

КАК ОБЕЗОПАСИТЬ СЕБЯ ОТ ЗЛОУМЫШЛЕННИКОВ?

1. не разглашать конфиденциальную информацию (персональные данные, реквизиты платежной карточки, ПИН-код, логин и пароль в Интернет-банк / VTB mBank, динамический пароль на проведение операций и т.п.) третьим лицам, в том числе работникам банка (именно таковыми представляются мошенники);

2. не переходить по ссылкам на незнакомые ресурсы, не открывать вложения в подозрительных сообщениях в социальных сетях, в электронной почте, использовать только проверенные браузеры и сайты, убедиться в правильности адресов интернет-сайтов (мошенники могут создавать сайты популярных компаний);

3. в Интернет-банк / VTB mBank:

- использовать установление минимальных лимитов на операции (наличные и безналичные), изменение лимитов осуществляется мгновенно;

- осуществлять настройку входа VTB mBank только с «доверенных» устройств (меню «Мои устройства» -> «Вход только с доверенных устройств»);

4. использовать услугу «SMS-информирование», а также сервис дополнительной аутентификации держателя карточки 3D-Secure для обеспечения безопасного проведения операций в сети Интернет;

5. при подозрении о факте либо попытках мошенничества незамедлительно блокировать карточку любым доступным способом (в Интернет-банке / VTB mBank, посредством USSD или звонка в банк), сообщать о данном факте в банк и правоохранительные органы;

6. оформлять отдельную платежную карточку для on-line покупок, зачисляя накануне сумму денежных средств, необходимую для совершения покупок.

7. устанавливать и регулярно обновлять антивирусное программное обеспечение.

АКТУАЛЬНЫЕ ПРИМЕРЫ

1. Звонок клиенту по телефону или в Viber от имени «работника банка» с предложением сообщить данные, необходимые злоумышленнику для совершения мошеннических переводов денежных средств со счетов клиента, под предлогом отмены «мошеннической» операции или отмены заявки на кредит.
2. Направление клиенту через социальные сети или мессенджеры ссылок для «получения предоплаты» за выставленный ею на площадках для on-line торговли товар.