесплатное ПО для рассылки писем (наше или другое Open Source решение) и отдельно отправлять ссылки на курсы тем, кто попался. Атаки можно делать так, чтобы попавшийся пользователь сразу же переадресовывался на онлайн-курс;
- купить расширенный вариант ПО у нас или у других вендоров и автоматизировать повышение осведомленности.

Критерии выбора платформы по повышению осведомленности вы можете найти в *приложении 5*.

Если вам необходимы курсы, которые нужно отправлять попавшимся сотрудникам, то два базовых курса вы можете получить у нас (см. *приложение 4 «Бесплатное в помощь службе ИБ и ИТ»*). Там рассмотрены следующие темы:

- как распознать вредоносное вложение в письме;
- как распознать вредоносную ссылку в письме.

Этого вполне достаточно, чтобы обучить пользователей самым распространенным векторам онлайн-атак и их распознаванию.

Вообще, на текущий момент нами создано 19 курсов, которые покрывают большую часть задач по осведомленности пользователей. Вы можете собрать свой сборник курсов на основе следующих тем и добавить к ним свои:

- Базовые правила информационной безопасности.
- Вводный курс по ИБ для новых сотрудников.
- Как распознать вредоносное вложение в письме.
- Как распознать вредоносную ссылку в письме.
- Как хакеры выдают себя за других.
- Определяем хакерское письмо по тексту.
- Личная информационная безопасность.
- Противодействие сценариям Find trap.
- Четыре вредоносных сценария, которые используют злоумышленники.
- Блокировка экрана компьютера.
- Как хакер может испортить вам жизнь.
- Как хакеры входят в доверие.

- Опасность найденных USB-устройств.
- Политика чистого стола.
- Безопасное хранение пароля.
- Работа с ПК (ПО, флешки, хранение данных).
- Базовые правила работы с конфиденциальной информацией.
- ИБ на рабочем месте.
- Безопасная работа с электронной подписью.
- Мобильная безопасность.

И четыре специфических курса:

- КИИ.
- GDPR.
- 152-ФЗ.
- АСУ ТП.

Курсы составлены согласно «Классификатору СИ» (см. *приложение 2*) так, чтобы они покрывали порядка 100 тыс. сценариев социальной инженерии. Остальные угрозы вы можете перекрыть технически.

Вообще-то, технической защите от СИ, процессу повышения осведомленности и методологии решения нестандартных ситуаций можно посвятить отдельную книгу, но кое-что мы уже раскрыли и в этой.

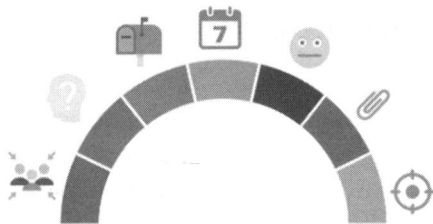
По поводу нестандартных ситуаций — действительно, бывало всякое:

- в одной организации сотрудники игнорировали назначенное обучение, и там попадались до 99,5% пользователей;
- в другой — сотрудники добавили email службы безопасности в «черный список», чтобы не получать «назойливые письма от ибэшников, мешающих работать».

Если вам будет интересно, несколько наших кейсов можно посмотреть здесь: <https://stopphish.ru/#rec275132752>.



Глава 5



Технические меры противодействия СИ

В этой главе мы рассмотрим некоторые аспекты защиты от социальной инженерии и фишинга с помощью технологических решений. Естественно, нельзя охватить все комбинации средств защиты в разных организациях и тем более дать конкретные настройки. При этом надо учесть, что программного обеспечения, защищающего конкретно от фишинга, в России единицы. Но некоторые решения и рекомендации, включая опыт коллег из-за рубежа, я постараюсь раскрыть. Как минимум будет от чего оттолкнуться.

Хочу также отметить, что вы наверняка используете какие-то решения в своей организации. Вы можете прислать мне свои отзывы с рекомендациями о том, что еще можно добавить в эту главу для будущих переизданий книги. Ведь когда мы делимся опытом с коллегами, то делаем вклад в безопасность всей страны и нашу личную безопасность в частности.

Софт

В этом разделе представлены либо конкретные вендоры ПО, либо практики, рекомендованные к внедрению и реализуемые с помощью ПО. Если указывается зарубежный вендор, то у своего интегратора вы можете запросить его аналог. Помимо конкретного ПО, мы обсудим и некоторые практики, которые внедряются с помощью ПО, опять же в разрезе защиты от СИ.

Корпоративный браузер

Израильская компания Island (island.io) выпустила корпоративный браузер, который, по их словам, является революцией XaaS (Everything as a Service, всё как сервис).

Некоторые возможности этого браузера: контроль всего, что происходит внутри браузера, подробный обзор всей активности, использование концепции нулевого доверия и — что важно в контексте этой книги — защита от фишинга.

Сегментация сети и Zero Trust

Для минимизации потерь организации следует выстраивать инфраструктуру по принципу Zero Trust, когда по умолчанию считается, что все рабочие машины и серверы уже взломаны, а вместо пользователей за ПК сидят хакеры. Для этого необходимо разбить сеть на мелкие сегменты, где каждый пользователь имеет минимальное количество прав. Сегментация поможет защититься не только от злоумышленников, но и предотвратит крах всей ИТ-системы в случае технической или человеческой ошибки.

На «Хабре» есть полезная статья на этот счет: «Сегментация сети для самых маленьких» (<https://habr.com/ru/articles/588705/>).



Невозможность залогиниться в почте с недоверенных IP-адресов

В случае, когда злоумышленник украдет логин и пароль вашего сотрудника и захочет войти в почту для проведения, например, ВЕС-атаки, можно усложнить ему жизнь, сделав авторизацию на ресурсах организации через тот же VPN.

Если у вас есть VPN-шлюз или Firewall с возможностью организовать удаленный доступ, то это хорошо. Если нет, можно использовать Open Source продукты: OpenVPN, SoftEther VPN и подобные.

Больше подробностей вы можете получить из статьи: «Как организовать удаленный доступ и не пострадать от хакеров» (<https://habr.com/ru/companies/jetinfosystems/articles/492872/>).



Обнаружение повторного использования пароля

В StopPhish мы сделали пока еще бесплатный плагин для браузера, который сигнализирует в службу ИБ о случаях повторного использования пароля. Плагин фиксирует, когда пользователь вводит пароль, например, от корпоративного портала, на любом другом сайте.

Зарубежный аналог этого плагина от компании Palantir называется PhishCatch (<https://github.com/palantir/phishcatch>).

В нашем решении, в отличие от PhishCatch, мы не обрабатываем и соответственно не сохраняем, введенный пользователем пароль. Нам достаточно лишь события, что пользователь что-то вводил в поле пароля на каком-то сайте.

Это еще не революция по борьбе с фишингом, но разработка определенно перспективная.

Фиды о фишинге

В этом разделе опишу некоторые источники данных, из которых можно пополнять свою базу фишинговых атак, чтобы своевременно блокировать угрозы для своей организации. Здесь указаны те сервисы, которые я проверил, и они действительно дают/продают данные на момент издания книги. К сожалению или счастью, ранее известные поставщики фидов превратились в продуктовые компании и перестали делиться данными.

- ❑ Kaspersky Phishing URL Data Feed — подписка на данные о доказанных фишинговых URL, масках и IP-адресах, обновляемые в режиме реального времени.
- ❑ OpenPhish — база данных OpenPhish предоставляется в формате базы данных SQLite и может быть легко интегрирована в существующие системы с помощью модуля API с открытым исходным кодом.
- ❑ PhishTank — ресурс для обмена данными и информацией. Кроме того, он предоставляет разработчикам и исследователям открытый API для бесплатной интеграции антифишинговых данных в свои приложения.
- ❑ SpamCop — интернет-сервис, помогающий выявлять и сообщать о спаме и фишинге в электронной почте.
- ❑ Spamhaus Project — некоммерческая организация, отслеживающая спам и связанные с ним киберугрозы, такие как фишинг, вредоносное ПО и ботнеты. Публичное зеркало предоставляется бесплатно для некоммерческого использования малыми и средними организациями.
- ❑ VirusTotal — крупнейшая краудсорсинговая база данных вредоносных программ и вредоносных сайтов.
- ❑ PhishStats — канал данных в реальном времени. Он собирает и объединяет данные о фишинге из нескольких источников, таких как VirusTotal, Google Safe Search, ThreatCrowd, abuse.ch и antiphishing.la.
- ❑ AlienVault OTX — сообщество по анализу угроз. Обеспечивает открытый доступ к глобальному сообществу исследователей угроз и специалистов по безопасности.
- ❑ Phishing.Database — хранилище фишинговых доменов, веб-сайтов и угроз.
- ❑ Google Safe Browsing — API безопасного просмотра, предназначенные только для некоммерческого использования.

Антифишинговый шрифт

Вы можете установить определенный шрифт по умолчанию для почтовых клиентов, который поможет пользователям различать фишинговые домены, похожие на официальные.

На рис. 5.1 приведены примеры отображения символов в зависимости от используемого шрифта.

Антифишинговый шрифт

Не секрет, что злодеи могут подменять символы в ссылках на похожие. Посмотрим, как может помочь изменение шрифта для распознавания подлога.

Исходные буквы и цифры:

I – латинская «И» большая

i - латинская «и» маленькая

l - латинская «л» маленькая

1 - единица

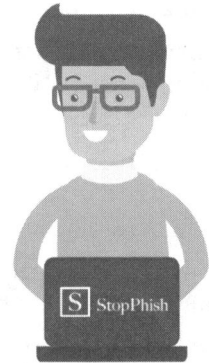
lil1 – Arial – «И» и «л» можно спутать. Paypal.com

Iil1 – Times New Roman – «л» и «1» можно спутать. Paypal.com

lil1 – Calibri – «И» и «л» можно спутать. Paypal.com

Iil1 – Courier New – «л» и «1» можно спутать, но уже лучше. Paypal.com

Iil1 – Tahoma – все буквы отличаются. Paypal.com



В

Рис. 5.1. Демонстрация отображения символов у разных шрифтов

Outlook это настраивается так — выберите **Файл | Параметры | Почта | Шрифты и бланки**.

Насколько я понял, Outlook не меняет шрифт для входящих HTML-сообщений, но для текстовых всё работает. А как раз массовые атаки часто осуществляются с помощью текстовых сообщений, поскольку в них меньше сигнатур для анти-спам систем.

Помимо этого, если в вашей организации не используется брендбук, то установка такого шрифта для новых писем поможет во внутренних переписках сотрудников. В том числе и при отправке HTML-писем. Если одного сотрудника взломают и отправят от его имени ссылку, то второй получит сообщение с «антифишинговым» шрифтом.

Настройка DKIM, SPF и DMARC

Настройка этих записей — это уже некий маст-хэв в защите электронной почты.

- DKIM — метод e-mail-аутентификации, разработанный для обнаружения подделки электронных писем.
- SPF — расширение для протокола отправки email через SMTP. С помощью SPF можно проверить, не подделан ли домен отправителя.

- ❑ DMARC — это техническая спецификация, предназначенная для снижения количества фишинга и спам-писем.

Как видно из приведенных описаний, такие настройки для домена вашей организации могут помочь в отражении некоторого количества угроз.

О непосредственной настройке этих подписей и записей можно почитать в статье: «Настройка DKIM/SPF/DMARC записей, или Защищаемся от спуфинга» (<https://habr.com/ru/articles/322616/>).



Как рекомендуется в статье, если и внедрять эти политики, то все три сразу, а не ограничиваться одной-двумя.

И еще, обязательно настройте DMARC для поддоменов, чтобы избежать подмены почты не только с основного домена.

Предотвращение выполнения исходного кода

Национальный центр кибербезопасности Великобритании (nsc.gov.uk) дает некоторые рекомендации о том, как снизить риски ИБ в случаях, когда сотрудник запускает вредоносный файл из вложения к письму, качает его на подозрительном сайте или приносит из дома на флешке.

- ❑ Создать список разрешенных к запуску расширений, чтобы гарантировать, что исполняемые файлы не могут запускаться из любой папки и каталога.
- ❑ Для всего, что не включено в список разрешенных расширений, использовать настройки реестра, гарантирующие, что опасные сценарии или типы файлов открываются в Блокноте и не исполняются. Для PowerShell вы можете минимизировать риск, используя ограниченный режим PowerShell.
- ❑ Отключить монтирование файлов *.iso на ПК пользователей.
- ❑ Убедиться, что запуск макросов заблокирован, или сделать так, чтобы эта возможность была только у сотрудников, которым они абсолютно необходимы. Разумеется, они должны быть обучены рискам, которые представляют макросы (и, в принципе, любое небезопасное содержимое в документах — например, PDF-файлы).
- ❑ Включить правила уменьшения поверхности атаки (см. статью от Microsoft на английском: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction>).

Чтобы не перепечатывать такую длинную ссылку в ваш браузер на ПК, погуглите: Attack surface reduction rules overview или перейдите по QR-коду.



- ❑ Обязательно обновлять стороннее программное обеспечение — например, программы для чтения PDF-файлов, или, что еще лучше, используйте для открытия таких файлов браузер.
- ❑ Будьте в курсе текущих угроз и более подробно узнавайте о любых новых векторах атак.

Последний пункт звучит как «мыслите позитивно» — т. е. эта рекомендация настолько обширна, что не знаешь, с какой стороны подойти.

Но как минимум всегда можно поискать на <https://nvd.nist.gov/vuln/search> используемое в организации ПО и попытаться защититься еще до того, как выйдет обновление безопасности.



Например, раз мы говорим о фишинге и СИ, на момент подготовки книги в этой базе есть информация CVE-2023-30433 об уязвимости IBM Security Verify Access 10.0, которая может позволить удаленному злоумышленнику проводить фишинговые атаки, используя атаку с открытым редиректом. Убедив жертву посетить специально созданный веб-сайт, злоумышленник сможет использовать эту уязвимость для подмены отображаемого URL и перенаправления пользователя на вредоносный веб-сайт.

Можно также подписаться на фид от ФинЦЕРТ (https://cbr.ru/information_security/fincert), если для вашей организации это имеет интерес. Насколько я понял, там можно получить сотни фишинговых писем, включая актуальные на настоящее время атаки.



Также можно мониторить «Банк данных угроз безопасности информации» от ФСТЭК (<https://bdu.fstec.ru/vul>), где описана, например, BDU:2023-02385 — уязвимость компонента Prompts браузера Google Chrome. Указанная уязвимость связана с некорректно реализованной проверкой безопасности для стандартных элементов, и ее эксплуатация может позволить нарушителю, действующему удаленно, проводить фишинг-атаки с помощью специально созданной HTML-страницы.



SSO

Single Sign-On — это метод аутентификации, который дает пользователям возможность безопасно войти в несколько приложений и веб-сайтов, используя одну пару логина и пароля.

Такая технология часто используется в организациях. С одной стороны, пользователю не нужно помнить несколько паролей, а утерянный пароль можно легко восстановить силами поддержки организации. С другой стороны, один пароль для всех служб — это как мастер-ключ в менеджере-паролей: узнал один пароль, узнал и остальные.

Я не против такого подхода, но нужно понимать, что пользователь должен быть осведомлен о сложности паролей, их хранении, возможностях утечки и т. д.

Дополнительной защитой при использовании SSO является использование одноразовых паролей. Их можно установить при входе в более чувствительные сервисы.

Помимо этого, кражу пароля можно предотвратить, если использовать качественных поставщиков SSO.

Sandbox

Так называемые песочницы запускают программы, открывают файлы и ссылки в изолированной виртуальной среде. Если пользователь запустит макрос в офисном документе, находясь в такой среде, то тем самым будет снижен шанс появления на компьютерах организации красной плашки с надписью о расшифровке файлов за несколько биткоинов.

Последовательность фильтрации того же почтового трафика обычно реализуют таким образом: антиспам-фильтры → брандмауэр (Firewall) → прокси-сервер → антивирус → песочница.

Больше об этом можно узнать из статьи: «Какие варианты “песочницы” (Sandbox) существуют и как экономить на внедрении» (https://www.anti-malware.ru/analytics/Technology_Analysis/What-sandbox-options-exist).



Технические аспекты защиты от СИ

Представляю вашему вниманию чек-лист по некоторым техническим аспектам защиты от социальной инженерии и фишинга.

Способы применения чек-листа

1. Убедитесь, что ваша система предотвращения вторжений, антиспам, сетевой экран или другие уместные системы сработают при различных методах показанной здесь визуальной и технической маскировки ссылок, вложений и текста сообщений.
2. На многих пунктах чек-листа можно строить собственные учебные материалы для повышения осведомленности сотрудников.
3. Корректировка внутренних регламентов и политик. Например, какая-то группа пользователей может отправлять или принимать определенные вложения или ссылки, а другая не может.

Выбирайте методы фильтрации вредоносного содержимого в зависимости от вашей тактики

1. Всё запрещено, и отдельные элементы разрешены.
2. Всё разрешено, и отдельные элементы запрещены.

Настройте защиту от фишинговых ссылок

1. Ссылки с символом @. Например: <https://yandex.ru:news-1421@yanedx.ru>.
2. Слеш в Unicode. Чаще всего комбинируется с символом @ в ссылке: <https://www.ya.ru/news:in@yanedx.ru>. Код символа: U+0B75.
3. С обфускацией IP через urlencode. Например, IP-адрес **mail.ru** может выглядеть так:
<https://0xd9.0x45.0x8b.0xca/company.ru>,
<https://0331.0105.0213.0312/google.ru>, <https://3645213642/ya.ru>
 + комбинация этих способов маскировки.
4. QR-коды в теле письма.
5. Текстовые ссылки в виде картинок в теле письма.
6. Некорректный синтаксис в атрибуте href HTML-тега <a>. Например: <http:\bank.ru>, <http:/bank.ru>, <//bank.ru>, <https://bank.com>, <https://bank.com>, <https://bank.com>. Домен нулевого уровня не относится к некорректному синтаксису, но его могут небезопасно обработать ваши ИТ-системы, — например: reg.ru/vps работает так же, как reg.ru/vps.
7. Ссылки в документах во вложении (PDF, DOC, EML, MSG и другие).
8. Очень длинные. Применяются, например, с символом @:
<http://yandex.ru.668-sdfsadf-ajay.com-123788125-ajay-asjjba.com-sdmasdlhuaoqw@zlo.ru/sdfsadf-ajay-asjjba.com/sdmasd.ru-lhuaoqw#sdfsadf-ajay-asjjbasdmasdlhuaoqw?sdfsadf-ajay-asjjba123955w&sdfsadf-ajay-asjjbasdmasdlhuaoqw>.
9. IP вместо домена. Например: <https://94.100.180.201/>
10. Редиректы: видимые <https://ya.ru/?r=bit.ly/12365>, скрытые <https://ya.ru/?r=12365>.
11. Неактивные. Ссылка не работает при клике на нее, что побуждает скопировать ссылку и вставить в браузер. например: yadnex.ru.
12. Домен совместно с типе: yandex.ru-auth.online.
13. Официальные домены в других доменных зонах.
14. В поддоменах. Пример: <https://yandex.ru.yanexd.ru>.
15. Текст ссылки один, а атрибут href отличается. Например, в письме видим ссылку <https://ya.ru>, которая на самом деле ведет на <https://yo.ru>. Не путайте со случаями, когда ссылка прописана, например, в виде текста, а не как URL, иначе будет много ложных срабатываний.
16. Кириллические. Используется совместно с другими способами маскировки. Например, домен **кто.рф** переводим в rунусcode и получаем: **xn--j1ail.xn--p1ai**. Теперь его можно использовать в редиректах: <https://ya.ru/?r=xn--j1ail.xn--p1ai> или задействовать urlencode и получить <http://%D0%BA%D1%82%D0%BE.%D1%80%D1%84>.

Ссылки, похожие на официальные сайты

1. Добавление цифр: **domain1.com**.
2. Разбавление с помощью точки или тире: **d.oma-in.com**.
3. Использование поддомена: **domain.com.email.online**.
4. Повторение символов: **dommain.com**.
5. Добавление приставок WWW, HTTP(S), WEB, ONLINE: **wwwdomain.com**, **https-domain.com**, **domain-online.com**.
6. Использование омоглифов (похожие символы из других алфавитов): **domaiṇ.com**, замена символов на похожие: вместо **good.local.domain.com** → **good.local.d0rnaj̣n.com**.
7. Замена гласных: **damain.com**.
8. Замена доменной зоны: **domain.online**.
9. Пропуск символов: **doman.com**.
10. Перестановка символов: **donaim.com**.

Настройте защиту от вредоносных вложений

Опасные расширения (я перечисляю, а вы решите, какие из них нужно блокировать в 100% случаев или разрешить для части пользователей. Например, у вас в организации могут использоваться расширения *.000, *.001 и т. д.):

ACCDB, ADE, ADP, APK, APPX, APPXBUNDLE, BAT, CAB, CHM, CMD, COM, CPL, DLL, DMG, EXE, HTA, INS, ISP, ISO, IMG, JAR, JS, JSE, LIB, LIBRARY-MS, LNK, MDE, MSC, MSI, MSIX, MSIXBUNDLE, MSP, MST, NSH, PIF, PS1, SCR, SCT, SEARCHCONNECTOR-MS, SHB, SYS, VB, VBE, VBS, VSDM, VSSM, VXD, WSC, WSF, WSH.

Возможные к запрету расширения, используемые в фишинге

1. SHTML, HTML, HTM, XHTML, MHTML.
2. Файлы с расширениями из приведенного ранее списка, включая сжатые (например, GZ или BZ2) и помещенные в архив (например, ZIP или TGZ).
3. Архивы, защищенные паролем.
4. Архивы, содержащие защищенные паролем архивы.
5. Документы с макросами.
6. Документы с макросами в архиве.

Настройте проверку заголовков email на подозрительные признаки

1. Reply-To и From не совпадают.
2. В поле Received один отправитель, а в From — другой.

Настройте защиту по содержимому письма

Эти методы маскировки будут использоваться скорее при массовых атаках или спаме:

1. Текст письма содержит цифры вместо букв: Оповещение, Добрый.
2. Латинские буквы вместо русских: Добрый день.
3. Юникод-буквы вперемешку с обычным алфавитом: Ответ на письмо.
4. Разбавление символами: Доб_рый д ень.

Hardware

Как и в *разд. «Софт» этой главы*, мы попытаемся рассмотреть здесь защиту не от всех угроз информационной безопасности, а ту ее часть, которая касается социальной инженерии и фишинга.

Межсетевые экраны

У разных производителей брандмауэров могут быть реализованы следующие функции. При этом нет смысла перечислять конкретные бренды — вы просто можете вписать указанные пункты в ТЗ при закупке или произвести настройку уже купленного устройства, если такая функциональность в нем предусмотрена.

❑ *Блокировка использования одинакового пароля на разных ресурсах.*

Некоторые брандмауэры обладают функцией сканирования логинов и паролей, которые пользователи вводят на сайтах в Интернете, сравнивая их с данными, вводимыми ими на сайтах организации. При выявлении таких действий сессия блокируется, и данные не уходят на фишинговый сайт. Можно сравнивать как домены сайтов, так и IP-адреса.

❑ *Использование black-листов.*

Сгенерируйте домены, похожие на домен вашей организации, с помощью сервиса <https://dnstwister.report> и добавьте в «черный список».

Несколько слов о сервисе **dnstwister.report** и его аналоге **dnstwist.it**. Они генерируют домены несколькими способами. Вариантов написания вашего легитимного домена может получиться больше тысячи, и будет опрометчиво добавлять их все в «черный список». Но как минимум вы можете посмотреть, какие домены, похожие на ваши, уже зарегистрированы, проверить их и заблокировать межсетевым экраном.

Затем я бы заблокировал домены во всех 1500+ доменных зонах, если в моем домене используется название бренда, — например, **stopphish.xyz**. Потом заблокировал бы домены, выполненные в виде поддоменов, вроде таких — **stopph.ish.ru**. И завершил бы это блокировкой доменов с омоглифами (символами из других алфавитов) — например, **stopphish.ru**.

❑ Фиды с фишинговыми сигнатурами.

В брандмауэрах также можно использовать фиды о фишинге, которые мы рассмотрели ранее в разд. «Софт».

Здесь можно добавить ссылку на еще один источник баз Threat Intelligence — IPsum (<https://github.com/stamparm/ipsum>), канал анализа угроз, основанный на более чем 30 различных общедоступных списках подозрительных IP-адресов, т. к. эксперт по ИБ Денис Батранков упоминал его именно в разрезе использования в межсетевых экранах.

FIDO

FIDO (Fast IDentity Online) — это стандарт безопасности для аутентификации в Интернете (<https://fidoalliance.org/specifications>).

Альянс FIDO опубликовал три набора спецификаций для более простой и надежной аутентификации пользователей:

❑ FIDO U2F, Universal Second Factor — универсальный второй фактор.

FIDO U2F поддерживает второй фактор аутентификации и позволяет онлайн-сервисам повысить безопасность существующей инфраструктуры паролей, добавив такой второй фактор ко входу пользователя. Пользователь входит в систему с именем пользователя и паролем, но служба также может предложить пользователю использовать второе факторное устройство, — например, ключ безопасности FIDO.

Во время регистрации и аутентификации пользователь предоставляет второй фактор, просто нажимая кнопку на USB-устройстве или касаясь приемника сигнала устройством с чипом NFC или BLE (Bluetooth Low Energy, Bluetooth с низким энергопотреблением). Пользователь может использовать свое устройство FIDO U2F во всех онлайн-сервисах, поддерживающих этот протокол, ориентируясь на встроенную поддержку браузера.

❑ FIDO UAF, Universal Authentication Framework — универсальная платформа аутентификации.

FIDO UAF — открытая спецификация, которая позволяет онлайн-сервисам выполнять аутентификацию без пароля. При использовании FIDO UAF пользователь носит с собой устройство с установленным стеком FIDO UAF.

❑ FIDO2, Client to Authenticator Protocols (CTAP) — протоколы взаимодействия клиента с аутентификатором. CTAP дополняет спецификацию веб-аутентификации W3C (WebAuthn), и вместе они известны как FIDO2.

Различия между UAF, U2F и FIDO2

Используя UAF, пользователь аутентифицирует устройство с помощью веб-сайта и в дальнейшем задействует биометрические данные с этого устройства, — ему будет необходимо только локально с него аутентифицироваться.

При использовании U2F служба дополнительно может запросить второй фактор. В этом случае у пользователя должен быть брелок, USB-флешка или другое устройство для входа в систему или регистрации на нем. Это увеличивает вероятность того, что только вы получаете доступ к своей учетной записи, поскольку для входа в систему вам потребуется более одного устройства.

FIDO2 поддерживает беспарольный, двухфакторный и многофакторный пользовательский интерфейс со встроенными или привязанными аутентификаторами (такими как биометрические данные или ПИН-коды) или внешними аутентификаторами — такими как ключи безопасности FIDO, мобильные и другие носимые устройства.

Беспарольная аутентификация исключает пароли как слабое звено в безопасности и делает фишинг учетных данных невозможным, а также предотвращает MiTM и утечки паролей.

В Google U2F используют более 85 тыс. сотрудников. За год работы у них не было ни одного подтверждения о краже аккаунтов с момента внедрения ключей безопасности. В общем, такое количество сотрудников дает нам достаточно достоверные статистические данные о работоспособности технологии.

Недостатки этого способа защиты

- ❑ Затраты — FIDO2 может стоить дороже, чем распространенные методы защиты.
- ❑ Время — внедрение FIDO в процессы организации может занять больше времени, чем внедрение привычных систем аутентификации.
- ❑ Межсайтовая поддержка — при организации доступа с несколькими ресурсами организации все они должны реализовать одинаковую аутентификацию. Если способы доступа к закрытым ресурсам будут разными, то не стоит тратить время на внедрение этой технологии.

ОТР-токены

Системы на ОТР-токенах и FIDO2/U2F принципиально различаются.

ОТР-токен (One-Time Password) — это генератор одноразовых паролей, он может быть как аппаратным (в виде носимого устройства), так и выполненным в виде приложения — например, Google Authenticator.

Используя связку: логин/пароль + одноразовый код, вы несколько усложняете жизнь преступнику. Если в вашей модели угроз этот способ аутентификации приемлем, то хорошо.

Но использование ОТР-токена — не панацея для веб-ресурсов в Интернете. Фишинговую атаку против пользователя всё равно можно провести. Указанное

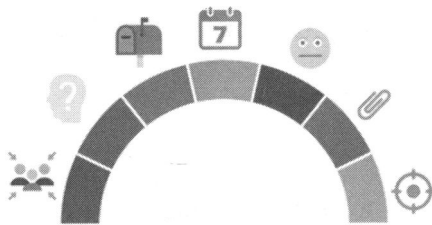
ПО является неким MiTM — собирает данные с фишингового сайта и отправляет их на легитимный ресурс.

В статье: <https://xakep.ru/2019/05/28/fuck-2fa/> упоминаются два ПО с открытым кодом, помогающие злоумышленнику перехватить и логин/пароль, и одноразовый код, которые жертва вводит на фишинговом сайте.



Указанное ПО выполняет роль своего рода MiTM — собирает данные с фишингового сайта и отправляет их на легитимный ресурс.

Глава 6



Организационные меры противодействия СИ

Как показала практика, нельзя просто взять и купить защитное ПО, обучить сотрудников правилам ИБ и тем самым свести риски ИБ к минимуму.

В этой главе мы рассмотрим некоторые практики, которые необходимо внедрить, чтобы выстроить процесс защиты от СИ. Я сделаю акцент на повышении осведомленности пользователей, т. к. эта сфера мне наиболее близка, а фантазировать, какой регламент составить, чтобы организовать работу сотрудников через VPN, мне не хочется, хотя этого мы тоже коснемся.

Модель зрелости осведомленности о безопасности

Для начала необходимо определиться, где мы находимся и к чему можно стремиться, обучая сотрудников правилам ИБ.

На сайте Института SANS (<https://www.sans.org/blog/security-awareness-maturity-model/>) описаны разные уровни, на которых может находиться организация, с точки зрения зрелости внедрения процессов повышения осведомленности пользователей:

1. Ничего нет.
2. Формальное соответствие.
3. Есть программа повышения осведомленности.
4. Ведется долгосрочный процесс повышения осведомленности как части корпоративной культуры.
5. Разработаны метрики повышения осведомленности всей организации, и они достигнуты.

Рассмотрим эти уровни немного подробнее и в наших реалиях.

1. Отсутствие обучения, учебных атак и каких-либо материалов по ИБ.
2. Есть регламенты или другие материалы по ИБ, которые доводятся до сотрудников. Учебные атаки проводятся не системно, не чаще 1–2 раз в год. Иногда

проходят брифинги для сотрудников. Новые сотрудники изучают базовые правила ИБ по неадаптированным обучающим материалам (использование слов и терминов, понятных лишь специалистам, слишком большие курсы, отсутствие проверки знаний).

3. Сотрудники регулярно (ежемесячно по 1–2 раза) тестируются с помощью учебных атак, но не все, а выборочные/ротирующиеся группы. В течение года проводится несколько других активностей в виде брифингов, вебинаров, рассылки учебных курсов, которые раскрывают другие аспекты ИБ и участия в них человека. Новые сотрудники проходят предварительное обучение правилам ИБ.
4. Повышение осведомленности касается всех сотрудников, включая топов, всех филиалов и дочерних организаций. Из среды рядовых сотрудников выращиваются секьюрити-чемпионы, которые на местах помогают службе ИБ соблюдать правила ИБ. Задействовано несколько каналов донесения важности ИБ, например: интерактивные тренажеры, онлайн-курсы, учебные пособия, памятки, плакаты, очное обучение, скринсейверы, видеоролики, игры (компьютерные, настольные), буклеты, викторины, ежемесячные дайджесты с угрозами ИБ (рекомендую делать дайджест небольшим и с упоминанием угрозы ИБ для физических лиц — так вы замотивируете сотрудников читать ваши рассылки). Новые сотрудники проходят предварительное обучение правилам ИБ и допускаются к работе только после успешного прохождения теста.
5. Метрики внедрены как важная часть процесса и системного подхода к процессу. При повышении осведомленности сотрудников у заказчиков мы используем в качестве бенчмарков следующие метрики:
 - более 50% сотрудников отправляют рапорты о подозрительных письмах через год повышения осведомленности — отлично;
 - если менее 5% — очень плохо;
 - через год максимум 1 из 25 сотрудников попадает на фишинг (4% от общего числа) — отлично;
 - 1 из 3 (33%) — плохо, но это среднестатистическое положение дел у большого количества организаций, если повышение осведомленности не проводится.

В модель зрелости я бы еще добавил пункт «б» — когда организация требует повышения осведомленности сотрудников поставщиков. С этим пунктом, естественно, не всё так просто и однозначно. Но если в организации с безопасностью строго, и если что-то случится, пострадает много людей, минимальные требования к контрагентам выставить можно, и это не что-то новое:

- у поставщиков ПО, которые должны сертифицировать свои продукты, или компаний, которые должны лицензировать свою деятельность, можно запросить эти самые сертификаты и лицензии;

□ также, по части минимальных требований к контрагентам, вы можете проверить, используют ли они настройки SPF, DKIM и DMARC к своим доменам, с которых будут отправлять вам письма.

Касательно обучения топов могут подтвердить, что да — это проблема во многих организациях. Не раз слышал от коллег, что руководители высшего звена просят не «шпионить» за ними и не мешать им. Так что, как сказал один безопасник, руководители должны руководить, поэтому единственное, что мы можем для них сделать, — это организовать брифинг, где эксперт расскажет им про ИБ и про те мероприятия, которые необходимо организовать для ее внедрения, а в конце показать им список требований, которые топ должен «спустить» в виде приказа.

Эксперт по ИБ, приглашаемый на эти брифинги, должен иметь уровень не ниже, чем руководитель организации. Например, для руководителей большой корпорации это может быть специалист с международным опытом, и, возможно, такой, кто уже выступал в организации из вашей отрасли или как-то с ней связан.

Итак, определите, на каком уровне находится ваша организация и решите, какого уровня вы хотите и можете достигнуть.

Одобрение процесса повышения осведомленности у руководителей

В разд. «Как повысить киберграмотность сотрудников?» главы 4, мы уже упоминали о плане по повышению осведомленности, — там он был составлен для проведения непосредственно рассылок.

На шаге 1 этого плана нам нужно получить одобрение от руководства на проведение мероприятий по повышению осведомленности. Чем выше будет руководитель, тем лучше.

Объясните ему, что человеческий фактор является ключевой проблемой ИБ (82% нарушений связаны с человеческим фактором), — см. соответствующие данные об этом на стр. 8 исследования, доступного по приведенному QR-коду.



Упомяните, что обучение сотрудников правилам ИБ — это признанная практика во всем мире, и дайте решение проблемы: организация процесса повышения осведомленности сотрудников вашего департамента, регулярная проверка их навыков с помощью учебных атак и обучение тех, кто не различает фишинг в email-корреспонденции. Можно также напомнить ему о рисках, которые возникают, если процессом обучения пренебрегают.

Говоря о рисках, опирайтесь на методический документ ФСТЭК «Методика оценки угроз безопасности информации» от 5 февраля 2021 г. — в приложении 4 к этому документу их перечислено достаточное количество.

Если ваша организация является субъектом критической информационной инфраструктуры (КИИ), то в разделе «XVII. Информирование и обучение персонала (ИПО)» приказа ФСТЭК от 25 декабря 2017 г. № 239 вы найдете то, что пригодится вам для утверждения программы повышения осведомленности.



С ИПО 1–4 мы как раз сейчас и разбираемся, а как выполнить ИПО.0 мы рассмотрим далее — в разд. «*Регламенты*» этой главы.

Обучение: памятки, курсы, форматы обучения

Итак, вы получили одобрение на проведение учебных атак и обучение сотрудников. Теперь необходимо заняться непосредственно внедрением намеченного.

В разд. «*Как повысить киберграмотность сотрудников?*» главы 4 рассмотрена последовательность действий и бесплатные инструменты с материалами по повышению осведомленности.

Говоря об организационных мерах, хотелось бы добавить пару слов про отчеты. Рекомендую показывать их не только руководству, но и сотрудникам. В одной из организаций мы повышали осведомленность в тяжелых условиях — сотрудники сопротивлялись обучению, и у большинства из них email безопасника был занесен в «черный список», так что с ИБ там всё было сложно.

Через три месяца учебных атак и обучения попавшихся безопасник организовал брифинг и показал результаты — в шесть раз снизилась попадаемость на фишинг. Магия нашей методологии и материалов сработала, но суть в другом: к безопаснику подошло много сотрудников (по его словам), которые поблагодарили его за то, что он делает, и заверили его, что теперь более внимательно ищут подозрительные признаки.

Поэтому советую не обделять вниманием сотрудников — брифинги делать не обязательно, а вот рассылку со статистикой организовать можно. Кстати, не забудьте поблагодарить их за проявленную бдительность.

Теперь о подходах к обучению новых сотрудников, недавно пришедших в организацию. Когда-то мы разработали памятку по распознаванию некоторых видов подозрительных писем, разместили ее на «Хабре» и даже не нахватили минусов :-). Потом я узнал, что эта памятка используется во многих организациях: от атомной промышленности до банковской сферы.

Надеюсь, она пригодится и вам. Вы можете давать ее новым сотрудникам при устройстве на работу, раздавать на брифингах или включить ее в свой обучающий курс.

Текст этой памятки вы, естественно, можете дополнить и переделать под себя.

ПИСЬМА СТОИТ СЧИТАТЬ ПОДОЗРИТЕЛЬНЫМИ, ЕСЛИ ОНИ СОДЕРЖАТ:

- Ссылки в виде цифр. Пример: 178.248.232.27.
- Ссылки, включающие символ @. Пример: <http://bank.ru@phish.ru>.

- Ссылки с двумя и более адресами. Пример:
https://bank.ru/bitrix/rd.php?go=https://bitly.com/bank.
- В начале адреса сайта — префикс **www**, но нет точки или стоит тире. Примеры:
wwwbank.ru или **www-bank.ru.**
- В начале адреса сайта — префикс **http** или **https**, но нет символов **://**. Пример:
httpsbank.ru.
- В адресе сайта — несколько символов **/**. Тогда смотрите, что написано в правой части, до первого символа **/**, — там вы обнаружите исходный сайт, и если он вам не знаком, ссылка подозрительна. Пример:
www.bank.ru.zlodey.ru/login?id=12/aa/bank.ru.

КРОМЕ ТОГО:

- Если при наведении указателя мыши ссылка выглядит по-другому. Пример: ссылка написана как **tele2.ru**, а при наведении мыши в нижнем углу браузера отображается **teie2.ru.**
- Ссылка может быть не кликабельна (при клике не происходит переход по ссылке), но содержать подмененные символы. Злоумышленник надеется, что вы скопируете ссылку и вставите в браузер. Пример: в письме указана ссылка **online.ru** — вы копируете ее и вставляете в браузер, но оказывается, что это **oniine.ru.**
- В своем email или в ссылке злоумышленник может заменить букву «o» на цифру «0», или маленькую латинскую букву «l» на большую букву «I», или b на d и т. д. Пример: **Online.dank.ru** вместо **online.bank.ru.**
- Если ссылка начинается с **https://** — это не значит, что она безопасна.
- В тексте сообщения, пришедшем вместе со ссылкой, встречается несколько ошибок и опечаток.
- Буквы в тексте частично подменены. Примеры: добрый денб, как дела.
- Любые сообщения с вложениями по умолчанию стоит считать подозрительными. Через вложения чаще всего заражают компьютеры, и ни один антивирус не гарантирует полной защиты.
- Если вы не ожидали сообщения с этим вложением, поищите подозрительные признаки в сообщении, описанные в приведенном списке.

Помните:

- Email в поле Отправитель может быть подделан, или знакомого отправителя могли взломать. Нельзя доверять всем пришедшим сообщениям, даже если отправитель вам знаком.
- Если в письме вас просят сделать действие, особенно срочное, ищите подозрительные признаки.

Регламенты

В этом разделе я опишу различные ситуации и риски ИБ, которые могут возникнуть, когда по отношению к пользователю будет применяться СИ, а вы с помощью регламентов попытаетесь это предотвратить.

Здесь я также приведу несколько ссылок на готовые регламенты, но, к сожалению, их не так много, поскольку не все организации хотят выкладывать свои документы на всеобщее обозрение — как минимум с точки зрения собственной безопасности.

Регламент обучения персонала

Как упоминалось в *разд. «Одобрение процесса повышения осведомленности у руководителей» этой главы*, существует приказ ФСТЭК от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов КИ РФ», содержащий пункт ИПО.0: «Регламентация правил и процедур информирования и обучения персонала».

Если собственного регламента у вас нет, можете использовать приведенный по QR-коду образец. Здесь также приводится образец плана обучения сотрудников на календарный год. Но, возможно, образцы этих регламентов есть и у вашего отдела кадров.



Некоторые аспекты для учета в регламентах

Давайте рассмотрим некоторые потенциально опасные ситуации, которые могут возникнуть у сотрудников в процессе работы. Убедитесь, что в регламентах, инструкциях или обучающих материалах:

- прописано, что делать, если с реального email руководителя пришло сообщение с просьбой, идущей вразрез с правилами и регламентами;
- указано, какие данные нельзя отправлять по электронной почте даже внутри организации (в основном касается гостайны);
- описаны опасные действия для вашей организации, выполнения которых может требовать злоумышленник, и пояснено, как их распознать;
- предписаны действия при обнаружении взлома почты;
- предписаны действия в ситуации, когда сотрудник запустил опасный файл или ввел данные на фишинговом сайте и понял, что совершил небезопасное действие;
- прописано, что делать, если вы сомневаетесь, кто вам пишет: хакер или обычный пользователь;
- рассказано, как безопасно проверить ссылку и не заразить компьютер;
- указано, какие сообщения стоит игнорировать, а о каких сообщать в службу безопасности;
- предписана установка ПО и дополнений в браузере на ПК;
- предусмотрено сохранение пароля в браузере;
- указано, кому можно сообщать свой пароль;
- прописано, что делать, если сотруднику пишет коллега из отпуска с просьбой отправить документы на его личную почту;
- прописано, что делать, если сотрудник хочет поработать на выходных и планирует отправить рабочие документы на личную почту;
- прописано, что делать, если сотруднику подарили USB-устройство с доставкой в офис;

- ❑ указано, какие рабочие вопросы нельзя обсуждать в общественных местах;
- ❑ предписаны действия с подозрительными бумажными документами, полученными от третьих лиц;
- ❑ прописано, что делать, если из одного отдела пришло подозрительное письмо в другой отдел (отправить в службу ИБ, позвонить по внутреннему телефону, встретиться лично и т. д.).

Контроль реквизитов

Однажды на наш счет в банке пришла оплата от заказчика (и тут же вернулась обратно). Дело в том, что наши банковские реквизиты изменились, и в счете были указаны новые. Но бухгалтер заказчика не изменил их в своем ПО и произвел оплату по старым. Что это значит? Что злоумышленник может подменить реквизиты в этом ПО на свои и получить чужие деньги.

Соответственно, необходимо внедрить регламент по «перепроверке» реквизитов перед оплатой.

Некоторые организации также устанавливают регламент, указывающий, каким образом необходимо менять реквизиты, если они отличаются от тех, что были прописаны в договоре изначально, потому что поддельные реквизиты бухгалтеру могут отправить через ВЕС-атаку или просто с email, похожего на официальный email контрагента.

У одного из заказчиков мы обучали работников правилам ИБ, и когда бухгалтеру пришел запрос от «поставщика» с просьбой перевести предоплату по договору в размере 30% (речь шла о сумме порядка 200 млн рублей), то она знала, как действовать. Бухгалтер отправила рапорт в отдел ИБ, а безопасник перезаключил с нами договор на повышение осведомленности на следующий год :-)

Дополнительная проверка перед оплатой

Если в предыдущем примере мы рассматривали подмену реквизитов, то в этом случае нам нужно убедиться, что злоумышленник не захотел получить больше средств, чем это предусмотрено договором.

Моя родственница работала на одном из предприятий юристом и немного рассказала мне об их процессе верификации оплаты. В соответствии с регламентом она сверяла все счета с договорами, и только после этого можно было проводить какие-либо оплаты. В случае несоответствия суммы даже на 1 рубль она обращалась к руководству предприятия. Таким образом, часть схем с оплатой фиктивных сделок становилась невыполнимой.

Как вести себя с гостями?

В организации должны быть регламентированы правила для идентификации посетителя и обеспечения его сопровождения, а для сотрудников следует провести инструктаж по взаимодействию с посетителями (клиентами, курьерами, грузчиками и др.).

Рядом с посетителем всегда должен присутствовать представитель организации. Если сотрудник организации обнаруживает посетителя, перемещающегося по зданию (территории) в одиночку, он должен иметь соответствующие инструкции для корректного выяснения цели посещения и необходимого сопровождения.

Также необходимо указать, что сопровождающему сотруднику делать, если ему необходимо срочно отойти от посетителя (позвонил руководитель, начался обеденный перерыв и т. д.).

Общение с коллегами

Необходимо создать правила идентификации коллег и передачи информации при общении с ними по телефону или в личной беседе.

Это особенно актуально в крупных организациях, где сотрудники могут быть не знакомы друг с другом, и злоумышленникам легко выдать себя за их коллегу.

Убедитесь, знает ли ваш сотрудник, что делать, если к нему действительно подошел новенький (возможно, это специально устроившийся на работу инсайдер), у которого сегодня первый рабочий день и который просит распечатать документ с флешки, т. к. ему только завтра дадут доступ к ПК.

72 минуты до начала конца

В среднем столько времени необходимо злоумышленнику, чтобы за-получить конфиденциальные данные, если сотрудник стал жертвой фишингового письма (см. стр. 1 исследования Microsoft по ссылке в QR-коде).



Как следует из статистики, скорость реагирования играет важную роль при защите информации.

Действия сотрудников не должны растягиваться во времени. В регламенте реагирования на атаку следует учитывать временной фактор. Чем быстрее мы узнаем об угрозе, тем быстрее снизим риски взлома или утечки.

Сотрудник должен знать, что как только он увидел подозрительное сообщение, ему необходимо незамедлительно обратиться в службу ИБ. Еще быстрее ему надо реагировать, если он совершил небезопасное действие и опомнился спустя несколько секунд. Он должен понимать, что если сейчас он видит это письмо, то десятки его коллег могли получить точно такое же, и именно он отведет угрозу от организации, если сообщит о подозрительном письме сразу, а не отложит это на «после обеда».

Сотни регламентов по информационной безопасности

Был такой сайт securitypolicy.ru — сборник политик по информационной безопасности. Был, потому что сейчас он работает, но не отображает статьи, воз-

можно, со временем что-то изменится¹. Подобных источников мне найти не удалось, поэтому приходится читать его содержимое через «Веб-архив».

Зайдите по ссылке в QR-коде в раздел с шаблонами, выберите нужную инструкцию, скопируйте ее URL и воспользуйтесь ресурсом <https://web.archive.org> для прочтения статьи.



Среди инструкций и регламентов вы здесь найдете:

- инструкцию по использованию электронной почты;
- антивирусную политику;
- инструкцию по организации парольной защиты;
- правила работы в локальной вычислительной сети;
- и многое другое.

Кроме того, десятки регламентов вы можете найти на сайте эксперта по ИБ Евгения Родыгина², включая парольную политику, работу с персональными данными, реагирование на инциденты, работу с VPN и др. Просто впишите в строку поиска сайта: регламент.

¹ Похоже, он все-таки заработал, проверьте.

² См. <https://wikisec.ru>.

Послесловие

Спасибо, что прочитали эту книгу. Надеюсь, она оказалась полезной.

Для меня социальная инженерия перестала быть загадкой, когда ее удалось разложить на составляющие. Теперь это не окутанная тайной «наука», доступная лишь избранным. Если ты человек и умеешь общаться — ты уже социальный инженер, ведь ты выпрашивал сладкое у взрослых, применяя разные схемы манипулирования, и тебя этому никто не учил.

Буду рад получить от вас обратную связь на почту dys@stopphish.ru, надеюсь, это поможет дополнить книгу при ее возможном переиздании.

Успехов в работе!

Приложение 1

Генератор онлайн-СИ

Что ж, в этой книге мы постарались рассмотреть наиболее применимые способы социальной инженерии.

Онлайн-векторы СИ мы объединили в Генератор (рис. П1.1). Когда в одном месте собрана систематизированная информация по какому-либо предмету, ее можно применять с большим успехом.

Регистрируйтесь здесь: <https://stopphish.ru/fb>. Эти материалы должны сначала попасть в руки безопасников и пентестеров, а только потом слиты для широкой общественности, которая будет применять их вовсе не для безопасности.



Онлайн-версия генератора сценариев находится тут: <https://gen.stopphish.ru>. Возможности его будут постепенно расширяться, но уже сейчас там можно сгенерировать несколько тысяч сценариев. Но сильно не рассчитывайте на генератор — он пока не пишет тексты писем, а лишь дает идеи для атаки, так что непосредственно тексты писем вам придется писать самостоятельно.

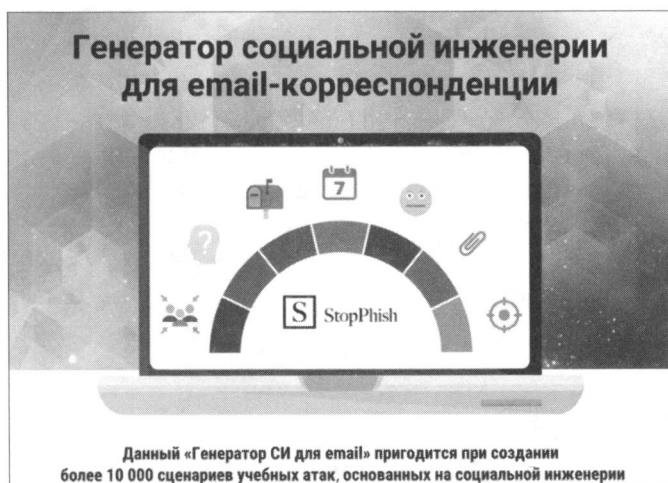


Рис. П1.1. Генератор социальной инженерии

Приложение 2

Классификатор СИ

Информация о методах онлайн и офлайн социальной инженерии собиралась нами несколько лет. Делить ее на составляющие — это ключ не только в ее применении, но и в защите от нее. Зная, что и как применяет злоумышленник, можно подготовить целевую защиту.

Применять Классификатор можно для составления учебных атак и принятия технических и организационных мер для недопущения нанесения вреда с помощью описанных векторов. Кроме того, вы можете создавать обучающие материалы на его основе.

Электронная социальная инженерия v0.81

Классификация по типу сообщения:

- таргетированная (персонализированная атака на компанию, отдел, человека);
- массовая (когда непринципиально, какой из сотрудников в какой компании получит письмо);
- смешанная (используется небольшая персонализация — например, на бухгалтеров, но рассылается по тысячам компаний, или заточенная на конкретную организацию, но непринципиально, кто получит вредонос).

Текст email-сообщения находится:

- в теле письма;
- в теме письма (включая текст вместе с ссылкой);
- во вложении.

Подделка отправителя:

- с подделкой отправителя email в заголовках;
- без подделки отправителя email в заголовках;

- подделка имени отправителя: Ф.И.О., сервис, организация (знакомые или незнакомые получателю);
 - имитация легитимного email в имени. Например, в поле **От кого** написано: Анна Иванова (anna@OfficialDomain.ru) <q@hack.com>.
- По каналам коммуникации:
- email (корпоративные и личные);
 - соцсети и сайты с возможностью общения (личные сообщения, комментариев к посту жертвы, группа или чат, где состоит жертва, упоминание в своем посте или комментарии username жертвы, чтобы ей пришло уведомление об упоминании);
 - мессенджеры;
 - онлайн-консультанты на сайте;
 - формы обратной связи на сайте.
- По направлению у организаций:
- внешняя от сотрудника (пишет из отпуска, командировки, из филиала/головного офиса);
 - внешняя от организации (имитация реального подрядчика, партнера, госоргана или сообщения от их имени после взлома этих организаций или их сотрудником, совершающим нелегитимные действия);
 - внешняя от физлиц (потенциальные/действующие клиенты, отклик на вакансию);
 - внешняя с подделкой отправителя email (изменяются заголовки email, и в почтовом клиенте виден легитимный отправитель);
 - внешняя с пересылкой внутри (клиентская поддержка пересылает письмо клиента в техподдержку или ИТ-отдел);
 - внутренняя с подделкой отправителя email (сотрудник пишет сотруднику);
 - внутренняя при реальном взломе инфраструктуры (рассылка идет из инфраструктуры организации со вновь созданного email, похожего на оригинальный email);
 - внутренняя при взломе email сотрудника (реальный или фиктивный взлом);
 - легализованная внутри (начальник попался на уловку и отдает приказ сотрудникам совершить вредоносное действие, получил акт выполненных работ и переслал бухгалтеру);
 - имитация уведомлений от внешних сервисов;
 - имитация уведомлений от внутренних сервисов.

□ По направлению у частных лиц:

- от близких (родственника, друга, знакомого);
- от незнакомых частных лиц;
- от представителя знакомой группы лиц (сообщество, партия, клуб, религиозная группа);
- от представителя незнакомой группы лиц (общество защиты синих китов);
- от организаций (государственных, коммерческих, некоммерческих);
- от сетевых ресурсов (техподдержка соцсети, почта и т. д., служба заботы).

□ По формату:

- веб-сайты (например, с вредоносной нагрузкой, фишинговые формы авторизации, с фейковой информацией);
- реклама (например, с геотаргетингом на определенный бизнес-центр);
- видео- и аудио-deerfake;
- find trap сценарий — побуждение пользователя самостоятельно найти вредоносный ресурс (сайт, канал, файл);
- приложения (в неофициальных и официальных магазинах, присылаемые и скачиваемые в виде файла);
- многоходовки (сначала общаемся с жертвой, потом отправляем вредонос);
- лидеры мнений — например, админ группы рассказал о ресурсе (платно или нет), а он был подменен вредоносным;
- вложения — классификация:
 - по типу: архивы с паролем и без (включая письма в виде заархивированных EML-файлов), офисные документы, ярлыки Windows (*.lnk), использующие функцию Chrome's Application Mode, HTML-файлы;
 - по небезопасному действию: разрешение макросов, разрешение небезопасного содержимого, запуск исполняемых файлов, фишинг;
- ссылки (с символом @, со слешем в юникоде, с обфускацией, кириллические, QR-коды, некорректный синтаксис, в виде картинок в теле письма или во вложении, в документах, очень длинные, в виде цифр, невидимые при наведении мыши, редиректы, неактивные, похожие на официальные сайты, в поддоменах, наклонная буква «l» или «I» вместо слеша);
- плагины для браузера (в неофициальных и официальных магазинах, на сайтах, требующих установить плагин для доступа к контенту. Например, просим сотрудника в письме проверить работоспособность электронной подписи (ЭП) на поддельном сайте. На сайте просим установить вредоносный плагин);

- email-MiTM (вид атаки, когда злоумышленник создает два поддельных email-адреса и отправляет с них сообщения двум жертвам, имитируя для них легитимную переписку).
- По целевым группам:
- топ-менеджмент;
 - ИТ-служба;
 - руководители подразделений;
 - линейный персонал;
 - производство;
 - финансисты;
 - отдел закупок;
 - специфические подразделения в конкретной организации.
- По контексту (повод, по которому пишут пользователю):
- event attacks (локальные праздники в стране или организации, мероприятия, выставки, корпоративы, новые законы и постановления. Такие сообщения будут уведомлять, поздравлять, информировать, приглашать, рекомендовать);
 - причина: «Что-то (не) произошло, и я вам пишу. Некто сказал, что по этому поводу писать вам»;
 - запросы: КП, сметы, счета, декларации, оплаты, документа, (не)конфиденциальной информации;
 - вопросы: «Эта почта работает?», «Вы на связи?», «По этому вопросу к вам?»;
 - отправка: в виде сообщения или с вложением: «Высылаю Вам: ТЗ, КП, акты, счета, анкеты, опросы, требование, регламенты (введение новых, изменение старых), приказы, правила, документы, приглашения, благодарности (за работу, за какое-то действие), уведомление, рекомендации»;
 - изменения (регламентов, расписания, правил, корпоративного портала).
- Усиление контекста:
- эмоции, которые мы пытаемся вызвать или имитируем сами: сочувствие (к чему-либо/кому-либо), страх (штраф, увольнение, лишение, потеря ценностей), гнев (от начальника, клиента, партнера), консерватизм (используем официальный тон сообщения), интерес (появление чего-то нового), радость;
 - оказание давления (авторитет, просьба о помощи, срочность, угроза);
 - вызов желания: бесплатность, экономия (скидки, акции, замена чего-либо альтернативным или более лучшим вариантом), деньги (повышение, премия, надбавка);

- совпадение — когда у жертвы часть идентности совпадает со злоумышленником, лояльность растет, например: однофамильцы, тезки, профпринадлежность, политические взгляды, земляки, увлечения, учебные заведения, воинская служба. Но акцент на этом в сообщении/профиле в соцсети можно специально не делать, жертва должна сама это заметить;
- ложь:
 - фейковая отсылка к людям (ссылаемся на других людей — например, на руководителя);
 - несуществующий разговор (якобы с кем-то обсудил то, что сейчас нужно сделать);
 - поддельная переписка со знакомыми или незнакомыми жертве людьми (подделка скриншотов из мессенджера или вставка придуманной переписки в email ниже);
 - подтасовка фактов (нечто нужно сделать на основании Указа Правительства № 1765, иначе всем будет плохо);
 - технические усилители в email (добавление в тему письма «Re:» и «Fwd:» для имитации переписки или пересылки сообщения).
- По персонализации:
 - имя: обращение по имени, имени и отчеству. Например, в начале письма пишем: «Андрей, добрый день»;
 - должность: нацеленность атаки на определенную должность или ее упоминание в сообщении. Например, в теме письма пишем: «В бухгалтерию, срочно»;
 - организация: нацеленность атаки на определенную организацию или ее упоминание в сообщении. Например, в теме пишем: «В АО “Альфа”» или просто название компании;
 - без персонализации — например: «Коллеги, добрый день»).
- Домен отправителя в email:
 - Похожий на официальный (целевой организации, связанных с ней организаций и сервисов). Используются следующие виды маскировки домена:
 - добавление цифр (domain1.com);
 - вставка точки или тире (d.oma-in.com);
 - использование поддомена (domain.com.email.online);
 - повторение символов (dommain.com);
 - добавление приставок www, http(s), web, online (wwwdomain.com, https-domain.com, domain-online.com);
 - использование омоглифов — похожих символов из других алфавитов: domainç.com, замена символов на похожие: вместо good.local, domain.com qood.local.b0rnajn.com;

- замена гласных (damain.com);
 - замена доменной зоны (domain.online);
 - добавление символов (dommain.com);
 - пропуск символов (doman.com);
 - перестановка символов (donaim.com).
 - письмо с общедоступного email-сервиса (со вставкой официального домена до символа @, с Ф.И.О. настоящего или выдуманного человека);
 - случайный домен, незнакомый получателю.
- Домен вредоносной или фишинговой ссылки:
- похожий на официальный (целевой организации, связанных с ней организаций и сервисов. Используются следующие виды маскировки домена:
 - добавление цифр (domain1.com);
 - вставка точки или тире (d.oma-in.com);
 - использование поддомена (domain.com.email.online);
 - повторение символов (dommain.com);
 - добавление приставок www, http(s), web, online (wwwdomain.com, https-domain.com, domain-online.com);
 - использование омоглифов — похожих символов из других алфавитов: domainç.com, замена символов на похожие: вместо good.local, domain.com — qood.local.b0rnajm.com;
 - замена гласных (damain.com);
 - замена доменной зоны (domain.online);
 - добавление символов (dommain.com);
 - пропуск символов (doman.com);
 - перестановка символов (donaim.com);
 - случайный домен, незнакомый получателю;
 - домен в punycode (<https://xn--jlail.xn--plai/company.ru>).
- По целевому вредоносному действию:
- шифрование данных;
 - шантаж (после шифрования данных или без);
 - фишинг (выманивание данных с целью неправомерного доступа к информации и ресурсам. Чтобы не путаться с определением фишинга и разными его видами, отталкиваемся от изначального его предназначения: ловля логинов и паролей в Интернете. Например, к: ПК, корпоративному portalу, email, аккаунту в соцсети, телефону, платежным ресурсам);
 - сговор;

- подкуп;
- переманивание сотрудников;
- взлом ИТ-инфраструктуры (получение несанкционированного доступа к ИТ-ресурсам);
- хищение активов;
- шпионаж — удаленное получение конфиденциальной и инсайдерской информации, которая может нанести непосредственный вред организации, финансовый или репутационный, в случае неправомерного использования или разглашения: через веб-камеру, микрофон, геопозицию (на смартфоне, ноутбуке, планшете), чтение сообщений в каналах коммуникации (email, корпоративный портал, мессенджеры);
- data-phishing — выманивание данных, которые пригодятся злоумышленнику для раскручивания атаки. Например, информация в email-автоответчиках, о том, кто из сотрудников сейчас в отпуске и к кому из коллег нужно обращаться, с Ф.И.О. и телефоном;
- нанесение ущерба репутации путем распространения ложной или конфиденциальной информации;
- подписание платежей и документов с помощью ЭП (на поддельных сайтах).

Офлайн социальная инженерия v0.2

□ Физические действия:

- проникновение на территорию организации (через черный ход, с заходящими сотрудниками, с поддельным пропуском, имитация представителя легитимной организации, имитация устройства на работу);
- мероприятия (корпоративные и внешние, использующиеся для знакомства с жертвой, сбора целевой аудитории техническими средствами);
- инсайдер (внедрение нового или вербовка действующего сотрудника).

□ Предметы:

- бумажные носители (предоставление ложной информации в письмах, журналах, документах);
- USB-устройства (дарение, подмена, подбрасывание, имитация поставки устройств со встроенными средствами сбора информации).

□ Линии связи:

- Wi-Fi (имитация текущей точки доступа, создание похожей или другой актуальной в текущем месте);
- смишинг (обман с использованием SMS);

- вишинг (атаки с использованием телефона, живое общение или бот-мощенник).
- Места:
- целевая организация и дочерние (включая территорию возле организации, курилки, парковки);
 - общественный транспорт;
 - гостиницы;
 - аэропорты и вокзалы.
- Создаваемый эмоциональный контекст:
- эмоции: сочувствие (к чему-либо/кому-либо), страх (штраф, увольнение, лишение, потеря ценностей), гнев (от начальника, клиента, партнера, близкого), консерватизм (официальный тон сообщения), интерес (появление чего-то нового), радость;
 - давление (авторитет, просьба о помощи, срочность, угроза);
 - желание: секс, халява, экономия (скидки, акции, замена чего-либо альтернативным, лучшим вариантом), деньги (повышение, премия, надбавка);
 - совпадение — когда у жертвы часть идентности совпадает со злоумышленником, лояльность растет, например: однофамильцы, тезки, профпринадлежность, политические взгляды, земляки, увлечения, учебные заведения, воинская служба. Но акцент на этом в сообщении/профиле в соцсети можно специально не делать);
 - ложь (сослаться на несуществующих людей), разговор (якобы с кем-то обсудил то, что сейчас нужно сделать) со знакомыми жертве людьми, подтасовка фактов).

Приложение 3

Таблица персонализации

О том, как составлять таблицу (рис. ПЗ.1) и ею пользоваться, подробно рассказано в *разд. «Подготовка» главы 1*.

Таблица помогает сориентироваться в том, кем можно представляться, когда вы пишете тому или иному сотруднику.

	Бухгалтер	Продавец	IT-специалист	Топ-менеджер
Гос. органы	*			*
Клиенты	*	*		
Руководитель	*	*	*	
СМИ				*

Рис. ПЗ.1. Таблица персонализации

Приложение 4

Бесплатное в помощь службе ИБ и ИТ

Нами создан ряд бесплатных материалов вам в помощь. Мы же не отъявленные коммерсанты и хотим внести вклад в сообщество информационной безопасности.

Перейдите по ссылке <https://stopphish.ru/free-base-coure> или по QR-коду.



Там вы найдете:

- классификатор онлайн-векторов социальной инженерии в виде отдельного файла;
- плагин для Outlook, который дает возможность вашим сотрудникам в два клика пересылать подозрительные письма в службу ИБ;
- генератор социальной инженерии для email-корреспонденции в виде инфографики с последовательными шагами по созданию векторов атак;
- чек-лист по техническим аспектам защиты от социальной инженерии и фишинга;
- памятку по подозрительным элементам в email-сообщениях — ее можно давать как базовое обучение по распознаванию фишинга;
- плакаты, которые можно повесить в офисе;
- плагин для Chromium-браузеров для оповещения службы ИБ о вводе сотрудником учетных данных на фишинговом сайте.

Ссылки на курсы сгенерированы так, что вы можете взять их и сразу отправить сотрудникам, не создавая копию в своей системе обучения.

Приложение 5

Критерии выбора платформы по повышению осведомленности

По роду деятельности мы часто сталкивались с тем, что заказчик хотел повышать осведомленность сотрудников с помощью какого-либо решения, продаваемого на рынке.

Но чтобы выбирать решение, требовались критерии. Для этого приходилось запрашивать у вендоров список функций их ПО, составлять сравнительную таблицу и пытаться понять, что действительно нужно, потом отправлять свое ТЗ вендорам и запрашивать коммерческие предложения.

Далее представлена совокупность возможных функций ПО, которые когда-либо требовались нашим заказчикам. Мы также кое-что подсмотрели у зарубежных вендоров — вам это тоже может оказаться полезным. Вы можете оттолкнуться от них, в зависимости от потребностей добавить что-то или удалить и отправлять вендорам для получения КП.

□ Цели и задачи:

- снижение рисков информационной безопасности, вызванных небезопасными действиями, совершаемыми сотрудниками;
- повышение интереса и участия пользователей в обеспечении ИБ организации;
- автоматизация процесса повышения осведомленности сотрудников в сфере ИБ путем имитации учебных атак и своевременного обучения правилам кибербезопасности.

□ Общие требования к ПО:

- система должна реализовывать веб-интерфейсы для работы администраторов и пользователей;
- онлайн- и офлайн-установка и обновление;
- возможность использовать ПО и получать обновления без доступа в Интернет;
- On-Premise вариант развертывания ПО;

- система должна поставляться либо в формате виртуальных машин, либо в виде дистрибутива, устанавливаемого на ОС Ubuntu, CentOS и Astra Linux;
 - наличие технической документации пользователя и администратора платформы;
 - система не должна нарушать работоспособность и целостность других систем заказчика и должна быть совместима с применяемыми у заказчика средствами и системами ИБ;
 - консоль администрирования системы должна функционировать в среде актуальных версий браузеров на движке Chromium;
 - предоставление обновлений в течение 1 года;
 - наличие методологии, помогающей повышать осведомленность пользователей.
- Сервисное сопровождение ПО:
- разработка целевых атак и кастомизация учебных фишинговых писем под специфику заказчика;
 - подбор и приоритизация наиболее актуальных векторов атак для заказчика;
 - проведение многоуровневых учебных атак;
 - актуализация представленных курсов под регламенты ИБ;
 - разработка новых курсов на основе регламентов заказчика;
 - применение специальной методологии атак и обучения для снижения инцидентов социальной инженерии;
 - использование специальных техник для повышения культуры ИБ в организации;
 - проработка ситуаций, когда сотрудники не хотят обучаться и игнорируют службу ИБ;
 - подготовка персональных отчетов с определенными выборками данных и визуальным оформлением.
- Обучение:
- встроенная LMS и возможность интеграции с LMS заказчика;
 - портал обучения должен управляться из веб-интерфейса системы и через программный интерфейс (REST API);
 - возможность автоподстановки контента в курсы с помощью макросов;
 - возможность авторизовать пользователей без запроса их имени и пароля;
 - возможность интеграции и запуска курсов в WebTutor;

- у администратора должна быть возможность разрешения сотрудникам самостоятельного доступа к произвольным курсам;
 - система должна содержать предустановленные курсы по вопросам ИБ, разработанные исполнителем, иметь возможность их доработки и корректировки, импорта новых курсов в формате SCORM;
 - голосовое сопровождение контента в курсах, которые не подвержены кастомизации;
 - интерактивные модули и элементы в курсах;
 - обновление курсов по мере появления новых атак, которые не предусмотрены текущей версией курсов;
 - возможность загрузки произвольного контента в список обучающих материалов;
 - наличие электронных обучающих курсов и тестов, доступных для изучения без дополнительных плагинов, на актуальных версиях браузеров для ПК и мобильных устройств;
 - возможность кастомизации курсов и тестов под заказчика;
 - возможность создания шаблонов писем для всех пользователей и частных шаблонов для тех, кто систематически допускает нарушения в определенной области.
- Дополнительные возможности:
- загрузка пользователей через файлы формата CSV, LDAP и вставкой из буфера обмена;
 - наличие интерфейса и контента на нескольких языках;
 - использование глобального «черного списка» email, по которым не идет ни одна рассылка;
 - возможность использования ПО под своим брендом;
 - произвольная группировка пользователей;
 - возможность создавать произвольные уведомления для пользователей;
 - выгрузка действий пользователей в кампаниях;
 - фильтры по числовым значениям в таблицах с результатами атак и обучения;
 - фильтрация групп пользователей;
 - фильтрация пользователей;
 - массовое редактирование пользователей;
 - массовое редактирование групп;
 - возможность назначения группы для выбранных с помощью фильтров пользователей;

- логирование действий администраторов системы;
 - вложенные подгруппы пользователей;
 - поиск по пользователям;
 - поиск по группам пользователей;
 - возможность добавления произвольных полей для сегментации пользователей;
 - создание сегмента из случайных пользователей;
 - кастомизация полей со значениями при импорте;
 - различные домены для LMS и административной панели;
 - DSN для отслеживания открытия писем без пикселя-трекера;
 - управление паролями администраторов и авторизация через LDAPS и LDAP;
 - привязка неограниченного числа фишинговых доменов;
 - установка прав доступа для разделения кабинетов и отдельного проведения атак по дочерним организациям;
 - выгрузка логов;
 - возможность интеграции курсов с LMS заказчика.
- Учебные атаки:
- планирование расписания учебных атак;
 - возможность проверки навыков пользователей через выполнение имитированных атак по email с использованием четырех векторов: со ссылками, с вложенным файлом (не менее пяти разных типов файлов, включая офисные документы), с компрометацией учетных данных на фишинговых страницах, с имитацией атаки со скачиванием «вредоносного» файла на поддельном сайте;
 - возможность создания шаблонов на основе реальных писем из файлов *.eml и *.msg;
 - наличие готовых для атак писем и сайтов;
 - наличие конструктора для создания фишинговых писем и сайтов;
 - граббер сайтов и форм авторизации;
 - разработка сценариев атак с учетом специфики заказчика;
 - Возможность создания атак с использованием USB- и HID-устройств;
 - рейтинг пользователей на основе результативности учебных атак и прохождения курсов;
 - возможность генерации ссылок и QR-кодов для атак через бумажные носители.

□ Плагины:

- Outlook-плагин, для отправки рапортов о подозрительных письмах в службу ИБ, включая сбор исходного сообщения;
- плагин, оповещающий подразделение ИБ о вводе учетных данных на фишинговых сайтах;
- проверка плагином входящих писем на предмет подозрительных элементов (маскировка фишинговых ссылок по более чем 10 признакам, вредоносных файлов, поддельных отправителей), включая проверку по «черному списку» доменов ссылок и отправителей.

□ Автоматизация:

- автоматическая синхронизация списка пользователей по LDAP;
- автоматическое назначение обучающихся курсов пользователей при наступлении определенных событий и на основе учебного плана;
- автоматическое формирование и отправка отчетности за выбранный период по определенным email;
- автоматическое уведомление пользователей о событиях, связанных с обучением (назначение курсов после атак и внеплановых курсов, приближение крайнего срока прохождения курса, напоминание о непройденных курсах);
- автоматическое повторение оргструктуры заказчика с неограниченной вложенностью по отделам;
- автоматизация рассылок с учебными атаками и назначением курсов;
- автоматическая выдача сотрудникам сертификатов об окончании обучения;
- автоматическая досылка учебных атак новым пользователям;
- автоматический выпуск SSL-сертификатов;
- автоматическая настройка сервера отправки и приема писем.

□ Отчетность:

- визуальные отчеты в ПО о результатах атак и обучения с динамикой результативности;
- статистика по каждой выполненной учебной атаке: процент небезопасных действий, количество людей, открывших письмо, перешедших по ссылке, разрешивших небезопасное действие в файле, заполнивших фишинговую форму;
- статистика по динамике обучения: количество и процент сотрудников, прошедших обучение на каждом курсе в отдельности;
- возможность выгрузки отчетов в форматах CSV, PDF и XLSX;

- интеграция с SIEM;
 - генерация отчетов в формате PDF;
 - общий отчет по состоянию организации.
- Требования к технической поддержке:
- техническая поддержка должна осуществляться исполнителем в режиме 5/7 в течение срока действия лицензии на ПО;
 - обращения в техническую службу поддержки исполнителя должны приниматься телефону и электронной почте;
 - срок ответа на обращение в техническую поддержку должен составлять до 24 часов;
 - исполнитель должен разрабатывать и поддерживать в актуальном состоянии собственную классификацию атак, эксплуатирующих человеческий фактор, включая технические способы введения в заблуждение.

Приложение 6

Словарь терминов

Как и в любой области, в ИБ существует много определений разных терминов, иногда они даже противоречат друг другу, иногда запутывают. Встречаются также попытки дать определение не в виде толкования, а просто привести как пример.

Например, пишут, что термин «социальная инженерия» — это когда тебе присылают ссылку, говорят, что это срочно, ты по ней переходишь и вводишь свой пароль на поддельном сайте. Мало того, что тут нет определения СИ, так еще и такое же определение вам могут дать на термин «фишинг». А фишингом еще могут назвать: «Это когда тебе подбрасывают флешку с вирусом».

Когда же все говорят на одном языке, область развивается, а не превращается в кашу.

Этот словарь не претендует на полноту или научную точность в значениях слов, но определенно представляет собой попытку разобраться, что есть что в СИ. Каждое определение мы постарались написать так, чтобы в нем не было двусмысленности.

В словарь вошли не все термины из индустрии, а наиболее спорные, толкования которых значительно различались.

Если при чтении у вас возникнет обоснованное возражение по какому-либо из терминов, и вы считаете, что для всех будет лучше, если это исправить, пишите мне на icast@bk.ru — в следующих изданиях книги мы поправим/дополним спорные определения. Главное, чтобы определения были емкими, недвусмысленными, полными и понятными ИБ-специалистам разного уровня подготовки.

- **Адвёртинг** — сценарий в социальной инженерии, когда злоумышленник предлагает популярному человеку рекламную интеграцию, говорит, что пришлет предмет рекламы для теста, но отправляет фишинговую ссылку или вредоносный файл.
- **Атака** (в информационной безопасности) — совокупность преднамеренных действий злоумышленника, направленных на нарушение одного из трех

свойств информации: доступности, целостности или конфиденциальности. Например, хакер провел атаку и украл базу клиентов.

❑ **Битсквоттинг** — атака, в рамках которой злоумышленник регистрирует поддельный домен, отличающийся от оригинального одним битом. Например, домен `ya.ru` в двоичном коде выглядит так: `01111001 01100001 00101110 01110010 01110101`. Если в сетевом оборудовании произойдет сбой, то один из битов будет заменен другим, и в результате пользователь попадет на `ve.com` `00111001 01100001 00101110 01110010 01110101`.

❑ **Вектор** (в информационной безопасности) — способ или средство для получения неавторизованного доступа к защищенной информационной системе. Сценарий атаки, в отличие от вектора атаки, — это последовательность действий злоумышленника при реализации вектора.

Например, хакер выбирает целью — кражу базы клиентов организации, вектором — использование социальной инженерии, а сценарием — атаковать через электронную почту, обмануть сотрудника и попросить отправить ему базу.

❑ **Вишинг** (*англ.* vishing от voice phishing) — использование голосовой связи для обмана пользователя или выманивания у него дополнительной информации.

❑ **Инсайдер** — действующий или внедренный сотрудник, работающий с целью получения конфиденциальной информации, которая может нанести организации непосредственный вред, финансовый или репутационный, в случае неправомерного ее использования или разглашения.

❑ **Кибербезопасность** (или информационная безопасность, или ИБ) — совокупность мер, направленных на защиту организации от цифровых атак (атак, направленных на компьютерные ресурсы).

❑ **Киберучения** — легитимная имитация действий злоумышленника, атакующего компьютерную сеть организации, с целью получения навыков защиты в случае реальной атаки.

❑ **Нагрузка** — содержимое сообщения злоумышленника, которое может нанести вред. Чаще так называют вредоносный файл — например, в email, реже фишинговую ссылку.

❑ **Претекстинг** — способ вхождения в доверие, подразумевающий использование ранее полученных данных о пользователе.

❑ **Социальная инженерия** (в ИБ) — совокупность методов обмана человека с целью побуждения к действиям, способствующим несанкционированному доступу к информации или инфраструктуре.

Более емкое определение СИ — обман человека с целью побуждения к действиям, выгодным злоумышленнику. Например, вам присылают письмо и говорят, что во вложении акты выполненных работ. Открываете файл из вло-

жения, а там вирус. В результате злоумышленник получает доступ к вашему компьютеру.

- **Сценарий атаки** — см. *Вектор*.
- **Тайпсквоттинг** (от *англ.* typosquatting, где typo — опечатка + cybersquatting — регистрация доменных имен, содержащих торговую марку, принадлежащую другому лицу) — регистрация доменных имен, близких по написанию к адресам популярных сайтов в расчете на ошибку части пользователей. Пример: вместо оригинального **yandex.com** регистрируем **yandeks.com**.
- **Фишинг** (от *англ.* fishing — рыбная ловля, выуживание) — процесс выманивания конфиденциальной информации у человека. Чтобы не путаться с определением фишинга и разными его видами, отталкиваемся от изначального его предназначения: ловли, как в рыбалке. Например, выманивание логина, пароля через поддельный сайт Facebook.
- **Фишинговая ссылка** — ссылка, при переходе по которой открывается фишинговый сайт.
- **Фишинговый сайт** — сайт, на котором злоумышленник крадет конфиденциальную информацию, оставляемую пользователем. На таких сайтах могут украсть как логины и пароли, так и данные банковских карт, конфиденциальные документы, загружаемые пользователем, личную и другую конфиденциальную информацию.
- **Black box** — тест на проникновение (пентест или Red Teaming), при котором атакующему ничего не известно о компании заказчика, только ее название или веб-сайт.
- **Callback phishing** (от *англ.* callback — обратный звонок и phishing — фишинг) — метод, когда жертву побуждают позвонить по определенному номеру телефона, где во время разговора мошенники выманивают у нее конфиденциальную информацию.
- **Data phishing** — выманивание данных, которые пригодятся злоумышленнику для раскручивания атаки. Например, рассылка пустых писем по списку email и изучение сообщений email-автоответчиков, содержащих информацию о том, кто из сотрудников сейчас в отпуске и к кому из коллег нужно обращаться, с Ф.И.О. и телефоном.
- **Email-MiTM** (MiTM — от *англ.* Man in The Middle — человек посередине) — вид атаки, когда злоумышленник создает два поддельных email-адреса и отправляет с них сообщения двум жертвам, имитируя для них легитимную переписку.

Например, пишет стороне А приветствие с поддельной почты, представляясь стороной Б. Получает ответ, изучает его и, возможно, изменяет. Пишет стороне Б приветствие с поддельной почты, представляясь стороной А. Получает ответ. Далее пересылает то, что предназначалось адресатам А и Б. Между ними завязывается общение.

Теперь злоумышленник будет читать переписку, модифицировать ее (если нужно) и пересылать адресатам. Пример здесь: <https://rb.ru/story/hacker-letter-vc>.



□ **Event attacks** — событийные атаки. Сообщение злоумышленника, использующего инфоповод из всемирных или локальных событий (включая корпоративные события). Например, праздники, эпидемии, новости, получившие широкое распространение, законы и т. д.

□ **Find trap** («поиск ловушки» или «самостоятельный поиск ловушки») — метод СИ, когда жертве доставляется часть информации, оставшуюся часть которой цель самостоятельно ищет в поисковых системах, попадая на вредоносный ресурс.

Пример: жертве отправляется письмо вызывающего характера: «Если Вы не отправите закрывающие документы сегодня, то мы подаем в суд». В подписи отправителя пишется что-то наподобие: «ООО “ОблСнабСервисМонтаж”» (необходимо уникальное, но реально несуществующее название). Жертве интересно, что это за отправитель, и она начинает его искать в поисковой системе, а на первом месте результатов выдачи размещен вредоносный сайт злоумышленника, на который и переходит жертва.

□ **Grey box** — тест на проникновение (пентест или Red Teaming) с условием того, что атакующему заказчиком предоставлена частичная информация — например, список email-адресов сотрудников.

□ **MiTM** (от *англ.* Man-in-The-Middle — человек посередине) — атака, когда между двумя устройствами вклинивается злоумышленник, который может прослушивать или изменять передаваемую информацию.

Например, вы подключаетесь в Wi-Fi в аэропорту и вводите пароль на защищенном сайте. Но оказывается, что этот Wi-Fi подконтролен злоумышленнику — он перехватывает пароль и отправляет его на сайт, куда вы собираетесь войти. Вы успешно заходите в личный кабинет сайта, но теперь пароль известен не только вам.

□ **OSINT** (от *англ.* Open Source Intelligence — разведка на основе открытых источников) — тип разведки, включающий в себя поиск и сбор информации из общедоступных источников.

□ **Pentest** (жарг. «пентест» от *англ.* penetration testing — тестирование на проникновение) — разовая проверка информационной защиты в организации, заключающаяся в поиске уязвимостей в ИТ-инфраструктуре и регламентах защиты информации. Осуществляется сторонней наемной командой.

□ **Piggybacking** — название этой атаки можно перевести как «катание на спине». Она предполагает использование активной сессии пользователя для получения несанкционированного доступа.

□ **Red Team** (и Red Teaming как процесс) — непрерывная проверка информационной защиты в организации, заключающаяся в поиске уязвимостей в ИТ-

инфраструктуре и регламентах защиты информации. Осуществляется сторонней наемной командой либо специальным отделом в организации.

- ❑ **Smishing** (смишинг) — термин можно определить как способ доставки вредоносного контента с помощью SMS.
- ❑ **Tailgating** — название этого типа атаки можно перевести как «упасть на хвост» или «паровозик». Она предполагает физическое следование за уполномоченным лицом для получения доступа в запрещенную зону или здание.
- ❑ **White box** — тест на проникновение (в рамках пентеста или работы команды Red Team) с условием того, что атакующему заказчиком предоставлена вся необходимая информация.

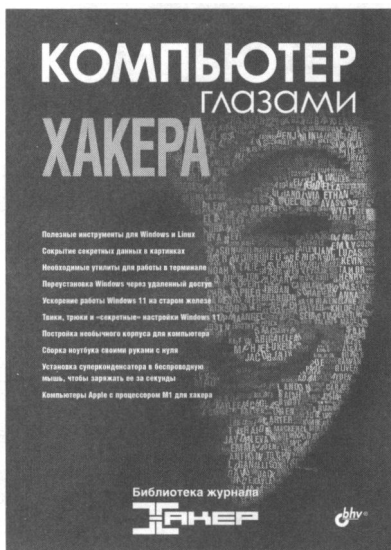


www.bhv.ru

Компьютер глазами хакера

Отдел оптовых поставок:

e-mail: opt@bhv.ru



- Полезные инструменты для Windows и Linux
- Скрытие секретных данных в картинках
- Необходимые утилиты для работы в терминале
- Переустановка Windows через удаленный доступ
- Ускорение работы Windows 11 на старом железе
- Твики, трюки и «секретные» настройки Windows 11
- Постройка необычного корпуса для компьютера
- Сборка ноутбука своими руками с нуля
- Установка суперконденсатора в беспроводную мышь, чтобы заряжать ее за секунды
- Компьютеры Apple с процессором M1 для хакера

Эта книга — сборник лучших, тщательно отобранных статей из легендарного журнала «Хакер». Рассмотрены операционные системы Windows 11 и Linux с точки зрения организации эффективной работы на ПК. Описаны полезные приложения для этих ОС, утилиты для работы в терминале. Рассказано о программах для стеганографии — скрывания полезных данных в графических изображениях. Даны практические советы для пользователей Windows 11 по удаленной установке ОС, отключению телеметрии, удалению программ и компонент, тонкой настройке системы, ее оптимизации для работы на несовместимом и устаревшем оборудовании. Подробно описаны различные настройки Linux для безопасной работы. Представлены примеры постройки самодельного корпуса для ПК, установки суперконденсатора в беспроводную мышь, сборки самодельного ноутбука. Приведен обзор возможностей устройств Apple на базе процессоров M1 и даны советы по их эффективному использованию.



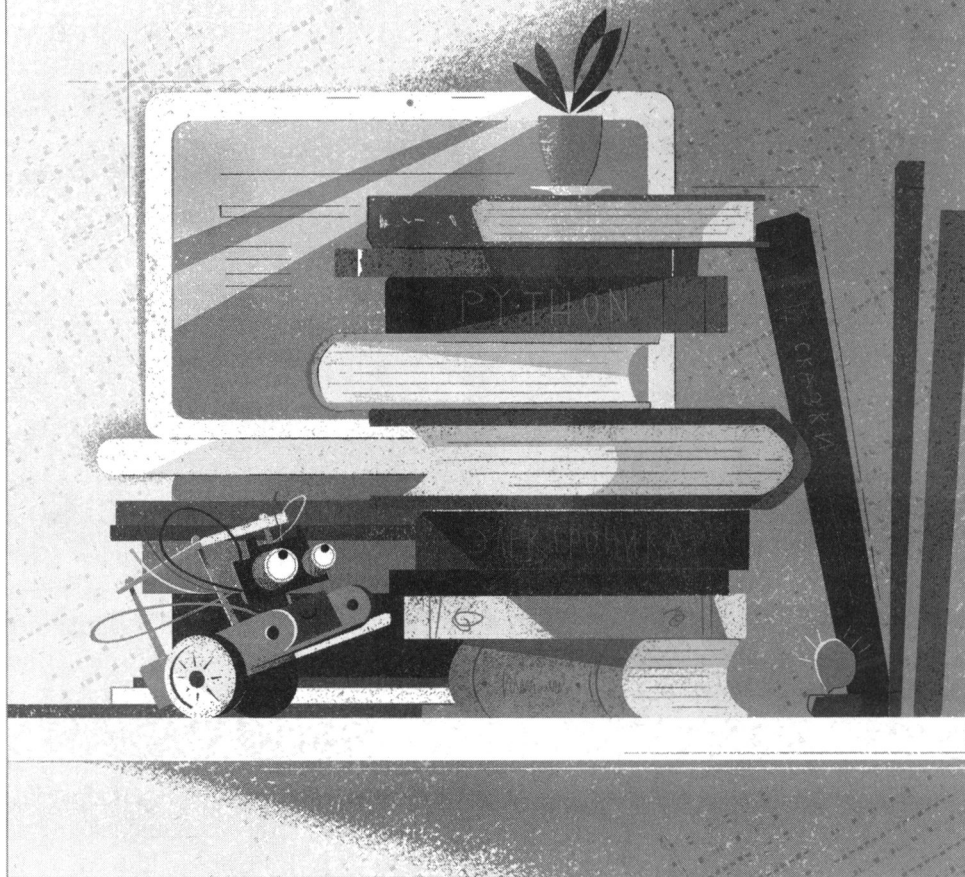
ИНТЕРНЕТ-МАГАЗИН

BHV.RU

КНИГИ, РОБОТЫ,
ЭЛЕКТРОНИКА

Интернет-магазин издательства «БХВ»

- Более 30 лет на российском рынке
- Книги и наборы по электронике и робототехнике по издательским ценам
- Электронные архивы книг и компакт-дисков
- Ответы на вопросы читателей



БХВ-Электроника bhv.ru/elements

Электронные компоненты
для мейкеров



КОНТРОЛИРУЕМЫЙ ВЗЛОМ БИБЛИЯ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Когда злоумышленники атакуют не компьютер или мобильный телефон, а пользователя, пытаясь заставить его совершить нужные им действия или выдать конфиденциальную информацию, это называется социальной инженерией. Иконой социальной инженерии считается известнейший американский хакер Кевин Митник. Широко известные случаи телефонного мошенничества от имени служб безопасности банков, фишинговые рассылки, заманивающие жертв на поддельные сайты, подложные страницы в социальных сетях, с помощью которых киберпреступники выманивают у пользователей деньги и конфиденциальные сведения, — все это частные проявления социальной инженерии.

Эта книга подробно рассказывает о большинстве известных на сегодняшний день методах социальной инженерии, направленных на получение несанкционированного доступа к корпоративной информации, а также предлагает конкретные способы защиты от нее — как организационные, так и технические. Приведены практические примеры фишинговых писем, раскрыты применяемые мошенниками тактики и психологические приемы, рассмотрен используемый ими программный инструментарий. Подробно описаны трюки, позволяющие вводить пользователей в заблуждение. Автор наглядно демонстрирует примеры использования различных векторов атак: по электронной почте, в мессенджерах, в социальных сетях, а также в реальной жизни. Во втором издании особое внимание уделено использованию в социальной инженерии и фишинге современных технологий искусственного интеллекта.

Книга будет полезна сотрудникам служб безопасности предприятий, пентестерам, руководителям IT-отделов компаний, желающих повысить осведомленность своих сотрудников, психологам, изучающим социальную инженерию, а также всем, кто интересуется вопросами защиты от сетевых мошенников.

В книге вы найдете:

- 130 практических примеров атак;
- методику создания 10 000 сценариев учебных атак;
- более 110 ссылок на дополнительную полезную информацию;
- пошаговую инструкцию для проведения учебных атак от этапа подготовки до составления отчета;
- десятки организационных и технических методов защиты от социальной инженерии в компаниях.



Другач Юрий Станиславович — участник программ Bug Bounty, находил уязвимости в PayPal, Google, «Яндекс», Mail.ru. Автор статей в журнале «Хакер», на порталах SecurityLab, «Хабр», а также создатель и автор блога о социальной инженерии icast.ru. Сооснователь компании по обучению киберграмотности StopPhish.

ISBN 978-5-9775-1990-8



191036, Санкт-Петербург,
Гончарная ул., 20
Тел.: (812) 717-10-50,
339-54-17, 339-54-28
E-mail: mail@bhv.ru
Internet: www.bhv.ru

