Добрый день!

Эксперты прогнозируют рост числа кибератак на компьютеры, оборудование и незащищенные домашние сети сотрудников компаний, которые из-за коронавируса перешли на удаленный режим работы. В группе риска — все пользователи, работающие удаленно, а целью кибератак станет кража денег или персональных данных.

Актуальные угрозы в период пандемии COVID-19:

1.            Увеличение числа мошеннических бесплатных сервисов: платформ для проведения

видеоконференций, онлайн-обучения, подписок на онлайн-кинотеатры, фейковых мобильных приложений для доставки еды и т.д.

2.            Повышение риска проведения атак с целью шпионажа.

3.            Рост количества целевых атак на сотрудников из финансовой, транспортной  отраслей..

4.            Увеличение мошеннической активности по отношению к людям пожилого возраста: доставка товаров на дом, предложения лекарств и тестов на COVID-19 и другое.

5.            Рост числа инсайдерских атак с использованием тех категорий сотрудников, которым понижают оклад при переходе на удаленный режим работы.

6.            Усиление мошеннической активности в туристической индустрии (центры возврата денежных средств авиалиний, отелей и т.д).

Поэтому настоятельно просим вас соблюдать простые правила:

1.  Обращайте внимание и не переходите на фишинговые сайты

2.  Скачивайте и устанавливайте программное обеспечение только с сайта производителя

3.  Будьте внимательны к получаемой электронной почте, СМС,  сообщениям мессенджеров WhatsApp, Viber или Telegram, не переходите по предложенным ссылкам, не открывайте подозрительные вложения. В качестве отправителей могут быть ваши коллеги, сотрудники банков, государственных органов. Характерными признаками данных писем могут быть необычная форма подачи обращений, орфографические ошибки, подозрительное время отправления(например ночью), требования совершить срочное действие по письму и как один из вариантов развития ситуации -  угрозы судами в случае отсутствия скорейшего ответа. Также могут быть затронуты  и другие обстоятельства, связанные в том числе и не с рабочей деятельностью работника. Если в письме или сообщении к вам обращаются по имени, ФИО, знают вашу должность, место работы или сферу интересов это не значит, что отправитель знаком с вами. Данную информацию можно взять в автоматическом режиме из социальных сетей, либо из других публичных источников. Помните, что любая личная информация, размещаемая вами в сети Интернет, будет со временем общедоступна и может быть использована злоумышленниками для социальной инженерии.

С уважением, Т. Е. Трошкина