Следственное управление СК России по Карачаево-Черкесской Республике информирует, как обезопасить себя в век информационных технологий

В связи с переходом на дистанционный формат работы, получение государственных услуг через удаленные сервисы и появление новых информационных технологий следственное управление Следственного комитета Российской Федерации по Карачаево-Черкесской Республике информирует как себя обезопасить от мошенников.

С одной стороны, электронный формат свидетельствуют о развитии информационно-телекоммуникационных технологий, с другой стороны -вместе с развитием должны быть предоставлены правовые механизмы защиты прав граждан, которые их используют.

Необходимо помнить, что главный метод защиты от телефонного и кибермошенничества - повышение финансовой и цифровой грамотности россиян.

Рост числа атак на клиентов банков и 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 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. Таким образом, оказывается психологическое воздействие на слабости человека, направленное на то, чтобы склонить его к действию, которое он не собирался делать. В том числе к разглашению конфиденциальной информации. Большинство звонков от злоумышленников происходит с использованием технологии подмены номера, чтобы скрыть их реальное местоположение. Поэтому жертва даже не догадывается, что общается с преступниками.

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 оказания 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, по статье 159.3 Уголовного кодекса Российской Федерации 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, удостоверять 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 Российской Федерации).

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.

26 Мая 2021

Адрес страницы: https://kchr.sledcom.ru/news/item/1573848