Мобильные мошенничества! Очередной способ перечисления денежных средств с банковских карт потерпевших.

В настоящее время все более распространенным способом хищений денежных средств граждан становятся хищения при помощи услуги «Мобильный банк». «Мобильный банк» - это СМС-сервис, позволяющий осуществлять банковские операции, с помощью мобильного телефона.

Наиболее распространенные способы мобильных мошенничеств:

1.Способ «Двойной «Мобильный банк».

Потерпевшим, при заключении договора, указывается абонентский номер, который и подключается к «мобильному банку». По различным причинам многие владельцы пластиковых карт банков перестают в дальнейшем пользоваться абонентскими номерами (потерял, переехал, сменил оператора и т.д.), в связи с чем, оператор сотовой связи через 6 месяцев перевыпускает СИМ-карту с данным абонентским номером и выставляет ее на продажу. Так же возможна утеря СИМ-карты и неотключение ее «мобильного банка».

Новый абонент, приобретая данную СИМ-карту, начинает получать СМС о движении денежных средств по счёту потерпевшего, кроме того он получает возможность управлять денежными средствами лицевого счета, к которому она подключена.

2.Способ «Вредоносные программы».

Способы заражения вредоносным программным обеспечением (ВПО) телефонных аппаратов на операционной системе «Android».

Потерпевший получает СМС-сообщение от контент провайдера, в котором находится ссылка на информационный ресурс, перейдя по которой, абонент закачивает на телефон вредоносное программное обеспечение.

После заражения телефона «вирус» проверяет наличие подключенной услуги «Мобильный банк». Если услуга подключена, то вирус с помощью нее осуществляет перевод денежных средств, с банковской карты протерпевшего, на различные абонентские телефонные номера, электронные платежные системы (Киви-кошелек[1] и др.), либо на лицевой счет абонентского телефонного номера потерпевшего и далее на электронные платежные системы, либо банковские карты преступника. При этом вирус блокирует (не выводит на дисплей телефона, а также удаляет из телефона потерпевшего) информационные СМС - сообщения о проведенных банковских операциях.

Следует пояснить, что данный перечень не исчерпывающий, так как возможны абсолютно иные способы хищений денежных средств, а также в какой то части измененные или скомбинированные из различных способов мошенничеств.

Межмуниципальный отдел МВД России «Сарапульский» напоминает: *если Вы стали жертвой мошенников, незамедлительно обратитесь в полицию по телефонам: 02, 4-83-50. Кроме того, Вам необходимо обратиться в банк для получения информации:*

- с какого номера Вам было отправлено СМС,

- куда были перечислены денежные средства,

-когда были сняты денежные средства, а иногда Вам могут сообщить абонентский номер, на счет которого перечислены денежные средства.

К своему сотовому оператору с запросом о детализации звонков, СМС – сообщений, а также выписки с лицевого счета. Данные документы помогут сотрудникам полиции наиболее эффективно сработать по Вашему обращению.

Инспектор направления по связям со СМИ