

## **Компьютерная гигиена или как обезопасить себя в информационный век**

Переход на дистанционный формат работы, получение государственных услуг через удаленные сервисы и появление новых информационных технологий с одной стороны свидетельствуют о развитии, с другой стороны вместе с развитием должны быть предоставлены правовые механизмы защиты прав граждан, которые используют данные технологии.

Рост числа атак на клиентов банков, частые звонки мошенников связаны в том числе с развитием информационных и телекоммуникационных технологий. Все больше потребителей совершают покупки онлайн, расплачиваются картой и меньше пользуются банкоматом. При этом появляются новые и работающие схемы мошенничества, которые не требуют особой квалификации или вложений средств. Например, распространенный способ — звонки от якобы сотрудников банка с просьбой перевести деньги на защитный счет, чтобы их сохранить. В настоящее время увеличивается розничная торговля в режиме онлайн. Отличительная черта этого вида мошенничества — низкая цена на определенный товар и отсутствие фактического адреса или телефона продавца. В этом случае предлагается подделка, некачественный товар либо деньги покупателей просто присваиваются, а товар не доставляется.

Чтобы не стать жертвой мошенников необходимо соблюдать правила цифровой или компьютерной гигиены, сохранять бдительность, использовать сложные и разные пароли.

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, при возможности открыть отдельную карту, на которой хранить определенную сумму денежных средств для осуществления безналичных платежей.

Основная задача граждан при принятии решения о приобретении товара через Интернет-магазин, поступлении посредством сотовой связи просьбы об оказании помощи в связи с непредвиденными обстоятельствами, сложившимися с их родственниками, быть осмотрительными и проверить доступным способом поступающую информацию, прежде чем перечислять денежные средства в адрес злоумышленников.

За мошенничество с использованием электронных средств предусмотрена уголовная ответственность. Так, уголовная ответственность предусмотрена по статье 159.3 Уголовного кодекса за мошенничество с использованием электронных средств платежа. Электронное средство платежа согласно Федеральному закону от 27.06.2011 № 161-ФЗ «О национальной платежной системе» признается средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверить и передавать распоряжения в целях осуществления перевода денежных средств

в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

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 лишением свободы до шести лет.