

# **ПАМЯТКА**

## **прокуратуры Ремонтненского района**

### **о профилактике и предупреждении дистанционных преступлений в сфере информационно-телекоммуникационных технологий**

Несмотря на принимаемые правоохранительными органами меры, дистанционные хищения с использованием информационно-телекоммуникационных технологий стремительно набирают силу.

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, используют человеческие слабости (стяжательство, алчность), чувства (сострадание, обеспокоенность за близких, жалость) в своих корыстных интересах.

Основные известные схемы телефонного мошенничества:

#### **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). 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. Телефонный заказ от руководителей правоохранительных и государственных органов власти.**

На телефон абонента (предпринимателя, руководителя объекта общественного питания, торгового центра либо их сотрудникам и др.) поступает звонок от правонарушителя, который представляется одним из руководителей правоохранительных органов (прокуратуры города и др.) и просит пополнить счет его телефона, дополнительно к этому просит, например, забронировать столик в ресторане и сообщает, что по приезду на объект рассчитается. Не дожидаясь приезда якобы должностного лица, руководствуясь принципом уважения и доверия к руководителю названной должности в правоохранительных органах, потерпевший переводит через терминал банка, либо через иные финансовые услуги денежные средства в указанной сумме.

### **5. 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.

### **6. 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.

### **7. 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 осуществлении вызова на которые с телефона снимаются все средства.

## **8. 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.

## **9. 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.

## **10. 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.

Цель мошенников под любым предлогом извлечь секретную личную информацию о кредитке. Для получения доступа к конфиденциальным данным владельца мнимые помощники используют телефонную связь как в автоматизированном режиме, так и напрямую от мнимого «операциониста» банковского сектора.

Во многих случаях в течение дня нам постоянно начинают звонить на мобильник с незнакомого московского номера, начинающегося на 495. Звонки с московских 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.

Использовать для выяснения сложившейся ситуации лучше другой свой номер, потому что на сегодняшний день у вымогателей существуют технологии, позволяющие перенаправлять все последующие звонки на телефонное устройство мошенников.

### **11. 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.

Также в текущем году злоумышленники продолжают активно использовать фишинг в социальных сетях и онлайн-мессенджерах. Наибольшую выгоду мошенникам приносят махинации через Авито, с помощью которых они получают доступ в онлайн-банк.

### **12. 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.

### **13. Телефонное мошенничество во время пандемии.**

Многие из нас ввиду пандемии находились дома, что активизировало мошенничество с банковскими картами по телефону. Очень оперативно этим моментом воспользовались вымогатели с помощью смартфона.

Вот лишь несколько новых примеров того, как происходит телефонное мошенничество с последующей кражей денег с кредитки, учитывая современную ситуацию:

- на телефон приходит СМС-уведомление о начислении компенсации за нерабочий период во время эпидемии, для получения которой предлагается перезвонить в банк и пообщаться с мнимым «сотрудником».

- злоумышленники звонят нам с уведомлением о том, что мы якобы находились в контакте с заболевшими Covid-19. В связи с этим предлагается срочно сдать платный анализ на коронавирус, а чтобы не нарушать режим самоизоляции, «сотрудники лаборатории» готовы приехать к нам на дом. Для срочного выезда бригады нужно совершить предоплату.

В обоих случаях подставной человек, будь это сотрудник банка или мед. персонал, предлагает свою онлайн-помощь, чтобы осуществить платеж, а для этого ему нужна информация о счете. После получения необходимых данных

мошенники выводят деньги, а мы, доверчивые граждане, остаемся с нулевым балансом.

Приведенный перечень мошеннических схем не ограничивается приведенными примерами. Преступники находят все новые и новые схемы и способы для достижения своих преступных замыслов.

## **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 и бдительностью.