**Кибермошенников «обезвредили»**

Более 600 сайтов российской доменной зоны больше не будут работать в интернет-пространстве из-за недобросовестного поведения на финансовом рынке, сообщают в Центре мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Банка России. Домены мошенников удалены из реестра зарегистрированных и уже не будут доступны для всех интернет-пользователей.

Но киберпреступность сегодня – это хорошо организованный и очень прибыльный бизнес: по экспертным оценкам, в России за последние пять лет число киберпреступлений выросло в шесть раз. Поэтому нужно быть очень осмотрительным при выполнении финансовых операций в сети и защищать персональные данные во всем онлайн-пространстве.

В преддверии праздников активизируются так называемые «социальные инженеры». По оценкам экспертов, в прошлом году мошенники с помощью социальной инженерии похитили с банковских карт россиян около 650 млн рублей, а в 2017 году ущерб может увеличиться до 750 млн рублей. «Задача любого мошенника, использующего методы «социальной инженерии», - войти в доверие к своей жертве и заставить ее выдать личную информацию или проделать какие-то манипуляции, которые позволят им украсть ваши деньги. А длительные новогодние выходные усыпляют бдительность населения, чем мошенники и пользуются», - уточняет и.о. управляющего Отделением Калуга ГУ Банка России по Центральному федеральному округу ВЛАДИМИР РЕПЕТА.

Например, на мобильный телефон может прийти сообщение, что карта заблокирована, а для разблокировки нужно позвонить по указанному в СМС номеру. Стоит перезвонить – и злоумышленник на другом конце провода так вас заговорит, что вынудит сообщить коды и пароли от карты, а то и пойти к банкомату якобы для разблокировки. Результат один – жертва сама переводит деньги мошенникам. Что делать? «Ни в коем случае не звонить по номеру телефона, указанному в СМС, а пользоваться только номером на обратной стороне карты, - советует ВЛАДИМИР РЕПЕТА. - Важно помнить, что представители банка никогда – ни по телефону, ни в переписке – не спрашивают полные данные карт, одноразовые пароли, пин-коды. Для консультации им достаточно имени и четырех последних цифр карты. Будьте бдительны!».