Защита от мошенничества с банковскими картами

Наверное, уже почти каждый догадывается, что использование при расчётах банковской карты вместо наличности уже не создает той иллюзии безопасности как десятилетие ранее. Наличие банковской карты несёт в себе угрозу подвергнуться нападению злоумышленников как в физическом плане, так и в виртуальном. Кибер-преступники уже давно выработали десятки способов отъёма денежных средств с Вашей банковской карты.

Не вдаваясь в премудрости этого “ремесла”, приведём ниже несколько рекомендаций по безопасному использованию банковских карт. Затем разберём наиболее часто встречающиеся способы мошенничества с платёжными банковскими картами в сочетании с банкоматами и меры предосторожности. Возможно, это немного поможет держателям карт уберечь свои сбережения от преступных посягательств.

Главное предостережение для всех держателей карт – **постарайтесь не использовать для оплаты или для получения наличности банкоматы, расположенные вне помещений кредитных учреждений**. Остерегайтесь снимать наличность в тех банкоматах, которые работают круглосуточно на улицах, как в слишком людных пешеходных зонах, так и в тихих переулках. Это предостережение относится ко всем без исключения странам.

Обязательно закажите в Вашем банке, если еще не заказали, услугу sms-информирования о транзакциях с Вашей картой. Это просто необходимо сделать! Стоит подобная услуга недорого и может впоследствии сохранить Ваши сбережения и время. Когда на Ваш мобильный ночью приходит сообщение, где указано, что Вы только что оплатили четырёхместный номер в одном из солидных отелей Европы, Вы сильно удивитесь и сон, скорее всего, будет испорчен. Однако паниковать ни в коем случае не стоит! Если транзакция покажется подозрительной банку, он Вам незамедлительно перезвонит или самостоятельно заблокирует карту, если нет – немедленно звоните в call-центр по номеру, указанному на пластиковой карте или, если знаете, по другому номеру банка, сообщите о произведенной злоумышленниками транзакции и требуйте заблокировать Вашу карту. Тем самым вы убережёте остаток своих средств на карте и, возможно, сможете в дальнейшем вернуть похищенные средства.

Совет. *Обязательно подключите в банке услугу sms-информирования. При любых операциях по Вашей карте на Ваш мобильный телефон будет приходить из банка sms-сообщение о совершенных транзакциях в режиме online.*

Совет. *Старайтесь всё-таки не хранить значительные суммы на своей карте, особенно если она у Вас зарплатная. Если зарплата позволяет – откройте в банке вклад и пусть по нему начисляются проценты без какого-либо риска. Если Ваша зарплатная карта по неосторожности будет скомпрометирована, Вы рискуете на какое-то время остаться без своевременной зарплаты, и добавите лишней головной боли бухгалтерии Вашего работодателя или банка.*

Если всё же сумма на Вашей банковской карте значительна и вклад Вы открывать не хотите – не используйте её для расчетов и покупок в интернет-магазинах, кафе, барах и ресторанах. Для этого заведите вторую карту - дебетовую, куда будете переводить средства по мере надобности, под конкретное приобретение. В случае компрометации с дебетовой карты злоумышленники не смогут списать сумму большую той, которая имеется на карте, в отличие от кредитной.

Вторую карту Вы можете использовать для любых расчётов и приобретений, но будьте готовы, что через месяц или год, в зависимости от степени Вашей осторожности и частоты использования, она все равно будет скомпрометирована, т.е. будут похищены Ваши данные, указанные на карте и этими данными попытаются

воспользоваться злоумышленники. Конечно, как было отмечено выше, Вы её заблокируете, и закажете в банке её перевыпуск. Через 2-3 недели у Вас появится новая карта.

Совет. *Никогда не выпускайте свою банковскую карту из вида, когда расплачиваетесь в магазине, кафе или ресторане. В противном случае Вы сильно рискуете – Ваша карта может быть скопирована, а подпись подделана.*

Кроме того, специально для интернет-покупок Вы можете заказать в банке «виртуальную» карту. На сегодняшний день значительное количество банков предоставляет подобную услугу. Виртуальная карта - это предоплаченная банковская карта международной платежной системы, как правило, не имеет физического носителя, и ей Вы не сможете рассчитаться за покупки в магазине или кафе. Такая карта предназначена только для совершения безопасных покупок в интернете.

Совет. *Старайтесь пользоваться банкоматами в отделениях банка или в крупных торговых центрах, где установлены камеры слежения за банкоматами. Тем самым, в спорных случаях, в качестве доказательства или опровержения Вы сможете предъявить видеозаписи с камер слежения.*

Совет. *Запишите и храните отдельно номер Вашей банковской карты. В случае если возникли проблемы с заеданием карты в банкомате, а банкомат не сети Вашего банка или Вы находитесь в другой стране - Вам обязательно понадобятся эти сведения.*

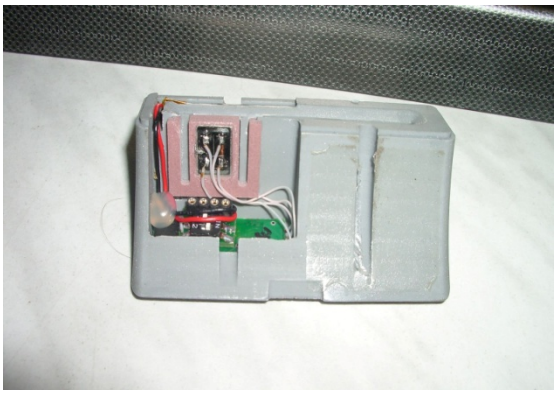
Совет. *Пользуйтесь виртуальной картой банка для покупок в интернете или заведите себе пару интернет-кошельков для оплаты в сети. Уделяйте внимание средствам антивирусной защиты Вашего компьютера. Никогда и никому не сообщайте сведения, указанные на Вашей банковской карте. Рассмотрим один пример: Вы разместили объявление о продаже автомашины. При поступлении от «потенциального покупателя» просьбы отсканировать с двух сторон Вашу карту и направить «покупателю» её двустороннюю копию для предоплаты или оплаты – от такого «покупателя» будет благоразумнее отказаться. Денег без карточки злоумышленники снять не смогут, но оплатить покупки в интернете по Вашей карте смогут элементарно.*

А теперь рассмотрим подробнее наиболее часто встречающиеся способы мошенничества с пластиковыми картами и банкоматами.

Способ мошенничества. Копирование данных с Вашей карты (skimming). Достаточно часто встречающийся вид мошенничества. Предусматривает использование специально изготовленных и дорогостоящих технических устройств, состоящих из накладной клавиатуры, имитирующей клавиатуру банкомата и считывателя данных с магнитной полосы карты (скиммера) – небольшое устройство, имитирующее картоприёмник банкомата. Указанные устройства устанавливаются злоумышленниками в течение нескольких секунд, как правило, на двустороннюю клейкую ленту. Работающие от батареек и имеющие в своём корпусе запоминающие устройства, эти девайсы запоминают Ваш пин-код и считывают всю информацию с Вашей карты за несколько секунд. Впоследствии злоумышленники с помощью специальных программных и технических средств изготавливают дубликаты считанных банковских карт.

Другой похожий способ – когда злоумышленники вместо накладной клавиатуры устанавливают на банкомате или внутри самого скиммера миниатюрную видеокамеру, которая транслирует изображение клавиатуры банкомата на монитор ноутбука или экран смартфона злоумышленника, когда Вы набираете свой пин-код.


Накладная клавиатура и считывающее устройство в комплекте

Оборотная сторона накладной клавиатуры и считывателя магнитной полосы карты

Данные устройства могут накапливать украденную информацию о пластиковых картах, либо дистанционно передавать её по радиоканалу злоумышленникам, находящимся поблизости.

Превентивные меры. При наличии подозрений, слегка потяните за крайний выступ клавиатуры каким-нибудь предметом вроде ключа, слегка вверх, и, если она поддастся не снимайте её и не прикасайтесь к этим устройствам, немедленно сообщите о накладке в банк, сотруднику охраны или полиции. Как правило, подобные устройства устанавливаются на уличных банкоматах, которые находятся не в очень людных местах, где мало других банкоматов, как правило, перед выходными или праздничными днями, когда бдительность клиентов заметно снижается.

При наборе пин-кода на клавиатуре банкомата всегда прикрывайте её ладонью во избежание несанкционированной видеозаписи.

Способ мошенничества. Разновидность скимминга – шимминг. (Shim — тонкая прокладка). Это копирование данных с Вашей карты при помощи тончайшей почти невидимой электронной пластины, располагаемой в картоприёмнике. В щель картоприёмника банкомата при помощи специальной карты-носителя злоумышленниками подсаживается тончайшая пластина-шим, которая подсоединяется к контактам, считывающим данные с карт, после чего карта-носитель удаляется. Далее всё работает, как и при традиционном скимминге — т.е. со вставляющихся в банкомат пластиковых карт незаметно считываются все важные данные, которые затем используются злоумышленниками для производства карт-дубликатов и снятия с их помощью денег.

Способ мошенничества. Заклеивание клейкой лентой кэш-диспенсера банкомата. При выдаче наличных денежных средств купюры не выходят из соответствующего разъёма. В состоянии недоумения или раздражённости Вы забираете карту и уходите искать другой банкомат. Затем злоумышленник, наблюдавший за Вами со стороны, подходит к банкомату, отклеивает скотч и забирает Ваши деньги.

Похожим способом является помещение в разъем картоприёмника тонкой плёнки, в которую помещается Ваша карта, когда вы захотите получить из банкомата наличные. Такое приспособление может вместить в себя карту, но не позволит банкомату работать с вашей картой и не выдаст вам ее обратно. За Вас это сделает злоумышленник с помощью подручных средств.

Превентивные меры. Перед снятием наличности в банкомате внимательно осмотрите кэш-диспенсер, картоприемник, клавиатуру, и если ничего подозрительного не обнаружили, можно снимать деньги. Остерегайтесь также снимать деньги в тех банкоматах, рядом с которыми находятся подозрительные лица. Если же банкомат по каким-либо причинам не выдает вам карту обратно, не спешите покинуть банкомат, свяжитесь с банком по контактному номеру телефона, указанного на банкомате и опишите ситуацию. И не пользуйтесь советами третьих лиц при заедании Вашей карты в банкомате.

Способ мошенничества. Наверное, самый дорогостоящий. Изготовление и установка злоумышленниками поддельных банкоматов. Это способ практикуется в Европе. Он полностью имитирует нормальный банкомат, но никогда не выдает наличных денег. К тому же, он запоминает введённые пин-коды и не выдает обратно пластиковые карты.

Превентивные меры. По возможности пользуйтесь только знакомыми банкоматами или, если Вы находитесь в незнакомой местности, снимайте деньги в банкоматах, расположенных в помещениях банка.