**Как обезопасить себя в кибер-среде?**

Граждане получают государственные услуги через удаленные сервисы, осуществляют покупки посредством сети Интернет, переходят на дистанционный формат работы, во многих сферах делопроизводство осуществляется в электронном виде, люди уже давно используют чаще электронные деньги, чем наличные.

Появление новых информационных технологий с одной стороны свидетельствуют о развитии, с другой стороны не всегда существуют правовые механизмы, позволяющие в полной мере защищать права граждан, которые используют данные технологии.

Кражи персональных данных, кражи денежных средств с банковских счетов и карт, мошенничество – также связаны с развитием информационных и телекоммуникационных технологий.

Выявляются новые способы и схемы мошенничества, которые не требуют особой квалификации или вложения средств.

Так, например, мошенники в последнее время стали использовать новую схему. Поступает звонок от якобы сотрудника банка, который предлагает перевести деньги на защитный счет, чтобы их сохранить. Естественно, после перевода гражданин понимает, что этот защитный счёт – является мифическим, а свои деньги он перевёл на счёт мошенников.

При осуществлении розничной торговли в режиме онлайн следует обращать внимание на цену товара, если она существенно ниже рыночной – это повод задуматься, а не скупать целую партию.

Низкая цена на товар, отсутствие фактического адреса или телефона продавца должны насторожить покупателя. Мошенники в последующем присылают поддельный или некачественный товар, а иногда деньги покупателя просто присваиваются, а товар не доставляется.

При каждой оплате товаров или услуг с помощью электронных средств платежа необходимо помнить следующие правила:

- не использовать подозрительные Интернет-сайты,

- подключить Интернет-банк и СМС-оповещение,

- не сообщать данные своей карты другим людям, в том числе банковским служащим, работникам интернет-магазинов,

- открыть отдельную карту, на которой хранить определенную сумму денежных средств для осуществления безналичных платежей,

- сохранять бдительность, использовать сложные и разные пароли.

За мошенничество с использованием электронных средств платежа предусмотрена уголовная ответственность по статье 159.3 Уголовного кодекса РФ. Также предусмотрена уголовная ответственность за мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей (статья 159.6 Уголовного кодекса РФ).

В зависимости от тяжести совершенного преступления Уголовным кодексом Российской Федерации за преступления, связанные с указанными видами мошеннических действий, предусмотрено наказание в виде штрафа, обязательных, исправительных и принудительных работ, либо лишения свободы до 10 лет.