Памятка

Что нужно знать, чтобы не стать жертвой

телефонного мошенничества

Отвергая нормы морали и права, мошенники стремятся похитить сбережения и ценности граждан, придумывая всё более сложные «схемы» отъема денег.

Сегодня, когда широко используются мобильные телефоны случаи телефонного

мошенничества растут с каждым годом.

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.

Наиболее распространенные схемы телефонного мошенничества:

1. СМС или звонок из банка о блокировке карты.

Вам приходит сообщение о том, что 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, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации, либо дойти до ближайшего банкомата и следуя «подсказкам» оператора самостоятельно разблокировать карту.

Как обезопасить себя. Не торопитесь немедленно выполнять требования лица, представившегося сотрудником банка. Свяжитесь со службой поддержки клиентов самостоятельно. Скорее всего, Вам сообщат, что никаких сбоев и блокировок не происходило.

2. Несчастный случай с родственником.

Мошенник представляется сотрудником полиции (следователем, врачом и т.д.) и сообщает, что Ваш родственник задержан за совершение преступления, попал в ДТП или в больницу и срочно требуются деньги для «решения» вопроса или срочной операции.

Злоумышленник может знать имя и другие данные родственника (узнав их, например, в социальные сети), может даже дать поговорить якобы с пострадавшим.

Мошенник держит взволнованную жертву в напряжении, не дает повесить трубку, чтобы подумать и разобраться в ситуации, строго убеждает, что деньги нужны без промедлений и на улице ждет «курьер» (сообщник мошенника), который готов забрать деньги.

Как обезопасить себя. В случае поступления подобного звонка не поддавайтесь панике, не давайте себя торопить, при возможности свяжитесь с родственником или спросите в каком отделе полиции/больнице он находится, чтобы позвонить туда. Запомните, что срочное требование денег ввиду экстренной ситуации – верный признак мошенника.

Отметьте в телефонной книжке мобильного телефона номера всех родственников, друзей и знакомых; не реагируйте на SMS без подписи и к звонкам с незнакомых номеров.

3. Внезапный выигрыш.

На мобильный телефон абонента звонит якобы представитель оператора связи, сотрудник банка или любой компании и поздравляет с крупным выигрышем (деньги, автомобиль, квартира) в розыгрыше, организованном среди клиентов, а также сообщает

номер «отдела выдачи призов».

Перезвонившему абоненту отвечает «сотрудник» отдела и подробно объясняет условия розыгрыша, убеждает в честности акции и сообщает условия получения приза. Разумеется, чтобы получить приз нужно внести немалый залог, который и станет добычей мошенника.

Стоит насторожиться даже если требования «отдела выдачи призов» не выглядят подозрительными, например, просят внести на свою банковскую карту крупную сумму денег, чтобы банк убедился, что у Вас есть деньги для оплаты налога на выигрыш. Возможно злоумышленники давно получили доступ к Вашей карте и лишь ждут появления на ней крупной суммы денег.

Как обезопасить себя. Если Вы узнали о проведении лотереи только в момент «выигрыша», и при этом ранее Вы не заполняли заявку на участие в ней и никак не подтверждали свое участие в розыгрыше, то, вероятнее всего, Вас пытаются обмануть. Оформление документов и участие в таких лотереях никогда не проводится только по телефону и Интернету.

4. Акции оператора сотовой связи.

Вам поступает сообщение об акции, проводимой его мобильным оператором. По

условиям «акции», Вы до конца недели (месяца, года, жизни) получаете возможность осуществлять бесплатные звонки по стране и для этого необходимо всего лишь отослать в службу информационной поддержки (телефоны прилагались в sms-сообщении) коды нескольких карт оплаты. После чего потом выясняется, что оператор рекламных акций не проводил, а карты оплаты пополнили счета мошенников.

Как обезопасить себя. В случае поступления подобного сообщения в первую очередь перезвоните своему мобильному оператору для уточнения правил акции, новых тарифов и условий разблокирования, якобы, заблокированного номера.

5. Компенсация за лекарственные препараты.

Через некоторое время после осуществления Вами заказа по почте лекарственного препарата поступает звонок по телефону и неизвестный (якобы представитель министерства здравоохранения, налоговый инспектор либо сотрудник правоохранительных органов) сообщает, что приобретенный препарат якобы оказался подделкой и покупателю положена компенсация в размере от 150 тысяч рублей и выше. Чтобы получить эти деньги необходимо заплатить подоходный налог с суммы, в связи с чем злоумышленник указывает номер счета, на который необходимо перевести деньги. В результате покупатель лишается крупной суммы денег.

Как обезопасить себя. В случае поступления подобного звонка необходимо прекратить телефонный разговор, после чего позвонить в ту организацию, представителем которой представился мошенник, в целях уточнения информации.

6. Телефонные вирусы.

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 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 счет они снимаются с телефона.

Как обезопасить себя. Не следует звонить по номеру, с которого отправлен SMS – вполне возможно, что в этом случае с Вашего телефона будет автоматически снята крупная сумма.

7. Ошибочный перевод средств.

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

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

Как обезопасить себя. Советуем Вам не поддаваться на обман. Если Вас просят перевести якобы ошибочно переведенную сумму, напомните, что для этого используется чек. Отговорка, что «чек потерян», скорее всего, свидетельствует о том, что с Вами общается мошенник.

Что нужно знать про безопасное использование банковской карты,

чтобы не стать жертвой телефонного мошенничества

- Никогда и никому не сообщайте ПИН-код Вашей карты и пароли из СМС-сообщений от банка. Ни сотрудники банка, ни любой другой организации не вправе требовать их. Относитесь к ПИН-коду и паролю из СМС как к ключам от сейфа с вашими средствами.
- При возникновении каких-либо подозрений в мошенничестве связывайтесь с клиентской поддержкой банка, номер телефона которой сохраните заранее.
- С осторожностью относитесь к предоставлению реквизитов своей банковской карты посторонним лицам (см. изображение ниже).