Социальная инженерия:
как мошенники выманивают личные данные и как этому противостоять

Практически половина преступлений с использованием информационных телекоммуникационных технологий приходится на мошенничества с использованием методов социальной инженерии.

Банковские данные похитить непросто, поскольку они охраняются системой безопасности банков. Мошенники пытаются выманить нужные им данные напрямую у граждан. В этом им помогают методы социальной инженерии.

Социальная инженерия – это психологические манипуляции с целью заставить человека добровольно сообщить ценную информацию – логины, пароли, номера банковских карт и счетов – чтобы с ее помощью похитить денежные средства. Это метод несанкционированного доступа к конфиденциальной информации или системам хранения, основанный на особенностях психологии людей.

Два самых распространенных способа социальной инженерии – это телефонное мошенничество и фишинг.

При телефонном мошенничестве - злоумышленник связывается с жертвой по телефону и пытается получить нужную ему информацию, используя сценарий в котором расставлены психологические ловушки.

Например, мошенник связывается с человеком, представляется ему сотрудником банка и убеждает его сообщить персональные данные (номер карты, пароль, CVC-код, код из СМС и т.д.) в целях отмены подозрительной операции, сохранения денежных средств, недопущения факта оформления кредита или обещая какой-либо бонус. При таком сценарии злоумышленники могут использовать телефонных ботов или серии звонков из полиции, службы поддержки банков.

При фишинге человек ловится на удочку, заранее заброшенную мошенниками. Фишинг – это техника, направленная на получение конфиденциальной информации при помощи смс-сообщений, ссылок, фальшивых веб-страниц. Если человек пройдет по ссылке направленной ему мошенником, в таком случае на его устройство попадает вредоносная программа, которая похищает конфиденциальную информацию. Либо это может быть ссылка на фальшивую веб-страницу, имитирующую официальную, которая содержит в себе форму, требующую введения информации от домашнего адреса до пин- кода банковской карты.

Как это работает?

1. Спровоцировать у человека сильные эмоции , под влиянием которых он не сможет критически оценивать ситуацию.
2. Вызвать доверие – для чего мошенники представляются сотрудниками сразу нескольких служб.
3. Убедить человека, что время для решения его проблемы ограничено. При этом, мошенники пытаются оставаться на связи с человеком, чтобы у него не было возможности спокойно обдумать ситуацию.

Как противостоять мошенникам ?

Есть несколько правил, при соблюдении которых шансы попасться на уловки мошенников минимальны:

1. Не сообщать никому – номера карты, счетов, логины, пароли, коды из СМС.
2. Не совершать никаких операций по счету по просьбе сотрудников банка. Необходимо помнить, что служба безопасности банка в случае необходимости самостоятельно предпринимает попытки с целью сохранить деньги их клиентов.
3. Не доверять собеседнику, даже если он называет ваше имя отчество и другую личную информацию, поскольку эта информация могла быть оставлена в интернете при заполнении различных анкет.
4. Прервать разговор и позвонить в свой банк для уточнения информации. Контактные номера указаны на карте, а если кто-то пытался сделать перевод от вашего имени, это находит свое отражение в банковской системе.
5. Прежде чем что-то предпринять – сообщите о случившимся своим близким, они помогут более спокойно оценить ситуацию, и возможно укажут на признаки мошенничества, которые вы из-за стресса могли упустить.

Если же у вас все-таки выманили конфиденциальную информацию и деньги, как можно скорее обратитесь в полицию и банк, чтобы был шанс заблокировать транзакции.