

1. Прокуратура Республики Мордовия разъясняет о новых способах дистанционного мошенничества

Под влиянием злоумышленников доверчивые граждане оформляют кредиты и переводят денежные средства мошенникам.

Для введения в заблуждение мошенники с использованием специальных программных средств подменяют абонентский номер, который определяется мобильным устройством как входящий.

Мошенники представляются службой поддержки государственных услуг, сообщают о взломе их личного кабинета, затем просят набрать определенную комбинацию цифр и символов, таким образом меняя настройки сим-карты, устанавливая переадресацию смс-сообщений и звонков на номер злоумышленника.

Получая информацию из сообщений, преступники открывают доступ к государственным услугам, личным кабинетам в банки и совершают операции по списанию денежных средств.

Чтобы не стать жертвой преступников необходимо запомнить и соблюдать следующие правила:

- не сообщать никому, в том числе лицам, представившимся сотрудниками банковских организаций, данные банковских карт, а также сведения из смс-сообщений для входа в онлайн-банк или совершения финансовой операции;
- не осуществлять поспешные переводы денежных средств, лицам, представившимся родственниками, без проверки данной информации;
- не загружать на мобильные устройства приложения и программы из непроверенных источников;
- проявлять бдительность при осуществлении онлайн-покупок, не переходить для покупок по ссылкам.

Если доверившись злоумышленнику Вы сообщили данные своих банковских карт и другую значимую информацию, необходимо незамедлительно позвонить на горячую линию банка по номеру телефона, указанному на обороте банковской карты, установить блокировку на совершение банковских операций и обратиться в правоохранительные органы.

2. Осторожно, мошенническая схема: «А вы продлили договор по использованию (обслуживанию) SIM-карты?»

В последнее время достаточно распространенной схемой для мошенников стало предложение по продлению либо подтверждению номера мобильного телефона.

Как правило, злоумышленник начинает телефонный разговор с информирования о том, что срок обслуживания SIM-карты заканчивается. Если его не продлить, то номер мобильного телефона переходит другому лицу. В офисе сотовой компании при этом, как утверждает мошенник, приезжать не обязательно – все можно сделать через личный кабинет «Госуслуги», для чего достаточно сообщить код из смс-сообщения.

Далее жертве приходит СМС-сообщение с кодом доступа в личный кабинет портала «Госуслуги». Сообщая данный код доступа мошенникам – тем самым Вы передаете им доступ ко всей персональной информации.

Гражданам следует помнить о том, что операторы сотовой связи не продлевают абонентские договоры по использованию или обслуживанию SIM-карт, не просят пароли от личного кабинета портала «Госуслуги» или других приложений.

Важно знать, что абонентские договоры по использованию или обслуживанию SIM-карт являются бессрочными и расторгаются только по желанию пользователя и при личном посещении салона связи.

3. Как обезопасить себя от мошенников в интернете?

Мошенники умело используют всю доступную информацию и технологии, разбираются в психологии людей, вынуждая жертву раскрывать всю информацию о себе, либо совершать те или иные действия, используют человеческие слабости (стяжательство, алчность) и чувства (сострадание, обеспокоенность за близких, жалость) в своих корыстных интересах.

Можно обозначить следующие направления мошенничества в сети «Интернет»: дешевые товары на интернет-досках объявлений и онлайн-магазинах, фишинг, фейковый сбор средств на благотворительность.

Дешевые товары на интернет-досках объявлений и онлайн-магазинах – для обмана граждан зачастую используют площадки различных интернет-магазинов, путем создания «выгодных» предложений, что зачастую приводит к ситуации, когда покупатель остается как без товара, так и без денег. Вполне возможно обезопасить себя от подобного рода мошенников, главное – всегда скептически относиться к подозрительным объявлениям с низкой ценой на товар, анализировать репутацию продавца – проверять отзывы. Старайтесь отдавать предпочтение проверенным интернет-ресурсам. С покупками, которые подразумевают пересылку товара из другого города от частного лица необходимо проявлять повышенную бдительность и осторожность.

Следующий вид распространенного мошенничества в сети «Интернет» – фишинг. Суть фишинга – поддельные сайты и интернет-ресурсы известных интернет-площадок. Мошенникам требуется, чтобы вы зашли на сайт и под каким-либо предлогом оставили данные своей карты. В отдельных случаях можно отличить подделку от официального сайта, но зачастую это довольно затруднительно. Главный способ обезопасить себя от такого рода мошенничества – игнорировать подозрительные ссылки, присланные на вашу электронную почту или телефон, а также ни при каких обстоятельствах не оставлять данные своей карты интернет-ресурсам, в которых вы не уверены до конца. Ваша задача – вовремя усомниться.

В сети «Интернет» зачастую можно встретить различные благотворительные сборы, мошенники в данном случае пользуются не только состраданием и доверием интернет-пользователей, но и бедами абсолютно незнакомых им людей. После таких объявлений в интернете всегда указываются банковские реквизиты для перевода денег, таких объявлений стоит избегать.

В случае, если вы решили перевести деньги – необходимо разобраться в ситуации и понять, не столкнулись ли вы с очередным мошенником.

О фактах незаконных действий (бездействия) граждане могут сообщить в органы прокуратуры.

4. О принимаемых коммерческими банками мерах по противодействию киберпреступлениям

В методических рекомендациях от 19.02.2021 № 3-МР Банком России предложено кредитным организациям усилить информационную работу, направленную на повышение осведомленности их клиентов в отношении сохранности информации, используемой в целях совершения банковских операций, в частности перевода денежных средств.

Одной из рекомендаций является предложение осуществлять на постоянной основе СМС-информирование клиентов по теме противодействия мошенничеству, например, не реже 1 раза в квартал.

Поскольку фактически коммерческими банками указанные рекомендации не исполняются, напоминаем об основных правилах безопасности при телефонном общении с незнакомыми лицами:

- не сообщайте конфиденциальную информацию (коды доступа, данные банковских карт, пароли, логины);
- не осуществляйте оформление кредитов по требованиям звонящих;
- не переводите денежные средства на указанные ими счета.

5. Вступают в силу механизмы по противодействию хищению денежных средств граждан дистанционным способом

С целью совершенствования механизма противодействия хищению денежных средств в качестве превентивных мер 24.07.2023 принят Федеральный закон от № 369-ФЗ «О внесении изменений в Федеральный закон «О национальной платежной системе».

По закону оператор по переводу денежных средств (банк) обязан осуществить проверку наличия признаков осуществления перевода денежных средств без добровольного согласия клиента либо с согласия клиента, полученного под влиянием обмана или при злоупотреблении доверием. Причем такая проверка должна быть проведена до момента списания денежных средств клиента.

При наличии признаков перевода денежных средств без согласия клиента, оператор должен приостановить прием к исполнению распоряжения клиента на два дня, а если операция производится с использованием платежных карт или путем перевода электронных денежных средств, то отказать в выполнении операции.

Законом также предусмотрены меры защиты клиента в случае необоснованного перечисления денежных средств.

Например, если оператор после перевода денежных средств получает от Банка России информацию о том, что проведенная операция содержит признаки перевода денежных средств без добровольного согласия клиента, оператор обязан возместить клиенту эту сумму в 30-дневный срок.

Кроме того, банк будет обязан приостановить использование клиентом электронного средства платежа, если к нему об этом счете или клиенте поступит информация от Банка России или правоохранительных органов о совершенных противоправных действиях с использованием этого счета.

Простыми словами счета, используемые для хищения денежных средств граждан, а также для их последующего вывода будут блокироваться банками. Более того, в некоторых случаях могут быть заблокированы все счета и платежные карты гражданина, открытые на его имя, независимо от того, какие из них использовались в противоправных целях.

Закон вступил в силу с 25.07.2024.