Противодействие мошенническим практикам

Для хищения денег у граждан злоумышленники используют все более изощренные сценарии. В результате тысячи людей страдают от их действий, теряют деньги, которые в некоторых случаях копили годами. Знания о том, как противодействовать мошенникам, помогут в нужную минуту принять правильное решение. В этом разделе Банк России представляет распространенные мошеннические схемы, которые будут регулярно дополняться, а также рекомендации по защите от них.

     Мошенники специально оказывают психологическое воздействие на человека таким образом, чтобы он раскрыл личные или финансовые данные, перевел им деньги или даже взял кредит для последующей передачи средств в чужие руки. Они могут неоднократно звонить жертве, в том числе используя технологию подмены телефонных номеров, направлять электронные письма и сообщения со ссылкой на поддельные (фишинговые) сайты как финансовых организаций, так и любых других компаний и маркетплейсов. Злоумышленники всячески пытаются вывести человека из спокойного состояния и отключить у него логическое мышление. Для этого они могут запугивать, торопить и оказывать давление или, напротив, стараться заинтересовать и обрадовать внезапной выгодой. Схемы мошенников часто выглядят очень правдоподобно, так как они используют самые обсуждаемые новости или события. Такое психологическое воздействие представляет собой методы социальной инженерии.

Телефонные мошенники поя*в*ляются *в*се чаще, поскольку со*в*ременные технологии поз*в*оляют им без проблем находить с*в*оих жерт*в* и зарабаты*в*ать неплохие деньги на их наи*в*ности. За последний год мошенники похитили со счето*в* жителей РФ от 3,5 до 5 миллиардов рублей. С одного человека в среднем преступники получают около 8 тыс. рублей. А учитывая, что среднестатистический мошеннический колл-центр в сутки может выполнять до нескольких тысяч звонков, масштабы поражают. Поэтому разобраться в особенностях схемы обмана точно не помешает, как и выстроить стратегию действий, если вам поступит сомнительный звонок или если станете жертвой другого типа мошенничества.

Как работают телефонные мошенники
Мошенничество набирает обороты благодаря огромному объёму информации о потенциальных жертвах. Преступники получают её на нелегальных рынках, куда «сливаются» данные из интернет-магазинов, государственных структур и финансовых учреждений.

Виды мошенничества по телефону

Телефонные мошенники – самая распространенная категория преступников. Иногда мошенничество выполняется старыми методами. Но нередко придумывают совершенно новые способы. Для наглядности разберем самые распространенные схемы.

Мошенничество с банковскими картами и счетами
Если у вас есть платежная карта – эта вещь, безусловно, удобная и полезная. Правда, она является целью мошенников, которые часто используют удобство рассматриваемого платежного инструмента.
Допустим, владелец карты Сбербанка выставляет объявление о продаже какого-то имущества. Высока вероятность, что ему может звонить

Телефонный мошенник, выказав желание приобрести продаваемый товар, но только если сбросит деньги на карту. Чтобы осуществить перевод на карту, мошеннику обязательно нужен не только номер, но и CVV-код и срок действия платежного инструмента. А также просят перевести SMS-код, полученный в сообщении из банка. Получив рассматриваемые данные, счет обнуляется. Средства обычно переводят на электронный кошелек, а после вывода этот кошелек уничтожается, и найти следы преступников становится невозможно.

Причем телефонный тип мошенничества возможен, даже если была передана не вся информация. Опытные хакеры могут звонить и опустошить ваш счет, имея минимум сведений. Именно потому с банковскими операциями стоит быть очень внимательными, иначе мошенничество может оставить вас без гроша.

Звонки от «служб безопасности» банков
Телефонный мошенник может звонить и представиться сотрудником банка. Причем мошенники банк могут быть убедительными, потому подозрительность манипуляции жертва осознает уже после того, как она будет совершена. Обычно схема простая – сотрудник банка (например, Сбербанка) сообщает, что с вашим счетом проводятся сомнительные операции. Иногда телефонный мошенник может говорить о сбоях программного обеспечения Сбербанка.

После того как потенциальная жертва мошенничества будет напугана, телефонный мошенник говорит, что для восстановления дееспособности карты Сбербанка нужны сведения, которые мы упомянули выше (номер, код и дата действия карты).

Также мошенники могут звонить и предложить скачать и установить на своих гаджетах вредоносные программы, которые маскируются под известные сервисы, что предлагает Сбербанк. Они являются средством для сбора данных о ваших счетах Сбербанка.

Звонки от «сотрудников» правоохранительных органов и государственных служб
Довольно цинично выглядят случаи, когда звонят мошенники, замаскированные под сотрудников правоохранительных органов. Их легенда состоит в том, что они расследуют случаи мошенничества. Своими разговорами, они усыпляют бдительность потенциальных жертв и выманивают информацию.

Также иногда телефонные преступники могут представляться сотрудниками Пенсионного фонда или Роспотребнадзора. Например, мошенники могут сообщить, что потенциальной жертве полагаются какие-то новые социальные выплаты. Чтобы получить эти выплаты, нужно предоставить мошенникам интересующие их сведения – информацию о платежных картах.

Звонки с подмененных номеров
Имитируя Сбербанк, мошенники иногда подменяют номера таким образом, чтобы они походили на номера банка. Многие банки используют специальные номера для общения с клиентами. Сбербанк обычно использует номер «900» или «9000».

Номера можно поменять, используя специальные программы-обманки. Их задача – замаскировать настоящий номер звонившего, чтобы абонент увидел знакомый номер. Причем проблема настолько острая, что летом текущего года, Владимир Путин подписал закон, благодаря которому звонить и отправить сообщение с подмененных номеров нельзя.

Махинации со счетами мобильных телефонов
Мошенники по телефону могут сообщить, что на телефонный номер ошибочно перевели деньги. Злоумышленник просит вернуть указанную сумму обратно. Чтобы больше дестабилизировать потенциальную жертву, телефонные мошенники могут сыпать угрозами – заблокировать ваш номер или сообщить в полицию.

Сообщения о попавшем в беду родственнике и просьбы о помощи
Существует махинация, согласно которой, с номера мошенников будто пытается звонить ваш родственник, сообщающий о попадании в беду. Обычно такие звонки поступают в ночное время, когда человек уже спит и в полусонном состоянии плохо соображает. Жертве могут сообщить о том, что её родственник попал в аварии или спровоцировал её, сбил человека и т.п. И ему нужны деньги, чтобы получить минимальную долю наказания. Телефонный мошенник может говорить не только о родственнике, но и друзьях. Дальше следует требование перевести крупную сумму на электронный кошелек или мобильный счет.

Рассматриваемый метод обмана один из самых жестких, поскольку иногда жертвы из-за переживаний получали сердечные приступы. Особенно если звонят пожилым гражданам, которые более доверчивые и у которых слабое здоровье.

Сообщения о выигрыше в лотерею
Более радостный, но также довольно циничный способ мошенничества – сообщение, что вы получили выигрыш в лотерею. Но чтобы покрыть некоторые издержки процедуры, нужно перевести определённую сумму. Когда человек переводит указанные деньги, понятное дело, что своего «выигрыша» он не получает. Следует помнить, что по законам РФ, все расходы и издержки ведения лотерейных розыгрышей ложатся на плечи организаторов. Телефонные мошенники рассчитывают, что жертвы не знают законы РФ.

Сообщения-грабители
Схема такого обманного маневра уже сложнее. Сначала потенциальной жертве отправляется SMS, где содержится просьба звонить по определенному номеру, чтобы получить важные сведения. Например, что вам положено наследство. Жертва звонит по указанному номеру, но на втором конце никто не берет трубку. Когда человек проверяет свой мобильный счет, с него сняли все средства.

Такое возможно благодаря тому, что телефонные мошенники регистрируются на сервисах с платными звонками. Причем своей жертве об оплате никто не сообщает, и деньги списываются до той поры, пока на счету вообще что-то есть. Причем такие сервисы вполне законны, но если их услугами пользуется добросовестная организация.

Махинации с короткими номерами
Чтобы провернуть махинацию с коротким номером, преступники пользуются мобильными сервисами. Например, пользователь хочет заказать какую-то услугу, но мошенники требуют, чтобы он отправил сообщение на какой-то короткий номер. Как только это будет сделано, со счета спишут определенную сумму.

Телефонные вирусы
Чтобы схема с вирусом сработала, на телефон человека приходит сообщение в мессенджере. Открыть его получится, только если перейти по ссылке. Перейдя по этой ссылке, на смартфон загрузится вирус, что позволит злоумышленнику получить доступ к гаджету.

