## Прокурор разъясняет

С развитием технологий значительно возросла доля различных проявлений хищений в телекоммуникационной среде, совершаемых посредством телефонных звонков и в сети «Интернет».

Так, покупки в интернете в последние годы приобрели значительную популярность и получили доверие со стороны граждан, чем и пользуются мошенники, при этом создать интернет-магазин и наполнить его фотографиями товаров, которые якобы есть у продавца в наличии - дело нескольких минут. После того как деньги за товар будут отправлены (как предоплатой, так и наложенным платежом), сотрудники магазина перестанут выходить на связь, либо будут придумывать отговорки, а потом магазин бесследно исчезнет.

Вскоре после прекращения работы сайт может возродится по другому адресу, с другим дизайном и под другим названием, ожидая очередных доверчивых клиентов.

Никогда не совершайте покупки в непроверенных интернет-магазинах. Уточните юридический адрес организации и проверьте существует ли такая организация в действительности, позвоните чтобы убедиться в том, что это действительно интернет-магазин.

Один из популярных способов мошенничества, основанный на доверии, связан с размещением объявлений о продаже товаров на электронных досках объявлений и интернет-аукционах. Мошенники также привлекают своих жертв заниженными ценами (например, ввиду срочности продажи). Как и с подозрительными интернет-магазинами будьте аккуратней, не сообщайте реквизиты своей карты посторонним лицам.

Популярным способом хищений являются кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации – создание сайтов-двойников. Внешне такие сайты не отличаются от оригинальных, разница как правило лишь в одной букве адреса.

Если невнимательный пользователь не заметит разницы и введет свои данные на таком сайте, то эти сведения окажутся в руках злоумышленника.

Обращайте внимание на правильность написания адреса сайта, а также же на показатели безопасности сайта, такие как значок закрытого замка в адресной строке браузера и наличие буквы «s» (обозначает «secure» – безопасный), «https://» в начале адреса сайта. Если эти элементы отсутствуют – на такой странице небезопасно вводить данные, особенно реквизиты банковских карт.

Также участились случаи краж денежных средств с банковских карт.

Злоумышленники, используя базы данных сотовых операторов, звонят на мобильные телефоны, представляясь работниками различных организаций. В процессе разговора преступники предлагают открыть более выгодные вклады, сообщают, что банковская карта заблокирована и необходимо перевести денежные средства на другой счет и дают инструкции как это сделать через банкомат или путем сообщения им кодов поступающих через

смс-сообщения. В реальности же деньги переводятся на счета злоумышленников, а номера телефонов, с которых они звонили, становятся недоступны.

Для противодействия указанным противоправным действиям необходимо соблюдать следующие правила:

- не сообщать данные о вашей карте неизвестным или малознакомым лицам;

- в случае получения сообщения о блокировки вашей банковской карты звонить по номеру технической поддержки банка, который указан на самой карте;

- никому не сообщать пароли, на списание денежных средств, поступившие в виде смс-сообщений. Только мошенники запрашивают пароли;

- не хранить сведения о пин-коде к банковской карте вместе с ней или в открытом доступе;

- никому не сообщать cvv-код указанный на обратной стороне банковской карты;