**Осторожно! Мошенники!**

В настоящее время, когда широко используются мобильные телефоны и личный номер может быть у всех, от десятилетнего ребенка до восьмидесятилетнего пенсионера, случаи телефонного мошенничества растут с каждым годом. Следовательно, каждый человек может стать жертвой злоумышленников, если не будет соблюдать простые правила безопасности.

**Обман по звонку**

Вам звонят с незнакомого номера. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции и обвинен в совершении того или иного преступления. Это может быть ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и даже убийство.

Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном сообщает, что уже не раз помогал людям таким образом. Для решения вопроса необходима определенная сумма денег, которую следует привезти в оговоренное место и передать названному человеку или перевести на указанный счет. Цена вопроса составляет от одной до нескольких сот тысяч рублей.

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 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 указанную сумму, звонящий называет адрес, куда нужно приехать. Нередко мошенники предлагают снять недостающую сумму в банке и сопровождают жертву лично. Но наиболее часто встречающийся способ – перечисление оговоренной суммы на указанный расчетный счет.

Мошенники стараются запугать жертву, не дать ей опомниться, поэтому ведут непрерывный разговор с ней вплоть до получения денег. После того как гражданин оставляет деньги в указанном месте, перечисляет их или кому-то их передает, ему сообщают, где он может увидеть своего родственника или знакомого.

**Как поступать в такой ситуации?** Первое и самое главное правило – прервать разговор и перезвонить тому, о ком идёт речь. 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 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 проблему, следует задавать вопросы, ответы на которые знаете только вы оба.

Если вы 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.

И не забывайте, что требование взятки является преступлением.

**SМS-просьба**

SМS-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.

Как это организовано? 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.

**Как поступать в такой ситуации?** Пожилым людям, детям и подросткам следует объяснить, что на SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники.

**Номер–грабитель**

Развитие технологий и сервисов мобильной связи упрощает схемы мошенничества. Вам приходит SMS с просьбой перезвонить на указанный номер мобильного телефона, которая 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.

На самом деле происходит следующее. Существуют сервисы с платным звонком. Чаще всего это развлекательные, 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.

**Как поступать в такой ситуации?** Настоятельно советуем не звонить по незнакомым номерам. Это единственный способ обезопасить себя от телефонных мошенников.

**Вирус по ссылке**

Очень часто используется форма мошенничества с использованием телефонных вирусов. На телефон абонента приходит сообщение следующего вида: «Вам пришло SМS-сообщение. Для получения пройдите по ссылке...». При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств с вашего счета.

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 счета 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. Существует множество вариантов таких мошенничеств. Будьте бдительны!

**Выигрыш в лотерее**

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

Карточки экспресс-оплаты упростили процедуру зачисления денежных средств на счет, но одновременно и открыли новые возможности для мошенников.

Как это организовано? На ваш мобильный телефон звонит якобы ведущий популярной радиостанции и поздравляет с крупным выигрышем в лотерее, организованной радиостанцией и оператором мобильной связи. Это может быть телефон, ноутбук или даже автомобиль. Чтобы получить приз, необходимо в течение минуты дозвониться на радиостанцию.

Перезвонившему абоненту сотрудник призового отдела:

- подробно объясняет условия игры;

- просит представиться и назвать год рождения;

- грамотно убеждает в честности акции (никаких взносов, переигровок и т.д.);

- спрашивает, может ли абонент перевести на свой номер денежные средства с карты экспресс-оплаты на определенную сумму (от 300 долларов и выше);

- объясняет, что в течение часа необходимо подготовить карты экспресс-оплаты любого номинала на указанную сумму и еще раз перезвонить для регистрации и присвоения персонального номера победителя;

- сообщает номер, куда надо перезвонить;

- поясняет порядок последующих действий для получения приза: с 10.00 до 20.00 такого-то числа абоненту необходимо с паспортом, мобильным телефоном и присвоенным персональным номером прибыть по указанному адресу для оформления радостного события.

Если по каким-то причинам абонент не сможет в течение часа купить экс- пресс-карту, то все равно должен позвонить для согласования дальнейших действий. Затем мошенник объясняет порядок активации карт:

- 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 чего присваивает ему персональный номер, с которым «победитель» должен ехать за призом.

Но если вы предложите самостоятельно активировать карты на свой номер и приехать с доказательными документами из сотовой компании, то это объявят нарушением правил рекламой акции.

**ПИН-код банковской карты**

Банковская карта – это инструмент для совершения платежа и доступа к наличным средствам на счете, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

Как это организовано? Вам приходит сообщение о том, что ваша банковская карта заблокирована. Предлагается бесплатно позвонить на определенный номер для получения подробной информации. Когда вы звоните по указанному телефону, вам сообщают о том, что на сервере сбой и просят назвать номер карты и ПИН-код для ее перерегистрации.

На самом деле происходит следующее. Чтобы ограбить вас, злоумышленникам нужен лишь номер с вашего счета.

**Как поступать в такой ситуации?** Не торопитесь сообщать реквизиты вашей карты! 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, вам ответят, что никаких сбоев на сервере не происходило, а ваша карта продолжает обслуживаться банком.

В последнее время наблюдается рост числа случаев мошенничества с пластиковыми картами. Вот почему ее владельцам нужно следовать правилам безопасности.

Никогда и никому не сообщайте ПИН-код вашей карты. Лучше всего его запомнить. Нельзя хранить ПИН-код рядом с картой и тем более записывать на нее – в этом случае вы даже не успеете обезопасить свой счет, заблокировав карту после кражи или утери.

Не позволяйте никому использовать вашу пластиковую карту – это все равно, что отдать свой кошелек, не пересчитывая сумму в нем.

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.

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