6. Продажа имущества на интернет-сайтах.

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

7. Телефонный заказ из правоохранительных, государственных и муниципальных органов.

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

8. 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 примеров того, как происходит телефонное мошенничество с последующей кражей денег с карты, 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 с уведомлением о том, что жертва якобы находилась 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.

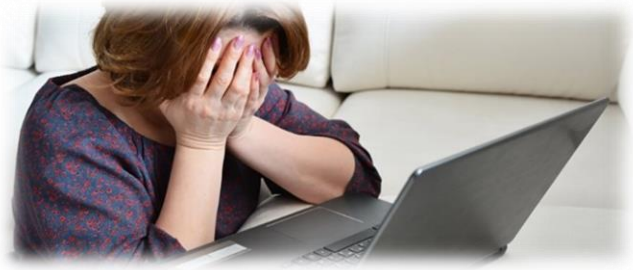
В обоих случаях подставной человек предлагает свою онлайн-помощь, чтобы осуществить платеж, а для этого ему нужна информация о банковской карте. После получения необходимых данных мошенники выводят деньги, а доверчивые граждане, остаются с нулевым балансом.

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 мошенников, необходимо соблюдать простые правила безопасного поведения и обязательно довести их до сведения родных и близких:

- не следует доверять звонкам и сообщениям, о том, что



близкий человек попал в беду или задержан сотрудниками полиции, особенно, если за этим следует просьба о перечислении денежных средств;

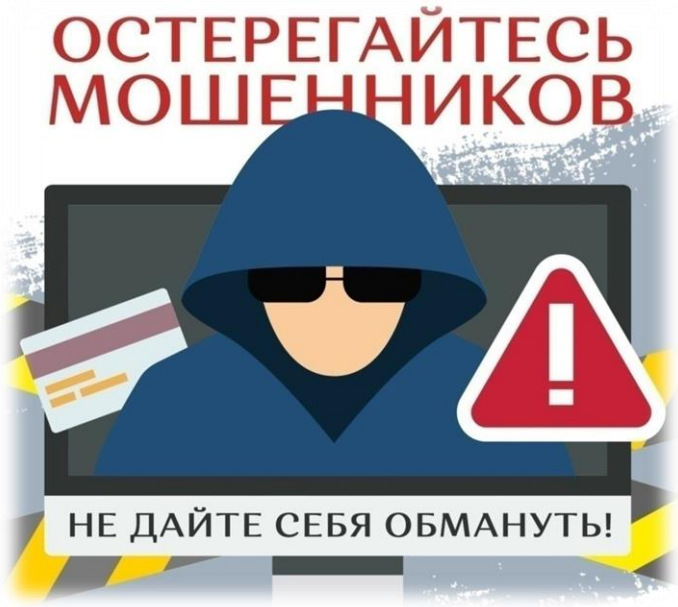
- не следует отвечать на звонки или SMS с неизвестных номеров с просьбой положить на счет деньги;

- не следует сообщать по телефону кому бы то ни было сведения личного характера и данные банковской карты.

Если Вы попались на удочку мошенников, немедленно сообщите в полицию (Мегафон, МТС, Теле2 – 020, Билайн - 002) или лично обратитесь с заявлением. В нем подробно опишите все обстоятельства: когда, и с какого номера сделан звонок (пришло сообщение), кто звонил, как представился, подробности разговора (сообщения), информацию, которую требовалось сообщить.

ПОМНИТЕ противостоять мошенникам возможно лишь повышенной внимательностью, здравомыслием и бдительностью!

Прокуратура Томской области



Томск
2020

Несмотря на принимаемые правоохранительными органами меры, дистанционные хищения с использованием информационно-телекоммуникационных технологий совершаются все чаще.

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 и чувства в своих корыстных интересах.

Основные известные схемы дистанционного мошенничества:

1. Фишинг.

Злоумышленники под любым предлогом вынуждают нас предоставлять конфиденциальные данные в «наших собственных интересах», то есть искусственно создается ситуация, требующая помощи от специалиста.

Цель мошенников - извлечь секретную информацию о карте. Для получения доступа к конфиденциальным данным владельца преступники 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 телефон 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 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 банковской карте, 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.

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

Активно используют фишинг также в социальных сетях и онлайн-мессенджерах. Наибольшую выгоду мошенникам приносят махинации через торговые площадки, с помощью которых они получают доступ в онлайн-банк.

2. 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.

3. 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 перевести на счет (абонентский номер телефона).

4. Розыгрыш призов.

На телефон абонента приходит смс-сообщение, из которого следует, что в результате проведенной лотереи он выиграл дорогой приз. 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 мошенники сообщают о том, что для выполнения необходимых формальностей (уплаты госпошлины, оформления документов, оплаты за комиссию перевода) счастливому обладателю приза 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.

5. SMS-просьба.

На телефон приходит 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.