Осторожно, мошенники!

Как не стать жертвой вредоносных программ и «мобильных хакеров»

Кражи совершаются с использованием сети Интернет, посредством вредоносного программного обеспечения, устанавливаемого на аппараты мобильной связи потерпевшего, при помощи которого третьи лица получают возможность удаленного управления услугой смс-сервиса, например «мобильный банк» и др.

Денежные средства переводятся с расчетного счета банковской карты на лицевые счета абонентских номеров, зарегистрированных на территории других регионов РФ. При этом СМС-сообщения, о произведенных без ведома владельца операциях, могут блокироваться «троянской» программой.

По мнению сотрудников уголовного розыска, самый простой и надежный способ не дать жуликам лишить вас сбережений: не подключать услугу «смс-сервиса» или подключить ее на сим-карту, поместить которую следует в самый простой мобильник – без доступа в интернет.

Особенно внимательными следует быть владельцами мобильных телефонов и планшетов с операционными системами Android и Windows Mobile.

В первую очередь, если на ваш телефон поступают смс-сообщения о снятии денег с банковского счета, необходимо как можно скорее заблокировать карту, позвонив в банк по телефону, указанному на карте!

- при утрате сотового телефона, на который подключен смс-сервис, позволяющий клиенту в режиме онлайн получать информацию о состоянии своего банковского счета, следует незамедлительно обратиться к своему оператору сотовой связи для блокировки SIM-карты, а также в Контактный Центр Банка для приостановки действия данной услуги;

- при смене номера телефона, на который подключена услуга, необходимо обратиться в филиал банка и оформить заявление на отключение услуги; (бывали случаи, когда человек долгое время не пользовался сим-картой, оператор сотовой связи продавал номер другому, после чего сообщения об операциях с банковским счетом старого владельца приходили на телефон нового владельца, открывая тому доступ к чужому счету).

- установите на телефон антивирус и своевременно его обновляйте. К примеру, для платформы Android рекомендованы бесплатные приложения DrWeb for Android Light (доступен для загрузки из Google Play) и Kaspersky Internet Security for Android;

- не реагируйте на сомнительные ММС и СМС-сообщения с незнакомых номеров;
- если вы стали жертвой мошенничества, совершенного «мобильными хакерами», оперативно обращайтесь в полицию по каналу связи «02» («102» с любого мобильного) или в дежурную часть Отдела полиции вашего района.

- Меры безопасности при пользовании интернет-банком:

- При совершении операций через интернет-банк нужно быть предельно внимательными. В первую очередь, необходимо убедиться, что вы находитесь на официальном сайте банка. Если хотя бы одна буква или знак в адресной строке не совпадает, это тревожный сигнал. Скорее всего, вы попали на сайт-клон.

- Злоумышленники могут распространять вирусные программы через различные интернет-ресурсы: от социальных сетей до обычных новостных сайтов. Поэтому при попытке войти в личный кабинет с зараженного компьютера Вы перенаправляетесь на так называемый «фишинговые» сайты, которые внешне практически не отличаются от подлинных сайтов интернет-банков. На поддельном сайте Вас могут попросить ввести идентификаторы и пароли, мобильный телефон и другие персональные данные.

- При входе в интернет-банк, как правило, на ваш мобильный телефон приходит сообщение от банка с одноразовым SMS-паролем, который вы должны подтвердить. Никому не разглашайте одноразовый пароль и ни в коем случае не вводите его, если полученные в SMS-сообщении реквизиты относятся к операции, которую Вы не совершали. Будьте более внимательны при работе с интернет-системами, и тогда мошенники не смогут завладеть Вашими персональными данными.

- Меры безопасности при работе с банкоматами и устройствами самообслуживания

Одним из самых «популярных» способов незаконного обогащения является скимминг, т.е. применение специального оборудования, сканирующего

информацию о пин-кодах банковской карты и личных данных клиента. Обычно списание средств с карты клиента происходит в течение суток после совершения каких-либо операций через банкомат, где скиммеры установили свою «ловушку».

- При проведении операции с вводом ПИН-кода всегда прикрывайте клавиатуру, например, свободной рукой. Это не позволит злоумышленникам увидеть ваш ПИН-код или записать его на видеокамеру.

- Замки доступа по картам в специальные помещения, где устанавливаются банкоматы, не должны требовать ввода ПИН-кода. Если для прохода в помещение от Вас требуется ввести ПИН-код, не делая этого, обратитесь в Банк. Если Вы ранее пытались воспользоваться подобным устройством, рекомендуем Вам срочно заблокировать карту, позвонив по телефонам, указанным на устройстве или на обратной стороне Вашей карты, независимо от того, получили ли Вы доступ к банкомату или нет.

- До проведения операции в банкомате осмотрите его лицевую часть, в частности, поверхность над ПИН-клавиатурой и устройство для приема карты в банкомат. В этих местах не должно находиться прикрепленных посторонних предметов или рекламных буклетов. При обнаружении подозрительных устройств нужно незамедлительно сообщить об этом сотрудникам филиала банка, обслуживающим банкомат, или по телефонам, указанным на устройстве или на обратной стороне Вашей карты. Операцию с использованием карты для получения наличных в банкомате в данном случае не проводить. Возможно, данное устройство было скомпрометировано мошенниками. Если вы все-таки воспользовались таким банкоматом, и только потом заметили что-то подозрительное, в целях безопасности и сохранности собственных средств немедленно заблокируйте имеющуюся у вас карту. Снять денежные средства вы сможете в ближайшем офисе банка при наличии паспорта.

- При приеме и возврате карты банкоматом не толкайте и не выдергивайте карту до окончания ее прерывистого движения в картоприемнике. Неравномерное движение карты является не сбоем, а необходимым средством защиты Вашей карты от компрометации.

В последнее время растет количество держателей пластиковых карт, ставших жертвами краж, в большинстве случаев это результат небрежного хранения конфиденциальной информации самими потерпевшими.

Банковские системы, как и методы работы и технические средства правоохранительных органов, постоянно совершенствуются с учетом актуальных рисков и угроз. Однако любые способы защиты будут бессильны, если граждане не соблюдают элементарных правил безопасности.