

# Противодействие мошенничеству

Метод получения необходимого доступа к информации, основанный на особенностях психологии людей называется **СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ**.

Основная цель — получение доступа к конфиденциальной информации, паролям, банковским данным и другим защищенным системам.

## Виды социальной инженерии

**Кви про кво** (услуга за услугу) — данная техника предполагает обращение злоумышленника к пользователю по электронной почте или корпоративному телефону. Злоумышленник может представиться сотрудником технической поддержки и сообщить о возникновении технических проблем на рабочем месте. В процессе «решения» проблемы, злоумышленник подталкивает жертву на совершение действий, позволяющих ему выполнить определенные команды или установить необходимое ПО на компьютере жертвы или получает интересующую его информацию.

**Обратная социальная инженерия** — данный вид направлен на создание такой ситуации, при которой жертва вынуждена будет сама обратиться к злоумышленнику за «помощью». Например, злоумышленник может выслать письмо с телефонами и контактами «службы поддержки» и через некоторое время создать обратимые неполадки в компьютере жертвы. Пользователь в таком случае позвонит или свяжется по электронной почте с злоумышленником сам, и в процессе «исправления» проблемы злоумышленник сможет получить необходимые ему данные.

**Претекстинг** — набор действий, отработанных по определенному, заранее составленному сценарию, в результате которого жертва может выдать какую-либо информацию или совершить определенное действие. Чаще всего предполагает использование Skype, телефона и т.п. Для использования этой техники злоумышленнику необходимо изначально иметь некоторые данные о жертве (имя сотрудника; должность; название проектов, с которыми он работает; дату рождения). Злоумышленник изначально использует реальные запросы с именем сотрудника компании и, после того как войдет в доверие, получает необходимую информацию.

**Плечевой серфинг** — наблюдение личной информации жертвы через её плечо. Этот тип атаки распространён в общественных местах (кафе, торговые центры, аэропорты, вокзалы), в общественном транспорте.

**Фишинг** (phishing: от английского fishing — рыбалка) — техника интернет мошенничества, направленная на получение конфиденциальной информации пользователей — логинов, паролей номера банковской карты, номера телефона и т.п.

**Цель** — получить доступ к онлайн-банкингу или кошельку жертвы в той или иной платежной системе и вывести средства на посторонние счета.

### Как работает фишинг?

На электронный адрес атакуемого приходит письмо, которое, в первую очередь, влияет на эмоции получателя, например, оповещение о большом выигрыше или же, наоборот, сообщение о взломе аккаунта с дальнейшим предложением перейти по ссылке и ввести данные авторизации. Пользователь переходит на предоставленный ресурс и «отдает» свой логин и пароль в руки мошенника, который, со своей стороны, достаточно быстро оперирует полученной информацией.

### Методы реализации фишинга:

- ✓ осуществление массовой рассылки электронных писем от имени знаменитых брендов; рассылка личных сообщений от имени Банков;
- ✓ получение информации из внутренней переписки внутри социальных сетей; использование фиктивных сайтов, похожих на официальный сайт Банка, на которых правонарушители пытаются побудить пользователя ввести свои логин и пароль от электронного банка, а также иную персональную информацию;
- ✓ использование поддельных сайтов интернет-магазинов/ туроператоров с крайне «доступными» ценами, за брендовые товары/ путешествия/ авиабилеты. В итоге есть вероятность заплатить за товар/ услугу, которые никогда не будут получены, так как их никогда не существовало.

## Как защититься от **ФИШИНГА!**

- ✓ Проверять доменное имя сайтов, на которых необходимо ввести персональные данные.
- ✓ Не доверять сообщениям, которые просят внести личные данные, лучше созвониться с банком и уточнить информацию (если правонарушители представляются работниками Банка).
- ✓ Регулярно обновлять антивирусное ПО.
- ✓ Критически оценивать «выгодные» предложения.

**Вишинг** (англ. vishing — voice+phishing) — один из методов социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, сотрудника правоохранительных органов, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определенных действий со своими счетами / платежными картами.

### Как работает вишинг?

Поступает звонок от «сотрудника банка, сотрудника правоохранительных органов, прокуратуры» или тому подобного.

Простят перезвонить на указанный номер или о необходимости немедленно предоставить полную информацию по банковским счетам/картам, иначе счет/карту заблокируют. Доверчивый пользователь, слыша подобную «угрозу», сразу же впадает в панику и может выдать все персональные данные вплоть до проверочного кода из SMS.

Также может быть предложена выгодная покупка с огромной скидкой или озвучена информация о выигрыше в какой-либо акции. Не нужно сразу же радоваться столь удачной покупке или выгодной акции, всегда стоит лишний раз перепроверить информацию, обратившись к официальным ресурсам. В последнее время мошенники пытаются завлечь жертв звонками/рассылками с предложениями социальных выплат, пособий и других доплат.

### Методы реализации вишинга:

- ✓ использование для связи с жертвой функции автонабора и возможностей интернеттелефонии;
- ✓ использование подмены номеров (при звонке, на телефоне у клиента отображается корректный номер реального Банка);
- ✓ использование информации о Банке/организации, от которой «якобы» звонят;
- ✓ использование базовых знаний о жизни жертвы, раскрытых ею в сети Интернет (открытые источники, социальные сети и т.д.).

## Как защититься от **ВИШИНГА!**

- ✓ Остерегайтесь незнакомых телефонных номеров с которых Вам звонят.
- ✓ Запросите номер телефона звонящего, уточните его ФИО и должность (если он представился сотрудником Банка) Вам человека и записав его, сообщите, что Вы перезвоните позже ему.
- ✓ Проверьте принадлежность номера телефона через сеть интернет.
- ✓ Чтобы подтвердить личность звонящих Вам людей, найдите альтернативный номер телефона организации, от которой звонят. Свяжитесь с представителем организацией напрямую по найденному номеру.
- ✓ Не перезванивайте по номеру телефона, который вам дали неизвестные люди (этот номер может быть подставным номером телефона).
- ✓ Правонарушители обладают изначально базовой информацией о Вас. Будьте бдительны и не думайте, что если звонящий раскрывает минимальную информацию о Вас, то он действительно является сотрудником фирмы от имени которой якобы звонит.

### **ВАЖНО!**

- ✓ Ни при каких обстоятельствах не раскрывайте данные своей карты (PIN код, номер карты, пароль от электронного Банка, код CVV). Организациям такие данные не нужны, а сотрудники банка и так знают необходимые им реквизиты.
- ✓ Не переводите денежные средства на счета, которые указывают правонарушители. В данном случае, Вы можете также стать соучастником преступления.
- ✓ Если Вы думаете, что это фиктивный звонок, вы можете сообщить об этом оператору сети, а также внесите данный телефон номер в свой черный список номеров в телефоне.

**Смишинг** (англ. smishing — sms+phishing) — один из методов социальной инженерии, направленный на переход пользователем по вредоносной ссылке из SMS-сообщения, либо на получение посредством SMS-сообщения конфиденциальной информации у держателя платежной карты.

### Как работает фишинг?

Смишинг-сообщение может иметь вид сообщения от известного банка, знакомой компании или быть просто оповещением о внезапном выигрыше в лотерею или в крупную акцию. В случае с SMS выявить подвох несколько сложнее, нежели при фишинге, т.к. сообщения небольшие и имеют меньше информации, помимо самой ссылки.

Скорее всего это будет предложение перейти по ссылке и ввести данные или же просто позвонить или отправить обратное сообщение, что понесет за собой некоторые затраты.

**Запомните!** Злоумышленники в sms могут не использовать слова такие как пароль, CVV и т.п., они их заменяют на схожие по понятиям.

Как одна из разновидностей — получение SMS-сообщения от банка о списании или начислении незначительной суммы (чаще всего 1 руб.) за услуги Яндекс-такси/ иных операторов перевозок, когда фактически поездки не совершались.

## Как защититься от СМШИНГА!

- ✓ Необходимо помнить, что любые подобные оповещения должны настораживать.
- ✓ Не стоит отвечать на них, следует еще раз перепроверить информацию с помощью звонка на горячую линию подлинного сервиса.
- ✓ При получении SMS-сообщения о списании/ начислении 1 руб. за пользование услугами такси следует совершить следующие действия:
  - Обратиться в Банк по номеру, указанному на карте, привязанной для оплаты услуг такси с целью блокировки карты;
  - Составить и подать в Банк заявление о возможной компрометации карты с описанием произошедшего;
  - Направить заявление в Яндекс-такси/ иному оператору перевозок с описанием произошедшего;
  - В случае причинения материального ущерба подать соответствующее заявление в правоохранительные органы.