

Памятка «Как не стать жертвой дистанционного мошенничества»

В период активного использования социальных сетей и мессенджеров дистанционное мошенничество вышло на новый уровень. Сеть Интернет, являясь крупнейшим средством обмена информацией, в то же время порождает стремительный рост преступлений, связанных с использованием информационных технологий. Кроме того, телефонное мошенничество остаётся на прежнем уровне, совершенствуются лишь его схемы.

Для интернет-мошенничества и мошенничества с использованием социальных-сетей и мессенджеров типичны следующие ситуации:

Мошенники, под видом продавца товара, просят оплатить 100% стоимости товара посредством перевода на банковскую карту, но впоследствии покупатель товар не получает;

Мошенники, под видом покупателей, просят предоставить реквизиты банковских карт и смс- коды под предлогом перечисления денежных средств за товар, после чего похищают денежные средства с банковских счетов продавца;

Мошенники, посредством доступа к чужому аккаунту в социальных сетях, под видом родственников или друзей просят перевести денежные средства или сообщить данные банковских карт и смс-кодов, после чего списывают денежные средства с банковских счетов.

Признаки мошенничества со стороны продавца при покупках в Интернете:

Отсутствует адрес и телефон, все общение предлагается вести через электронную почту или программы обмена мгновенными сообщениями.

Отсутствует реальное имя продавца, человек использует псевдоним.

Продавец зарегистрирован на сервисе недавно, объявление о продаже - единственное его сообщение.

Объявление опубликовано с ошибками, составлено небрежно, без знаков препинания, заглавными буквами и т. д.

Отсутствует фото товара, либо же приложен снимок из Интернета (это можно определить, используя сервисы поиска дубликатов картинок).

Слишком низкая цена товара в сравнении с аналогами у других продавцов.

Продавец требует полную или частичную предоплату (например, в качестве гарантии, что вы пойдете получать товар на почте с оплатой наложенным платежом).

Продавец принимает оплату только на анонимные реквизиты: электронные кошельки, пополнение мобильного телефона или на имя другого человека (родственника, друга и т. д.).

Признаки мошенничества со стороны покупателя при продажах в Интернете:

Покупатель не особо интересуется товаром, быстро демонстрирует свое желание сделать покупку и переходит к разговору о способе оплаты.

Покупатель просит вас назвать полные реквизиты карты, включая фамилию-имя латиницей, срок действия и CVC-код. При помощи этих данных он сам легко сможет расплатиться вашей картой в Интернете.

Покупатель просит вас сообщить ему различные коды, которые придут к вам на мобильный телефон, якобы необходимые ему для совершения платежа.

Как не стать жертвой интернет - мошенничества:

Следует внимательно изучить информацию интернет-сайта, отзывы, сравнить цены за интересующий товар. Отсутствие информации, запутанная система получения товара зачастую являются признаками мошенничества;

Получить максимум сведений о продавце или магазине: адреса, телефоны, историю в социальных сетях, наличие службы доставки и т. п. Действующие легально интернет-магазины или розничные продавцы размещают полную информацию и работают по принципу «оплата товара после доставки»;

Нельзя сообщать (посылать по электронной почте) информацию о своих пластиковых картах. Преступники могут воспользоваться их реквизитами и произвести, например, различные покупки.

Зачастую телефонные мошенники используют следующие схемы:

Мошенники, под видом сотрудников банков России, сообщают о несанкционированных списаниях денежных средств с банковских карт или сообщают о необходимости блокировки банковской карты. Просят предоставить смс-коды или скачать мобильное приложение, после чего происходит списание денежных средств с банковских счетов;

Мошенники, посредством смс-сообщений или телефонных звонков, сообщают, что родственник/друг попал в беду и просят перевести денежные средства с целью оказания им помощи. А также мошенники, путём искажения голоса или создания помех при разговоре, под видом родственника/друга просят перечислить денежные средства для решения сложной жизненной ситуации (ДТП, лечение от COVID-19);

Мошенники, звонят в организации и, представляясь директором/ начальником/руководителем, просят перечислить или передать денежные средства с целью решения рабочих вопросов.

Как не стать жертвой телефонного мошенничества:

При телефонном звонке от имени якобы родственников и сообщении о трудной ситуации следует дозвониться до родных и близких, о которых идет речь, выяснить подробности случившегося, а не переводить и не отдавать деньги незнакомым людям;

Перезвонить (а лучше всего подойти) в любое отделение банка, от имени которого пришло сообщение о проблемах обслуживания по расчетному счету/карте, и решить все возникшие вопросы. Можно также позвонить своим близким, которые хорошо разбираются в современных технологиях, рассказать о поступившем сообщении и спросить совета. Следует запомнить: ни один банк не будет просить владельца карты совершать какие-либо действия по телефону или сообщать реквизиты карты;

Не сообщать незнакомым людям (как при личном контакте, так и по телефону или интернет- переписке) данные о себе, своих близких, родственниках, банковских картах, то есть любую конфиденциальную (личную) информацию;

Не осуществлять предоплату за товар или обещанную выплату (услугу), производить оплату только при их фактическом получении.