30 ЦЕНТОВ ЗА КРЕДИТКУ

ОПЛАТА ТОВАРОВ И УСЛУГ ЧЕРЕЗ ИНТЕРНЕТ ПРИ ПОМОЩИ КРЕДИТНЫХ КАРТ НАБИРАЕТ ВСЕ БОЛЬШУЮ ПОПУЛЯРНОСТЬ В МИРЕ. ОДНАКО СТОЛЬ ПРОСТОЙ И УДОБНЫЙ СПОСОБ СТАНОВИТСЯ ВСЕ БОЛЕЕ РИСКОВАННЫМ ИЗ-ЗА КРЕДИТНЫХ МОШЕННИКОВ, ИЛИ КАРДЕРОВ. ИЗОБРЕТАТЕЛЬНЫЕ СХЕМЫ ВНЕДРЕНИЯ ПОДДЕЛОК И БЕСЧИСЛЕННЫЕ УТЕЧКИ ИНФОРМАЦИИ ПРИВЕЛИ К ТОМУ, ЧТО ЗА ПОСЛЕДНИЕ ДВА ГОДА БОЛЕЕ 100 МЛН ЧЕЛОВЕК СТАЛИ ЖЕРТВАМИ ИНТЕРНЕТ-МОШЕННИЧЕСТВА. АРТЕМ КУЛАКОВ

Приобрести информацию о кредитках сегодня может едва ли не любой человек. Для этого вполне достаточно сделать запрос в интернет-поисковике «купить номера кредитных карт». Мошенники даже не пытаются себя законспирировать — первые же ссылки выводят на искомые ресурсы. И как можно убедиться, стоит это совсем смешных денег.

«Зачем тратить свои кровные, если за ваши покупки сможет расплатиться рядовой американец, который сидит себе в „Макдональдсе", спокойно пережевывает бигмак и не знает, что деньги с его кредитки утекают... А все потому, что он однажды имел неосторожность расплатиться своей карточкой в on-line-магазине или в одном из многочисленных порносайтов, которые он посещал». Такую аннотацию можно прочитать на сайте *http://mccrack.narod.ru/* — одном из многочисленных ресурсов, торгующих номерами кредитных карт. Далее идут расценки. Полная информация о 30 кредитках стоит всего $9, которые необходимо перевести на кошелек системы WebMoney. То есть всего за 30 центов вы приобретаете полный комплект информации, достаточной для снятия денег со счета незадачливого американца. Кроме номеров кредитных карт на сайте продаются базы данных одного из московских сотовых операторов.

ZUMA PRESS

НОМЕРА ПЛАСТИКОВЫХ КАРТ С КРУПНЫМ КРЕДИТНЫМ ЛИМИТОМ ИЛИ ОСТАТКОМ НА СЧЕТЕ — ЛАКОМЫЙ КУСОК ДЛЯ ЛЮБОГО КАРДЕРА

КРЕДИТНЫЕ РИСКИ Не секрет, что в западных странах пластиковые карты почти полностью заменили кошелек. Интернет-торговля дала возможность применять кредитки для оплаты товаров и услуг различных онлайн-магазинов. Это неудивительно: кредитка имеет ряд преимуществ перед классическими наличными деньгами. Достаточно вбить номер кредитки на сайте магазина, и через пару дней можно получить заказ. Однако за любое удобство приходится платить. Номер кредитки на сайте может использовать другой человек, и именно он получит заказ. А деньги будут перечислены с банковского счета владельца карты.

Ведь что, по сути, представляет собой кредитная карта? С одной стороны, это обычный кусок пластика с вшитым внутрь чипом. С другой — набор различных данных, необходимых для финансовых операций. Поэтому держатель карты подвергается двум видам рисков. Первый связан с потерей пластика. Но такой риск не слишком высок: держатель может быстро заблокировать карту и затем выпустить новую. Опаснее риск утечки информации о карте. И особенно опасен потому, что держатель, как правило, о ней не знает.

Для совершения покупки в интернет-магазине с помощью кредитной карты необходимо знать номер карты, CVC-код (последние три цифры на обороте карты), имя владельца и срок действия карты (expiration date). Имея эти данные, можно приобрести в онлайне все что угодно. Большинству интернет-магазинов абсолютно все равно, кто именно купит товар: он получит деньги в любом случае. Даже если трансакция окажется поддельной, вина за нее ляжет на другие организации — банк, допустивший утечку данных, или самого держателя карты. Поэтому многие магазины просто закрывают глаза на подозрительные заказы.

Правда, стоит отметить, что такая схема проходит не с каждым интернет-магазином. Некоторые из них (например, *www.ozon.ru*) требуют специального подтверждения заказа, если имя держателя карты не совпадает с именем получателя. Если же заказ оформляется на держателя, то курьер при получении товара должен проверить его личность. Кроме того, покупая товар по чужой карте, человек легко может скомпрометировать себя. Если поддельная трансакция обнаружится, то мошенника легко вычислят по адресу доставки товара.

КРЕДИТНЫЕ РАЗВОДКИ Существует огромное количество источников информации о кредитных картах. Пластиковые карты широко распространены, и многие компании так или иначе работают с ними. А значит, хранят данные о картах в корпоративной информационной системе, откуда их можно извлечь. В группу особого риска попадают финансовые компании и банки, а также крупнейшие розничные сети. Такие организации вынуждены обрабатывать огромное количество кредиток, хранить и защищать информацию о них. Защита осуществляется в двух направлениях: обезопасить данные необходимо от хакеров, вирусов и других внешних угроз, а также от сотрудников компании, имеющих к ней легальный доступ (инсайдеров).

Простейший способ получить «кредитную» информацию — ее кража непосредственно у владельца. Более прогрессивные способы — это кражи с использованием вирусов или троянских коней. Вредоносная программа попадает на компьютер жертвы, ищет там номера кредиток и высылает их мошеннику. Но как правило, кража «кредитных» данных происходит путем комбинации «внешних» и «внутренних» методов. Взломать современные системы безопасности без помощи инсайдеров практически невозможно. В ряде случаев инсайдеры принимают лишь косвенное участие в краже, например приносят в офис ноутбук с троянцем. В других — самое прямое: записывают данные на флэшку и выносят их из офиса или закачивают на определенный интернет-сайт. Чаще всего это происходит в тех компаниях, где до сих пор отсутствует система внутренней безопасности.

Еще одна схема кражи получила название «фишинг». Потенциальная жертва получает электронное письмо от якобы надежного источника (например, интернет-магазина, платежной системы, банка и т. д.). Наивный пользователь переходит по одной из ссылок письма и оказывается на сайте источника, где требуется заполнить некую форму. Держатель карты благополучно заполняет ее, и информация о его кредитной карте оказывается в руках мошенника. Подвох состоит в том, что ссылка, указанная в письме, ведет на подставной сайт, который очень похож на реально существующий сервис сети (имеет похожее имя и дизайн).

Летом нынешнего года в России произошел серьезный инцидент, связанный как раз с фишингом. Тысячи российских жителей получили электронные письма с заголовком «Ваш аккаунт в системе „Яndex.Деньги" заблокирован». После нажатия одной из внутренних ссылок жертва попадала на подставной сайт, где спокойно оставляла данные о своем аккаунте в платежной системе. Естественно, эта рассылка не имела никакого отношения к «Яндексу».

КРЕДИТНЫЕ ПРЕСТУПНИКИ В мире существует черный рынок кредитной информации с черными игроками и черными же правилами игры. Однако это все же рынок, где любой игрок стремится предложить лучший продукт. Например, продавать номера кредиток с серьезным кредитным лимитом и остатком на счете. Такие номера извлекаются с территории богатых государств — США или стран Европы. Россия к таким государствам пока не относится. «С другой стороны, говорить об отсутствии угроз также было бы неправильно,— считает Илья Шабанов, ведущий аналитик „Лаборатории Касперского".— Крупные преступники стремятся воровать данные из США и стран Европы, но если им подвернется российская база, то они приберут к рукам и ее. К тому же существуют и другие мошенники (например, создатели подставных сайтов), которые тоже не прочь поживиться за чужой счет».

Среди киберпреступников довольно много выходцев из стран бывшего СССР. Так, в начале августа турецкая полиция арестовала Максима Ястремского, известного украинского мошенника по пластиковым картам (кардера). Следствие предполагает, что Ястремский был одним из организаторов торговли кредитками, украденными из компании TJX. На данный момент это крупнейшее мошенничество с картами, в результате которого пострадало более 45 млн человек.

Деятельность кардеров этим не ограничивается. Можно, например, не делать карты самостоятельно, а получать их в банках, выдавая себя за владельцев крупных счетов. Такая схема становится возможной из-за того, что всю информацию о потенциальной жертве можно приобрести на черном рынке за совсем небольшие деньги. Технология крайне проста: мошенник приезжает в банк на лимузине, выдает себя за состоятельную жертву с идеальной кредитной историей и получает карту с крупным лимитом. Для пущей убедительности мошенник предъявляет номер социального страхования жертвы и поддельное удостоверение личности.

КРЕДИТНАЯ ЗАЩИТА Известно, что пользоваться услугами интернет-магазинов в принципе небезопасно, поэтому обычным пользователям прежде, чем оставить информацию о кредитке, необходимо удостовериться в честности и защищенности интернет-магазина или банка и убедиться в том, что вы имеете дело не с подставным сайтом.

Сегодня не существует способа, гарантирующего стопроцентную защиту от кражи «кредитной» информации. Единственное, что может сделать каждый человек,— не сообщать собственные данные кому попало. Это значит не хранить их на компьютере в незащищенном виде, не передавать в интернет без лишней надобности, уничтожать все источники, где эти данные написаны. И постоянно обновлять антивирусную защиту. «Полностью обезопасить компанию от утечек в принципе невозможно,— считает Денис Зенкин, директор по маркетингу компании InfoWatch.— Технические средства контролируют только утечки по электронным каналам, но даже если все каналы перекрыты, утечка все равно возможна. Сотрудник компании с легальным доступом способен записать нужные данные на бумажку и спокойно их вынести. Или же просто их запомнить».

Если же утечка все-таки произошла и информация о ней просочилась в СМИ, на помощь приходит услуга «мониторинг кредитной активности». Она позволяет отследить все операции с банковским счетом. Для каждой карты, подписанной на подобную услугу, банк выделяет специального человека, отслеживающего трансакции со счетом. Если этот человек видит, что со счетом произведено подозрительное действие (например, снятие денег в другом конце света), он тотчас же звонит держателю и спрашивает у него подтверждение. В дальнейшем любую трансакцию можно оспорить в установленном банком порядке. Подписка на эту услугу позволяет чувствовать себя почти защищенным. Проблема только в том, что эта услуга платная (около $120 в год на территории США) и ей пользуются далеко не все. К тому же утечка из банка или интернет-магазина может просто остаться незамеченной как самим банком, так и его клиентами.

Современное общество пока испытывает серьезные трудности с защитой «кредитной» информации. Нет ясности, как эти проблемы можно решить. Невозможно запретить покупки по картам в интернет-магазинах. И неразумно осложнять процесс покупки, требуя каких-то дополнительных сведений (например, фотографии карточки). К тому же совершенно непонятно, как защищать пластиковые карты от подделок. Внедрять в них дополнительные системы защиты бесполезно, поскольку уже установленные банкоматы их не поддерживают. А менять весь парк банкоматов нереально.

Остается только одна альтернатива — не давать «кредитным» данным утекать за пределы банковских организаций. Если утечку допустил не банк, то ответственность за кражу перекладывается на клиента. Однако проблема в том, что банки не всегда могут доказать свою невиновность. Для этого необходимы специальные системы защиты, которые не только блокируют утечки, когда они происходят, но и при необходимости доказывают их невозможность. Пока банки не будут готовы потратиться на подобные системы, утечки будут продолжаться, а расплачиваться придется самим банкам. ■

«ЗАЧЕМ ТРАТИТЬ СВОИ КРОВНЫЕ, ЕСЛИ ЗА ВАС МОЖЕТ РАСПЛАТИТЬСЯ РЯДОВОЙ АМЕРИКАНЕЦ, КОТОРЫЙ ЖУЕТ БИГМАК И НЕ ЗНАЕТ, ЧТО ДЕНЬГИ С ЕГО КРЕДИТКИ УТЕКАЮТ... А ВСЕ ПОТОМУ, ЧТО ОН ИМЕЛ НЕОСТОРОЖНОСТЬ РАСПЛАТИТЬСЯ СВОЕЙ КАРТОЧКОЙ В ON-LINE-МАГАЗИНЕ ИЛИ НА ПОРНОСАЙТЕ»

ПОЛНЫЙ ЦИКЛ МОШЕННИЧЕСТВА

В июне этого года управление «К» (подразделение по борьбе с технологичными преступлениями) МВД России задержало организованную криминальную группировку, занимавшуюся подделкой карт. Группировка состояла из двух команд, одна из которых искала информацию о кредитках, а другая выполняла все остальное. Вторая команда базировалась как раз на территории России. По версии следствия, группировка подделывала карты жителей Евросоюза, Китая, США. Минимальный ущерб от ее деятельности составляет 8 млн руб. Впрочем, многие эксперты называют эту сумму консервативной. «Остается только гадать, сколько денег сняли злоумышленники с карточек своих жертв. Сумма 8 млн руб. выглядит чересчур низкой, и я совсем не удивлюсь, если реальные доходы банды были на несколько порядков выше»,— считает Денис Зенкин, директор по маркетингу компании InfoWatch. Этот случай уникален тем, что банда контролировала «полный цикл» подделки банковских карт. Как правило, злоумышленники используют более специализированный подход: кто-то ворует информацию, кто-то заливает ее на карты, а кто-то снимает с них деньги. Таким образом, преступники решают сразу две задачи — обеспечивают лучшую конспирацию и более высокое качество работы на каждом из этапов. Зачастую стадии «преступного цикла» выполняются в географически разделенных регионах, что затрудняет возможность их отследить.