Пять способов SMS-мошенничества, о которых должен быть предупрежден каждый

3 декабря 1992 года было отправлено первое SMS-сообщение. Это сделало удаленную связь еще удобнее, однако открыло и новую лазейку для мошенников. Рассмотрим пять самых распространенных способов нечестного «отъема» денег с помощью SMS.

1. **«Я ошибся номером и случайно перечислил свои деньги на ваш номер»**
   SMS-сообщением «Мама, срочно положи денег на этот номер, потом все объясню» уже никого не проведешь, теперь мошенники действуют более продуманно. Помогает им в этом интернет-сервис, позволяющий отправлять сообщения от чужого имени: можно «сымитировать» любой номер - хоть банка, хоть мобильного оператора, хоть платежной системы «QIWI». Таким образом, на телефон абонента приходит сообщение якобы от «QIWI» о зачислении денег на счет, а следом вскоре приходит SMS от «рассеянного» незнакомца. Мол, «извините за беспокойство, ошибся цифрой и случайно перечисли свои деньги на ваш счет, не могли бы вы мне их вернуть?» Иногда, вдобавок к этому, обманщик может подавить на жалость, и впечатлительный человек отправляет нужную сумму на номер собеседника. После выясняется, что на счет ничего не приходило, никто номером не ошибался, а операторы платежных систем и банков ничем не могут помочь. Получив такое послание необходимо в первую очередь проверить свой денежный баланс и убедиться, что «нежданные» деньги действительно пришли на ваш счет.
2. **«Ваша банковская карта заблокирована»**
   Еще один вариант «маскировки» под банк: мошенники рассылают SMS с номера, похожего на номер банка, и сообщают о блокировке карты или о задолженности по ней. Клиенту предлагают перезвонить по указанному телефону, после чего оператор фиктивной службы поддержки сообщит, что для разблокирования или погашения задолженности клиенту требуется перевести определенную сумму на определенный счет. Будьте внимательны: проверьте номер, с которого пришло сообщение. Возможно, он не будет стопроцентно совпадать с номером банка. Подобный случай уже был: «Сбербанк» осуществляет SMS-рассылку о состоянии счета с номера 900, а мошенники, рассылающие SMS от имени «Сбербанка» пользовались номерами «СБ900» или «9оо», где «нули» - это буквы «о». Следует насторожиться, если оператор не может внятно объяснить причину блокировки карты, просит назвать конфиденциальные данные. Лучше всего придти в отделение вашего банка и попросить информацию о состоянии вашей карты.
3. **Смишинг**
   Этот термин SMS-мошенничества происходит от слова фишинг (с английского «рыбная ловля») - способ «выуживания» у клиента логинов и паролей в интернете. Смишинг (от «SMS» и «фишинг») преследует те же цели, пользуясь при этом SMS-рассылками. В сообщении абоненту предлагают посетить какой-либо сайт, скачать новое приложение загрузить на мобильное устройство музыку, фильм или игру — для этого, якобы, нужно отправить в ответном SMS-сообщении логин и пароль к платежным ресурсам. На самом деле легальные сервисы, которым можно доверять, никогда не затребуют от вас конфиденциальных данных.
4. **«Убедитесь, что все легально»**
   Есть другой способ вымогать большие деньги за скачивание медиа-файлов или «активацию уже скаченного контента» (программа даже может имитировать процесс скачивания файла на ваше мобильное устройство). Для этого мошенники предлагают отправить SMS-сообщение на предложенный номер. А чтобы развеять сомнения абонента, ему даже предлагают зайти на сайт агрегатора и убедиться в минимальной стоимости этих услуг. При этом они дают ссылку на легальный сайт, где указаны вполне приемлемые расценки для каждого мобильного оператора. Однако внимательный абонент заметит, что номер на сайте агрегатора не соответствует номеру, на который предлагают отправить оплату SMS-мошенники. И отправка сообщения на этот номер снимет с вашего счета гораздо большую сумму, нежели заявлена на официальном сайте. Поэтому стоит обходить стороной ресурсы, где предлагают зарегистрироваться путем отправки SMS, и вообще отправлять сообщения только на те номера, которым вы можете доверять.
5. **«Бесплатные» SMS-рассылки**
   Иногда предложенный вам контент, действительно, может быть бесплатным.... пару дней. Мало кто обращает внимание на мелкий шрифт на сайтах, где указывается, что данная рассылка будет бесплатна лишь пару дней, а потом со счета будут списываться деньги за каждое входящее сообщение. И это еще ничего — тут уж абонент сам не доглядел. А бывали и такие случаи, когда пользователи «подписывались» на SMS-рассылки... просто прочитав сообщение. Открыл SMS и автоматически подписался на какую-то неведомую рассылку, о которой ничего неизвестно: что за условия подписки, как от нее отписаться... Самой лучшей защитой в этом случае является услуга от мобильных операторов, при которой невозможно отправлять платные запросы на короткие номера. А

еще нелишним будет проверять список услуг в личном кабинете на сайте оператора связи: если заметите лишние услуги или непонятные списания со счета, свяжитесь с оператором службы поддержки.

По материалам Интернет – издания «КомсомольскаяПравда»