ПАМЯТКА
ДЛЯ НАСЕЛЕНИЯ

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Основные схемы телефонного мошенничества:

ПРИМЕР:

Вам звонят с незнакомого номера. Мошенник представляется родственником, знакомым или коллегой по работе и взволнованным голосом сообщает, что задержан сотрудниками полиции и обвинён в совершении какого-нибудь преступления: хранение оружия или наркотиков, нанесение телесных повреждений, хулиганство, участие в ДТП.

Далее в разговор вступает второй мошенник и представляется сотрудником правоохранительных органов. Он уверенным голосом сообщает, что совершено преступление и, если Вы хотите помочь, необходимо привезти определенную сумму в оговоренное место и передать какому-либо человеку или перевести на счет с помощью платежного терминала. Как правило, цена вопроса от 1 до 30 тыс. долларов США.

МЕХАНИЗМ:

В организации мошенничества с требованием денежных средств участвуют несколько преступников. Звонящий может находиться в любом месте, в т.ч. в исправительном учреждении.

Набирая заранее подготовленные телефонные номера или даже наугад, мошенник произносит определенные фразы, а далее действует по обстоятельствам.

Нередко гражданин сам случайно подсказывает имя того, о ком он волнуется.

Если Вы поддались на обман и согласились передать денежные средства, звонящий называет адрес, номер счета или куда нужно приехать для передачи. Мошенники, зачастую, предлагают снять недостающую сумму в банке и сопровождают гражданина лично. Они стараются запугать Вас, не дать опомниться, поэтому ведут непрерывный разговор с Вами вплоть до получения денег. После передачи денег Вас сообщают, где можно увидеть своего родственника или знакомого.

ЧТО ДЕЛАТЬ:

Прервать разговор и перезвонить тому, о ком идёт речь. Если его телефон отключён, свяжитесь с коллегами, друзьями или родственниками для уточнения информации.

Беспокойство за близкого человека нередко мешает объективно оценить ситуацию. Помните, что звонок незнакомого человека с требованием передачи денег означает, что с Вами общается мошенник.

Аналогично следует поступать в случае, если Вас информируют о возбуждении уголовного дела в отношении родственника и необходимости

передать деньги должностным лицам правоохранительных органов, готовым урегулировать вопрос.

Если Вы разговариваете, «якобы», с представителем правоохранительного органа, уточните, из какого он подразделения, в дежурной части которого проверьте, действительно ли к ним доставлен родственник и проходит ли позвонивший службу в названном органе.

Ошибочный перевод средств

ПРИМЕР:

Вам приходит SMS-сообщение о поступлении денежных средств на счет, переведенных с помощью услуги «Мобильный перевод» либо с терминала оплат. Сразу после этого поступает звонок или SMS о том, что на Ваш счет ошибочно переведены деньги, которые просят вернуть обратно тем же «Мобильным переводом» либо перевести на «правильный» номер. Вы переводите деньги, после чего такая же сумма списывается с Вашего счёта.

МЕХАНИЗМ:

Чтобы во второй раз списать сумму с Вашего счёта, мошенник 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 Вы переводите деньги по его просьбе, а во второй раз он получает их по правилам возврата средств.

ЧТО ДЕЛАТЬ:

Предложите звонящему использовать для возврата денег чек из терминала.

Если в ответ сообщат о его утрате, скорее всего, с Вами общается мошенник, просьбы которого выполнять не следует.

Сообщение-просьба о помощи

ПРИМЕР:

На мобильный телефон, «якобы», от близкого человека поступает сообщение о необходимости срочного перевода определенной суммы на телефон, причину которого объяснят позже.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Объясните своим близким, что на SMS такого характера реагировать не стоит, для уточнения информации лучше созвониться с «якобы» нуждающимся в переводе денег лицом.

Телефонный номер-грабитель.

ПРИМЕР:

Вам поступает сообщение с просьбой перезвонить на определенный номер мобильного телефона. Например – помощь другу, изменение тарифов связи, проблема с банковской картой. При звонке Вас длительное время держат на связи, но не беседуют, а после отключения, оказывается, что со счёта списана крупная сумма.

МЕХАНИЗМ:

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.

ЧТО ДЕЛАТЬ:

Не звоните на незнакомые номера.

Выигрыш в лотерее

Каждому пользователю мобильного телефона хотя бы раз в жизни поступало уведомление о рекламной акции, выигрыше в лотерею или проведению розыгрыша подарков с участием операторов связи, известных теле-радио каналов. Мошенники часто используют их для прикрытия своей деятельности, поздравляя Вас с выигрышем и предлагая сообщить код карты экспресс-оплаты, которые упростили процедуру зачисления денежных средств на счёт, но одновременно и стали новым способом хищения денежных средств мошенниками.

Вам может поступить звонок от «якобы» представителя сотовой компании, который предложит пополнить счет карточкой экспресс-оплаты, предварительно сообщив оператору личный ПИН-код и перезвонив на определенный номер.

МЕХАНИЗМ:

Мошенники убеждают Вас купить карты экспресс-оплаты на крупную сумму и сообщить код, скрытый на ее оборотной стороне, что позволит присвоить денежные средства, а сообщение о победе призвано ослабить Ваше внимание.

ЧТО ДЕЛАТЬ:

Активировать карточки экспресс-оплаты следует исключительно через специальный короткий номер на ней. Личный код может быть использован только Вами и не подлежит сообщению другим лицам.

ПРИМЕР:

На мобильный телефон в ночное время приходит SMS о том, что Вы стали победителем лотереи и выиграли путешествие, ноутбук или иной приз, а для ознакомления с условиями акции предлагают посетить определенный сайт либо позвонить по одному из указанных телефонных номеров.

Во время разговора мошенники сообщают о том, что надо выполнить небольшие формальности: оплатить изготовление документов или налоги, для чего необходимо перевести на счет своего мобильного телефона указанную сумму, а затем набрать определенную комбинацию цифр для проверки их поступления на счет и получения «кода подтверждения».

МЕХАНИЗМ:

Комбинация цифр, которую Вы набираете, на самом деле является кодом, с помощью которого мошенники получают доступ к перечисленным средствам. Как только код набран, счет обнуляется.

ЧТО ДЕЛАТЬ:

Если Вы не участвовали в лотерее, а узнали об этом, только получив SMS – сообщение - это обман. Не выполняйте поступившие команды.

Телефонные вирусы

ПРИМЕР:

На Ваш телефон приходит информация: «Вам пришло SMS-сообщение. Для получения пройдите по ссылке...». При выполнении данной команды на телефон скачивается вирус и происходит постепенное списание с него денежных средств.

Также возможно, что при заказе какой-либо услуги через «якобы» мобильного оператора или при скачивании мобильного приложения Вам приходит предупреждение: «Вы собираетесь отправить сообщение на короткий номер ..., для подтверждения операции отправьте сообщение с цифрой 1, для отмены с цифрой 0». Если Вы согласитесь, то с телефонного счета будут списаны деньги.

Мошенники используют специальные программы, позволяющие автоматически генерировать тысячи таких сообщений, следствием чего является списание средств с телефонов.

ЧТО ДЕЛАТЬ:

Не звоните по номеру, с которого отправлено SMS-сообщение.

Сообщение от «якобы» оператора связи

ПРИМЕР:

Вам приходит SMS-сообщение «якобы» от сотрудника службы технической поддержки оператора мобильной связи, с предложением, например, о подключении новой эксклюзивной услуги, перерегистрации во избежание отключения связи из-за технического сбоя, защиты от СПАМ-рассылки, для чего предлагается набрать под диктовку код или SMS-сообщение, которое подключит новую услугу.

МЕХАНИЗМ:

Код, который Вам предлагают набрать, является комбинацией для мобильного перевода денег с Вашего счета без последующего предоставления каких-либо услуг.

ЧТО ДЕЛАТЬ:

Обратитесь к своему мобильному оператору для уточнения достоверности предлагаемой в SMS-сообщении услуги. При подозрении на мошенничество оператор заблокирует данного абонента.

МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

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

ПРИМЕР:

Вам приходит SMS-сообщение о том, что Ваша банковская карта заблокирована, а для получения подробной информации необходимо перезвонить на указанный в сообщении номер.

Когда Вы звоните по указанному телефону, Вам сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой и просят сообщить номер карты и ПИН-код для ее перерегистрации.

МЕХАНИЗМ:

Как только Вы сообщите номер карты и код от нее - деньги будут сняты.

ЧТО ДЕЛАТЬ:

Удостоверьтесь в правдивости информации в службе поддержки Вашего банка. Не сообщайте свой ПИН-код никому.

ПРОФИЛАКТИКА МОШЕННИЧЕСТВА С БАНКОВСКИМИ КАРТАМИ:

ПИН-код необходимо запомнить и не хранить его рядом с картой, например, в кошельке, сумке, мобильном телефоне. Так, в случае утраты или хищения карты, Вы успеете обезопасить свой счёт, заблокировав ее.

Если Вам позвонили из какой-либо организации или Вы получили письмо по электронной почте с просьбой сообщить реквизиты карты и ПИН-код по различным причинам, то не спешите ее выполнять. Позвоните в службу поддержки банка и сообщите о данном факте. Не переходите по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники.

Если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям его сотрудника.

Номер телефона службы помощи банка должен быть в списке контактов Вашего мобильного телефона.

При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения или охраной, например, в государственных учреждениях, банках, крупных торговых центрах.

При возможности посещения банка старайтесь не использовать карту в уличных банкоматах.

Обращайте внимание на картоприемник и клавиатуру банкомата. Они не должны быть оборудованы какими-либо дополнительными устройствами.

Все действия с пластиковой картой в ресторанах, кафе, магазинах, супермаркетах и других местах должны происходить в Вашем присутствии.