

### **Угрозы социальной инженерии для информационной безопасности.**

Для построения системы безопасности следует ввести следующие понятия.

**Информация** – является одним из важнейших активов компании. Информация может составлять коммерческую тайну компании, т.е. при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или принести иную коммерческую выгоду компании. Соответственно, такую информацию необходимо защищать.

**Кви-про-кво**- Злоумышленник может позвонить по случайному номеру в компанию, и представиться сотрудником техподдержки, опрашивающим, есть ли какие-либо технические проблемы. В случае, если они есть, в процессе их «решения» цель вводит команды, которые позволяют злоумышленнику запустить вредоносное программное обеспечение.

**Претекстинг** — это действие, отработанное по заранее составленному сценарию (претексту). В результате цель (жертва) должна выдать определённую информацию, или совершить определённое действие, чтобы содействовать злоумышленникам.

**Социальная инженерия** — это метод (атак) несанкционированного доступа к информации или системам хранения информации без использования технических средств. Метод основан на использовании слабостей человеческого фактора и является очень эффективным.

**Фишинг** — техника, направленная на жульническое получение конфиденциальной информации. Обычно это информационное письмо которое после прочтения просит оставить отзыв или перейти по ссылке тем самым заставляет запускаться вредоносное ПО, или переход на вредоносные сайты.

Подобными видами атак в основном подвергаться средние и крупные корпорации, банки, промышленные и научно исследовательские центры, отследить такие атаки становится зачастую довольно проблематично, особенно когда злоумышленники получают доступы к специализированному ПО компании. Что же тогда может уберечь ИТ безопасность от подобных посягательств.

Во первых это правильно спроектированное ПО, постоянная проверка насколько эффективно построены процессы идентификации и управления этими рисками. Процесс управления ИТ построенного отдельно от общего процесса управления компании или встроен в него? Покрывают ли существующие программы все ИТ-активы компании, включая теневое ИТ (Excel-файлы с макросами, личные флешки, использование онлайн сервисов: Google Docs, Skype и т.д.)? Используется ли специальное программное обеспечение для управления рисками?

Во вторых это способы защиты обучением персонала. Работники компании должны знать об опасности раскрытия информации и способах ее предотвращения. Кроме того, сотрудники компании должны иметь четкие инструкции о том, как, на какие темы говорить с собеседником, какую информацию для точной аутентификации собеседника им необходимо у него получить.

В третьих каждый сотрудник компании должен нести ответственность за ту информацию которой он обладает и нести ответственность за её распространение, компанией тратятся огромные финансовые средства на обеспечение информационной безопасности техническими методами, однако эти технические средства могут быть обойдены, если сотрудники не будут применять меры по противодействию социальным инженерам.

В книге The Art of Deception — «Искусство обмана» Кевина Д. Митника — доказывається, насколько мы все уязвимы. В современном мире, где безопасность подчас выходит на первый план, на защиту компьютерных сетей и информации тратятся огромные деньги. Деньги тратятся на технологии безопасности. Эта книга объясняет, как просто бывает перехитрить всех защитников и обойти технологическую оборону, как работают социоинженеры и как отразить нападение с их стороны Кевин Митник и его соавтор, Бил Саймон рассказывают множество историй, которые раскрывают секреты социальной инженерии. Авторы дают практические советы по защите от атак, по обеспечению корпоративной безопасности и снижению информационной угрозы.

Лучше всего смотреть на социальную инженерию со стороны реальных примеров, такие примеры описаны в книге Кевина Митника основоположника социальной инженерии, а также на примере людей, которые получают от других то, что они хотят, используя тактику социальной инженерии. Торговые представители, учителя, актеры, журналисты, менеджеры, эксперты безопасности – все они в своей профессиональной деятельности пользуются внушительным арсеналом социальной инженерии.

#### Верифицированный отправитель

Иногда администраторы сайтов по недосмотру не включают фильтрацию поля «Имя» в форме регистрации (скажем, при подписке на рассылку или при отправке какой-нибудь заявки). Вместо имени можно вставить текст (иногда килобайты текста) и ссылку на вредоносный сайт. В поле email вставляем адрес жертвы. После регистрации этому человеку придет письмо от сервиса: «Здравствуйте, уважаемый...», а дальше — наш текст и ссылка. Сообщение от сервиса будет в самом низу.

Как это превратить в оружие массового поражения?

Элементарно. Вот один случай из моей практики. В одном из поисковиков в декабре 2017 года была обнаружена возможность отправки сообщений через форму привязки запасного email. До того как я выслал отчет по программе bug bounty, имелась возможность отправлять 150 тысяч сообщений в сутки — нужно было только немного автоматизировать заполнение формы.

Этот трюк позволяет отправлять мошеннические письма с настоящего адреса техподдержки сайта, со всеми цифровыми подписями, шифрованием и так далее. Вот только вся верхняя часть оказывается написанной злоумышленником. Такие письма приходили и мне, причем не только от крупных компаний вроде booking.com или paypal.com, но и от менее именитых сайтов.

Здравствуйте, теперь вы можете пользоваться [www.goo.gl/YHPtz](http://www.goo.gl/YHPtz) !

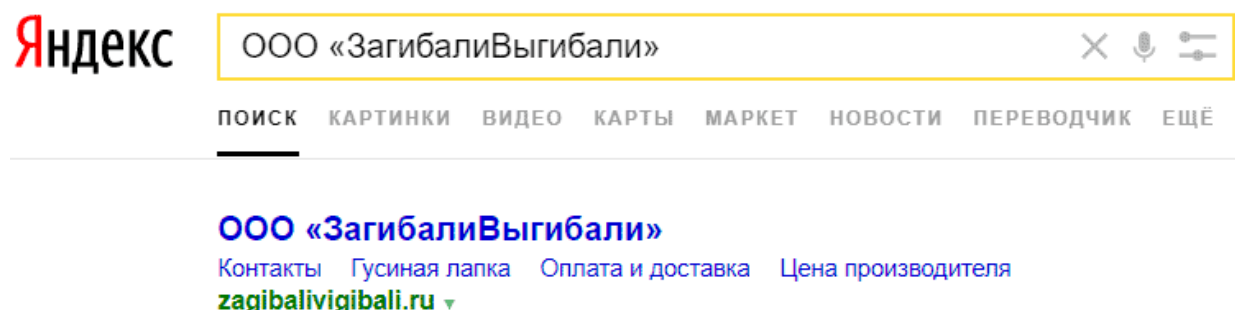
Чтобы подтвердить привязку этого адреса к аккаунту **a\*\*\*7**, введите код **921956** или перейдите по ссылке: [REDACTED]

Если аккаунт **a\*\*\*7** не ваш, не обращайте внимания на это письмо

Примеры социальной инженерии. Метод «Верифицированный отправитель»  
В моем тесте по ссылке перешло около 10% получателей. Комментарии излишни.

## Любопытство

Этот метод заставить человека перейти по ссылке требует некоторой подготовки. Создается сайт фейковой компании с уникальным названием, которое сразу привлекает внимание. Ну, например, ООО «ЗагибалиВыгибали». Ждем, пока поисковики его проиндексируют.



Теперь придумываем какой-нибудь повод разослать поздравления от имени этой компании. Получатели тут же начнут его гуглить и найдут наш сайт. Конечно, лучше и само поздравление сделать необычным, чтобы получатели не смахнули письмо в папку со спамом. Проведя небольшой тест, я легко заработал более тысячи переходов.

## Фейковая подписка на рассылку

О фишинге путем заманивания на фейк-страницу вы уже наверное знаете. Вот совсем легкий способ заставить пользователя перейти на сайт по ссылке в письме. Пишем текст:

«Спасибо, что подписались на нашу рассылку! Ежедневно вы будете

получать прайс-лист железобетонной продукции. С уважением, ...». Дальше

добавляем ссылку «Отписаться от рассылки», которая будет вести на наш

сайт. Конечно, никто на эту рассылку не подписывался, но вы удивитесь,

узнав число спешно отписывающихся.

## Майнинг имейлов

Чтобы составить свою базу, необязательно даже писать собственный краулер и обходить сайты в поисках плохо лежащих адресов. Достаточно списка всех русскоязычных доменов, которых сейчас насчитывается около пяти миллионов. Добавляем к ним info@, проверяем получившиеся адреса и в итоге имеем где-то 500 тысяч рабочих почт.

Точно так же можно приписывать director, dir, admin, buhgalter, bg, hr и так далее. Под каждый из этих отделов готовим письмо, рассылаем и получаем от сотен до тысяч ответов от сотрудников определенной сферы деятельности.

А что это там написано?

Чтобы заманить людей с какого-нибудь форума или сайта с открытыми комментариями, не нужно выдумывать заманчивые тексты — достаточно всего лишь запостить картинку. Просто выберите что-нибудь попривлекательнее (какой-нибудь мем) и ужмите так, чтобы различить текст было невозможно. Любопытство неизменно заставляет пользователей кликать по картинке. Я в своих исследованиях провел эксперимент и получил

таким примитивным способом около 10k переходов. Этим же способом злоумышленники когда-то доставляли трояны через ЖЖ (живой журнал).



Как вас зовут?

Заставить пользователя открыть файл или даже документ с макросом не так сложно, даже несмотря на то, что многие слышали о подстерегающих опасностях. При массовой рассылке даже просто знание имени человека серьезно повышает шансы на успех.

Например, мы можем отправить письмо с текстом «Этот email еще активен?» или «Напишите, пожалуйста, адрес вашего сайта». В ответе как минимум в 10–20% случаев придет имя отправителя (чаще это встречается в крупных компаниях). А через какое-то время пишем «Алёна, здравствуйте. Что такое с вашим сайтом (фото приложил)?» Или «Борис, добрый день. Никак не разберусь с прайсом. Мне 24-я позиция нужна. Прайс прикладываю». Ну а в прайсе — банальная фраза «Для просмотра содержимого включите макросы...», со всеми вытекающими последствиями.

В общем, персонально адресованные сообщения открываются и обрабатываются на порядок чаще.

Массовая разведка

Этот сценарий — не столько атака, сколько подготовка к ней. Предположим, мы хотим узнать имя какого-то из важных сотрудников — например,

бухгалтера или руководителя службы безопасности. Это несложно сделать, если отправить кому-то из сотрудников, которые могут обладать этой информацией, письмо следующего содержания: «Подскажите, пожалуйста, отчество директора и график работы офиса. Нужно отправить курьера».

Время работы спрашиваем, чтобы замылить глаза, а спрашивать отчество — это трюк, который позволяет не выдавать, что мы не знаем имени и фамилии. И то и другое, скорее всего, будет содержаться в ответе жертвы: ФИО чаще всего пишут целиком. Мне в ходе исследования удалось таким образом собрать ФИО более чем двух тысяч директоров.

Если нужно узнать почту начальства, то можно смело писать секретарю: «Здравствуйте. Давно не общался с Андреем Борисовичем, его адрес andrey.b@company.ru еще рабочий? А то ответ не получил от него. Роман Геннадьевич». Секретарь видит email, выдуманный на основе настоящих ФИО директора и содержащий сайт компании, и дает настоящий адрес Андрея Борисовича.

### Персонализированное зло

Если нужно заставить отреагировать на письмо большое количество организаций, то первым делом надо искать болевые точки. Например, магазинам можно направлять жалобу на товар и грозить разбирательствами: «Если вы не решите мою проблему, буду жаловаться директору! Это что вы мне такое доставили (фото прилагаю)?! Пароль от архива 123». По базе автосервисов точно так же можно рассылать фотографию с поломкой и вопросом, смогут ли отремонтировать. По строителям — «проект дома».

В моем небольшом исследовании на такие письма откликались как минимум 10% получателей.

## Сайт не работает

Базу сайтов с почтовыми адресами владельцев легко превратить в переходы на любой другой сайт. Отправляем письма с текстом «Почему-то страница вашего сайта `www.site.ru/random.html` не работает!» Ну и классический прием: в тексте ссылки жертва видит свой сайт, а сама ссылка ведет на другой URL.

## Мультилендинг

К этому способу нужно будет подготовиться. Создаем сайт-одностраничник, оформляем под новостной ресурс. Ставим скрипт, который меняет текст на сайте в зависимости от того, по какой ссылке человек перешел.

Делаем рассылку по базе, состоящей из адресов и названий компаний. В каждом письме — уникальная ссылка на наш новостной ресурс, например `news.ru/?1234`. Параметр 1234 привязывается к определенному названию компании. Скрипт на сайте определяет, по какой ссылке пришел посетитель, и показывает в тексте название компании, соответствующее почте из базы.

Зайдя на сайт, сотрудник увидит заголовок «Компания ... (название компании жертвы) снова бесчинствует». Далее идет короткая новость с какими-нибудь небылицами, а в ней — ссылка на архив с разоблачительными материалами (троянem).

## Выводы

Социальная инженерия в рамках безопасности информационных систем где способы доступа техническими средствами всё более усложняются для злоумышленников на передний план выходит социальная инженерия и человеческий фактор которые более податливы.