**Как не стать жертвой телефонного или интернет-мошенничества**

Вместе с развитием современных технологий появляются и новые виды преступлений с использованием информационно-коммуникационных технологий. В последнее время наиболее распространено мошенничество в сфере информационно-телекоммуникационных технологий или компьютерной информации. Отмечается значительное увеличение числа краж, совершённых с банковского счёта или в отношении электронных денежных средств. Избежать роли потерпевшего поможет осведомлённость о наиболее распространённых методах, которые используют телефонные мошенники с целью обмана граждан для незаконного заработка. Как показывает статистика, чаще в сети телефонных мошенников попадаются пожилые или доверчивые люди. Каждый человек может стать жертвой мошенничества, если не будет следовать простым правилам безопасности.

Рассмотрим типовые схемы обмана, используемые мошенниками. Обман по телефону. Человеку звонят с незнакомого номера, мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками правоохранительных органов и обвинён в совершении того или иного преступления. Далее в разговор вступает якобы сотрудник правоохранительного органа. Он уверенным тоном сообщает, что уже не раз помогал людям таким образом. Для решения вопроса необходима определённая сумма денег, которую следует перевести на определённый расчётный счёт или передать какому-либо человеку. Цена вопроса составляет такую-то сумму. В организации обмана по телефону с требованием выкупа участвуют несколько преступников. Звонящий может находиться как в исправительно-трудовом учреждении, так и на свободе. Набирая телефонные номера наугад, мошенник произносит заготовленную фразу, а далее действует по обстоятельствам. Нередко жертва сама случайно подсказывает имя того, о ком она волнуется. Если жертва преступления поддалась на обман и согласилась привезти или перечислить указанную сумму, звонящий называет адрес, куда нужно приехать, либо номер счёта. Первое и самое главное правило - прервать разговор и перезвонить тому, о ком идёт речь, либо в указанный государственный орган. Если телефон отключён, 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 звонок получен 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?", то есть задавать вопросы, ответы на которые знаете только Вы".

Если человек разговаривает якобы с представителем правоохранительных органов, поинтересуйтесь, из какого он именно подразделения и кто у него руководитель. А после звонка следует набрать "02", узнать номер дежурной части данного отделения и поинтересоваться, действительно ли такой сотрудник там работает.

Также одним из видов подобного рода мошенничества являются 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 счёт. Абонент получает на мобильный телефон сообщение: "У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам". Нередко добавляется обращение "мама", "друг" или другие". В такой ситуации пожилым людям, детям и подросткам следует, во-первых, объяснить, что на SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники. Кроме этого, 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 счёта 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. Единственный способ обезопасить себя от телефонных мошенников - не звонить по незнакомым номерам. Это было бы самым наилучшим вариантом, просто не брать трубку, когда звонит незнакомый номер. Но сегодня существуют и так называемые телефонные вирусы, причём сегодня эта распространено довольно широко. Рассмотрим технологию того, как это происходит.

На телефон абонента приходит сообщение следующего вида: "Вам пришло MMS-сообщение. Для получения пройдите по ссылке...". При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств с вашего счёта. Другой вид мошенничества выглядит так. При заказе какой-либо услуги через якобы мобильного оператора или при скачивании мобильного контента абоненту приходит предупреждение вида: "Вы собираетесь отправить сообщение на короткий номер..., для подтверждения операции, отправьте сообщение с цифрой 1, для отмены с цифрой 0". При отправке подтверждения, со счёта абонента списываются денежные средства. Мошенники используют специальные программы, которые позволяют автоматически генерировать тысячи таких сообщений. Сразу после перевода денег на фальшивый счёт они снимаются с телефона. Не следует звонить по номеру, с которого отправлен SMS – вполне возможно, что в этом случае с вашего телефона будет автоматически снята крупная сумма.

Ещё один распространённый вид незаконного отъёма денег у доверчивых сограждан - разного рода лотереи. Когда Вы якобы выиграли крупную сумму или автомобиль, но для получения приза вам необходимо, перечислить указанную сумму денег. Это обман в чистом виде. Всегда.

Выигрыш приза может стать не только приманкой, но и поводом затребовать перечисления крупных денежных средств для оформления нужных документов. На мобильный телефон человека приходит SMS-сообщение, в котором говорится о том, что в результате проведённой лотереи вы выиграли автомобиль. Для уточнения всех деталей его просят посетить определённый сайт и ознакомиться с условиями акции либо позвонить по одному из указанных телефонных номеров. Во время разговора мошенники сообщают о том, что надо выполнить необходимые формальности: уплатить госпошлину и оформить необходимые документы. Для этого необходимо перечислить на счёт своего мобильного телефона, например, 30 тысяч рублей, а затем набрать определённую комбинацию цифр и символов якобы для проверки поступления денег на счёт и получения кода регистрации. Комбинация цифр и символов, которую набирает человек, на самом деле является кодом, благодаря которому злоумышленники получают доступ к перечисленным средствам. Как только код набран, счёт обнуляется, а мошенники исчезают в неизвестном направлении.

Если человек узнал о проведении лотереи только в момент выигрыша, и при этом ранее не заполнял заявку на участие в ней и никак не подтверждал своё участие в розыгрыше, то вероятнее всего его пытаются обмануть. Оформление документов и участие в таких лотереях никогда не проводится только по телефону и интернету.

Мошенники могут позвонить даже под видом вашего мобильной связи. Но верить им тоже не стоит. Бывает так, что человеку поступает звонок либо приходит SMS-сообщение якобы от сотрудника службы технической поддержки вашего оператора мобильной связи. Обоснования этого звонка или SMS могут быть самыми разными: предложение подключить новую эксклюзивную услугу, для перерегистрации во избежание отключения связи из-за технического сбоя, для улучшения качества связи, для защиты от спам-рассылки, предложение принять участие в акции от имени сотового оператора. Человеку предлагается набрать под диктовку код или сообщение SMS, которое подключит новую услугу, улучшит качество связи и тому подобное. Код, который вам предложат отправить, является комбинацией для осуществления мобильного перевода денежных средств со счёта абонента на счёт злоумышленников. Как только он набирается, счёт будет опустошён. Любая упрощённая процедура изменения тарифных планов выглядит подозрительно. Так что лучше для уточнения условий перезвонить своему мобильному оператору.

В последнее время используется ещё одна схема - ошибочный перевод средств. Человеку приходит SMS-сообщение о поступлении средств на счёт, переведённых с помощью услуги "Мобильный перевод" либо с терминала оплат услуг. Сразу после этого поступает звонок, и ему сообщают, что на его счёт ошибочно переведены деньги и просят вернуть их обратно тем же "Мобильным переводом" либо перевести на "правильный" номер. После перевода денег такая же сумма списывается со счета. Чтобы во второй раз списать сумму со счета, злоумышленник использует чек, выданный при переводе денег. Он обращается к оператору с заявлением об ошибочном внесении средств и просьбой перевести их на свой номер. То есть первый раз деньги переводятся по его просьбе, а во второй раз он получает их по правилам возврата средств. Советуем не поддаваться на обман. Если человека просят перевести якобы ошибочно переведённую сумму, нужно напомнить, что для этого используется чек. Отговорка, что "чек потерян", скорее всего, свидетельствует о том, что с человеком общается мошенник.

На каком-либо сайте размещается информация о продаже какого-либо движимого или недвижимого имущества, автомобиля, дома. Подробно описывается товар, выкладываются фотографии и всё это по очень привлекательной цене. Низкую стоимость транспортного средства злоумышленники объясняют вполне житейскими ситуациями: переезд в другой регион, семейные проблемы, финансовые трудности и так далее. Желающему приобрести автомобиль предлагается внести задаток, поскольку, к примеру, на транспортное средство нашлось множество покупателей. Деньги злоумышленники просят перечислить переводом через банк либо на абонентский номер телефона. Получив желаемое, мошенники отключают телефоны и на связь с обманутой жертвой больше не выходят. Поэтому в таких случаях лучше не переводить никому денежные средства.

Совет - не переводить незнакомым людям денежные средства касается всех видов мошенничества. Не стоит платить преступникам. Которые, кстати, могут попытаться снять средства и с вашей банковской карты. Причём этот вид мошенничества один из самых распространённых. Ведь банковская карта - это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке.

Причём этот вид мошенничества один из самых распространённых. Ведь банковская карта - это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Однако такая простота использования банковских карт оставляет множество лазеек для мошенников. Как же это происходит. Человеку приходит сообщение о том, что его банковская карта заблокирована. Предлагается бесплатно позвонить на определённый номер для получения подробной информации. Когда он звонит по указанному телефону, ему сообщают о том, что на сервере, отвечающем за обслуживание карты, произошёл сбой, а затем просят сообщить номер карты и ПИН-код для её перерегистрации. Чтобы ограбить, злоумышленникам нужен лишь номер карты и ПИН-код. Как только их сообщат, деньги будут сняты со счёта. Ни одна организация, включая банк, не вправе требовать ваш ПИН-код! Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка. Скорее всего там ответят, что никаких сбоев на сервере не происходило, а карта продолжает обслуживаться.

Итак, ещё раз напомним, нельзя доверять мошенникам, которые утверждают, что карта заблокирована или со счетами что-то происходит. Лучше прервать общение и перезвонить в банк.

Как, общаясь по телефону, определить, что это мошенники? Существуют наиболее распространённые признаки, свидетельствующие о том, что вы имеете дело с мошенниками. Например,  
неизвестный просит сообщить CVV банковской карты (специальный код на обратной стороне карты), кодовое слово или код из СМС, указывают реквизиты для перевода, по которым просят перевести средства, просят предоставить какие-либо личные сведения, звонят с целью предупредить о мошеннической операции со счётом клиента, нет стопроцентной уверенности в том, откуда исходит звонок, сотрудник банка отказывается называть свои Ф.И.О., должность и рабочий номер телефона, обещают лёгких денег или выгоды без усилий, оказывают давление для ускорения принятия решения, торопят, описывают пугающие сценарии, собеседника пугает предупреждение о том, что разговор записывается, просят никому не рассказывать о разговоре и о том, что вас просят сделать. Это повод задуматься, не мошенник ли этот собеседник.

Будьте бдительны и осторожны! Берегите свои деньги!