Противодействие IT-преступлениям. Полиция предупреждает

В настоящее время все сферы жизнедеятельности государства, общества и человека напрямую связаны с процессами информатизации и цифровизации.

IT-технологии значительно ускорили и упростили гражданам процессы совершения финансовых операций. Вместе с тем, открылись и новые возможности для осуществления противоправной деятельности, способы совершения преступлений с использованием IT-технологий становятся все изощрённее. Мошенники оказывают психологическое воздействие на человека таким образом, чтобы он раскрыл личные или финансовые данные, перевел им деньги или даже взял кредит для последующей передачи средств в чужие руки. Они могут неоднократно звонить жертве, в том числе используя технологию подмены телефонных номеров, направлять электронные письма и сообщения со ссылкой на поддельные (фишинговые) сайты как финансовых организаций, так и любых других компаний и маркетплейсов. Злоумышленники всячески пытаются вывести человека из спокойного состояния и отключить у него логическое мышление.

Для этого они могут запугивать, торопить и оказывать давление или, напротив, стараться заинтересовать и обрадовать внезапной выгодой. Схемы мошенников часто выглядят очень правдоподобно, так как они используют самые обсуждаемые новости или события.

Как себя обезопасить?

- перед снятием денег в банкомате убедитесь, что на картоприемнике нет посторонних предметов, клавиатура не шатается;
- набирая ПИН-код, всегда прикрывайте клавиатуру;
- подключите мобильный банк и СМС-уведомления;
- для работы с банковскими картами, банковскими приложениями используйте отдельное мобильное устройство, не предназначенное для разговоров и «серфинга» в сети Интернет;
- не указывайте номера мобильных устройств, используемых для работы с банковскими картами и дистанционного управления банковским счетом, как контактных в сети Интернет, в объявлениях и на страницах социальных сетей;
- установите на мобильное устройство и компьютер лицензионное антивирусное программное обеспечение из официальных источников;
- не храните данные банковских карт на компьютере или в смартфоне;
- ограничьте круг операций, установите лимит, который можно переводить с помощью мобильного устройства;
- совершая покупки через интернет, никому не сообщайте секретный код для подтверждения операций, который приходит по СМС;
- не переходите по неизвестным ссылкам, не перезванивайте по неизвестным номерам, всегда сверяйте адреса с доменными именами официальных сайтов организаций.

Если вам говорят, будто вы что-то выиграли или с вашей карты случайно списали деньги и нужно назвать свои данные, чтобы остановить операцию, закончите разговор и перезвоните в банк по номеру телефона, указанному на обратной стороне вашей карты. Если пришло СМС (похожее на банковское оповещение) о зачислении средств, а затем звонит человек, который по ошибке зачислил вам деньги и просит их вернуть, закажите выписку в онлайн-банке или позвоните в банк, чтобы проверить состояние вашего счета, прежде чем переводить кому-то деньги. Никому не сообщайте персональные данные, пароли и коды, сотрудники банка их никогда не запрашивают.

Если вам сообщают, что у родственников или друзей неприятности, постарайтесь связаться с ними напрямую.

Если в отношении вас совершили мошеннические действия, сообщите о мошеннической операции в банк, заблокируйте карту. Это можно сделать с помощью банковского приложения или позвонив на горячую линию банка. В тот же день, когда вы получили уведомление о незаконной операции, обратитесь в отделение банка, чтобы опротестовать ее. Запросите выписку по счету и напишите заявление о несогласии с операцией, которую вы не совершали. Обратитесь с заявлением в полицию.