

Карточным мошенникам ужесточат наказание

Аферистам, ворующим деньги с банковских карт россиян, может грозить серьезное наказание. Правительство РФ поддержало законопроект об усилении уголовной ответственности за мошенничество с банковскими картами. Предлагается внести изменения в Уголовный кодекс, которые усилят ответственность за хищение электронных денежных средств или чужого имущества с банковского счета. Также предусматривается ответственность за мошенничество, совершенное с использованием поддельной или принадлежащей другому лицу платежной карты. Сейчас подобные правонарушения караются штрафом. Согласно предлагаемым изменениям мошенникам может грозить реальный срок.

Как считают эксперты финансового рынка, необходимость в усилении наказания назрела давно. Возможностей у нечистых на руку людей добраться до чужих денег на карточном счете предостаточно – они активно этим пользуются, прибегая к современным техническим уловкам или методам социальной инженерии. К примеру, серьезная опасность для владельцев карт – это вирусы, которые распространяются через ссылки в соцсетях, письма, sms-сообщения. Открыв подозрительную ссылку или скачав ненадежную игру, пользователь может загрузить вирусную программу, которая обеспечит мошенникам доступ к онлайн-банку или мобильному банку. «Задача владельцев карт со своей стороны – знать об уловках преступников и не поддаваться на них. В целях безопасности загружайте только лицензированные продукты и приложения с официальных сайтов, не открывайте письма и ссылки, поступившие с подозрительных адресов. Обязательно следует установить антивирус на свой компьютер и мобильный телефон и периодически его обновлять», – рекомендует и. о. управляющего Отделением по Рязанской области ГУ Банка России по ЦФО Алексей Киреев.

В последнее время кибермошенники стали воровать данные банковских карт с помощью сайтов, которые обещают легкий заработок в Интернете или заманивают граждан «беспроигрышными лотереями». Мошенники, которые используют подобные схемы, любыми способами подводят жертву к тому, что человек якобы должен оплатить некий налог или комиссию. При этом кроме «оплаты» аферисты крадут конфиденциальные данные чужой карты. Как отмечают в компании «Яндекс», на уловки мошенников попадают около 12 тыс. пользователей в сутки – часть из них гарантированно соглашается ввести данные карт в зараженных формах для оплаты налогов или комиссий.

И, конечно, не следует передавать свою банковскую карту посторонним. К сожалению, сотрудник кафе или магазина может под предлогом проведения оплаты в другом помещении скопировать данные вашей карты и расплатиться ею, к примеру, в интернет-магазине. Ни в коем случае не следует записывать PIN-код на карте или держать его в кошельке вместе с картой. Нередки случаи, когда нашедший или похитивший карту человек, имея PIN-код, тут же направляется к банкомату и обчищает счет жертвы до копейки.

Вот реальный случай, произошедший совсем недавно. В одну из рязанских кредитных организаций обратился клиент с жалобой на неправомерное, по его мнению, списание денежных средств с банковской карты. Было установлено, что операции с его картой совершены за пределами Российской Федерации, в то время как сам клиент в это же время находился в России, и карта, по его словам, всегда была при нем. Также выяснилось, что списание средств производилось в иностранной валюте путем проведения нескольких транзакций - за короткий промежуток времени с карты пропало более 100 тысяч рублей. По факту списания денежных средств через кредитную организацию подготовлены запросы в платежную систему на опротестование транзакций. Однако запросы не были удовлетворены: оказалось, что все операции с картой прошли с корректным вводом PIN-кода. А это говорит, что пострадавший не соблюдал правила безопасного использования, в результате чего PIN-код стал известен мошенникам.

Как отметили в Отделении по Рязанской области ГУ Банка России по Центральному федеральному округу, во избежание подобных ситуаций стоит придерживаться следующих простых рекомендаций. Никогда и никому не следует сообщать данные своей карты (ее номер, PIN-код, срок действия, код CVC/CVC2, кодовое слово и т.д.) - даже близким родственникам. И уж тем более не стоит эти данные разглашать с использованием электронных средств связи: они могут легко оказаться в руках мошенников. Также, при использовании карты в банкоматах и терминалах во время ввода PIN-кода следует позаботиться о его сохранности от посторонних взглядов. Не следует применять банковскую карту в терминалах и банкоматах, которые выглядят подозрительно либо имеют признаки неисправности. При совершении операций с картой в сети Интернет следует крайне внимательно подходить к процедуре ввода реквизитов карты на сайтах, дабы не стать жертвой мошенников, использующих сайты-двойники для кражи данных о карте. При использовании мобильных и онлайн-сервисов для управления банковской картой необходимо обеспечить антивирусную защиту устройства, на котором эти сервисы применяются.

«Если вы стали жертвой кибермошенников, немедленно сообщите в банк о происшествии по телефону, а затем и в письменном виде. О факте хищения следует также сообщить в полицию, – поясняет Алексей Киреев. – А для совершения интернет-платежей лучше использовать отдельную карту, на которой в момент оплаты следует иметь ограниченную сумму: так риск «засветить» свой счет и потерять все средства снижается».

Врез:

- *В России объем несанкционированных операций с использованием платежных карт за 2016 год составил 1,08 млрд рублей против 1,15 млрд рублей за 2015 год.*
- *«Яндекс» уже заблокировал около 2 тыс. мошеннических сайтов, предлагающих легкий заработок в сети.*