ПРОКУРАТУРА ДУБЕНСКОГО РАЙОНА РАЗЪЯСНЯЕТ

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

Ежедневно каждый человек использует множество разнообразных высокотехнологичных устройств – пластиковых карт, мобильных телефонов, компьютеров. Регулярно появляются новые модели, программы и сервисы. Одновременно с развитием таких устройств появляются соответствующие виды мошенничества, позволяющие обмануть и присвоить денежные средства граждан.

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).

При этом, зачастую говорится чтобы лицо не клало трубку, ведь если звонок прекратится, то помочь уже не смогут.

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.

Сюда же можно отнести способы с якобы выигрышем, для чего нужно перейти по указанной ссылке, перейдя по которой с вашего мобильного счета просто спишут все деньги, либо получат доступ к привязанным к устройству счетам и картам.

Такие сайты зачастую либо вообще одноразовые, как вариант – зеркало другого сайта, либо сайт-клон с минимальным отличием в названии (латиница/кириллица), либо рассчитаны на очень короткий промежуток времени.

3. SMS-просьба.

SMS-сообщения позволяют упростить схему обмана по телефону. Такому варианту мошенничества особенно трудно противостоять пожилым или слишком юным владельцам телефонов. Дополнительную опасность представляют упростившиеся схемы перевода денег на счет. 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, сайта Госуслуги и т.п.

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, потерпевший переводит через терминал банка, либо через иные финансовые услуги денежные средства в указанной сумме. Как вариант, могут сообщить, что проводится проверка, и чтобы проверка ничего не нашла, или, к примеру, вообще не приехала, нужны определенная сумма денег.

Мошенники, представляющиеся сотрудниками сайта Госуслуг говорят, что данные либо уже скомпрометированы, либо вот прям сейчас их пытаются взломать и пытается получить доступ к личному кабинету.

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, нужно продлить действие симкарты или договора сотовой связи, хотя они бессрочные) и, соответственно, ему необходимо оплатить штраф в определенном размере, купив карты экспресс-оплаты и сообщив их коды из смс.

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, Юла, ФарПост, Дром, даже интернет сервисы типа Озон, Вайлдберрис и Яндекс-маркет) 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. Есть и более сложные варианты мошенничества.

10. Звонок от банка.

Мошенник, представляющийся специалистом банка, звонит и сразу сообщает важную информацию о возникших проблемах с нашей картой, например, что она заблокирована, а служба безопасности банка предотвратила попытку несанкционированного списания, или что на нее пытаются оформить кредит. 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.

При этом, зачастую говорится чтобы лицо не клало трубку, ведь если звонок прекратится, то платеж пройдет, то есть звонок как бы создает некую защиту.

Также бывают случаи, когда требуют установить якобы дополнительную программу поддержки клиентов, называя так программу для удаленного доступа к устройству – AnyDesk.

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.

12. Взлом аккаунта друга в социальных сетях.

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. Телефонный номер-грабитель.

Развитие технологий и сервисов мобильной связи упрощает схемы мошенничества. Вам приходит SMS с просьбой перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной – помощь другу, изменение тарифов связи, проблемы со связью или с Вашей банковской картой и так далее. После того как Вы перезваниваете, Вас долго держат на линии. Когда это надоедает, Вы отключаетесь – и оказывается, что с Вашего счета списаны крупные суммы. Существуют сервисы с платным звонком. Чаще всего это развлекательные сервисы, в которых услуги оказываются по телефону, и дополнительно взимается плата за сам звонок. Реклама таких сервисов всегда информирует о том, что звонок платный. Мошенники регистрируют такой сервис и распространяют номер без предупреждения о снятии платы за звонок.

14. Продажа авиа и железнодорожных билетов, а также различных товаров, в том числе «брендовых», на сайтах, похожих на официальные.

15. «Брачные мошенничества»

Типичный механизм: с использованием сети Интернет преимущественно на сайтах знакомств преступники выбирают жертву, налаживают с ним электронную переписку от имени девушек, обещая приехать с целью создания в будущем семьи. Затем под различными предлогами «невесты» выманивают деньги (на лечение, покупку мобильного телефона, приобретение билетов, оплаты визы и т.д.). Переписка ведется главным образом студентами лингвистических ВУЗов. Направленные жертвами деньги преступники получают на подставных лиц. После получения средств переписка под различными предлогами прекращается.

16. «Нигерийские письма»

Ранее один из самых распространённых видов мошенничества. Типичная схема: жертва получает на свою почту письмо о том, что является счастливым обладателем многомиллионного наследства. Затем мошенники просят у получателя письма помощи в многомиллионных денежных операциях (получение наследства, перевод денег из одной страны в другую), обещая процент от сделки. Если получатель согласится участвовать, то у него постепенно выманиваются деньги якобы на оплату сборов, взяток чиновникам и т.п.

17. Брокерские или инвестиционные конторы под предлогом заработка при «игре» на бирже, инвестирования.

Данные преступления совершаются в результате поиска потерпевшими дополнительного источника дохода. Как правило, потерпевшие оставляют в сети интернет заявку на регистрацию и спустя некоторое время им перезванивает злоумышленник, который предлагает создать личный кабинет на платформе одной из бирж либо перечислить денежные средства для инвестирования, а также убеждает потерпевшего установить программы удалённого доступа «Team - Viewer» или «AnyDesk» с целью оказания «помощи» и контроля за личным кабинетом потерпевшего. После чего жертва под влиянием злоумышленника систематически перечисляет денежные средства различными сумма на лицевой счет, который отображается в личном кабинете биржи либо на банковские карты мошенников, думая, что инвестирует денежные средства. Злоумышленник, в свою

очередь, закрывает доступ к личному кабинету и потерпевший не может вывести данные денежные средства. Для этого его убеждают в необходимости внесения дополнительной суммы денег.

А еще есть VPN и изменители номера…

КАК ПОСТУПАТЬ В СИТУАЦИИ ТЕЛЕФОННОГО МОШЕНИЧЕСТВА: Первое и самое главное правило — прервать разговор и перезвонить тому, о ком идет речь (либо в указанный государственный орган). Если телефон отключен, постарайтесь связаться с его коллегами, друзьями и родственниками для уточнения информации. Хотя беспокойство за родственника или близкого человека мешает мыслить здраво, следует понимать: если незнакомый человек звонит Вам и требует привезти на некий адрес денежную сумму – это мошенник. Если Вы получили звонок от якобы близкого родственника или знакомого с информацией о том, что он попал в неприятную ситуацию, в результате которой ему грозит возбуждение уголовного дела, и если звонящий просит передать взятку якобы сотруднику правоохранительных органов, готовому урегулировать вопрос, следует задать уточняющие вопросы: «А как я выгляжу?» или «Когда и где мы виделись последний раз?», т.е. задавать вопросы, ответы на которые знаете только вы оба. Если вы разговариваете якобы с представителем правоохранительных органов, спросите, из какого он правоохранительного органа (другого ведомства). После звонка следует набрать «02», узнать номер дежурной части данного отделения и поинтересоваться, действительно ли родственник или знакомый доставлен туда. Само требование взятки должностным лицом является преступлением.

Особое внимание уделяйте обеспечению безопасности данных ваших банковских карт. Никогда и никому не сообщайте ПИН-код Вашей карты. Лучше всего его запомнить. Относитесь к ПИН-коду как к ключу от сейфа с вашими средствами. Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё – в этом случае Вы даже не успеете обезопасить свой счет, заблокировав карту после кражи или утери.

2. НИ У КОГО НЕТ ПРАВА ТРЕБОВАТЬ ВАШ ПИН-КОД

Если Вам позвонили из какой-либо организации, или Вы получили письмо по электронной почте (в том числе из банка) с просьбой сообщить реквизиты карты и ПИН-код под различными предлогами, не спешите ее выполнять. Позвоните в указанную организацию и сообщите о данном факте. Не переходите по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники. Помните: хранение реквизитов и ПИН-кода в тайне – это Ваша ответственность и обязанность.

3. НЕМЕДЛЕННО БЛОКИРУЙТЕ КАРТУ ПРИ ЕЕ УТЕРЕ

Если Вы утратили карту, срочно свяжитесь с банком, выдавшим ее, сообщите о случившемся и следуйте инструкциям сотрудника банка. Для этого держите телефон банка в записной книжке или в списке контактов Вашего мобильного телефона.

4. ПОЛЬЗУЙТЕСЬ ЗАЩИЩЕННЫМИ БАНКОМАТАМИ

При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д. Граждане, пользующиеся банкоматами без видеонаблюдения, могут подвергнуться нападениям злоумышленников.

5. ОПАСАЙТЕСЬ ПОСТОРОННИХ

Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей. Если это невозможно, снимите деньги с карты позже либо воспользуйтесь другим банкоматом. Набирая ПИН-код, прикрывайте клавиатуру рукой. Реквизиты и любая прочая информация о том, сколько средств Вы сняли и какие цифры вводили в банкомат, могут быть использованы мошенниками.

8. БАНКОМАТ ДОЛЖЕН БЫТЬ «ЧИСТЫМ»

Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нем телефону.

9. БАНКОМАТ ДОЛЖЕН БЫТЬ ПОЛНОСТЬЮ ИСПРАВНЫМ

В случае некорректной работы банкомата – если он долгое время находится в режиме ожидания или самопроизвольно перезагружается – откажитесь от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.

10. СОВЕТУЙТЕСЬ ТОЛЬКО С БАНКОМ

Никогда не прибегайте к помощи либо советам третьих лиц при проведении операций с банковской картой в банкоматах. Свяжитесь с Вашим банком – он обязан предоставить консультационные услуги по работе с картой.

11. НЕ ДОВЕРЯЙТЕ КАРТУ ОФИЦИАНТАМ И ПРОДАВЦАМ

В торговых точках, ресторанах и кафе все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.

Самое главное – будьте бдительны и не поддавайтесь эмоциям!

Прокурор Дубенского района
Старший советник юстиции
Фридрих Г.Л.