Памятка

для граждан об основных способах дистанционного мошенничества

ПРОКУРАТУРА ЛЕВОКУМСКОГО РАЙОНА СТАВРОПОЛЬСКОГО КРАЯ

Код междугородней связи: 8 (865-43), адрес: ул. Карла Маркса, 176 с. Левокумское, 357960, факс 8(865-43)3-21-02, электронная почта: lev@26.mailop.ru

Прокуратура Левокумского района предупреждает граждан об опасности стать жертвами телефонных мошенников, а также дает простые и действенные методы защиты своих средств и банковских счетов.

Надзорное ведомство приводит примеры самых распространенных способов, которыми злоумышленники отнимают деньги у населения.

Наибольшее количество преступлений в сфере электронных платежей совершено в отношении граждан средней возрастной группы.

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

Выделяется несколько основных схем телефонного мошенничества.

1. Случай с родственником.

Мошенник представляется родственником (знакомым) и взволнованным голосом по телефону сообщает, что задержан сотрудниками полиции за совершение преступления. 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).

2. 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. Будьте осторожны!

3. 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.

4. 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.

5. Штрафные санкции оператора.

Злоумышленник представляется сотрудником службы технической поддержки оператора мобильной связи и сообщает, что абонент сменил тарифный план, не оповестив оператора (также могут быть варианты: не внес своевременную оплату, воспользовался услугами роуминга без предупреждения) и, соответственно, ему необходимо оплатить штраф в определенном размере, купив карты экспресс-оплаты и сообщив их коды.

6. Ошибочный перевод средств.

Абоненту поступает SMS-сообщение о поступлении средств на его счет, переведенных с помощью услуги «Мобильный перевод». Сразу после этого поступает звонок и мужчина (или женщина) сообщает, что ошибочно перевел деньги на его счет, при этом просит вернуть их обратно тем же «Мобильным переводом». В действительности деньги не поступают на телефон, а человек переводит свои собственные средства. Если позвонить по указанному номеру, он может быть вне зоны доступа. Кроме того, существуют такие номера, при

7. Предложение получить доступ к СМС-переписке и звонкам абонента.

Учитывая склонность некоторых граждан «пошпионить» за близкими и знакомыми, злоумышленниками используется следующая схема мошенничества в сети Интернет: пользователю предлагается изучить содержание смс-сообщений и список входящих и исходящих звонков интересующего абонента. Для этого необходимо отправить сообщение стоимостью от 10 до 30 рублей на указанный короткий номер и вписать в предлагаемую форму номер телефона абонента. После того, как пользователь отправляет смс, с его счета списывается сумма гораздо больше той, что была указана мошенниками, а интересующая информация впоследствии так и не поступает.

8. Продажа имущества на интернет-сайтах.

В Интернете действует большое количество мошеннических сайтов, предлагающих товары и услуги. Важно доверять только проверенным ресурсам или производить оплату лишь при получении товара.

При покупке товаров через Интернет злоумышленники могут использовать сайты и соцсети, где размещают ложные объявления о покупке или продаже товаров. Они заинтересовывают граждан своим предложением и

убеждают перечислить им деньги якобы в качестве предоплаты. После этого лже-продавцы прекращают контакты с обманутыми людьми. В этом случае не рекомендуется перечислять предоплату, не увидев в реальности покупаемые вещи. Также не следует пользоваться услугами непроверенных сайтов. Необходимо обратить внимание на предупреждающую информацию на сайте и ознакомиться с отзывами других посетителей.

9. Новая схема телефонного мошенничества «Вишинг».

Одной из распространенных схем киберпреступников в последние годы стал «Вишинг» – это вид мошенничества, при котором злоумышленники под любым предлогом вынуждают нас предоставлять конфиденциальные данные в «наших собственных интересах», то есть искусственно создается ситуация, требующая помощи от специалиста.

Во многих случаях в течение дня нам постоянно начинают звонить на мобильник с незнакомого номера. Звонки с номеров обычно настолько настойчивы (иногда до десяти звонков за день), что мы зачастую уступаем и отвечаем на них.

Как только мы отвечаем на звонок, нам сразу сообщают важную информацию о возникших проблемах с нашей картой, например, что она заблокирована, а служба безопасности банка предотвратила попытку несанкционированного списания. Затем звонящий предлагает помощь в сложившейся ситуации, на которую многие из нас соглашаются.

Нас убеждают в срочном решении возникшей ситуации, пока еще не все деньги украдены. Очень последовательно мошенники стараются получить от нас всю личную информацию о кредитке, присылают новые пароли и ПИН коды в СМС-уведомлениях. Успокаивающим голосом «банковские работники» предлагают различные возможные варианты защиты.

Догадаться о том, что любезный помощник на другом конце провода является мошенником не всегда легко, но в любом случае это возможно.

Изначально можно поблагодарить за бдительность и узнать должность, инициалы звонившего сотрудника кредитной организации и предпринять попытку дозвониться по горячей линии.

10. Хищения с карт, подключенных к опции бесконтактных платежей.

Для проведения оплаты по такой карте достаточно приложить её к терминалу. Ввод ПИН-кода не требуется если сумма не превышает 1 000 рублей. При этом количество расходных транзакций не ограничено. Чтобы получить деньги, мошеннику даже не понадобится воровать карту у клиента. Если в общественном транспорте поднести устройство к сумке или карману владельца, то средства спишутся. Для этих целей мошенники изготавливают самодельные переносные считыватели или используют банковские терминалы, оформленные по фиктивным документам.

11. Взлом аккаунта друга.

Люди могут даже не подозревать, что им пишет посторонний человек под видом родственника, друга, с просьбой перевода денег в связи с

произошедшим горем. Таким образом, войдя в доверие, мошенники пытаются украсть ваши деньги.

Так, в последнее время массовый характер приняла рассылка через мессенджер WhatsApp сообщений с просьбой проголосовать за ребёнка в конкурсе. Сообщение содержит ссылку на страницу голосования, посредством которой злоумышленники получают полный доступ к сообщениям и контактам WhatsApp жертвы.

Если Вы уже стали жертвой такой атаки, в iPhone в настройках приложения WhatsApp необходимо зайти в раздел «Связанные устройства» и удалить все устройства, которые там имеются.

В телефонах с операционной системой Android в приложении WhatsApp в правом верхнем углу необходимо нажать три точки, в выпадающем меню перейти в раздел «Связанные устройства» где также удалить все устройства, которые там имеются.

После перехода по ссылке Вы попадаете на страницу голосования, а после нажатия кнопки «проголосовать» переходите на страницу авторизации в WhatsApp WEB где, введя свой номер телефона, Вы даёте доступ к своим данным.

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:

- 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 отвечать на звонки или SMS-сообщения с неизвестных номеров с просьбой положить на счет деньги;

- не следует сообщать по телефону кому бы то ни было сведения личного характера.

Своевременное обращение в правоохранительные органы может помочь другим людям не попасться на незаконные уловки телефонных мошенников.

Противостоять мошенникам возможно лишь повышенной внимательностью, здравомыслием, бдительностью и контролем за собственными действиями.