Генератор “фотографий” https://thisxdoesnotexist.com/
Инструменты, которые будут полезны **для подготовки фишинга:**

- https://screenchat.live/
- https://zeoob.com/
- https://fakedetail.com/
  Эти сервисы помогут создать скриншот правдоподобной переписки в мессенджерах, которые можно использовать как пруфы во время атаки.

Фреймворк фишинга с открытым исходным кодом (getgophish.com).

- **Функции**:
  - Упрощает настройку фишинговых кампаний.
  - Сохраняет настройки SMTP-сервера для отправки писем.
  - Включает редактор WYSIWYG для создания шаблонов писем.
  - Позволяет запланировать отправку писем.
  - Обеспечивает аналитику: сколько писем отправлено, открыто или нажато.

Для создания фишинговых ресурсов традиционно используются сервисы:

- Evilginx2
- Modlishka
- Zphisher

https://tryhackme.com/r/room/phishingyl

Домены

Ошибка в написании: goggle.com против google.com
Дополнительный период: go.ogle.com против google.com
Переключение цифр на буквы: g00gle.com против google.com
Фразировка: googles.com против google.com
Дополнительное слово: googleresults.com против google.com

Создание сертификатов SSL/TLS для выбранного вами доменного имени добавит дополнительный уровень аутентичности атаке.

Настройка записей DNS, таких как SPF, DKIM, DMARC, улучшит доставляемость ваших писем и гарантирует, что они будут попадать в папку «Входящие», а не в папку «Спам».

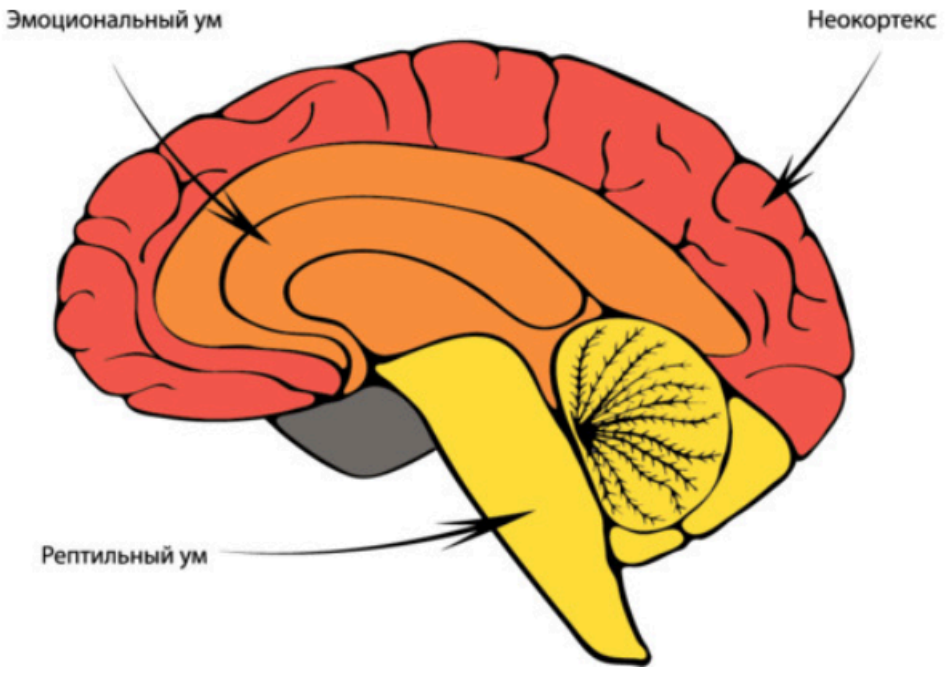
TLD (Top Level Domain) — это часть доменного имени .com .net .co.uk .org .gov и т. д.,
сейчас существует сотни вариантов TLD. Распространенный трюк при выборе домена — использовать то же имя,
но с другим TLD. Например, зарегистрируйте tryhackme.co.uk, чтобы выдать себя за tryhackme.com.

Unicode
Первоначально доменные имена состояли из латинских символов (a-z) и цифр (0-9).
Однако в 1998 году была внедрена поддержка IDN (интернационализированных доменных имен),
что позволило использовать символы из различных алфавитов,
таких как арабский, китайский, кириллица, иврит и другие.
Основная проблема IDN заключается в визуальной схожести символов из
разных языков. Например, символ Unicode U+0430 (кириллическая строчная буква "а")
выглядит идентично символу Unicode U+0061 (латинская строчная буква "a"), что даёт
злоумышленникам возможность регистрировать доменные имена, почти идентичные существующим.

Введение

Социальная инженерия (*social engineering*) — это метод, который базируется на психологических особенностях личности и основных закономерностях человеческого мышления, и предусматривает действия по манипулированию мыслями и поступками людей. Кибератака, при которой используются методы социальной инженерии, всегда **адаптирована под индивидуальные особенности объекта нападения**. Кажется, что для применения социальной инженерии нужно быть хорошим психологом, актёром, разбираться в людях, иметь талант (нужное подчеркнуть). Но на самом деле принципов не так и много, большинство из них стары, как мир.

Устройство мозга



1. Нижний, наиболее примитивный — “Рептильный ум” наиболее старый и **отвечает только за примитивные действия**, непосредственно связанные с выживанием, продолжением рода, властью, питанием, контролем, ритуалам и стадным поведением.
2. Следующая кора нашего мозга присуща млекопитающим и в разных источниках может называться **“Лимбической”** или **“Эмоциональной”**. Она отвечает за построение отношений и семьи, эмоции, удовольствия, социализацию.
3. Наиболее внушительную часть человеческого мозга занимает **сложная и развитая кора головного мозга** — “Неокортекс”. Именно Неокортекс отвечает за мышление, визуализацию, речь, интеллект, сенсорику. Человек является обладателем наиболее развитой “Новой коры”, хотя она есть и в разной степени развита у дельфинов и некоторых других животных.

Социáльная инженерия — психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации с использованием инструментов хакинга.

В бестселлере «Психология влияния» (1984 г.), профессор психологии Роберт Чалдини описал **шесть методов влияния, которые применяют в социальной инженерии:**

1. Последовательность: придерживаемся убеждений, соответствующих нашим ценностям.
2. Взаимность: подразумевает плату добром за добро.
3. Социальное доказательство: относится к психологическому явлению, когда человек соглашается с тем, что делает большинство людей.
4. Симпатия: желание исполнять просьбы людей, которые нам нравятся.
5. Власть и авторитет: подразумевает готовность идти за людьми, к которым есть доверие и уважение.
6. Дефицит: желание иметь то, что недоступно.
   В странах, где преобладает население славянской группы народов, в отличии от западных стран, выделяют

и *7 метод влияния*:

7. Желание помочь.
   Именно поэтому у нас так хорошо работают просьбы направить некую сумму, даже если просящий мало нам знаком.

Претекстинг (*pretexting*) — это техника атак, в которой злоумышленник представляется другим человеком и получает нужные данные.

Легендирование — это тот же претекстинг, но с качественно продуманной легендой и скриптом на случай нештатных ситуаций.
Под каждую атаку и даже ситуацию следует продумать легенду.
При атаке с продуманной легендой необходимо:

- продумать и следовать целям;
- ориентироваться в легенде и отличать её от реальности;
- работать с краткосрочной памятью;
- уметь аргументировать факты легенды.

Полезным ресурсом для атак этого типа в социальных сетях будет генератор “фотографий” *DoesNotExist*. Сервис позволяет генерировать уникальные “фотографии” пользователей, сдаваемых квартир, пейзажи и многое другое. Эти фотографии не будут находиться поиском на фотобанках.

В 1906 году неподалеку от Берлина в городе Кёпенике безработный Вильгельм Фогт в купленной для этого форме прусского капитана зашёл в казармы и приказал небольшому отряду гренадёров захватить городскую ратушу. Когда ратуша пала, он забрал у сдавшегося бургомистра несколько тысяч казённых марок, а отряду приказал охранять здание. Сбросив форму Фогт покинул город.

сточник: Вильям Фогт ведёт отряд гренадеров на захват ратуши.

Ярким примером, объединяющим несколько этих способов будет звонок сотруднику от “руководителя”, который быстрым темпом, явно спеша, скажет что он находится на совещании и ему срочно нужна какая-либо информация или даже логин с паролем от системы. Срочность, важность и желание помочь будут решающими, даже если голос окажется мало похож на нужный.

Стрессовая ситуация может полностью отключить рациональное мышление и люди начинают помогать “начальнику”, даже если у них нет такого руководителя или он давно уволился.

Вне зависимости от способа — важно действовать решительно.

Эффект коломбо

Если вспомнить ранее описанные методы Чалдини, можно выделить два социальных: желание обладать властью и всё контролировать. Если сразу предоставить в диалоге все преимущества оппоненту и удерживать его в состоянии комфорта, можно усыпить его бдительность и получить дополнительную информацию, необходимые доступы.

Преуспел в этом известный киногерой второй половины 20-го века Комиссар Коломбо, воплощенный Питером Фальком.

Его персонаж является антонимом классическому всегда идеальному детективу. Коломбо был в мятом плаще, передвигался на маленьком старом автомобиле, постоянно что-то ронял или оставлял. Просил ручку у подозреваемого, чтобы записать его слова, рассказывал о жене и собаке. Всё это происходило в аристократических декорациях и идеальный преступник? не воспринимая детектива-простака всерьез, выдавал ему всю информацию об убийстве сам спокойно и легко. Раскрывал все карты лейтенант обычно фразой похожей на “Ещё один маленький вопрос”. Раскрывать карты социальному инженеру обычно не требуется, но остальные ситуации, в которые попадает лейтенант можно переосмыслить для атаки и создать образ живого неидеального человека.

Если собеседник не идеальный, человек намного легче и расслабленнее ведёт диалог. Специально допущенные оплошности в скрипте общения помогут собеседнику остаться в состоянии комфорта и взаимодействовать со средним эмоциональным мозгом для налаживания контакта. Неидеальный собеседник воспринимается ближе и понятнее, с таким человеком можно наладить длительное общение, например, дружбу.

Ещё один способ быстрее наладить общение, это найти что-то общее с собеседником, например, имя, увлечения, Родина, учебное заведение. Чтобы быстрее попасть в точку, используя этот способ, конечно, нужна разведка и подготовка — нужно хорошо представлять то, о чём вы планируете общаться. Самый популярный способ применения — представиться тем же именем, что и у вашего собеседника. Когда человек слышит или видит своё имя, это является дополнительным фактором, положительно настраивающим его.

Также достаточно часто мы сталкиваемся с социальной инженерией, направленной на то, чтобы «извлечь» из пользователя данные, необходимые для восстановления пароля или доступа к ящику. Например, паспортные данные пытаются запросить под видом получения выигрыша в лотерею. Ответ на секретный вопрос могут выпытать в обычной беседе в соцсетях («У тебя есть кот? Какой симпатяга! А как его зовут?»). Всё объясняет классическая шутка с Баша:

```
_Коннект: Слушай, мож мы родственники?_

_ALEXA: думаешь???_

_Коннект: Ну, может дальние. Какая девичья фамилия была у твоей матери?_

_ALEXA: *енко_

_Коннект: О, у тебя 8 новых писем )_

_ALEXA: в смысле???_
```

Обратная социальная инженерия

Ещё один интересный метод заключается в том, чтобы инициатором взаимодействия был не атакующий, а жертва. Для этого у жертвы создаётся нестандартная ситуация и как бы между делом даются решения этой ситуации. Например, поломка компьютера и контакты “технической поддержки” на видном месте.

Интересный способ обратной социальной инженерии основан на **буллинге**. Используя подставной профиль, можно добавиться в друзья жертве и начать флиртовать. После получения реакции от жертвы ответить резкими угрозами. Жертва или на этапе флирта, или на этапе угроз начнёт собирать о собеседнике информацию и изучать страницу атакующего, где в контактах можно разместить фишинговую ссылку. Вероятность нажатия на неё будет достаточно высокой.

Для обратной социальной инженерии можно применить и **схему, предложенную Чалдини**, в которой человек всегда старается ответить добром на добро и вернуть долг. Если оказать человеку услугу или даже подарить некий презент, собеседник почувствует себя обязанным вам -> следующим этапом можно попросить открыть его нужную дверь или переслать фишинговое письмо внутри компании.

Фишинг

Несложно догадаться о происхождении слова фишинг (от англ. *fishing*), что значит «рыбалка» или «рыбная ловля». В сети Интернет в роли рыбаков выступаю злоумышленники, а «рыбы» — это данные, за которыми ведётся охота.

В письме используются все те же методы, что и для общения, но к ним добавляется файл или ссылка.

Эмоция	Типовая фраза из письма
Страх	Ваш компьютер заражен и заблокирован. Кликните здесь.
Раздражение	Чтобы отписаться, перейдите по ссылке.
Невнимательность	Похожие домены.
Любопытство	Мы сделали несколько фотографий на прошлом мероприятии и планируем сделать прессрелиз. Проверьте и выберите фото для публикации.
Жадность	Выиграй путевку в Дубаи.
Желание помочь	Кажется, ваш коллега потерял вещи - помогите ему.

Для реализации социального доказательства в письмо достаточно добавить строчку, например: “проверено *Kaspersky Mail Checker*”.

--> Во-первых, чем официальнее письмо, тем более грамотно, с точки зрения орфографии, оно составлено. Письмо из государственной организации редко содержит ошибки.

--> Во-вторых, письмо должно содержать какие-либо контакты внизу. И здесь важно подобрать номер для письма: будет ли он настоящим и официальным роботом автоответчиком, будет всегда выключенным, или на другом конце может ответить атакующий. Главное, чтобы на другом конце не ответил настоящий сотрудник организации.

Хорошим решением будет использовать фишинг с подделкой автоматически-рассылаемых писем, например, о смене пароля или входа в аккаунт. Это автоматически создаёт состояние стресса и нехватки времени. Системное письмо может расцениваться как экспертное. Контакты в таком случае оставлять не обязательно. Для таких писем важно в точности повторить дизайн оригинального письма.

Одним из самых-самых запомнившихся мне фишинговых писем было просто повторяющаяся бесполезная рассылка с небольшой серой кнопкой "Отписаться внизу письма". Вредоносное содержимое было как раз в кнопке.

--> Третье, на что нужно обратить внимание — это адрес отправителя. Необходимо или использовать подмену адреса отправителя (это текстовое поле), или использовать имя домена, которое выглядит или звучит похоже.

Чтобы письма проходили проверки антифишинговых и антиспам-систем, будет полезным настроить *SPF*-записи на *DNS*-сервере и указывать корректные *DKIM*-подписи для создаваемых писем. Этот подход позволяет обойти верификацию адреса почтового сервера отправителя, но оставляет дополнительные цифровые следы для криминалистов.

Исследования атак успешных хакерских группировок показали, что часто применяется **многоэтапная схема фишинга**.

На первом этапе фишинговые письма рассылаются по всем собранным на этапе разведки адресам. Далее злоумышленник получая доступ к инфраструктуре случайного сотрудника закрепляется и изучает компанию

изнутри, в том числе читает переписку. Из почты злоумышленник узнаёт формат общения внутри компании, внутренний сленг и схемы взаимодействия сотрудников между собой. Спустя время, при переходе к активной фазе готовятся фишинговые письма для атаки внутри компании - с внутренних почтовых ящик на нужных сотрудников.

При **внутреннем фишинге** злоумышленник получает огромное преимущество:

- внутренняя переписка редко проходит спам. фильтры и песочницы;
- злоумышленник знает, как выглядит типовое письмо и фишинговое выглядит максимально неотличимо;
- знает, как в компании принято писать имена;
- доверие к коллеге выше, чем к чужому;
- обратиться к читателю по имени проще, так как имена сотрудников уже известны.

В итоге получаем много тонкостей, которые нужно учесть при подготовке рассылки. Также из внутренней переписки получаем базу внутренних телефонов, что позволяет использовать дополнительный вектор атаки.

Дорожное яблоко

Это один из самых древних способов. Заключается он в том, чтобы подбросить на пути жертвы некий ценный предмет, который захочется использовать по назначению.

Во времена древней греции это был статуя Троянского коня, которую хотелось поставить на видное место. Теперь же дорожными яблоками чаще всего оказываются флешки, зарядки или блютус устройства.

На них записывается эксплойт и подбрасывается жертве по пути к двери или к машине так, чтобы жертва наверняка его заметила и взяла.

Недавно этот способ был открыт заново при помощи криптокошельков. Группа злоумышленников рассылала жертвам по слитой базе вредоносные криптокошельки в фирменной упаковке с инструкцией по замене. Сообщалось, что криптокошелёк, которым пользуется жертва скомпрометирован и его необходимо заменить присланным. Жертва подключала кошелёк и запускала приложение из комплекта. Действуя по инструкции, жертва вводила код восстановления и таким образом передавала управление криптовалютой злоумышленникам.

Плечевой серфинг

Под этим понятием обычно скрывается незаметное наблюдение за экраном компьютера из-за плеча жертвы. Пандемия и удалённая работа развили этот способ до невиданных ранее масштабов — секретные данные могут быть в открытом виде на ноутбуке удалённщика, который работает из кафе. Так, для получения конфиденциальной информации не требуется попадать в офис и придумывать причину стоять за спиной нужного вам работника. Достаточно узнать, где теперь он работает и быть ближе к нему.

Компьютеры всё чаще остаются незаблокированными, а пароли в общественном месте снять не составляет большого труда. Использование биометрических систем тоже нельзя считать непреодолимой преградой.

Trash Bin серфинг

Ещё одно понятие социальной инженерии, обозначающее разведку через поиск информации в мусорном контейнере. Большинство компаний не имеет привычки проводить выбрасываемый мусор через шредер. И много информации можно почерпнуть из анализа выброшенного мусора и бумаг.

Так, уже упомянутый Кевин Митник, испытывающий особую любовь к телефонии, получил внутреннюю документацию, технологии работы и программы на телефонные аппараты и телефонные станции. Это позволило ему использовать незарегистрированные телефонные номера, звонить с чужих номеров, прослушивать чужие разговоры. Практически всю основную информацию для этих действий Кевин получил из мусорных контейнеров компаний-разработчиков.

Профайлинг

Для качественной атаки необходимо готовиться к ней и собирать информацию о жертве, заранее подбирать наиболее результативные методы.

Профайлинг («англ. *profile*» — профиль) — это совокупность психологических методов оценки и прогнозирования поведения на основе анализа собранной информации.

Социальные сети максимально упростили процесс сбора информации о компании и конкретной жертве. Это избавляет от необходимости подключения к каналам связи и копания в мусоре. Сотрудники банка получив работу сами пишут место работы на видном месте в социальных сетях и сразу становятся целью для атакующих этот банк злоумышленников. В пару кликов можно вывести весь список сотрудников организации, гордящихся своей работой напоказ. У них в друзьях несложно отыскать и большую часть оставшихся коллег.

Отыскав страницу руководителя целевой организации можно увидеть, что он на море. Находим в друзьях подчиненных можно отправить им эксплойт с кликбейтным заголовком и фишинговой ссылкой на “фотографии”

Попадание в офис

Но если попасть в офис всё же требуется? для этого также есть несколько надежных способов. Например, взять с собой громоздкую коробку? так вам даже наверняка откроют дверь, чтобы занести было легче.

Другой способ — найти людей, которые курят у входа. Присмотреться к ним (как выглядят их пропуски и дресс-код) и, когда вы будете уверенно смешиваться с толпой, зайти вместе с ними. Можно даже взять с собой электронный ключ похожего формата и приложить его к двери, чтобы он издал соответствующий звук.

В офисный центр можно зайти под предлогом заинтересованности в аренде помещения. С большой вероятностью вам выдадут временный пропуск, который откроет вам основные двери офиса.

Когда всё здание относится к одной компании, для проникновения внутрь определяется место, находящееся по близости к работающим там сотрудникам и не вызывающее никаких подозрений. Данная точка может располагаться, например, у ворот, через которые сотрудники заходят на территорию организации.

Рядом с ними можно попробовать скопировать их пропуск и получить их права доступа на территории здания.

Кроме вышеперечисленных примеров, не стоит забывать о следующих **важных пунктах**:

- права доступа к помещениям (например, по аналогии с привилегиями в *AD*);
- лазейки на периметре;
- логика СКУД;
- физическая защищённость линий коммуникации.
- мертвые зоны видеонаблюдения;
- работоспособность сигнализации;
- замки — на предмет устойчивости к взлому.

Противодействие социальной инженерии

Методы выявления и противодействия против таких атак публикуются практически ежедневно в различных изданиях. Банкам и кредитным организациям “Банк России” рекомендует ежеквартально уведомлять клиентов о безопасности банковских карт и защите их от злоумышленников. Поэтому большинство рекомендаций приведённых в юните покажутся слишком банальными, но, как ни странно, они остаются эффективны против социальной инженерии.

Выявление социальной инженерии в диалоге

Вишинг (англ. *vishing*, от *Voice phishing*) — метод социальной инженерии с использованием звонков, где злоумышленник, играя определённую роль (сотрудника банка, покупателя и т. д.), выманивают информацию или деньги у жертвы.
! Поэтому не разговаривайте с незнакомцами.

В качественно продуманной *APT*-атаке все ответы записываются и распределяются в зависимости от реакции:

Номер недоступен	**Звонок пропущен**	**Собеседник положил трубку сразу**	**Собеседник распознал СИ, стал угрожать и противодействовать**	**Собеседник вовлёкся в диалог**

Далее, в зависимости от реакции по базе будет совершена повторная атака с учётом наработок первой.

Злоумышленники обычно прибегают к психологическим уловкам, описанным в предыдущем юните. Главной уловкой является создание ощущения неотложной ситуации.

Фактор срочности может заставить жертву действовать необдуманно. Срочные решения сложно принимать именно потому, что приходится действовать в условиях нехватки достоверной информации. В таких ситуациях некогда советоваться и проверять все сообщённые атакующим данные, поэтому жертва начинает действовать, руководствуясь сильными чувствами: желанием помочь, стремлением получить признание или поскорее отделаться от неожиданной проблемы.

Небольшая пауза позволяет включить аналитический ум и избавиться от навязываемого злоумышленником дефицита времени.

Часто звонящий просит вас перевести звонок другому сотруднику, рассказывая легенду, почему он не может позвонить напрямую. При переводе звонка коллега увидит только ваш номер и не увидит номер злоумышленника, такой звонок коллега может рассмотреть как доверительный, переложив на вас ответственность. Поэтому переводить звонки следует, только если есть уверенность, что звонок не вредоносный.

При любом сомнении в пришедшем вам письме, ссылке, телефонном звонке или любых других подозрительных ситуаций необходимо взять паузу и дополнительно проверить информацию, самостоятельно перезвонить по достоверным контактам.

Запрашиваемую информацию также не следует сообщать сразу. Государственные организации для этого делают официальный запрос на официальный адрес организации.

Расчёт атакующих на то, что информация не будет вдумчиво анализироваться и проверяться. Следует **рационально оценить ситуацию и подумать:**

- Каким способом связался бы в текущей ситуации человек или компания?
- Какая вероятность указанного события?
- Может ли в действительности потребоваться запрошенная информация тому, кто её спрашивает?

Ещё одним триггером, который чувствуется в большинстве атак является **неприкрытое давление.** Атакующий уверенно диктует действия и требует их исполнения. Такое давление явно ощущается и в письмах, и в переписках. Пауза в разговоре будет универсальным решением и в этой ситуации.

Если атака не целевая, то злоумышленник с большей вероятностью переключится на следующую цель в базе.

Итак, в диалоге **при ощущении методов социальной инженерии, давления, неотложности** необходимо:

- запросить больше информации о звонящем;
- взять паузу;
- проверить информацию;
- при необходимости самостоятельно перезвонить по достоверному контакту.

Встреченных в закрытой части офиса незнакомых людей лучше проводить до общественных мест офиса, где они имеют право находиться самостоятельно или передать сопровождающему.

Противодействие фишингу

Фишинг — первый и самый часто используемый инструмент хакера для попадания в периметр организации и эксплуатирует он вечную уязвимость любой информационной системы, расположенную между креслом и монитором. Человеческий фактор, усталость, потеря концентрации и внимательности, недостаток информации и её плохое структурирование усиливает эффект. Поэтому часто атакующие выбирают для атаки конец квартала перед отчетностью или время черных пятниц, когда персонал наиболее уставший, а часть систем безопасности отключена.

Обычно фишинг не направлен на кого-то одного, а рассчитывается на большее количество людей. Фишингом, например, может стать, массовая рассылка писем с вредоносным программным обеспечением, раздача бесплатных устройств usb, создание ложного сайта и другое.

Перед получением письма человеком, оно должно проходить как минимум спам-фильтры и антивирусные проверки, а подозрительные - специализированные песочницы.

Рассылающие фишинговые письма не всегда могут знать кому отправляют, так как используют все адреса, которые удалось собрать. Поэтому письма могут приходить явно не по адресу и они редко персонализированы.

Как мы уже знаем из предыдущего юнита адреса отправителя или подменяются на нужный или используется как можно более похожий по написанию.

В самом письме могут быть различные ссылки или формы, или еще что угодно, требующее совершить какие - либо действия. Но если письмо выглядит подозрительным, совершать эти действия опасно.

Таким образом, при запросе каких - либо действий, желательно проверять домен, отличается ли он от корпоративного. Также следует относится ко всем сторонним доменам, с большой подозрительностью и не отправлять им никаких личных данных.

Если работа сотрудника заключается в общении с внешними подрядчиками, то для него возможен следующий сценарий:

Качественно оформленное письмо с чистым вложением и ссылкой. Кажется, что ссылка вставлена прямым текстом вместе со всей вложенностью. Но при наведении на неё, будет видно, что ссылка ведёт по другому адресу, а в письмо вставлен синий подчёркнутый текст, изображающий ссылку.

При переходе по вложенному файлу, пользователь попадет на сайт, где потребуется ввести аутентификационные данные. Делать этого конечно не стоит.

На что *следует обратить внимание при переходе на ресурс*, где просят ввести личные данные:

1. ***Url*** — неизвестный сайт, где просят ввести наши данные, однозначно он не принадлежит почте, к которой просит логин и пароль.
2. **Отсутствие шифрования** — в адресной строке видно отсутствие шифрования, а именно отсутствие зеленого замочка, который показывает наличие надежного сертификата шифрования, а значит если ввести логин и пароль, он может быть отправлен кому угодно без шифрования.

По логике, не следует переходить по неизвестной ссылке, но в случае если уже перешли, нужно провести полное сканирование устройства на наличие вредоносного ПО.

С ростом популярности QR-кодов вредонос для мобильных устройств может быть размещен в QR-коде. При качественной подготовке такое письмо спокойно пройдет все возможные проверки и достигнет сканера в смартфоне.

Вариаций может быть много, но в каждом случае, стоит присмотреться и не открывать присылаемые документы и отчеты.

Первое, о чем нужно подумать при получении подозрительного письма - по адресу ли оно пришло и ожидали ли вы его. Так или иначе, все получаемые письма обычно ожидаемые - рассылки, сообщения от коллег, информация об оформленных подписках.

Если письмо пришло явно не по адресу, например, бухгалтерский запрос системному администратору, следует присмотреться к письму внимательнее и осторожнее.

Следом стоит проверить источник письма, если письмо внутреннее и Exchange сервер подключен к базе AD, вместо адреса у правильного отправителя будет Имя из AD. Часто вместо подмены адреса злоумышленники регистрируют близкий по написанию адрес, который выявляется внимательным рассмотрением адреса. Сравните адрес с предыдущими письмами отправителя.

Проверьте ссылки в письме и нет ли в ссылке подмены. Подозрительные ссылки можно проверить через *VirusTotal* или в песочнице. Для базовых проверок писем **без чувствительной информации** можно использовать песочницу *Any.Run*.

Письмо с плохой орфографией также с головой сдаст начинающих злоумышленников.

Каким хочет быть фишинг?

Идеальным как в этом примере: