

Уважаемые жители Сахалинской области!

Обращаем Ваше внимание на значительный рост количества преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Сеть Интернет, являясь крупнейшим средством обмена информацией, в то же время порождает возможность осуществления противоправных деяний, связанных с использованием информационных технологий.

Наиболее распространенными способами хищений с использованием информационных технологий являются:

- **незаконное использование третьими лицами данных банковских карт,**
- **двойное списание денежных средств с банковских карт под предлогом ошибки,**
- **хищение при бесконтактной оплате,**
- **хищение с использованием дубликата сим-карты мобильного телефона,**
- **хищения, связанные с обманом доверчивых граждан, которые сами передают информацию о банковских картах либо сами переводят денежные средства малознакомым людям, производят оплату в сети Интернет.**

Признаки мошенничества со стороны покупателя **Признаки мошенничества со стороны продавца**

- покупатель не особо интересуется товаром, демонстрирует свое желание сделать покупку и переходит к разговору о способе оплаты;

- покупатель просит 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 сообщить ему различные коды, ошибками, составлено небрежно, без

- отсутствует адрес и телефон, все общение предлагается вести через электронную почту или программы обмена мгновенными сообщениями;

- отсутствует реальное имя продавца, человек прячется за «ником»;

- продавец зарегистрирован на сервисе недавно, объявление о продаже – единственное его сообщение;

- объявление опубликовано с ошибками, составлено небрежно, без

которые придут к вам на мобильный телефон, якобы необходимые ему для совершения платежа.

знаков препинания, заглавными буквами и т. д.;

- отсутствует фото товара, либо же приложен снимок из Интернета (это можно определить, используя сервисы поиска дубликатов картинок);

- 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.).

Как не стать жертвами мошенничеств сети Интернет:

– при поступлении сообщения на телефон либо в социальной сети от имени родственников и знакомых 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 или 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.

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. д. 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.

Уважаемые граждане, будьте осторожны и бдительны! Если все же было совершено мошенничество, следует незамедлительно обратиться в органы полиции, сообщив обстоятельства произошедшего и предоставив, имеющиеся документы (расчетные чеки, распечатки звонков и т. п.).