Профилактика преступлений в сфере высоких технологий

В настоящее время большую популярность среди мошенников имеет обман пользователей, продающих свои вещи на популярных в сети Интернет-ресурсах. Чтобы не стать жертвой мошенников и сохранить свои деньги, следует запомнить основные правила безопасности:

1. По возможности ведите переписку с потенциальным покупателем в личных сообщениях платформы, на которой продаёте вещи. Сотрудники электронных досок объявлений делают всё возможное, чтобы оградить вас от мошенников.

2. Если вам написали в мессенджере (Viber, Telegram, WhatsApp) с целью покупки продаваемой вами вещи, посмотрите, какой номер привязан к аккаунту собеседника. Если номер иностранный (начинается с префикса, отличного от +375), стоит воздержаться от диалога. В большинстве случаев с иностранных абонентских номеров пишут мошенники с целью сохранения анонимности.

3. Если же вам написали с аккаунта, привязанного к белорусскому абонентскому номеру, перезвоните на этот номер по обычной телефонной связи (не через мессенджер). Это обезопасит вас от мошенников, которые используют «взломанные» аккаунты. Вас должно насторожить, когда продавец или покупатель под любым предлогом пытается избежать личного общения по телефону. Если же при звонке собеседник скажет, что покупкой не интересовался, немедленно прекратите диалог с мошенниками.

4. Не переходите по ссылкам, которые вам отправляет собеседник, особенно если собеседник их присылает якобы для получения вами денежных средств. Обычно такие сайты создаются злоумышленниками для кражи ваших денег, при этом могут быть схожи по внешнему виду с досками объявлений, почты или интернет-банкинга вашего банка. Если вы всё же перешли по ссылке, ни

при каких обстоятельствах не вводите на сайте реквизиты банковской карты, логин и пароль интернет-банкинга, а также коды, поступающие вам в смс-сообщениях.

Помните, что трёхзначный код (CVC2/CVV2), расположенный на обороте карты, даёт возможность проводить операции с использованием вашей карты! Для перевода средств на вашу карту данный код никогда не требуется. Если у вас просят указать трехзначный код под предлогом того, что эти сведения запрашивает банк, это говорит о том, что с вами общается мошенник.

5. Никому не передавайте коды, поступающие в смс-сообщениях от банка. Для перевода денежных средств на вашу карту каких-либо подтверждений не требуется. Коды из данных сообщений могут быть необходимы лишь для подтверждения списания денег с вашей карты либо для входа в интернет-банкинг с целью последующего их списания.

Если вы стали жертвой мошенников или же свидетелем преступления, просьба обратиться районное управление внутренних дел по территориальности либо сообщить об этом по номеру 102.

Рекомендации от правоохранителей:

Не сообщайте кому бы то ни было паспортные данные, реквизиты банковской карты, пароли, коды доступа, CVV-код. Сотрудника банка обладают всеми необходимыми данными о клиенте и не станут спрашивать их у вас во время телефонного разговора;

Сотрудники банка не станут сверять с вами информацию о банковской карте, ее номере или CVV-коде, а также не будут предлагать вам разрешить какие-либо вопросы с картой без вашего личного посещения банковского учреждения.

В случае, если злоумышленнику удалось получить реквизиты карты или вами был установлен факт хищения денежных средств, следует незамедлительно заблокировать карточку и обратиться с заявлением к правоохранителям.

Помните, что только ваша осторожность и соблюдение простых правил поможет уберечь вас от злоумышленников!

Источник: minsk.mvd.gov.by/ru/news/4065