Приложение к письму
МАУ «ИМЦ»
от 26.04.2022 № 02/10-121/129

**Памятка
об основных способах
дистанционного мошенничества**

С переходом населения на безналичный расчет, выпуском и начислением заработных плат, пенсий, пособий и других выплат на пластиковые карты, появлением большого количества интернет-магазинов, возможностью оплачивать услуги онлайн, интернет становится более доступным, расширяются зоны покрытия сетей сотовой связи, как следствие, все больше людей пользуются современными технологиями.

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.

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

Однако раскрываемость этих преступлений остается невысокой, порядка 40 %, что связано со спецификой преступных технологий.

Этому способствует анонимность и отсутствие непосредственного контакта преступника с потерпевшим, трансграничный характер посягательств, поскольку большая часть деяний совершена лицами, находившимися за пределами региона, либо денежные средства потерпевших переведены на счета и телефоны, используемые на территории иных субъектов России.

Основные известные схемы телефонного мошенничества:

**1. Мошенничества через сайты объявлений.**

Преступник, выступая в роли продавца, размещает на сайтах объявлений (Авито, ФарПост, Дром и др.) информацию о продаже какого- либо товара, сдаче в аренду недвижимости или же оказании тех или иных услуг, за которые в последующем получает предоплату, тем самым похищая деньги.

В другом случае мошенник выступает в роли покупателя. Он звонит по объявлению потерпевшего, размещенному на интернет-площадке, и говорит, что желает приобрести его товар и готов внести задаток, для чего просит продиктовать контрольные данные по банковской карте и поступивший код и в последующем похищает денежные средства.

**2. Мошенничества со взломом страниц социальных сетей.**

Злоумышленники взламывают страницы социальных сетей, а затем отправляют всем друзьям из списка сообщения мошеннического характера с просьбой занять денежные средства под различными предлогами (заболел родственник, не хватает на срочную покупку и т.д.).

**3. Мошенничество, совершенное под предлогом несанкционированных списаний с банковской карты.**

Мошенник, используя IP-телефонию, звонит потенциальной жертве с виртуального номера и сообщает о том, что по его банковской карте либо по счету осуществляются несанкционированные списания денежных средств, или происходит оформление кредита, и для сохранения средств необходимо их перевести в безопасную ячейку. После чего, потерпевший, следуя инструкциям мошенника, сообщает все реквизиты своих карт, их проверочные коды или коды, поступившие в смс-сообщении.

**4. Мошенничество, совершенное с использованием фишинговых сайтов.**

Фишинг дословно переводится как «рыбная ловля» или «ловля на живца». Конечная цель такого мошенничества - получить данные банковской карты потерпевшего, выудить его деньги либо получить прочее его имущество. Видов фишинга великое множество. Самый распространенный случай - это поддельный сайт, который маскируется под интернет-магазины, агрегаторы билетов и пр.

**5. Мошенничество, совершенное по схеме мнимого вложения денежных средств в лже-инвестиционные компании.**

Мошенники предлагают гражданам инвестировать свои сбережения в одну из крупнейших газодобывающих компаний страны, обещая сверхвысокий доход за короткий срок. А когда получают деньги, то перестают выходить на связь.

**6. 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 гоном 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).

**7. 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!

**8. 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.

**9. 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.

**10. 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.

**11. 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.

**12. 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.

**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.

Если человек все-таки стал жертвой преступления, то ему следует немедленно заблокировать свою банковскую карту и обратиться в полицию.

Получение у оператора сотовой связи детализации по исходящим и входящим звонкам, а в банке - выписки по движению денежных средств будет способствовать своевременному установлению обстоятельств преступления.

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.

Отдел по надзору за уголовно-процессуальной
и оперативно-розыскной деятельностью
прокуратуры Камчатского края