**Новые киберугрозы: самопереводы, вирусы, социальная инженерия. Как не стать жертвой**



Кибермошенники становятся все более изощренными. Как правило, это люди с неплохим образованием, не обязательно ранее осужденные, но обязательно — великолепные психологи. Их жертвой может стать каждый из нас.

По данным Сбербанка, самым распространенным видом мошенничества остается социальная инженерия — злонамеренное введение в заблуждение путем обмана или злоупотребления доверием. Более 80% случаев хищений приходится именно на этот метод получения несанкционированного доступа к конфиденциальной информации.

Преступники умело пользуются доверчивостью и невысокой киберграмотностью людей. Аферисты маскируются под сотрудников служб безопасности банков, социальных служб, полиции, прокуратуры, ремонтников, сантехников и даже медиков только для того, чтобы обокрасть своих легковерных жертв. На это попадаются все категории населения без исключения. Случаев и видов мошенничества масса, и преступники придумывают все новые схемы. Рассмотрим наиболее популярные из них.

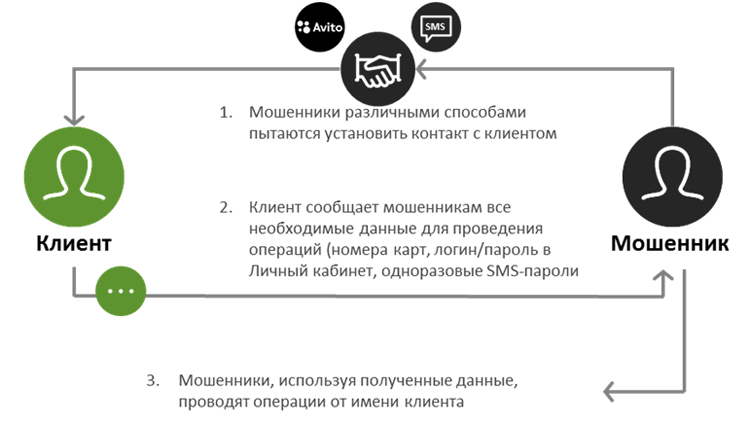
Кража «личности» — это кража личных данных жертвы в целях открытия банковских счетов или оформления тарифа у мобильного оператора на имя потерпевшего и получение доступа к существующим учетным записям и счетам.

Преступники умело пользуются доверчивостью и неосведомленностью людей. Аферисты маскируются под сотрудников служб безопасности банков и т.д.

Злоумышленники стараются заполучить персональные и иные данные клиентов различных банков самыми различными способами — как правило, через прямой контакт с потенциальным потерпевшим, от которого путем обмана им удается получить нужную информацию. Если клиент сообщает мошенникам свои данные для проведения операций (номера карт, логин/пароль для входа в личный онлайн-кабинет, одноразовые СМС-пароли), то у злоумышленников появляется полный доступ к счетам жертвы.

Последние полгода злоумышленники при совершении звонков якобы от имени служб безопасности банков стали активно пользоваться услугами дешевой и доступной связи посредствам сервисов передачи голоса по IP (Voice over IP, VoIP). География звонков с сообщениями о том, что ваша карта якобы заблокирована или по ней происходит операция, которую вы не совершали, может быть какой угодно. К примеру, IP-телефония позволяет мошенникам имитировать звонки из Москвы, хотя сам человек при этом находится в Ростове.

**Рисунок 1. Классическая схема мошенничества методами социальной инженерии**



Весной прошлого года в полицию обратились несколько жителей Москвы с заявлениями о том, что им поступали звонки от девушки, которая, представляясь сотрудником социальной службы, предлагала получить путевку на санаторно-курортное лечение либо денежную компенсацию.

Граждане выбирали получение денежных средств, сообщали злоумышленнице всю конфиденциальную информацию. Позже с их карт были украдены сбережения. Действовала целая группа, подозреваемые были задержаны сотрудниками полиции — ими оказались 23-летняя девушка и трое мужчин в возрасте от 24 лет до 41 года, проживающие в Московской области.

Обезопасить себя от такого мошенничества довольно просто: не стоит называть данные своей карты по телефону (особенно CVC/CVV код, пароли, пришедшие в смс-сообщениях) никому.

**Самопереводы**

Из всего разнообразия схем мошенничества самой распространенной по-прежнему остается схема с самопереводами, когда жертва под воздействием третьих лиц самостоятельно совершает операцию по переводу денежных средств мошенникам. В зоне риска оказываются граждане, которые что-то продают или покупают на сайтах бесплатных объявлений или в социальных сетях, а также те, с кем мошенники вступают в переписку в социальных сетях со странички «взломанного» друга.

Мошенники знают, как вызвать доверие у своих жертв, — они будут обращаться по имени, вежливо, предоставят все дополнительные фото с товарами, покажут отзывы «покупателей» и ответят на все вопросы. После того, как клиент самостоятельно перевел деньги мошеннику, тот тут же пропадает, а человек не может связаться с ним и жалуется в банк на несанкционированный перевод.

Самопереводы в симбиозе с VoIP дают еще одну популярную схему мошенничества. Под видом сотрудников службы безопасности банков мошенники просят своих жертв перевести деньги на «резервный счет» для их сохранности. Конечно же, никакого резервного счета у банка нет и быть не может, мошенники пользуются доверчивостью граждан, которые в итоге сами переводят деньги на их счета.

**Рисунок 2. Схема мошенничества с самопереводом**



В последнее время самопереводы чаще делают не пенсионеры, а молодые люди в возрасте от 18 до 30 лет. Так, в апреле этого года в Иркутске сотрудники полиции задержали интернет-мошенницу — ей оказалась 28-летняя женщина, которая размещала на Avito объявления о продаже детских кроваток и колясок. Мошенница тщательно подбирала в Интернете красочные картинки, ставила низкую цену, а покупатели радостно попадались на крючок. В итоге пострадало не менее 20 жителей области и близлежащих регионов. Позвонив по номеру телефона, указанному в объявлении, покупатели беседовали с «сотрудницей крупной компании из Новосибирска», которая просила перевести всю сумму сразу, авансом. Когда деньги оказывались на счете злоумышленницы, она просто отключала телефон. Опыт «развода» у мошенницы уже имелся. В 2018 году ее приговорили к шести годам лишения свободы с отсрочкой на 14 лет за 12 фактов мошенничества. После смены фамилии рецидивистка вернулась к криминальному прошлому, и теперь ей грозит новый срок до пяти лет.

Что важно знать во избежание таких случаев: даже если вам поступил звонок с номера телефона, похожего на номер вашего банка, но при этом «сотрудник» просит вас сообщить конфиденциальную информацию, то просто положите трубку и перезвоните в банк по номеру телефона, указанному на сайте банка или оборотной стороне вашей банковской карты. Кроме того, не соглашайтесь перевести деньги за понравившуюся вещь на мобильный телефон продавца — в большинстве случаев это элемент мошеннической схемы.

Также не стоит обращаться по объявлениям о товаре, цена по который явно занижена, просите подтвердить наличие товара видеосъемкой, сессией по скайпу.

**Обман пенсионеров**

Время от времени мы видим в новостной ленте сообщения о том, как мошенники под видом социальных служб или полиции обманывают доверчивых граждан. Вот, например, некоторые случаи за последнее время: выманивали деньги у пожилых людей якобы для поимки мошенников, обещали помочь оправдать осужденных близких родственников, продавали «чудодейственные» БАДы (биологически активные добавки к пище), предлагали получить по акции подарки «почти задаром», установить счетчики на воду и т.д.

Исторически сложилось так, что люди пожилого возраста имеют высокий уровень доверия к государственным структурам. Этим и пользуются мошенники, которые понимают, что пенсионеры очень легко предоставляют всю свою конфиденциальную информацию фактически любому встречному.

**Рисунок 3. Наиболее распространенный вариант схемы обмана пенсионеров**

В конце прошлого года в Сбербанк обратилась пенсионерка, являющаяся его клиентом, и сообщила, что мошенники обманом вынудили ее перевести на их карты почти полмиллиона рублей (деньги она откладывала на похороны).

Пенсионеры — одна из наиболее уязвимых категорий граждан, поскольку восполнить финансовые потери они практически не могут

Несколько лет назад женщина покупала БАДы, которые оказались пустышками. Примерно за месяц до визита пенсионерки в банк ей на стационарный телефон позвонил мужчина, представившийся сотрудником прокуратуры, и сообщил, что за купленные препараты ей полагается компенсация. Мошенник сразу обратился к ней по фамилии, имени и отчеству, был очень доброжелателен, знал, какие лекарства она покупала и даже на какую сумму, ему было известно, из какого она города. И она поверила, что это сотрудник банка.

Затем пенсионерке поступали звонки от другого мужчины, уже якобы от сотрудника Сбербанка, который сообщал о порядке выплат и необходимости оплатить различные услуги. Сначала это были услуги адвоката, затем страховая комиссия, далее налог и банковские сборы, при этом мнимая компенсация продолжала расти. За несколько недель такого обмана мошенники вынудили клиентку перевести им почти все ее сбережения в размере полумиллиона рублей, которые, в свою очередь, они обналичивали в банкоматах Подмосковья.

В феврале 2019 года данная группа мошенников была задержана. На протяжении нескольких лет они выманивали у пожилых людей средства на суммы от 30 тыс. до 300 тыс. рублей, обещая солидную компенсацию за совершенную ранее покупку лекарственных средств, медицинских приборов или БАДов.

**Вирусное заражение устройств с операционной системой Android**

Устройства с операционной системой Android особенно уязвимы. Наиболее подвержены вирусной атаке могут быть клиенты банков, использующие СМС-банкинг и мобильные банковские приложения на таких устройствах.

Вирусы могут распространяться как через СМС/MMС-сообщения, так и через популярные мессенджеры, что резко снижает возможность их выявления и детектирования со стороны операторов сотовой связи.

Владелец смартфона получает сообщение, в его тексте ссылка, которая при открытии инициирует загрузку вирусной программы. Как только вирус попадает в смартфон, он начинает рассылать «вирусные» СМС по контактным листам пользователя. Параллельно он делает запрос на номер СМС-банкинга и узнает баланс счета владельца смартфона. После этого вирусная программа переводит деньги на счета, подконтрольные злоумышленникам. Вирус способен перехватывать входящие СМС-сообщения, поэтому владелец смартфона может не знать о снятии денег со счета, оповещения о списаниях просто не доходят. Кроме того, вирус может открывать окна браузера, визуально похожие на окна авторизации банковских приложений, и при вводе данных своих карт пользователи отправляют средства напрямую мошенникам. В некоторых случаях вирус может блокировать смартфон.

**Рисунок 4. Схема мошенничества с использованием вируса**



За последнее десятилетие сами мошеннические схемы, по сути, не изменились. Появляются новые способы и предлоги, под которыми можно незаконно завладеть чужим имуществом — если раньше преступникам требовалось получить физический доступ к деньгам жертвы (зайти в квартиру, разрезать сумку и т.д.), то теперь достаточно получить доступ к конфиденциальной информации. Именно при помощи такой информации, которую граждане зачастую сами охотно сообщают аферистам, последним удается удаленным способом (дистанционно) похитить любые суммы денежных средств, вывести их на любые выбранные ими реквизиты и обналичить в любой точке мира.

Без участия правоохранительной системы бороться с мошенниками невозможно, какие бы усилия ни прикладывались

Исследование Сбербанка подтверждает о том, что жертвами телефонного и интернет-мошенничества все чаще становятся молодые люди в возрасте от 18 до 30 лет. Для Сбербанка безопасность транзакций клиентов — один из важнейших приоритетов при разработке цифровых сервисов. Поэтому в Банке реализована эшелонированная защита, которая включает в себя подтверждение операций с помощью одноразовых паролей, шифрование трафика, встроенные антивирусные решения в приложениях, а также системы фрод-мониторинга. Последние, за счет использования AI-моделей, нацелены как раз на предотвращение кейсов, в которых мошенникам удалось получить доступ к информации клиента.

Мы понимаем, что без участия правоохранительной системы бороться с мошенниками невозможно, какие бы усилия ни прикладывались. Долгое время киберпреступники чувствовали себя практически в безопасности благодаря малозначительным и условным срокам, к которым их приговаривал суд за многомиллионные кражи. Киберпреступники не вызывали в обществе негативных реакций, в отличие, например, от убийц. Сейчас отношение меняется — например, генеральный прокурор РФ считает, что актуальность роста числа киберпреступлений говорит о необходимости усиления уголовной ответственности за них. И такие приговоры уже есть — суды их выносят.

Таким образом, новым трендом на государственном уровне должно стать повышение правовой и киберкультуры граждан, а также эффективности деятельности государственных органов — в первую очередь по профилактике дистанционных (компьютерных) преступлений.