«Социальные инженеры»

По оценкам аналитиков компании Zecurion, 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», – уточняет управляющий Отделением Белгород ГУ Банка России по Центральному федеральному Беленко А.Н..

Например, на мобильный может прийти сообщение, что карта заблокирована, а для разблокировки нужно позвонить по указанному 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 – уж это точно номер банка, а не киберворов.

С помощью социальной инженерии мошенники пытаются узнать реквизиты, достаточные для совершения перевода с карты на карту: номер карты, срок ее действия, CVV-код (три цифры с обратной стороны банковской карты). 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.

Поскольку кибермошенники непрерывно придумывают что-то новенькое, нам с вами следует всегда быть настороже, не забывая про здравый смысл.