Текст к слайдам

**Социальная инженерия** — совокупность приёмов, методов и технологий создания такого пространства, условий и обстоятельств, которые максимально эффективно приводят к конкретному необходимому результату, с использованием социологии и психологии.

Злоумышленники выманиванивают конфиденциальную информацию у жертв либо побуждают жертв к совершению действий, направленных на проникновение в систему в обход системы безопасности.

С помощью методов и способов социальной инженерии совершаются практически все IT-преступления.

Рассмотрим основные схемы совершения IT-преступлений.

**Претекстинг** - это набор действий, отработанных по определенному, заранее составленному сценарию, в результате которого жертва может выдать какую-либо информацию или совершить определенное действие. Злоумышленник изначально использует реальные запросы с именем сотрудников (например представляется сотрудником банка или сотрудником полиции) и, после того как войдет в доверие, получает необходимую ему информацию.

Сегодня весьма распространены преступления, когда неизвестные представляются сотрудниками известных нам с вами банков. Под различными предлогами пытаются завладеть код-паролями, которые приходят вам на телефон в процессе разговора, а затем зайти в ваш личный кабинет и вывести оттуда ваши денежные средства якобы на безопасный счет. В конечном итоге мошенники оставляют вас с нулевым балансом.

Кроме того, зачастую неизвестные представляются сотрудниками различных ведомств (полиция, следственный комитет и др.). Сообщают вам ложную информацию о каком-либо преступлении, которое совершил ваш родственник или знакомый. Якобы от уклонения от уголовной ответственности, предлагают передать курьеру денежные средства. Такому виду преступлений подвержены в основном люди пенсионного возраста, то есть наши с вами бабушки и дедушки!

Обязательно расскажите им о таких преступлениях, предотвратите возможное совершение преступлений в отношении них.

**Фишинг** – техника интернет-мошенничества, направленная на получение конфиденциальной информации пользователей - авторизационных данных различных систем. Основным видом фишинговых атак является поддельное письмо, отправленное жертве по электронной почте, которое выглядит как официальное письмо от платежной системы или банка. В письме содержится форма для ввода персональных данных (пин-кодов, логина и пароля и т.п) или ссылка на web-страницу, где располагается такая форма. Причины доверия жертвы подобным страницам могут быть разные: блокировка аккаунта, поломка в системе, утеря данных и прочее.

**Троянский конь** – это техника основывается на любопытстве, страхе или других эмоциях пользователей. Злоумышленник отправляет письмо жертве посредством электронной почты, во вложении которого находится «обновление» антивируса, ключ к денежному выигрышу или компромат на сотрудника. На самом же деле во вложении находится вредоносная программа, которая после того, как пользователь запустит ее на своем компьютере, будет использоваться для сбора или изменение информации злоумышленником.

**Кви про кво** – данная техника предполагает обращение злоумышленника к пользователю по электронной почте или корпоративному телефону. Злоумышленник может представиться, например, сотрудником технической поддержки и информировать о возникновении технических проблем на рабочем месте. Далее он сообщает о необходимости их устранения. В процессе «решения» такой проблемы, злоумышленник подталкивает жертву на совершение действий, позволяющих атакующему выполнить определенные команды или установить необходимое программное обеспечение на компьютере жертвы.

**Обратная социальная инженерия** - данный вид атаки направлен на создание такой ситуации, при которой жертва вынуждена будет сама обратится 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.

Перейдем к конкретным способам совершения IT-преступлений.

Рассылку проводят на любые номера.

Заставляют получателя связаться со «службой безопасности для блокировки мошеннической транзакции. Во время звонка, злоумышленники при помощи социальной инженерии узнают полные данные карт и коды одноразовых паролей.

В последствии схема уже перестала работать, а злоумышленники придумали текст с новым сообщением: «На вашем счету заморожена сумма 3650 рублей из-за факта мошенничества». Клиента также звонит обратно по номеру и рассказывает все.

Позже получатели рассылки стали игнорировать такие сообщения, которые пришли с левых номеров. Тогда мошенники пошли еще дальше. Они стали подделывать номер 900 в Сбербанке и их клиентам все те же сообщения. Граждане при этом видят, что сообщение пришло из банка и действуют по намеченной схеме.

Жертве присылают с короткого номера, якобы "900", СМС, что с банковской карты будет совершен перевод в размере такой-то суммы. И примерно такой текст: «Подтвердите действие, отправив 1 на этот же номер. Если не подтвердите, то через 600 секунд это произойдет автоматически».

И тут в игру вступает «сотрудник банка», который звонит жертве и представляется сотрудником безопасности.

Суть схемы в том, что СМС приходит не с номера 900, мошенники заводят 9 и две буквы "о" -- 9оо, 9ОО, 9-00. Если не приглядываться - выглядит похоже.

Голос, записанный на автоответчик, представляется сотрудником банка, сообщает клиенту о списании с его счета 14 тысяч рублей и просит перезвонить по указанному номеру для установления причин этой операции. Далее уже «живой» псевдосотрудник, пользуясь беспокойством звонящего, просит назвать его личные данные, в частности код, указанный на обратной стороне его банковской карты.

Обращайте внимание на звонки, поступающие на ваш мобильный телефон. Сотрудники банков и правоохранительных органов никогда не будут вам звонить в мессенджерах Вотсап или Вайбер. Никогда не сообщайте свои персональные данные. В случае сомнения, сразу прекратите телефонный разговор! Для проверки информации сообщайте о подозрительных номерах по номеру, указанному на вашей банковской карте, или в чат официального приложения банка.

Расскажите о сегодняшней лекции своим родным и близким. Поделитесь информацией по QR-коду с людьми, которых вы бы хотели предотвратить от таких преступлений.

Берегите себя и своих близких!