МЧС России рекомендует: правила кибербезопасности

Дополнительный «побочный эффект» COVID-19 — активизация интернет-преступности.

Мошенники легко используют страхи людей во времена неопределенности, недостаточности информации, обещая помощь и предлагая мнимую заботу. Главная цель преступников — ввести человека в состояние аффекта и заставить выполнить действия, направленные на открытие sms-уведомлений, почтовых сообщений, осуществить отправку денежного перевода, сброса пароля от своего аккаунта, что позволит им получить несанкционированный доступ к персональным данным.

Способы воздействия мошенников:

- письма якобы от Всемирной организации здравоохранения или учреждений здравоохранения с ссылками, ведущими на зараженные или поддельные страницы
- организация сбора пожертвований на борьбу с коронавирусом
- предложения о продаже тестов для проверки на коронавирус

Как только пользователь активирует ссылку в сообщении, его перенаправляют на фишинговый сайт и предлагают поделиться личной информацией, которая попадает в руки злоумышленников.

Как не стать жертвой мошенников:

Ни в коем случае не переходите по ссылке! Если сообщение вас заинтересовало, то наберите адрес в браузере самостоятельно.

Проверьте, куда ведет ссылка. Для этого наведите на нее курсор мыши и, если перед вами URL (адрес) из сервиса коротких ссылок (is.gd. Is.gd, bit.ly и т.д.), то удалите письмо. Это мошенники!

ВАЖНО:

Настороженно относитесь к любому письму или сообщению, в котором затронута тема коронавируса.

Немедленно прекращайте любые телефонные разговоры информационного характера с незнакомыми вам людьми.

Реальные сервисы не рассылают писем с просьбами сообщить свои учетные данные, пароль и прочее.

Если вы получили SMS, в котором содержится просьба обновить платежные или прочие реквизиты — удалите его.

Если вы не знаете, что делать в случае получения письма с темой «Банк» или «Финансы», следует позвонить в банк на их официальный телефон.

Будьте бдительны!

Рекомендации подготовлены ФГБУ ВНИИ ГОЧС (ФЦ)