Памятка "Профилактика преступлений с использованием ИТТ (информационно-телекоммуникационных технологий)"

Мошенники постоянно придумывают новые уловки и способы обмануть нас, поэтому попытки защитить мобильные устройства уже стали частью нашей цифровой жизни. Тем не менее некоторые виды мошенничества опознать непросто, поэтому важно следить за появлением новых схем обмана и уметь их выявлять.

К наиболее распространенным видам дистанционного мошенничества относятся:

- «фишинг» - вид дистанционного мошенничества, при совершении которого злоумышленники (в ходе телефонного разговора, посредством направления электронного письма или смс - сообщения) получают личные конфиденциальные данные о банковской карте, номере счета, логины и пароли для входа в интернет-банк, а также пароли безопасности, позволяющие произвести списание находящихся на банковской карте денежных средств. Жертвами указанного вида мошенничества зачастую становятся незащищенные, малообразованные, доверчивые слои населения.

Представляясь зачастую сотрудниками кредитных организаций, преступники вводят в заблуждение граждан относительно совершаемых несанкционированных списаний денежных средств, осуществляемых покупках и т.п., после чего просят назвать конфиденциальные сведения с целью пресечения возможного совершения преступления. Граждане, доверяя полученной информации, желая обезопасить свои денежные средства от преступных посягательств, сообщают запрашиваемую информацию, в результате чего злоумышленники похищают принадлежащие им денежные средства.

- «фарминг» - процедура скрытого направления на ложный IP-адрес, то есть направление пользователя на фиктивный веб-сайт, чаще всего используемый для приобретения товаров и услуг (ozon.ru, avito.ru, aliexpress.ru, joom, biglion, купинатор, кассир.ру, билетер и другие)

- «двойная транзакция» (при оплате товаров и услуг продавец сообщает об ошибке и предлагает повторить операцию, а в дальнейшем денежные средства описываются дважды по каждой из проведенных операций)

Основные схемы телефонного мошенничества:

1.Обман по телефону.

Мошенник звонит с незнакомого номера и представляется родственником (знакомым) и взволнованным голосом сообщает, что задержан сотрудниками правоохранительных органов и обвиняется в совершении того или иного преступления (это может быть ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и даже убийство). Далее в разговор вступает якобы сотрудник правоохранительных органов, который уверенным тоном сообщает, что уже не раз помогал людям таким образом. Для решения вопроса необходима определенная сумма денег, которую следует перевести на определенный расчетный счет или передать какому-либо человеку. В организации обмана по телефону с требованием выкупа участвуют несколько преступников. Набирая телефонные номера наугад, мошенник произносит заготовленную фразу, а далее действует по обстоятельствам, но нередко человек, которому звонит мошенник, сам случайно подсказывает имя того, кому нужна помощь.

Аналогичным образом могут звонить мошенники сотрудникам государственных органов, либо предпринимателям и, представляясь, например, руководителем какого-либо государственного органа (правоохранительного, надзорного, контролирующего), под предлогом приезда комиссии проверяющих и требуют организовать либо «теплый прием» в форме бесплатного предоставления услуг (питание, подарки, организация отдыха и т. д.), либо перечислить определенную сумму денежных средств на указанный расчетный счет для организации досуга проверяющих или достижения необходимых положительных результатов проверки.

Как поступить в такой ситуации?

Прервать разговор и перезвонить тому, о ком идет речь (либо в указанный государственный орган). Если телефон отключен, нужно связаться с его коллегами, друзьями и родственниками для уточнения информации.

2. SMS-просьба о помощи.

SMS-сообщения позволяют упростить схему обмана по телефону. Абонент получает на мобильный телефон сообщение: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «друг» или другие. На сообщения с незнакомых номеров реагировать нельзя.

3. Телефонный номер-грабитель.

На телефон приходит SMS с просьбой перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной - помощь другу, изменение тарифов связи, проблемы со связью или с Вашей банковской картой и так далее. После того как Вы перезваниваете, Вас долго держат на линии. Когда это надоедает, Вы отключаетесь - и оказывается, что с Вашего счета списаны крупные суммы. Мошенники регистрируют такой сервис и распространяют номер без предупреждения о снятии платы за звонок. Единственный способ обезопасить себя от телефонных мошенников - не звонить по незнакомым номерам.

Другой вид мошенничества выглядит так. При заказе какой-либо услуги через якобы мобильного оператора или при скачивании мобильного контента абоненту приходит предупреждение вида: «Вы собираетесь отправить сообщение на короткий номер для подтверждения операции, отправьте сообщение с цифрой 1, для отмены с цифрой 0». При отправке подтверждения, со счета абонента списываются денежные средства. Мошенники используют специальные программы, которые позволяют автоматически генерировать тысячи таких сообщений. Сразу после перевода денег на фальшивый счет они снимаются с телефона. Не следует звонить по номеру, с которого отправлено SMS - вполне возможно, что в этом случае с Вашего телефона будет автоматически снята крупная сумма.

4. Выигрыш в лотерее или какого-либо приза.

В связи с проведением всевозможных рекламных акций, лотерей и розыгрышей, особенно с участием радиостанций, мошенники часто используют это для своей деятельности и обмана людей. На Ваш мобильный телефон, как правило, в ночное время - приходит SMS- сообщения, в котором говорится о том, что в результате проведенной лотереи Вы выиграли автомобиль. Чаще всего, упоминаются известные иностранные модели, марки. Для уточнения всех деталей Вас просят посетить определенный сайт и ознакомиться с условиями акции, либо позвонить по одному из вышеуказанных телефонных номеров. Во время разговора мошенники сообщают о том, что надо выполнить необходимые формальности: уплатить госпошлину и оформить необходимые документы. Для этого необходимо перечислить на счет своего мобильного денежную сумму, а затем набрать определенную комбинацию цифр и символов, якобы для проверки и получения «кода регистрации». Комбинация цифр и символов, которую Вы набираете, на самом деле является кодом, благодаря которому, злоумышленники получают доступ к перечисленным средствам. Как только код набран, счет обнуляется, а мошенники исчезают в неизвестном направлении.

5. Простой код от оператора связи.

Поступает звонок, якобы от сотрудника службы технической поддержки оператора мобильной связи, с предложением подключить новую эксклюзивную услугу или для перерегистрации во избежание отключения связи из-за технического сбоя, или для улучшения качества связи. Для этого абоненту предлагается набрать под диктовку код, который является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников.

Как поступить в такой ситуации?

Перезвонить своему мобильному оператору для уточнения условий, а также узнать, какая сумма спишется с вашего счета при отправке SMS или звонке на указанный номер, затем сообщите о пришедшей на Ваш телефон информации. Оператор определит того, кто отправляет эти SMS и заблокирует его аккаунт.

6. Ошибочный перевод средств.

Абоненту поступает SMS - сообщение о поступлении средств на его счет с помощью услуги «Мобильный перевод». Сразу после этого поступает звонок и мужчина (или женщина) сообщает, что ошибочно перевел деньги, при этом просит вернуть их обратно тем же «Мобильным переводом». В действительности, деньги не поступают на телефон, а человек переводит свои собственные средства. Если позвонить по указанному номеру, он может быть вне зоны доступа.

Как поступить в такой ситуации?

Если Вас просят перевести, якобы ошибочно переведенную сумму, напомните, что для этого используется чек. Отговорка, что «чек потерян», скорее всего, свидетельствует о том, что с Вами общается мошенник.


МВД России
ОСТОРОЖНО МОШЕННИКИ
3 МИНУТЫ ОБЩЕНИЯ
КРЕДИТ НА ВСЮ ЖИЗНЬ!
НЕ СОГЛАШАЙТЕСЬ!
НИ НА ЧТО! НЕ НАЗЫВАЙТЕ ДАННЫЕ
НЕ БЕРИТЕ КРЕДИТЫ, НИКАКИХ
ДЕЙСТВИЙ НЕ ВЫПОЛНЯЙТЕ!
НЕ ВЕРЬТЕ!
ПОХОЖИМ НА БЛИЗКИХ
ГОЛОСАМ! КРИКАМ И
ПРОСЬБАМ О ПОМОЩИ
НЕ ПАНИКУЙТЕ!
СРАЗУ ЖЕ СБРОСЬТЕ ЗВОНОК!
И ПОЗВОНИТЕ СВОИМ БЛИЗКИМ!
НЕ ОТКРЫВАЙТЕ!
ДВЕРЬ И НЕ ВПУСКАЙТЕ В ДОМ
НЕ ПОД КАКИМ ПРЕДЛОГОМ!
ЧТО ДЕЛАТЬ
СБРОСИТЬ ЗВОНОК
ПОЗВОНИТЬ БЛИЗКОМУ
ПОЗВОНИТЬ В ПОЛИЦИЮ
РАССКАЖИ БЛИЗКОМУ

Банк России

Министерство внутренних дел Российской Федерации

Генеральная прокуратура Российской Федерации

КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

Фишинг — вид мошенничества, когда у человека крадут персональные данные или деньги с помощью сайтов-подделок. Часто мошенники делают сайты, которые как две капли воды похожи на сайты реальных организаций

КАК МОЖНО ОКАЗАТЬСЯ НА ФИШИНГОВОМ САЙТЕ?

По ссылкам из интернета или электронной почты, СМС, сообщений в соцсетях или мессенджерах, рекламы, объявлений о лотереях, распродажах, компенсациях от государства

! **Хакеры часто взламывают чужие аккаунты, и фишинговая ссылка может прийти даже от знакомых**

КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?

- **Адрес** отличается от настоящего лишь парой символов
- **В адресной строке** нет https и значика закрытого замка
- **Дизайн** скопирован некачественно, в текстах есть ошибки
- **У сайта** мало страниц или даже одна — для ввода данных карты

КАК УБЕРЕЧЬСЯ ОТ ФИШИНГА?

- **Установите** антивирус и регулярно обновляйте его
- **Сохраняйте** в закладках адреса нужных сайтов
- **Не переходите** по подозрительным ссылкам
- **Используйте** отдельную карту для покупок в интернете, кладите на нее нужную сумму прямо перед оплатой

Подробнее о правилах кибергигиены читайте на fincult.info

Финансовая культура

Банк России

ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

5 ПРИЗНАКОВ ОБМАНА

1 НА ВАС ВЫХОДЯТ САМИ

Аферисты могут представиться службой безопасности банка, налоговой, прокуратурой

Любой неожиданный звонок, СМС или письмо – повод насторожиться

2 РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУГАЮТ

Сильные эмоции притупляют бдительность

3 НА ВАС ДАВЯТ

Аферисты всегда торопят, чтобы у вас не было времени все обдумать

4 ГОВОРЯТ О ДЕНЬГАХ

Предлагают спасти сбережения, получить компенсацию или вложиться в инвестиционный проект

5 ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Злоумышленников интересуют реквизиты карты, пароли и коды из банковских уведомлений

ВАЖНО!

Сотрудники банков и полиции НИКОГДА не спрашивают реквизиты карты, пароли из СМС, персональные данные и не просят совершать переводы с вашей карты

НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ:

- коды из СМС
- трехзначный код на оборотной стороне карты (CVV/CVC)
- PIN-код
- пароли/логины к банковскому приложению и онлайн-банку
- кодовое слово
- персональные данные

Как защитить свои финансы, читайте на fincult.info

Финансовая культура

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

МОШЕННИКИ

Представляются сотрудниками **СЛУЖБЫ БЕЗОПАСНОСТИ**

Присоединяйся к группе в телеграм **«МЫ ВМЕСТЕ!»:**

@rfvmeste

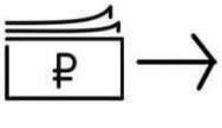
НЕ СООБЩАЙТЕ НИКОМУ ДАННЫЕ вашей карты

ПАРОЛЬ CVC-КОД с оборота карты и секретный код из СМС

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

ЗВОНЯТ ИЗ БАНКА И СООБЩАЮТ О ПОПЫТКАХ КРАЖИ ДЕНЕГ СО СЧЕТА

ЗВОНЯЩИЙ ПРОСИТ СООБЩИТЬ ИНФОРМАЦИЮ О КАРТЕ



ИЛИ ПЕРЕВЕСТИ ДЕНЬГИ НА «БЕЗОПАСНЫЙ СЧЕТ»

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

1. НЕ ВЫПОЛНЯЙ НИКАКИХ ТРЕБОВАНИЙ!

2. ЗАВЕРШИ ТЕЛЕФОННЫЙ РАЗГОВОР, ПОЛОЖИ ТРУБКУ!

3. ОБРАТИСЬ В БЛИЖАЙШИЙ ОФИС СВОЕГО БАНКА!