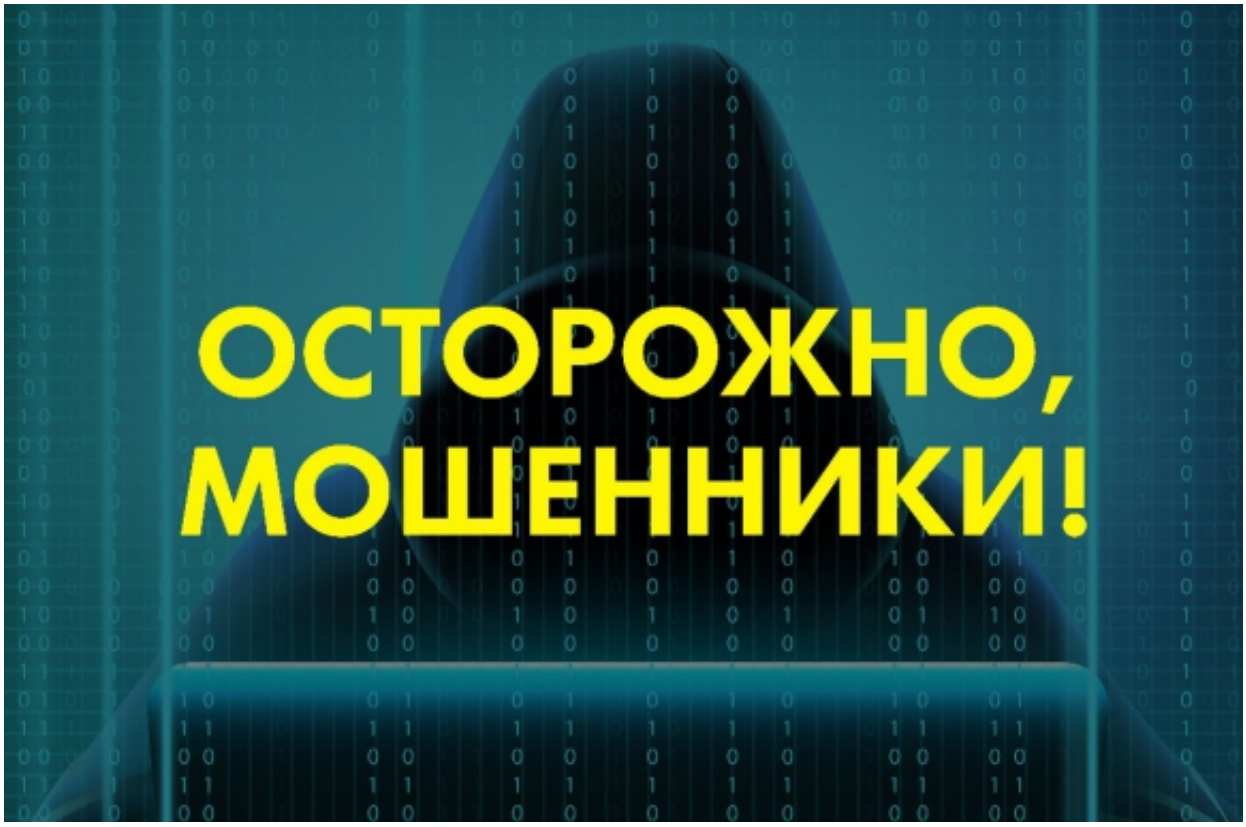
Следственное управление СКР по Ставропольскому краю призывает граждан быть внимательными и соблюдать «цифровую и компьютерную гигиену»



Развитие информационных технологий, получение государственных услуг через удаленные сервисы, возможность совершения банковских и иных финансовых операций в несколько кликов упрощают жизнь граждан. Вместе с тем, всё это требует правовых механизмов защиты прав граждан, которые используют данные технологии.

Современные реалии и анализ судебно-следственной практики говорит о систематическом появлении новых схем мошенничества, которые не требуют особой квалификации или вложений средств.

СРЕДИ РАСПРОСТРАНЕННЫХ СПОСОБОВ ВЫДЕЛЯЮТ:

- звонки от якобы сотрудников банка с просьбой перевести деньги на защитный счет, чтобы их сохранить;

- сообщение о том, что Ваша банковская карта заблокирована - предлагается бесплатно позвонить на определенный номер для получения подробной информации. Когда Вы звоните по указанному телефону, Вам сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации;

- мошенничество при осуществлении розничной торговли в режиме онлайн (имеет место низкая цена на определенный товар, отсутствие фактического адреса или телефона продавца). Предлагается подделка, некачественный товар либо деньги покупателей просто присваиваются, а товар не доставляется;

- сообщение о выигрыше в лотерею - преступник представляется менеджером известной компании и сообщает, что клиент стал победителем розыгрыша. Для получения вознаграждения необходимо срочно выслать реквизиты своей банковской карты.

ПОМНИТЕ, что телефонные мошенники всегда говорят уверенно, имеют хорошо поставленный голос, а на любой вопрос клиента имеют заранее подготовленный ответ.

Чтобы не стать жертвой мошенников НЕОБХОДИМО СОБЛЮДАТЬ ПРАВИЛА цифровой или компьютерной гигиены:

- сохраняете бдительность, используйте сложные и разные пароли;

- не доверяйте личные данные незнакомым лицам, откажитесь от сделки, если имеются сомнения в надежности покупателя (продавца);

- не используйте подозрительные Интернет-сайты;

- подключите Интернет-банк и СМС-оповещение;

- не сообщайте данные своей карты другим людям, в том числе банковским служащим, работникам интернет-магазинов (Помните, ни одна организация, включая банк, не вправе требовать Ваш ПИН-код!);

- не следует звонить по номеру, с которого отправлен SMS – есть вероятность, что в этом случае с Вашего телефона будет автоматически снята сумма денежных средств;

- при возможности откройте отдельную карту, на которой храните определенную сумму денежных средств для осуществления безналичных платежей;

- используйте специальные программы, устанавливаемые на смартфоны, которые определяют организацию, из которой исходит звонок, и предупреждают владельца телефона о нежелательности ответа.

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.

Если деньги были перечислены мошеннику через электронную платежную систему или банк, необходимо незамедлительно обратиться в службу поддержки клиентов этих организаций. Кроме того, подать жалобу на компьютерное мошенничество можно на сайте Роскомнадзора (государственный орган по надзору в сфере информационных технологий).

За мошенничество с использованием электронных средств предусмотрена УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ.

Так, уголовная ответственность предусмотрена по ст. 159.3 УК РФ за мошенничество с использованием электронных средств платежа.

Электронным средством 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 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.

Буклет: предоставлен ГУ МВД России по Ставропольскому краю

Изображения

27 Мая 2021

Адрес страницы: https://stavropol.sledcom.ru/news/item/1574134