Понятие «кардинг» возникло одновременно с появлением электронных денег. С одной стороны, пользоваться кусочком пластика удобнее и в какой-то мере безопаснее, чем рассчитываться наличными и носить их в бумажнике. С помощью карты можно оплачивать товары и услуги практически во всех странах мира, в любой валюте. И даже если карта будет потеряна (или украдена), без знания специального кода она окажется бесполезной для злоумышленника. Но когда ему удается добраться до секретных знаков, на банковском счету появляются нули.

Защити себя сам

Кардинг - это род мошенничества, при котором операция с использованием банковской карты или ее реквизитов производится не ее держателем. Отчего-то принято считать, что русские кардеры предпочитают атаковать американских владельцев карт. Отчасти это верно, ведь трансграничные преступления расследовать намного сложнее. Однако и в России, по разным данным, годовой объем незаконных операций с банковскими картами составляет от 300 млн до 1 млрд рублей, и эти цифры имеют тенденцию к росту.

Мошенников интересует информация, которую можно добыть, даже не прибегая к краже самой карты

Пластиковая карта является ключом доступа к размещенным на банковском счету средствам. Для банка «пластик» - это всего лишь физический носитель реквизитов карты, которые отправляются в банк при проведении различных операций. Поэтому поддельная карта с той же информацией, что и на подлиннике, будет распознана банком как настоящая. А для некоторых операций - к примеру, интернетпокупок - достаточно ручного ввода реквизитов. Соответственно, мошенников интересует

информация, которую можно добыть, даже не прибегая к краже самой карты.

Авторы платежных систем постоянно работают над повышением безопасности операций с применением банковских карт. Например, используется привязка к карте специального пароля, известного только владельцу карты и банку.

Свои фильтры доступа для защиты клиентов имеют и банки, и интернет-магазины. В сомнительных случаях банки перезванивают держателям карт и уточняют, была ли проведена транзакция.

Операция «Махинация»

Мошеннические источники получения информации для доступа к банковским счетам сегодня хорошо известны. Самым популярным из них является вовсе не хакерская атака, а игра на человеческих слабостях. Чаще всего мошенники получают необходимые данные через банкоматы. В ход идут как банальные подглядывания-подслушивания, так и использование технических ухищрений.

История

Когда врач одного из красноярских медицинских центров Наталья Семина обнаружила пропажу своего кошелька буквально через несколько часов после того, как сняла деньги с карты, она тут же вспомнила, что незнакомец, стоявший в очереди следом за ней, находился слишком близко. Вскоре Наталья получила сообщение об операции, совершенной с ее картой. Лишь оперативность работников банка и самой Натальи спасли ее от еще больших расходов - по телефонному звонку карту заблокировали, а операцию отменили.

Для успешного снятия денег в банкомате мошеннику необходимо знать ПИН-код карты и иметь саму карту - или же узнать ее данные, чтобы нанести на чистый кусок пластика. Для получения данных чаще всего используется скиммер - специальное устройство для банкомата, которое считывает номер банковской карты. Оно накладывается на кардридер, в который вставляется карта, и выглядит незаметно.

Необходимо проверять «обстановку» вокруг карты

Есть несколько способов узнать ПИН-код. Можно подсмотреть, можно подслушать (иногда владелец карты во время набора кода шепотом проговаривает его). Мошенник может распылить на клавиатуру специальный спрей, на котором будут четко видны нажатые клавиши. Рядом с банкоматом иногда устанавливается микрокамера,

спрятанная где-нибудь за выступом стены или пачкой рекламных буклетов.

Существуют накладные клавиатуры, которые практически невозможно отличить от банкоматных, также считывающие ПИН-коды. А панели, накладываемые на всю поверхность банкомата, предназначены для выяснения и кода, и номера карты. То же самое проделывает банкоматфантом. Он выглядит как обычный банкомат, однако на самом деле представляет собой пустую коробку-скиммер. При попытке снять средства на экран выводится сообщение о технических неполадках или отсутствии наличных денег, а мошенник получает всю необходимую информацию о карте.

Для того чтобы завладеть банковской картой, мошенники могут использовать нехитрый фокус под названием «ливанская петля». В кардридер помещается специальный карман, изготовленный с помощью фотопленки, концы которого незаметно закрепляются снаружи. В этом случае помещенная в кардридер карта обратно не возвращается.

Совет

Установка скиммера и тем более банкоматафантома связана с определенным риском, и мошенники нередко делают это ночью. Поддельный банкомат часто появляется наутро в многолюдных местах. Чтобы не рисковать, стоит обналичивать деньги в одних и тех же банкоматах, лучше всего в помещении банка.

Если же есть необходимость снять деньги в незнакомом банкомате, нужно проверить периметр кардридера на наличие выступающих краев «ливанской петли». Если для того, чтобы вставить карту в банкомат, требуется применить усилие, лучше поискать другой аппарат.

Следует держаться подальше от любопытных в очереди и, конечно же, никому не сообщать свой ПИН и не записывать его на карту. Слип, то есть чек, выданный банкоматом, не нужно выбрасывать в корзину для мусора - его лучше хранить в течение двух-трех месяцев.

Кстати, скимминг карт возможен не только в банкомате. Официант в ресторане или продавец в магазине могут воспользоваться карманным скиммером. Поэтому не стесняйтесь просить, чтобы считывание производили у вас на глазах.

Татьяна Ходенкова, заместитель управляющего по развитию бизнеса ФКБ «Юниаструм Банк» (ООО) в Красноярске:

- Наиболее часто встречается такое мошенничество, как считывание данных пластиковых карт в банкоматах, которые мошенники оборудуют специальными накладками. В случае обнаружения сомнительных транзакций или утери карты следует

немедленно звонить в московский call-центр по указанному на карте номеру телефона. Карта блокируется сразу после звонка клиента. Чтобы оспорить незаконную транзакцию, необходимо подать в банк заявление. Возможный срок возврата средств - до 180 дней. Однако если факт мошенничества не будет доказан, клиенту придется возместить банку фактически понесенные расходы в соответствии с установленными тарифами.

Против взлома нет приема

В декабре прошлого года, находясь на отдыхе, красноярский бизнесмен Александр Малахов заметил, что средства на его счету постепенно уменьшаются. А вернувшись в январе в Россию, и вовсе обнаружил отрицательный баланс. Во время пребывания Александра за границей мошенники оплачивали с его счета услуги Интернета и мобильной связи.

Хакеры взламывают интернет-магазины, порталы финансовых учреждений, электронные платежные системы. В результате средства с банковского счета переводятся на счета кардеров и затем обналичиваются либо расходуются на покупку товаров и услуг через Интернет.

Своевременное получение информации о совершенных незаконно транзакциях способно спасти деньги держателя карты. В этом случае выручает подключение услуги мобильного банкинга. Мгновенно заблокировать карту можно даже без звонка в call-центр, достаточно отправить на определенный номер SMS-сообщение. Также имеет смысл установить суточный лимит на снятие средств по карте - тогда у кардеров, по крайней мере, не получится изъять со счета очень крупную сумму.

Осторожно - магазин!

Часто жертвами мошенников становятся держатели карт, делающие покупки в Интернете.

История

Красноярец Игорь Сенькин зарегистрировался в международной системе расчетов PAYPAL для участия в аукционе EBay. В феврале прошлого года ему вдруг пришло SMS-сообщение, что по его карте произведены две странных транзакции - оплата неких

интернет-услуг. Написанная в PAYPAL претензия, приложенная к ней копия паспорта, подтверждающая, что именно Игорь является владельцем счета, и копии выписок по транзакциям сделали свое дело: сделки были блокированы, а деньги возвращены на счет.

Для CNP-транзакций (транзакция без использования карты; CNP - Card Not Present) достаточно указать только фамилию владельца карты, ее номер и срок действия, иногда - домашний адрес. Лишь в некоторых случаях запрашивается дополнительный код безопасности. Впрочем, многие онлайновые магазины применяют специальные фильтры: например, если покупатель заходит на сайт через анонимный прокси-сервер, такая транзакция, вероятнее всего, будет отклонена. Однако лучше использовать для покупок в Интернете отдельную карту, на которую следует переводить лишь ту сумму, которую предполагается потратить в ближайшее время.

Рыбалка в Сети

Фишинг (от английского fishing - «рыбалка», «выуживание») является распространенным способом добычи конфиденциальной информации через Интернет. Хакерство здесь ни при чем: ПИН-код мошенникам сообщают сами держатели карт. Деньги, «уведенные» таким путем, практически невозможно вернуть. По словам Александра ЯЦЕНКО, заместителя генерального директора компании «Первый Поверенный», чтобы уменьшить риск ответственности банка за осуществление операции по распоряжению неуполномоченного лица, в договоры с клиентами банки включают пункт, согласно которому держатель карты обязуется сохранять коды доступа в тайне.

«Использование пароля или ПИН-кода является достаточным условием для признания выдачи распоряжения уполномоченным лицом, и доказывать обратное должен клиент», - отмечает Александр Яценко. В таких случаях вина за проведение незаконных транзакций обычно возлагается на владельца.

Информация о карте должна оставаться неприкосновенной

Чаще всего аферисты действуют так: кардер якобы от имени банка присылает владельцу карты электронное письмо, уведомляя его о составлении новых списков клиентов или об утерянной базе данных. Держателя карты просят сообщить данные о ней; иногда в письме дается ссылка на сайт, весьма похожий на официальный банковский, где также требуется ввести карточную информацию.

Существует и неэлектронный фишинг. Выше уже было сказано о способах вычисления ПИН-кода через банкомат. Кроме того, известны массовые случаи мошенничества в турецких торгово-сервисных предприятиях, схожих с обычными пунктами выдачи наличных. Процедура выдачи денег выглядит для банка как покупка в магазине, не требующая введения ПИН-кода. Тем не менее владельца карты просят ввести код,

который затем используется вместе с изготовленной поддельной картой.

Совет

Перепроверить информацию, присланную в письме, очень просто: нужно зайти в Интернет не по предложенной ссылке, а на официальный банковский сайт. Или позвонить в банк. Производя покупку в интернет-магазине, стоит обращать внимание на строку адреса в браузере - домен на протяжении всего процесса должен оставаться неизменным. При редиректе на подозрительный домен лучше отказаться от покупки, так как он может оказаться фишинговым сайтом, собирающим карточные данные.

Что касается неэлектронного фишинга, то особенно осторожными следует быть за рубежом. Наиболее опасными в этом плане странами для россиян признаны Таиланд, Турция и Украина.

Александр Яценко, Заместитель генерального директора ООО «Первый Поверенный»:

- Как показывает практика, гражданские дела средней сложности по возмещению ущерба банком могут рассматриваться от двух до восьми месяцев. Стоимость юридических услуг по представительству интересов в суде по одному гражданскому делу составляет от 15 000 до 50 000 рублей. Кроме того, необходимо учитывать оплату государственной пошлины, а в необходимых случаях - услуг специалистов, экспертов, переводчиков; транспортные, почтовые расходы; затраты на поиск и сбор доказательств. Все вместе может составить весьма внушительную сумму. При рассмотрении дела судебные расходы возлагаются на сторону, против которой состоялось решение. Однако для этого нужно фиксировать их документально, кроме того, суд может уменьшить размер судебных расходов. Все вышесказанное часто приводит к тому, что клиенты, столкнувшиеся с нарушением своих прав при незначительном размере убытков, не прибегают к судебной защите.

Кто заплатит?

В рамках международных платежных систем, таких как Visa, MasterCard и других, существует понятие «банк-эмитент», т.е. банк, который выпускает и выдает пользователю кредитную карту, и «банк-эквайр», который обеспечивает прием кредитных карт к оплате. Один и тот же банк может выступать и как эмитент, и как эквайр.

Когда держатель карты осуществляет покупку в магазине, информация с кредитки передается в обслуживающий его банк-эквайр, а оттуда в банкэмитент, проверяющий

правильность информации о карте и доступность средств на счете. Разрешение покупки банком-эмитентом подтверждает, что банк-эквайр получит деньги и переведет их на счет магазина. Поэтому за мошеннические операции с пластиковыми картами, совершенные в обычных магазинах, ресторанах и т.д., ответственность несет банк-эмитент. Если же незаконная транзакция была проведена с участием виртуального магазина, возврат средств владельцу карты должен обеспечить банк-эквайр. Чаще он перекладывает ответственность на интернет-магазин, через который прошла мошенническая транзакция.

Следующий шаг держателя карты после ее блокировки - обращение в банк с заявлением о несогласии с операцией. Если факт мошенничества будет доказан, банк возвращает деньги владельцу карты. Многие банки страхуют подобные финансовые риски и после возмещения суммы клиенту получают компенсацию от страховых компаний.

Банк может и не вернуть «угнанные» средства. Если по истечении полугода ущерб не возмещен, держатель карты имеет право обратиться в суд. Однако, как отмечает Александр Яценко, «в целом защита прав клиента перед банком всегда значительно затруднена: во-первых, отсутствием доказательств у клиента и избытком их у банка и, во-вторых, невнимательностью клиента при заключении договора с банком. Хотя банк, как и любой другой профессиональный предприниматель, несет ответственность независимо от вины, на началах риска. К сожалению, об установлении единообразной практики в отношении судов общей юрисдикции в подобных случаях говорить пока рано».

Источник: ibank.ua