Важно знать

Осторожно: вам звонят!

Чаще всего в сети телефонных аферистов попадаются излишне доверчивые люди

Магнитогорцы продолжают наступать на одни и те же грабли: доверяют незнакомым людям, верят в «волшебные» выигрыши и отдают свои сбережения по первому требованию. Чтобы уметь противостоять мошенникам, нужно знать хотя бы основные схемы, которыми пользуются преступники.

Требование выкупа

Казалось бы – старое «разводилово», но по-прежнему работает. Вам звонят с незнакомого номера. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции и обвинён в совершении того или иного преступления. Это может быть ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений или даже убийство. В общем, любое деяние, которое может вызвать шоковое состояние и породить невозможность мыслить ясно.

Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном сообщает, что уже не раз помогал людям в такой ситуации. Для решения проблемы необходима определённая сумма денег, которую следует привезти в оговорённое место или передать какому-либо человеку.

На самом деле происходит следующее. В организации обмана по телефону с требованием выкупа участвуют несколько преступников. Звонящий может находиться как в исправительно-трудовом учреждении, так и на свободе. Набирая телефоны наугад, мошенник произносит заготовленную фразу, а далее действует по обстоятельствам. Нередко жертва сама подсказывает имя того, о ком она волнуется. Если жертва преступления поддалась на обман и согласилась привезти указанную сумму, звонящий называет адрес, куда нужно приехать. Часто мошенники предлагают снять недостающую сумму в банке и сопровождают жертву лично. Стараются запугать, не дать опомниться, поэтому ведут непрерывный разговор вплоть до получения денег. После того, как человек передаёт деньги или оставляет их в условленном месте, ему сообщают, где он может увидеть родственника или знакомого.

В подобной ситуации первое и самое главное – прервать разговор и перезвонить тому, о ком идёт речь. Если телефон отключён, постарайтесь связаться с его коллегами, друзьями и родственниками для уточнения информации. И хотя беспокойство мешает порой мыслить здраво, следует понимать: если незнакомый человек звонит и требует на некий адрес привезти 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 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 в последний раз», то есть задавать вопросы, ответы на которые знаете только вы оба. Если разговариваете якобы с представителем правоохранительных органов, спросите, из какого он отделения полиции. После звонка следует набрать «02», узнать номер дежурной части данного отделения и поинтересоваться, действительно ли родственник или знакомый доставлен туда.

СМС-просьба о помощи

Письменное сообщение позволяет 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.

Организовано это так. Абонент получает на мобильный сообщение: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется слово «мама», «друг» и подобные.

Как поступить? Пожилым людям, детям и подросткам следует объяснить, что на СМС с незнакомых номеров реагировать нельзя, потому что это могут быть мошенники.

Телефонный номер-грабитель

Развитие технологий и сервисов мобильной связи упрощает схемы мошенничества. Вам приходит сообщение с просьбой перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной – помощь другу, изменение тарифов связи, проблемы со связью или вашей банковской картой. После того, как вы перезваниваете, вас долго держат на линии. Когда это надоедает, вы отключаетесь – и оказывается, что со счёта списаны крупные суммы денег.

На самом деле происходит следующее. Существуют сервисы с платным звонком. Чаще всего они развлекательные, в которых услуги оказываются по телефону, и дополнительно взимается плата за само соединение. Реклама таких сервисов всегда информирует о том, что звонок платный. Мошенники регистрируют такой сервис и распространяют номер без предупреждения о снятии платы за звонок.

Что делать? Не звонить по незнакомым номерам. Это единственный способ обезопасить себя от телефонных мошенников.

Телефонные вирусы

Очень часто используется форма мошенничества с использованием телефонных вирусов. На «трубку» приходит сообщение типа: «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 приходит предупреждение: «Вы собираетесь отправить сообщение на короткий номер…, для подтверждения операции отправьте сообщение с цифрой 1, для отмены цифру 0». При отправке подтверждения со счёта абонента списываются деньги. Мошенники используют специальные программы, которые позволяют автоматически генерировать тысячи таких сообщений.

Не следует звонить по номеру, с которого отправлено сообщение, – вполне возможно, что в этом случае с вашего телефона будет снята крупная сумма денег. Существует множество вариантов такого мошенничества.

Выигрыш в лотерее

В связи с проведением всевозможных рекламных акций, лотерей и розыгрышей, особенно с участием радиостанций, злоумышленники часто используют их для прикрытия своей деятельности и обмана людей.

«Вы победили, сообщите код карты экспресс-оплаты» – такие карты упростили процедуру зачисления средств на счёт, но одновременно открыли новые возможности для мошенников.

Как это организовано: на мобильный звонит якобы ведущий популярной радиостанции и поздравляет с крупным выигрышем в лотерее, организованной совместно радио и оператором мобильной связи. Это может быть телефон, ноутбук или даже автомобиль. Чтобы получить приз, необходимо в течение минуты дозвониться на радиостанцию. Перезвонившему абоненту отвечает сотрудник «призового отдела» и подробно объясняет условия игры: просит представиться и назвать год рождения, грамотно убеждает в честности акции (никаких взносов, переигровок), спрашивает, может ли абонент перевести на свой номер определённую сумму с карты экпресс-оплаты. Объясняет, что в течение часа необходимо подготовить карты экспресс-оплаты любого номинала на указанную сумму и ещё раз перезвонить для регистрации и присвоения персонального номера победителя. И сообщает номер, куда перезвонить. Потом поясняет порядок последующих действий для получения приза: с 10 до 20 такого-то числа нужно с паспортом, мобильным телефоном и присвоенным персональным номером прибыть по указанному адресу для оформления. Если абонент по каким-то причинам в течение часа не может купить карту экспресс-оплаты, он всё равно должен перезвонить для согласования дальнейших действий.

Затем мошенник объясняет порядок активации карты: стереть защитный слой, позвонить в призовой отдел, при переключении на оператора – сообщить свои коды. Якобы оператор их активирует на номер абонента, а призовой отдел контролирует правильность его действий. После этого победитель получает персональный номер, с которым должен ехать за «призом». Если вы предложите самостоятельно активировать карту на свой номер и приехать за доказательными документами из сотовой компании, то это объявят нарушением правил рекламной акции.

Есть и другой вариант. Вам может поступить звонок от якобы представителя вашей сотовой компании, который предложит пополнить счёт карточкой экспресс-оплаты. Но прежде чем совершить оплату, вы должны сообщить оператору код, перезвонив на определённый номер.

На самом деле происходит следующее. Задача мошенников – вынудить купить карты экспресс-оплаты на крупную сумму и сообщить личный код с этих карт. Это позволит злоумышленникам присвоить средства с этих карт. Приз и «победа» – приманка, призванная усыпить ваше внимание и бдительность.

Как поступать в такой ситуации. Управление «К» МВД РФ (подразделение, работающее в сфере информационных технологий) напоминает, что активировать карточки экспресс-оплаты следует исключительно через специальный короткий номер, указанный на ней, а личный код никому никогда не сообщается. Всё это указано на самой карте экспресс-оплаты – и в первую очередь нужно следовать этим правилам.

«Вы выиграли машину»

Выигрыш приза может стать не только приманкой, но и поводом затребовать перечисления крупных денежных средств для оформления нужных документов.

Организуется это так. На мобильный, – как правило, в ночное время – приходит смс-сообщение, в котором говорится, что в результате проведённой лотереи вы выиграли автомобиль. Чаще всего это машина премиум-класса.

Для уточнения всех деталей вас просят посетить определённый сайт и ознакомиться с условиями акции либо позвонить по одному из указанных телефонных номеров. Во время разговора мошенники сообщают, что нужно выполнить определённые формальности: оплатить госпошлину и оформить документы. Для этого нужно перечислить на счёт своего мобильного 30 тысяч рублей, а затем набрать определённую комбинацию цифр и символов якобы для проверки поступления денег на счёт и получения «кода регистрации».

На самом деле комбинация цифр и символов – код, благодаря которому злоумышленники получают доступ к перечисленным средствам. Как только код набран, счёт обнуляется, а мошенники исчезают в неизвестном направлении.

Если вы узнали о проведении лотереи только в момент «выигрыша», и при этом заранее не заполняли никаких заявок на участие и не подтверждали участие в розыгрыше, значит, вас пытаются обмануть. Оформление документов и участие в таких лотереях никогда не проводятся только по телефону и Интернету.

Продолжение следует.