Основные способы дистанционного мошенничества: как не стать их жертвой

С развитием телекоммуникационных технологий общество столкнулось с таким видом преступных посягательств, как мошенничества, совершаемые на удаленном расстоянии, т.е. дистанционные мошенничества.

Дистанционные мошенничества отличаются многообразием способов совершения, а также умением мошенников быстро подстраиваться под обстановку и представляют собой преступления, при которых злоумышленник, используя телефон и сеть «Интернет», оказывает воздействие на сознание граждан, столкнувшихся с мошенниками.

Основными способами совершения дистанционного мошенничества в России являются:

1. **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). Также может позвонить якобы «сотрудник полиции», который «поможет решить» эту проблему, а деньги необходимо привезти в определенное место, передать какому-либо человеку, либо перевести на счет (абонентский номер телефона).

2. **Ошибочный перевод средств.**

Абоненту поступает СМС-сообщение о поступлении средств на его счет. Сразу после этого поступает звонок и мужчина (или женщина) сообщает, что ошибочно перевел деньги на его счет, при этом просит вернуть их обратно. В действительности деньги не поступают, а человек переводит свои собственные средства.

3. **Сотрудники правоохранительных органов.**

Относительно новая преступная схема дистанционного мошенничества, при которой мошенники представляются сотрудниками правоохранительных органов, расследующих дело о массовой утечке персональных данных из банков. Человеку звонят и сообщают, что среди украденных из банка данных могут быть и его персональные сведения. Потенциальной жертве предлагают свериться с базой утечек, чтобы привлечь его в качестве потерпевшего. Ради большей правдоподобности истории жертве могут выслать в мессенджере или на электронную почту фото поддельного документа о проведении следственных мероприятий.

Далее у человека спрашивают, в каком банке он обслуживается и просят назвать данные карты, в том числе трехзначный номер с ее обратной стороны. После, доверчивый гражданин, полагающий, что ему действительно позвонил сотрудник правоохранительных органов, следует указаниям последнего и впоследствии теряет все свои деньги.

4. **Фишинг (англ. Phishing – «выуживание»).**

Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Это

достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с автоматической пересылкой. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

5. Розыгрыш призов.

На телефон абонента сотовой связи приходит смс-сообщение, из которого следует, что в результате проведенной лотереи он выиграл автомобиль, а для получения приза необходимо перечислить на счет злоумышленников определенную сумму денежных средств, 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.

6. Продажа имущества на интернет-сайтах.

При звонке на телефон, размещенный на Интернет-сайтах объявлений (Авито, ФарПост, Дром и др.) правонарушитель просит пополнить счет его телефона, либо сообщить данные и номер карты потерпевшего для перевода денежных средств в качестве задатка за товар. После сообщения данных карты происходит списание денежных средств.

Чтобы не стать жертвой дистанционных мошенничеств и хищений денежных средств на Ваших банковских счетах следует запомнить простые правила:

- сотрудники любого банка никогда не просят сообщить данные вашей карты (номер карты, срок её действия, секретный код на оборотной стороне карты), так как у них однозначно имеются ваши данные. Не передавайте злоумышленникам коды СМС-сообщений для перевода денег.

- при поступлении звонка «Ваш родственник в опасности» - позвоните своему родственнику или при личной встрече уточните его нуждаемость в Вашей финансовой помощи.

- совершая покупки на интернет-сайтах, доверяйте только проверенным продавцам и сайтам.

Похитить Ваши денежные средства, хранящиеся на банковском счете, возможно, завладев банковской карточкой и ПИН-кодом, поэтому не сообщайте его посторонним, а при утрате банковской карты оперативно примите меры к ее блокировке.

За истекший период 2023 года на территории района зарегистрировано 20 хищений денежных средств с банковских счетов, ущерб по которым превысил 500 тыс. рублей. Прокуратурой района в суд направлено 2 уголовных дела указанной категории.

Противостоять мошенникам возможно повышенной внимательностью, здравомыслием и бдительностью, что убережет Вас от уловок мошенников.

Своевременное обращение в правоохранительные органы поможет найти виновных и привлечь их к уголовной ответственности, а также обезопасит других от незаконных уловок телефонных мошенников.

Если Вы не согласны с результатами рассмотрения обращения ОМВД России по Симферопольскому району, Вы можете обратиться в прокуратуру района ежедневно на личном приеме без предварительной записи: с понедельника по четверг с 09.00 до 13.00, 13.45 до 18.00; в пятницу с 09.00 до 13.00, 13.45 до 16.45 часов.

Обращение можно отправить по адресу: ул. Долгоруковская, д. 2, г. Симферополь Республика Крым, 295000, а также воспользоваться Интернет-приемной на портале Генеральной прокуратуры Российской Федерации по адресу: https://epp.genproc.gov.ru/web/proc_91/internet-reception; записаться на прием или подать обращение также возможно в личном кабинете на портале: https://www.gosuslugi.ru.

Прокуратура Симферопольского района