

В ОМВД России по г. Мегиону обратилась горожанка, сообщившая, что стала жертвой телефонных мошенников.



Она объяснила, что получила смс-сообщение с текстом «я тебя люблю» и просьбой пройти по ссылке для дальнейшего просмотра картинки. Женщина решила, что признание прислал её муж, находившийся в то время на работе. Ничего не подозревая, прошла по указанной ссылке и осталась без денег на банковской карте. Выяснилось, что у пострадавшей была подключена услуга «мобильный банк», «привязанная» к номеру телефона.

Несколькими днями раньше от телефонных мошенников пострадала ещё одна горожанка. Она через Интернет покупала билеты, а рассчитывалась со своего банковского счета. В результате: ни билетов, ни денег.

В первом случае на счёт мошенников отправилось 20 тысяч рублей, во втором – около 60 тысяч рублей.

В настоящее время полицейские устанавливают личности злоумышленников.

– Этот способ мошенничеств становится в последнее время самым распространенным. Хищения денег с банковских карт происходит через заражение мобильных телефонов вирусом, – рассказывает оперуполномоченный уголовного розыска Станислав Дмитриев. – Вредоносная программа действует на операционную систему при наличии подключенной услуги «Мобильный банк». Вирус считывает информацию о карте, просчитывает пин-коды. Сначала мошенники переводят их на сим-карты, потом на банковские карты, электронные кошельки и дальше. Проследить за ходом денежных

потоков и обналичиванием средств, сложно.

Вот несколько советов от сотрудников полиции и работников банков, которые обезопасят ваш телефон и банковскую карту от мошенников:

- не загружать в смартфон приложения от неизвестных разработчиков;
- не открывать сообщение с незнакомых номеров телефонов и не переходить по ссылкам в СМС;
- использовать лицензионное антивирусное программное обеспечение, не включать в настройках смартфона режим «разработчика» (он дает свободный доступ к сотовому телефону);
- в смартфонах не должна отсутствовать галочка в пункте «меню/настройки/безопасность/неизвестный источник»; все скачанные приложения и обновления для них проверять через систему «антивирус»;
- не отключать защитные механизмы телефона, заложенные производителем;
- отключить опцию «быстрый платеж», все платежные операции с карты осуществлять только с подтверждением смс-сообщения;
- пользоваться услугой «Мобильный банк» через персональный компьютер;
- не оставлять телефон без присмотра третьим лицам.

Если с вашей банковской карты незаконно списали деньги, нужно обязательно обратиться в полицию.

В случае, если с карты сняли деньги, можно обратиться к техническим специалистам банка. Написать заявление, изложить суть произошедшего. Технический специалист сделает запрос в главный центр процессинга банка с просьбой приостановить следующие транзакции, так как они несанкционированные и приложить выписку. Как только транзакции приостановят, мошенники не смогут вывести деньги и в течение трёх месяцев они разблокируются и вернуться к вам на карту.