ПАМЯТКА
об основных способах дистанционного мошенничества

С переходом населения на безналичный расчет, выпуском и начислением заработных плат, пенсий, пособий и других выплат на пластиковые карты, появлением большого количества интернет-магазинов, возможностью оплачивать услуги онлайн, интернет становится более доступным, расширяются зоны покрытия сетей сотовой связи, как следствие, все больше людей пользуются современными технологиями.

Мошенники умело используют всю доступную информацию и современные технологии, разбираются в психологии людей, вынуждая раскрывать всю информацию о себе либо совершать те или иные действия, используют человеческие слабости, чувства в своих корыстных интересах.

Основные схемы телефонного мошенничества:

1. Мошенничества через сайты объявлений.

Преступник, выступая в роли продавца, размещает на сайтах объявлений (Авито, ФарПост, Дром и др.) информацию о продаже какого-либо товара, сдаче в аренду недвижимости или же оказании тех или иных услуг, за которые в последующем получает предоплату, тем самым похищая деньги.

В другом случае мошенник выступает в роли покупателя. Он звонит по объявлению потерпевшего, размещенному на интернет-площадке, и говорит, что желает приобрести его товар и готов внести задаток, для чего просит продиктовать контрольные данные по банковской карте и поступивший код и в последующем похищает денежные средства.

2. Мошенничества со взломом страниц социальных сетей.

Злоумышленники взламывают страницы социальных сетей, а затем отправляют всем друзьям из списка сообщения мошеннического характера с просьбой занять денежные средства под различными предлогами (заболел родственник, не хватает на срочную покупку и т.д.).

3. Мошенничество, совершенное под предлогом несанкционированных списаний с банковской карты.

Мошенник, используя IP-телефонию, звонит потенциальной жертве с виртуального номера и сообщает о том, что по его банковской карте либо по счету осуществляются несанкционированные списания денежных средств, или происходит оформление кредита, и для сохранения средств необходимо их перевести в безопасную ячейку. После чего, потерпевший, следуя инструкциям мошенника, сообщает все реквизиты своих карт, их проверочные коды или коды, поступившие в смс-сообщении.

4. Мошенничество, совершенное с использованием фишинговых сайтов.

Фишинг дословно переводится как «рыбная ловля» или «ловля на живца». Конечная цель такого мошенничества – получить данные банковской карты потерпевшего, выудить его деньги либо получить прочее его имущество. Видов фишинга великое множество. Самый

распространенный случай – это поддельный сайт, который маскируется под интернет-магазины, агрегаторы билетов и пр.

5. Мошенничество, совершенное по схеме мнимого вложения денежных средств в лже-инвестиционные компании.

Мошенники предлагают гражданам инвестировать свои сбережения например в одну из крупнейших газодобывающих компаний страны, обещая сверхвысокий доход за короткий срок. А когда получают деньги, то перестают выходить на связь.

6. Случай с родственником.

Мошенник представляется родственником (знакомым) и взволнованным голосом по телефону сообщает, что задержан сотрудниками полиции за совершение преступления (совершил ДТП, хранил оружие или наркотики, нанёс тяжкие телесные повреждения). Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном сообщает, что уже не раз «помогал» людям таким образом. Но если раньше деньги привозили непосредственно ему, то сейчас деньги необходимо привезти в определенное место, передать какому-либо человеку, либо перевести на счет (абонентский номер телефона).

7. Розыгрыш призов (это могут быть телефон, ноутбук, автомобиль и др.).

На телефон абонента сотовой связи приходит смс-сообщение, из которого следует, что в результате проведенной лотереи он выиграл автомобиль. Для уточнения всех деталей потенциальной жертве предлагается посетить определенный сайт и ознакомиться с условиями акции, либо позвонить по одному из указанных телефонных номеров. Во время разговора по телефону мошенники сообщают о том, что для выполнения необходимых формальностей (уплаты госпошлины, оформления необходимых документов, оплаты за комиссию перевода) счастливому обладателю новенького автомобиля необходимо перечислить на счет указанную ими сумму, а затем набрать определенную комбинацию цифр и символов, якобы для проверки поступления денег на счет и получения «кода регистрации». Как только жертва завершает указанные манипуляции, счет обнуляется, а мошенники исчезают в неизвестном направлении.

Если вы узнали о проведении лотереи только тогда, когда «выиграли» автомобиль, если вы не заполняли заявку на участие в ней либо каким-либо другим способом не подтверждали свое участие в розыгрыше, то, вероятнее всего, вас пытаются обмануть.

8. SMS-просьба.

Абонент получает на мобильный телефон сообщение: «У меня проблемы, позвони по такому-то номеру, если номер не доступен, положи на него определенную сумму и перезвони». Человек пополняет счёт и перезванивает, телефон по-прежнему не доступен, а деньги вернуть уже невозможно.

9. Платный код.

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.

10. Установление вредоносного программного обеспечения.

Мошенники пишут людям в мессенджерах (WhatsApp, Viber, Telegram и др.), устанавливая на фото профиля логотипы банков. Для убедительности они присылают снимки поддельных удостоверений или банковских документов.

В ходе переписки под предлогом «сохранения сбережений» злоумышленники предлагают жертвам установить на телефон или компьютер программу, которая предоставляет дистанционный доступ к устройству. С помощью этого приложения мошенники могут дистанционно оформить кредит на владельца счета и похитить средства.

11. Мошенничество с QR-кодом.

Многие еще не разобрались, как работают QR-коды, и верят «сотруднику банка», который разъясняет «правила безопасности» и «пытается помочь» сохранить средства.

Мошенники звонят клиентам якобы из банка и сообщают, что поступил запрос на снятие денег со счета. После этого просят прислать QR-код для отмены операции. Остается лишь выполнить снятие наличных вместо Вас.

Злоумышленники рассчитывают на то, что клиент может быть не знаком с особенностями снятия наличных с помощью QR-кода, поэтому может легко передать его мошенникам. Но важно знать, что им так же нельзя делиться с незнакомцами, как и данными карты.

12. Социальная инженерия.

К осторожным жертвам мошенники нашли особый подход посредствам серии звонков с целью вызова доверия. В первую телефонную беседу никто не будет пытаться узнать у вас данные карты. Сначала могут уточнить, довольны ли вы сервисом, спросить о пожеланиях по улучшению работы.

В следующий раз уже знакомый голос может поинтересоваться, какие банковские продукты вам интересны и сделать привлекательное предложение. А когда привыкнете к звонкам, под каким-нибудь предлогом могут спросить данные карты (попытка обезопасить ваши сбережения или другой повод).

Как уберечься от телефонных мошенничеств?

Чтобы не стать жертвой злоумышленников, необходимо соблюдать простые правила безопасного поведения и обязательно довести их до сведения родных и близких:

- понятия «безопасный счет» не существует, если поступает предложение перевести имеющиеся денежные средства, взять кредит и положить на счет через банкомат – это в любом случае мошенничество;

- если вам неизвестные предлагают в срочном порядке взять кредит, чтобы предотвратить получение кредита третьими лицами – это мошенничество;

- предложения о получении в короткий срок кратной прибыли от игры на бирже, инвестировании в определенные компании – это мошенничество;

- нельзя сообщать позвонившим неизвестным лицам коды, поступающие в приложении Госуслуги. Это чревато взломом личного кабинета о оформлением кредитов от вашего имени. В случае ограничения доступа к личному кабинеты незамедлительно лично обратитесь в МФЦ;

- не следует доверять звонкам и сообщениям, о том, что родственник или знакомый попал в аварию, задержан сотрудниками полиции за совершение преступления, особенно, если за этим следует просьба о перечислении денежных средств. Как показывает практика, обычный звонок близкому человеку позволяет развеять сомнения и понять, что это мошенники пытаются завладеть вашими средствами или имуществом;

- не следует реагировать на звонки или SMS-сообщения с неизвестных номеров с просьбой положить на счет деньги, провести другие финансовые манипуляции;

- не следует сообщать по телефону кому бы то ни было сведения личного характера, а также сообщать коды из поступающих СМС-сообщений;

- осуществляйте покупки только на проверенных сайтах.

Если человек все-таки стал жертвой преступления, то ему следует немедленно заблокировать свою банковскую карту и обратиться в полицию.

Получение у оператора сотовой связи детализации по исходящим и входящим звонкам, а в банке – выписки по движению денежных средств будет способствовать своевременному установлению обстоятельств преступления.

Также одним из эффективных способов обезопасить себя от преступных посягательств – оформление самозапрета на получение кредитов.

Этот механизм позволяет блокировать возможность оформления займов на ваше имя. Даже если мошенники получат ваши данные, оформить кредит без вашего участия не получится.

Самозапрет можно установить через Единый портал Государственных услуг и банковские учреждения.