Виды афер и махинаций с платежными картами - как распознать обман и не стать жертвой

Пластиковые карточки стали привычным способом хранения денег. Казалось бы, финансы надежно защищены, ведь кредитка всегда под рукой, а получить наличность или рассчитаться в магазине можно, только зная пин-код. Однако не все так гладко. Мошенничество с банковскими картами набирает обороты, поскольку мошенники каждый раз придумывают новые схемы и махинации, целью которых является снятие денег с карточного счета. Для того чтобы не стать жертвой воров и защитить собственные сбережения, нужно знать всевозможные методы кражи данных и варианты защиты от них.

Виды мошенничества с банковскими картами

Банковская карта является чуть ли не универсальным средством в финансовом мире – на нее перечисляют заработную плату, выдают кредиты, ею рассчитываются в точках продаж и интернете. Если кому-то понадобились деньги на другом конце земли – их тоже можно перечислись при помощи карты. Одновременно растет и число преступлений, связанных с хищениями денежных средств с пластика. Большая их часть происходит из-за невнимательности и чрезмерного доверия владельцев кредиток. Существует много способов похищения денег с карточки, рассмотреть которые стоит подробнее.

Через мобильный банк. Устанавливая сторонние приложения из интернета, для работы с которыми нужна привязка карточки, следует быть очень внимательным. Дело в том, что создатели программы специально заражают ее вирусом, который, проникая в смартфон, начинает работать на мошенников. Он заменяет окно мобильного банкинга фишинговым, то есть поддельным, а владелец телефона вводит туда свои данные, ничего не подозревая. Вирус отправляет их аферистам, которые затем незаконно получают доступ к карточному счету клиента.

Кроме этого, программа может получать доступ к смс-оповещениям клиента при работе в программе. С их помощью воры под видом владельца дебетовой карты они могут входить в банкинг и совершать кражу денег. Клиент может ничего не подозревать, так как вирусы блокируют сообщения о снятии наличных и переводе денег, которые должны поступать на телефон. Избежать попадания трояна в телефон просто – необходимо устанавливать лишь лицензионные программы (в том числе и антивирусники) и регулярно проверять счет.

По телефону. Если к телефонному номеру была привязана банковская карточка, то мошенник может воспользоваться и этой ситуацией. При краже/утере телефона или сим-карты, преступники получают доступ в интернет-банкинг и спокойно переводят все деньги с кредитки. Кроме этого, злоумышленники могут взломать сайт мобильного оператора. После этого они устанавливают переадресацию всех смс-сообщений пользователя и используют их для доступа к мобильному или интернет банкингу.

СМС мошенничество. Владельцу кредитки приходит сообщение на сотовый, что карта заблокирована. Для ее разблокировки предлагается сделать обратный звонок оператору финансового учреждения по указанному в смс номеру. При телефонном звонке мошенник представляется сотрудником банка-эмитента кредитки и просит дать секретную информацию: номер с пластика, кодовое слово и цифры пин-кода, якобы необходимых для разблокировки. При помощи этих данных аферисту не составит труда воспользоваться денежными суммами с карточного счета.

Через интернет. Покупка товаров через интернет очень популярна, поскольку помогает существенно сэкономить. Мошенники могут перехватывать данные прямо во время проведения оплаты, а потом применять реквизиты банковской карточки для дальнейшего вывода денег. Избежать это можно, следуя простым правилам:

- не делать покупки на большие суммы через всемирную паутину;
- использовать для оплаты виртуальную карту;
- установить лимит по разовой оплате;
- использовать для совершения покупок только проверенные сайты;
- подключить услугу Secure Code.

Кража пластиковой карты. Мошенничество с банковскими картами путем воровства кредитки – дело распространенное. Если такое обнаружено, необходимо срочно связаться с оператором и заблокировать карту или сделать это самостоятельно через мобильное или интернет-приложение. Это крайне важно, когда пластик имеет лишь магнитную полосу. Снять деньги без пин-кода с него не представляется возможным, однако расплачиваться в магазине не составит труда. Карточками с чипом или с бесконтактной оплатой воспользоваться сложнее, потому что для любых операций понадобиться ввести номер секретного пароля.

С помощью поддельных банкоматов. Злоумышленники идут на разные уловки, лишь бы завладеть чужими финансами. Они даже могут изготовить псевдобанкомат. Устанавливается он в людном месте, чтобы чем можно больше людей воспользовались им. Вставив карту в устройство, человек видит

информацию об отсутствии наличности либо неисправности системы. Тем временем мошенники завладевают всей необходимой им информацией для вывода денег. Фальшивый банкомат может возвратить карточку, а может оставить ее у себя. В этом случае снять деньги будет еще проще, ведь есть оригинал и известен пин-код.

При платежах по терминалу. При покупках в магазине стоит внимательно следить за кассирами, которые берут пластик в свои руки для оплаты по терминалу. Если сотрудник магазина проводит банковской карточкой два раза по терминалу, то в первый раз он делает это, чтобы списать деньги, а второй – для снятия информации с пластика, чтобы потом увести деньги. Кроме этого, он может запомнить cvv код и данных на лицевой стороне, при помощи которых легко проводить покупки в интернете.

Как мошенники снимают деньги с банковской карты

Снять деньги при помощи самого хозяина кредитки элементарно. Для этого используются известные способы. Первый из них – мошенничество с банковскими картами путем заклеивания скотчем той части банкомата, откуда подаются деньги. Клиент вставляет карту, вводит пин-код, слышит счетчика банкомата, а деньги не получает, поскольку устройство выдачи денег не открывается. Во втором случае аферисты изготавливают специальное устройства из фотопленки, которое вставляется в картоприемник – банкомат принимает кредитку, выдает деньги, а карточку не возвращает.

Способы получения доступа к конфиденциальной информации

Завладеть необходимой информацией, содержащейся на пластике намного проще, чем об этом думают пользователи банковских карточек. Часто мошенничество происходит по вине самих клиентов банков из-за халатности и невнимательности. Аферисты могут легко подсмотреть секретный код из-за плеча при расчете владельцем банковской карточки в магазине, снятии наличности в банкомате и пр.

Кроме этого, существует сговор злоумышленников с продавцами, которые могут предоставлять мошенникам информацию с платежных карт покупателей. Иногда аферисты договариваются с банковскими работниками. Те сообщают им, по какому адресу придет заказанная по почте кредитка, которую воры перехватывают и снимают наличность. Распространенным способом является заражение мобильных устройств троянами, которые крадут данные при расчете держателем банковской карточки в сети.

Новые виды мошенничества с банковскими картами

Прогресс не стоит на месте. То же можно сказать и про аферы с кредитками. Если раньше мошенничество с банковскими картами ограничивалось заклеиванием

отделения для выдачи налички и кражей пластика, то в современном мире махинации перешли в новую плоскость. Сейчас на «помощь» злоумышленникам приходят новые бесконтактные технологии и интернет, хоть и здесь большую роль играет безалаберность пользователей.

Звонок от работников банка по сервисному номеру. В последнее время стали известны факты махинации с банковскими картами Сбербанка. Для этого мошенники используют сервисному номеру организации, ведь технологически это возможно. На телефон жертвы мошенников приходит смс с номера 900 с просьбой перевести определенную сумму денег. Для этого необходимо отправить в ответ код, содержащийся в сообщении, либо операция пройдет автоматически через 600 секунд.

Через некоторое время раздается звонок с официального номера Сбербанка (8-800-555-5550), где человек, назвавшись специалистом службы безопасности банковского учреждения, просит от клиента отправить ответное смс, где указать код, пробел и словосочетание «отмена перевода». После отправки сообщения, деньги, равно как и сотрудник Сбербанка, бесследно исчезают.

Запуск вирусной программы в банкоматах и терминалах. Этот вид мошенничества – новинка на российском финансовом рынке и поражает он не владельцев зарплатных и кредитных карточек, а банкоматы. Суть мошеннической схемы заключается в том, что устройства выдачи денег заражаются специальным вирусом-трояном, который дает злоумышленникам возможность снять наличность из банкомата, введя на клавиатуре специальный код. Впервые с таким явлением столкнулись весной 2019 года.

Бесконтактные считывающие устройства с технологией Paypass. Использование платежной карточки с технологией бесконтактной оплаты PayPass разрешает производить оплату на сумму не более 1000 рублей без ввода пин-кода. Преступники пользуются этой возможностью, потому что для осуществления операции нужно лишь приложить переносной терминал к сумке или одежде, где находится кредитка. Осуществить такую махинацию е составляет труда, особенно в местах с большим скоплением народа.

Распространенные схемы мошенничества

С каждым годом количество так называемых «примочек» увеличивается. Преступники применяют в своих аферах как технические уловки, в виде специальных накладок, вставок, камер, так и нематериальных средств. Способы мошенничества с банковскими картами и используемые методы могут быть настолько простыми, что с первого раза владельцы пластика даже не понимают, что их пытаются обмануть.

Скимминг личных данных с карты. Способ хищения, постепенно уходящий в прошлое из-за внедрения чиповых карт, но тем не менее не потерявший своей актуальности. Заключается он в установке специального устройства скиммера на место картоприемника банкомата, от которого отличить его внешне очень сложно. Клиент банка вставляет пластик, а злоумышленники копируют всю нужную информацию с магнитной полосы карты для изготовления дубликата. Пин-код добывается двумя способами – при помощи установки специальной накладки на клавиатуру банкомата или путем монтажа миниатюрной видеокамеры.

Одной из разновидностей скимминга является **шиминг**. Это усовершенствованный вариант, поскольку вместо накладного устройства в картоприемник помещается тонкая плата. Впоследствии она считывает всю необходимую информацию с карточки. Используют скимминг злоумышленники не только в банкоматах, но и магазинах или кафе. В этом случае применяется портативное устройства – ручной скиммер.

Впоследствии воры выпускают копии банковских кредиток, куда наносится информация с украденного пластика. После того как мошенники подделали банковские карты, снять с них деньги или расплатиться в магазине не составит труда, поскольку коды подтверждения известны. Для того чтобы не стать жертвой скимминга, нужно стараться не снимать деньги в банкоматах, расположенных в отдаленных и слабоосвещенных местах, потому что такие устройства проще всего оснастить считывателями. В торговых точках желательно оплачивать кредиткой самостоятельно, а не передавать ее в чужие руки.

Электронный и неэлектронный фишинг. «Ловить на удочку» – так можно перевести этот вид воровства. Суть его заключается в том, что на электронную почту с мошеннических сайтов или телефон жертвы приходит сообщение с просьбой указать данные кредитки. Это может быть акция от платежной системы или банка, но стоит понимать, что все это является разводом, поскольку ни одна банковская организация не будет рассылать такого рода предложения с целью «выудить» личные данные клиента.

Вишинг. Вид мошенничества сродни вышеприведенному фишингу с одной только разницей, что для того, чтобы завладеть данными владельца пластика

используется телефонная связь, причем разговор может происходить как в автоматизированном режиме – при помощи автоответчика, так и напрямую с так называемым оператором банковского учреждения. Злоумышленники под любым предлогом стараются разузнать информацию о кредитке, секретном коде и данных клиента.

Может звонить покупатель, если владелец кредитки размещал на популярном сайте объявлений информацию о продаже дорогостоящей вещи. Под предлогом того, что для транспортной компании, которая будет забирать товар, необходимы полные персональные данные продавца, а ему самому сведения с карточки, чтобы перевести деньги, он выманивает всю необходимую информацию, после чего исчезает, а вместе с ним и средства со счета.

Создание подставного интернет-магазина. Воры давно перешли в виртуальное пространство, только бы завладеть деньгами доверчивых покупателей. Для этого создаются интернет-магазины, предлагающие товары по бросовым ценам, чтобы как можно больше покупателей захотели приобрести их. Оплату покупки предлагается произвести при помощи банковского пластика. Целью аферистов является получение данных с карточек покупателей, в том числе и cvv-код, а потом с их помощью самостоятельно рассчитываться в интернете.

Двойное списание со счета. Этот вид скорее можно отнести не к злому умыслу, а к техническим ошибкам, возникшим со стороны процессингового центра, который обрабатывает все платежные операции по банковским карточкам, или банка-эмитента. Кроме этого, двойное списание средств можно отнести на неопытность продавца или проблемы с терминалом оплаты в самой точке продаж. Избежать таких действий невозможно, а вот вовремя заметить их легко – для этого нужно подключить услугу смс-информирования. При обнаружении случившегося необходимо незамедлительно сообщить в банк, выдавший кредитку.

Как защитить карту от мошенников

Перед тем как вставлять пластик в банкомат, нужно убедиться, что на поверхности отсутствуют подозрительные накладки – как правило, они отличаются цветом и видов. Для владельцев кредиток с бесконтактным способом оплаты рекомендуется установить минимальный кредитный лимит при оплате без пин-кода или вовсе его отменить. Дополнительно можно минимизировать риски, поместив карту в радиэкранированный кошелек (для этого нужно лишь положить внутрь его фольгу), металлическую коробочку или фольгированный пакет.

Ни под каким предлогом нельзя отдавать свою кредитку в руки третьим лицам, а тем более сообщать пин-код, ведь это секретная информация, которая доступна только владельцу карты, даже сотрудникам банка она неизвестна, потому что формируется автоматически. Не стоит производить оплату в ответ на смс-сообщение и электронные письма, пришедшие из неизвестных источников. В случае каких-либо подозрений или несанкционированного списания средств с баланса, нужно звонить в банк и осуществлять блокировку.

Куда обращаться, если похитили деньги с карты

Первое, что необходимо сделать, если списаны деньги без ведома владельца, это позвонить в банковское учреждение по номеру, указанному на обратной стороне пластика. Им следует сообщить об исчезновении денежных средств с карточного счета и следовать всем предписаниям. После этого нужно прийти в ближайшее отделение полиции и написать заявление.

Можно ли вернуть деньги

Если клиент полностью уверен, что он не совершал никаких несанкционированных операций по карте (необходимо удостовериться, что и родственники не причастны к этому), нужно писать заявление в банк на возврат денег. Если банк отказывает, можно смело обращаться в суд. Вернуть исчезнувшие средства крайне сложно, особенно если для проведения транзакций необходим ввод пин-кода, но такие случаи известны. Проще возвратить деньги, если зафиксирована хакерская атака на банк или пострадало большое количество граждан.

Правовая ответственность за мошенничество

Уголовный кодекс (статья 159.3) признает мошенничество с банковскими картами преступлением, за которое виновные несут ответственность в соответствие с законодательством. Согласно кодексу за содеянное предусматривается штраф, арест, исправительные работы или ограничение свободы. Денежное возмещение, количество часов принудительных работ или время ареста напрямую зависят от похищенной суммы, совершалось ли злодеяние самостоятельно или организованной группой.