Западно-Сибирское следственное управление на транспорте СК России напоминает физическим и юридическим лицам о необходимости повышения уровня правовой и финансовой грамотности, а также «компьютерной гигиены»

Современный человек без информационных сетей и виртуального общения уже не представляет свою жизнь. Практически каждый из нас является частью информационного пространства.

Преступления против жизни и здоровья человека, собственности, государственной власти сегодня совершаются с использованием информационных технологий. Поэтому вопросы профилактики киберпреступности являются ключевыми для правоохранительных органов как Российской Федерации, так всего мира. В таких условиях повышается роль участия каждого пользователя сети Интернет в формировании безопасного информационного пространства. Для этого необходимо соблюдать следующие рекомендации.

- Используйте лицензионное программное обеспечение. В таком случае отсутствует риск заразить компьютер или мобильное устройство при установке неизвестной программы.
- Установите антивирусную программу и файрволлы не только на персональный компьютер, но и на смартфон и планшет.
- Не переходите по ссылкам, содержащимся в спаме и других подозрительных письмах. При работе с электронными почтовыми ящиками необходимо настроить автоматическое блокирование приходящего спама, а также механически сортировать корреспонденцию, своевременно удаляя подозрительные письма без их просмотра.
- Аккаунты в социальных сетях, как и электронные почтовые ящики, периодически подвергаются хакерским атакам, поэтому необходимо минимизировать передачу персональных данных в электронном виде, особенно не указывать логины и пароли мобильного банка, электронных кошельков, номера, пароли и коды банковских карт.
- Используйте сложные пароли, состоящие из комбинаций цифр и букв или иных символов. Воздержитесь от паролей - дат рождения, имен, фамилий, то есть тех, которые легко вычислить либо подобрать.

Также, необходимо обезопасить и ограничить пребывание в сети пользователей, которые не готовы к угрозам безопасности. Как правило, это лица, не имеющие навыков использования информационного пространства – дети и лица пожилого возраста. Установление контролирующих программ и использование конкретных приложений вместо выхода в открытое Интернет-пространство позволят снизить риски заражения компьютера случайным переходом по вирусной ссылке или загрузкой фишинг-страницы.

Кроме того, в наше время 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. 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.

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, 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, 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.

Западно-Сибирское следственное управление на транспорте Следственного комитета Российской Федерации рекомендует гражданам проявлять бдительность, а также соблюдать перечисленные и другие рекомендации по обеспечению безопасной работы в информационной сети Интернет.

24 Мая 2021

Адрес страницы: https://zapsib-sut.sledcom.ru/news/item/1572523