Мошенники умнеют…

Бухгалтеры, секретари и специалисты по финансовой, налоговой и другой отчетности регулярно обращаются к Интернету и ищут шаблоны документов. Злоумышленники придумали мошенническую схему, воспользовавшись этим обстоятельством.

Информируем жителей Камчатского края, как она работает:

1. Мошенники создают поддельные сайте государственных ведомств, организаций и известных справочно-правовых систем и выкладывают на них зараженные вирусами документы. При этом хакеры используют метод SEO-poisoning («отправление» поисковой выдачи), который позволяет таким ресурсам занимать одну из первых строчек в предлагаемом списке.
2. Пользователь скачивает документ, после чего на его компьютере запускается программа удаленного доступа. С помощью неё хакеры могут дистанционного менять банковские реквизиты в договорах компаний, например, с подрядчиками или поставщиками. Вместо данных настоящего получателям средств они указывают свои.

3. Как правило, сотрудники компании обнаруживают вирусное программное обеспечение (ПО) не сразу. Иногда мошенники блокируют доступ к рабочим компьютерам, а за его восстановление вымогают деньги.

Обратите внимание на способы защиты:

1. Установите и регулярно обновляйте антивирус.
2. Настройте запрет на автоматическую установку и запуск разных программ.
3. Обращайте внимание на адрес сайта – поддельный может отличаться от официального всего одним символом.
4. Будьте осторожны при работе с сайтами, если в их адресной строке нет значка безопасного соединения (замочек).
5. Скачивая документ, обращайте внимание на него формат. Безопасными считаются pdf, docx, xlsx, jpg, png.

По материалам пресс-службы УМВД России

по Камчатскому краю