В чью пользу банковский счет?

16 копеек – много ли это? С одной стороны, для покупателя это повод сказать «сдачи не надо», а продавцу, к примеру, округлить стоимость товара. С другой стороны, даже такую незначительную, казалось бы, сумму не хочется дарить преступникам. Именно 16 копеек с каждой 1000 рублей смогли похитить кибермошенники со счетов россиян в 2017 году.

Киберпреступность развивается вслед за расширением сферы безналичных расчетов. Ежегодно количество и объем операций с использованием пластиковых карт растут на 25-30 процентов. Но это не значит, что потери увеличиваются пропорционально. В Банке России действует Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ). По данным ФинЦЕРТа, год от года благодаря слаженным действиям множества структур, а еще повышения бдительности самих граждан потери снижаются. В 2015 году они составили 1,150 млрд рублей, в 2016м – 1,08 млрд. В 2017 году преступникам не удалось взять рубеж в миллиард рублей, их незаконная добыча – 961,3 миллиона. И если сейчас показатель 16 копеек на тысячу рублей, то ранее он был почти в два раза выше – 28 копеек. Снижается и средняя сумма одной несанкционированной операции. В прошлом году она составила 3 тысячи рублей, что на 17 процентов меньше, чем годом ранее.

Технические данные или психологический расчёт?

Схемы обмана постоянно обновляются. Раз в три-четыре месяца мошенники меняют направление деятельности, хотя цель остается той же – похищение чужих средств. Основной источник несанкционированных операций – это Интернет. По данным компании InfoWatch, специализирующейся на информационной безопасности, в прошлом году объем утечек информации вырос более чем в четыре раза. 86% украденных данных — личная и финансовая информация, в частности реквизиты пластиковых карт.

Еще одна тенденция последнего времени – персонифицированный подход. Сегодня преступники получают информацию о конкретном человеке, например, через социальные сети. Как зовут кошку, когда родился человек, какой была девичья фамилия матери – все эти данные люди нередко используют в качестве пароля и при этом не стараются их скрыть.

Данные, а вслед за ними и деньги, могут быть похищены, стоит лишь на несколько секунд выпустить карту из рук, к примеру, расплачиваясь в кафе. Злоумышленник может сфотографировать или запомнить нужные сведения (номер, трехзначный код), а затем воспользоваться чужим счетом для оплаты собственных нужд.

По-прежнему часто мошенники используют навыки социальной инженерии. Звонок или СМС-сообщение от родственника, оповещение якобы от банка, предложение получить компенсацию – «легенд» в арсенале преступников немало, и каждая из них, как показывает практика, весьма действенна. Способ защиты здесь один – быть начеку и многократно перепроверять информацию.

Основы самообороны от киберпреступников

В электронные кошельки киберпреступнику залезть так же просто, как карманнику в обычное портмоне. И остановить его может только бдительность. Есть простые, но действенные рекомендации.

Во-первых, никогда не следует сообщать посторонним PIN-код карты. При вводе кода в банкомате или терминале клавиатуру лучше прикрывать рукой, даже если рядом никого нет: современные мошенники не подглядывают из-за плеча, а укрепляют миниатюрную камеру над устройством. Также PIN-код нельзя вводить при оплате покупок через Интернет. Кроме того, каждый может самостоятельно изменить код. Если делать это регулярно, защищенность повышается.

Во-вторых, для оплаты товаров и услуг лучше завести отдельную карту и вносить на нее лишь сумму, необходимую для совершения предстоящей покупки. Касается это и платежей на кассах, и дистанционных. А при оплате в сети интернет всегда стоит перепроверить адрес магазина. Нередко мошенники создают клоны популярных ресурсов, меняя всего один символ. А деньги в этом случае уже пойдут не по назначению, а в карман злоумышленника.

Сегодня в роли кошелька нередко выступает мобильный телефон. Платежные сервисы, мобильный банк – все это создано для удобства пользователя, но порой удобны они и для преступника. Стоит мошеннику заполучить аппарат без пароля, как он получает доступ ко всему счету. «Кроме того, такие приложения могут быть уязвимы для вирусов, - напоминает управляющий Отделения Рязань ГУ Банка России по Центральному федеральному округу Сергей Кузнецов. – Не следует забывать о лицензированном антивирусном программном обеспечении. А вот чего не надо делать, так это открывать или скачивать сомнительные файлы и устанавливать приложения из непроверенных источников».

Что со счета упало, то пропало?

Если получено сообщение о списании средств с карты, но при этом никаких операций держатель карты не совершал, в первую очередь ему необходимо лишить злоумышленника возможности управлять деньгами. Для этого следует связаться с банком, в котором открыт счет, и заблокировать карту. Телефоны горячей линии обычно указаны на самой карте, на официальном сайте банка или в договоре обслуживания. Затем следует написать заявление в правоохранительные органы, а из банка запросить выписку по счету и подать заявление о несогласии с операцией. Если спорная операция была совершена на территории Российской Федерации, такие заявления рассматриваются банком в течение 30 дней. Для международных операций срок рассмотрения 60 дней. На возмещение ущерба можно рассчитывать, если банк не докажет, что держатель карты нарушил условия ее использования, в том числе меры безопасности, и обратился в банк не позднее дня, следующего за днем получения уведомления о совершении операции. Но это не касается проблем с электронным кошельком и прочими неперсонифицированными платежными средствами.

«Остап Бендер знал 400 способов отъема денег у населения. Сегодняшние мошенники мало уступают литературному прототипу, - считает управляющий Отделения Рязань Сергей Кузнецов. - Они крадут пароли, списывают деньги со счета человека без его ведома, обещают огромные проценты по вкладам... И жертвой может стать любой. Банк России старается работать на опережение. Но в первую очередь все зависит от самого человека: окажется он начеку, сможет ли защитить свои сбережения. Если вооружиться знаниями, эту задачу решить под силу каждому».