Услышал по радио, что с начал года работа 600 сайтов из российской доменной зоны была остановлена Банком России, поскольку он наносили вред нашим финансам. Есть ли уверенность, что эти интернет-воры не возродятся?

Евгений Сучков, г. Тверь

Отвечает заместитель управляющего Отделением Тверь ГУ Банка России по ЦФО Владимир Николаевич Чирков

Действительно, в этом году более 600 сайтов из российской доменной зоны были «пойманы за руку» за нечистоплотное поведение на финансовом рынке. Такой очисткой интернет-пространства занимается, в частности, Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Банка России. Обращаю внимание, что все эти сайты были не заблокированы, а сняты делегирования. В чем разница? В том, что блокировка домена – это если к нему перекрывается доступ пользователей, но права владения сохраняется. Такой домен может быть разблокирован, если причина, по которой он был заблокирован, устранена. При этом домен, например, заблокированный на территории России, может быть доступен в других странах. А вот если сайт снят с делегирования - это лишение владельца домена права собственности на него, права контроля и распоряжения. Такой домен удаляется из реестра зарегистрированных, он «закрыт» в принципе для всего интернета.

Разделегированные домены под тем именем, которыми они вводили в заблуждение доверчивых потребителей финансовых услуг, работать уже не смогут. Но киберпреступность сегодня – это хорошо организованный и очень прибыльный бизнес: по экспертным оценкам в России с 2013 года число киберпреступлений выросло в шесть раз. Поэтому нужно быть очень осмотрительным при выполнении финансовых операций онлайн и защищать персональные данные.

Например, в интернете распространена схема, когда возможно перенаправление на сайт-двойник. Если вы планируете через интернет купить авиабилеты, перевести деньги с карты на карту, совершить покупку в онлайн-магазине, тщательно проверьте адресную строку. Фишинговый сайт визуально может быть очень похож на настоящий, но доменное имя у него иное. Если не будете внимательны – деньги потеряете, а товара и услуги так и не дождетесь.

Хочу дать обладателям всем несколько советов, которые помогут в существенной степени обезопасить от кражи средств. Ни в коем случае не реагируйте на электронные сообщения, в которых вас просят предоставить реквизиты счета, PIN-коды, пароли или персональные данные. Всегда используйте надежные уникальные пароли для максимально возможного количества учетных записей в интернете, а лучше всего – индивидуальный пароль для каждой из них. Не храните логин и пароль на своем смартфоне: в электронном сообщении, в виде заметки или для «автоматического заполнения» при открытии интернет-сайта или приложения. Эта информация станет настоящим Клондайком для мошенников в случае утери или кражи вашего мобильного устройства.