Мошенничество с картами

Самые простые рекомендации, чтобы избежать кражи денег с карты

Вот наиболее распространенные виды махинаций с пластиковыми картами:

- Использование потерянных/украденных карт (lost/stolen card), когда банк вовремя не блокирует счет пропавшей карточки, и мошенник его обнуляет.
- Подделка карт (counterfeit/skimming), когда полученная незаконным путем информация о чужой карте эммбоссируется на пластик (белый пластик) или записывается на магнитную полосу подделки или подлинной карты.
- Заказ по почте, телефону, Интернету (MO/TO) различных товаров и услуг с использованием данных платежной карточки человеком, не являющимся владельцем этой карты.
- Использование чужого банковского счета кредитной или дебетовой карты, лицом, получившим доступ к этому счету незаконным путем, например, путем изменения адреса или требования повторного выпуска кредитной или дебетовой карты.

- Использование карт, неполученных законным держателем (NRI) хищение новой или повторно выпущенной карты из почты при пересылке законному держателю с последующим ее использованием.
- Указание ложных данных в заявлении на получение карты (fraudulent application).
- Двойная прокатка карт (multiple imprint fraud) — сговор торгово-сервисных предприятий, предусматривающий многократную прокатку платежной карты с получением дополнительных копий слипов, используемых впоследствии в мошеннических целях.

Интернет-мошенничество — использование реквизитов карты, полученных незаконным путем, для транзакций в виртуальной среде. Номер карты мошенники получают различными путями, включая кражу из компьютерной системы торговой точки в сети Интернет, не имеющей необходимых средств безопасности для предотвращения несанкционированного доступа (firewalls). Термин интернет-мошенничество имеет широкое значение и может предполагать несколько сценариев:

- мошеннические транзакции с использованием номеров существующих карт;
- злоупотребления торгово-сервисных точек в сети Интернет (выставление завышенной цены или несанкционированный сбор многочисленных подписчиков);
- мошенничество фиктивных торговцев, организующих веб-страницы для обмана держателей карт и сбора данных о держателях платежных карт;
- фиктивные банки или агенты, организующие фиктивные веб-страницы для сбора информации о держателях карт и торгово-сервисных предприятиях;

- получение информации о реквизитах карт через взлом баз данных (в т. ч. через электронные доски объявлений и информационные веб-страницы, где говорится о том, как можно совершить мошеннические действия).

Следующие действия жулика очень просты: он получает карту, кладет на счет $100 и отправляется в увлекательное путешествие по странам Азии или Европы. Его интересуют только магазины, которые устанавливают лимит на сумму покупки (как правило, $100–200), при которой не производится авторизация (проверка суммы на счете). Посетив несколько таких магазинов, можно приобрести все необходимое для себя и друзей, прихватить кое-что на продажу.

При покупке в таких магазинах с карточки при помощи импринтера делаются слипы (товарный чек с оттиском карты и подписью держателя), которые затем предъявляются в компанию VISA для оплаты. А поскольку учет слипов требует времени, а stop-list (информация об утерянных и украденных картах) обновляется во многих торговых точках не чаще одного раза в неделю, то квазитурист успевает основательно отовариться.

Помните: подавляющее большинство случаев мошенничества в Интернете имеет отношение к развлекательными веб-страницам для взрослых и играм.

Советы для держателей платежных карт

1. Никому и никогда не сообщайте ПИН-код, не пишите его на бумажке и, конечно же, не храните рядом с картой.
2. Не стесняйтесь закрывать от посторонних клавиатуру банкомата, а особо любопытных — попросить отойти, а лучше всего, одной рукой закройте сверху клавиатуру (так как мошенники могут установить микрокамеру на банкомате), а другой введите пин-код.
3. Снимать деньги лучше стараться в банкоматах, которые расположены либо в офисах Банка, либо рядом с офисами банков (эта территория просматривается видеокамерами служб безопасности банков и мошенники стараются туда не соваться), а в ряде стран (особенно на Украине, Болгарии, Венгрии, Польше, странах Юго-Восточной Азии) наличные лучше снимать в кассах банков, а не в банкоматах.
4. Не пользуйтесь советами третьих лиц и не прибегайте к помощи незнакомцев при возникновении проблем в работе с банкоматом — сразу звоните в службу поддержки клиентов банка, телефоны которой, как правило, указаны на банкомате.
5. Если у вас возникли любые вопросы по расчетам по карте, позвоните в клиентскую службу или обратитесь к сотрудникам банка.
6. Если карта утрачена или у вас есть подозрения, что данные карты стали известны третьему лиц, немедленно позвоните в банк и заблокируйте карту. Сделать это можно в любое время дня и ночи.

7. Если вы подключены к сервису «Мобильный банк», то блокировку карты можно сделать и при помощи SMS, отправив короткое сообщение на специальный номер.
8. Пользуясь картой в Интернете, особенно внимательно отнеситесь к своевременному обновлению антивирусной защиты.
9. Не совершайте покупки на подозрительных сайтах, обратите внимание на поддержку сайтами, на которых вы совершаете покупки, технологии 3D-Secure (наличие данной технологии обозначено на сайтах логотипами Verified by Visa и MasterCard SecureCode). Данная технология позволяет подтвердить совершаемую вами операцию одноразовым паролем, который вы получите на ваш мобильный телефон, либо можете распечатать на чеке в банкомате или информационно-платежном терминале.
10. Не держите на карте, которую используете для интернет-платежей, большие суммы. Для крупных покупок дешевле и безопасней выпустить «виртуальную» карту. Эту услугу предоставляют всё больше и больше банков, в частности, «Альфа-банк».
11. Обратите внимание на возможность страхования вашей банковской карты. Это поможет вам вернуть денежные средства в ряде случаев: например, если вы потеряли карту и ею воспользовались мошенники либо если данные карты были похищены; если вы сняли средства с карты и в течение двух часов после снятия они были у вас похищены и т.д. При подключении к программе страхования, финансовые средства на банковской карте будут под защитой 24 часа в сутки в любой точке мира.
12. В банке, который выдал Вам карту, подключить услугу «СМС-информирование». По любой операции по Вашей карте будет из банка приходит смс-сообщение на Ваш мобильный телефон, это позволит Вам контролировать операции в он-лайне. Такую услугу предоставляют фактически все крупные банки.
13. Установите лимит (дневной) снятия наличных денег с карты. Для этого необходимо обратиться в обслуживающий Вас банк с заявлением.

Скиммер

Для простого пользователя обнаружить скиммер на банкомате непросто. Чаще всего его вид и размеры которого подгоняются под определённый вид банкомата и на вид практически неотличимы от его конструктивных деталей.

На что следует обратить внимание? На банкомате не должно быть ничего постороннего и добавленного (рекламных блоков, брошюр, полочек) — всё это неродные элементы банкомата. Клавиатура для ввода не должна выделяться (возможно, это накладка), и не должно быть никаких мелких отверстий в корпусе (это может быть камера). Все банкоматы всегда антивандальные, поэтому можно смело дёргать любые элементы: если что-то отвалится, то это явно не родная деталь. Также рекомендуем заглядывать в щель картоприёмника — она должна быть ровная. Если там что-то есть, похожее на считывающую головку на кассетном магнитофоне, будьте уверены — это скиммер.

Желательно выбирать банкоматы внутри отделений банков или в крупных торговых центрах — там, где работают системы видеонаблюдения и охрана. Установить скиммер в таких местах весьма проблематично.

14. Когда Вы расплачиваетесь в магазине или ресторане, не выпускайте карту из виду. Попросите, чтобы слип прокатали в Вашем присутствии. Пусть принесут импринтер или сами подойдите к кассе. Иначе с Вашей карты могут снять копию, а подделать Вашу подпись не составит труда.
15. Если в магазине Вам прокатали слип, но Ваш банк не дал авторизацию или Вы передумали делать покупку, проследите, чтобы Ваш слип был уничтожен ПРИ ВАС. Ведь это оттиск Вашей карты! Если первый слип плохо пропечатался, обязательно заберите бракованную квитанцию!
16. Проверяйте выписку по карте не реже одного раза в месяц. В этом случае Вы успеете выставить претензию своему банку, а он — платежной системе. Существуют строго оговоренные сроки, в течение которых Вы можете что-то предпринять.

Кроме того:

- старайтесь пользоваться привычными банкоматами или выбирайте банкоматы в крупных торговых центрах или отделениях банка; постарайтесь не пользоваться «подозрительными» банкоматами или банкоматами, которые расположены на улице;
- перед использованием банкомата осмотритесь вокруг, не следует использовать «пластик» в присутствии подозрительных людей, или если банкомат выглядит небезопасно или слишком изолированно;
- ни в коем случае никому не сообщайте ПИН-код к своей пластиковой карте, ни сотруднику банка (они, кстати, его НИКОГДА не требуют), ни отзывчивому прохожему, который изъявляет желание помочь вам с банкоматом, в случае возникновения у вас каких-либо проблем;
- следует убедиться, что люди, которые ожидают своей очереди снять деньги, находятся на достаточном от вас расстоянии; в любом случае постарайтесь прикрывать рукой клавиатуру, когда вводите свой ПИН-код;
- банкомат не должен выглядеть подозрительно; следует проверить, не прикреплены ли к банкомату какие-либо дополнительные устройства (скиммеры); на экране банкомата не должно быть никаких дополнительных инструкций, а также вызывающих сомнение пустых экранов;
- не позволяйте никому отвлекать вас при пользовании банкоматом, не откликайтесь на предложение о помощи в совершении операции или разрешения какой-либо другой сложившейся ситуации;
- воспользуйтесь другим банкоматом, если требуется усилие для погружения карты в отверстие банкомата, или в случае, если вы чувствуете, что банкомат работает не так, как обычно;
- немедленно сообщите в банк по телефону горячей линии, если ваша карта осталась в банкомате или с ней что-либо произошло, в случае если вы не помните телефон своего банка, то обратитесь в другой банк (телефон должен быть указан на банкомате). В случае обращения в другой банк необходимо помнить номер карты, поэтому сохраняйте отдельно номер вашей карты;
- также необходимо регулярно проверять выписки с вашего банковского счета, а также остаток по карте; в случае малейшего несоответствия необходимо незамедлительно обратиться в банк за разъяснениями;
- в некоторых случаях целесообразнее заплатить комиссию за снятие наличных средств в чужом банкомате, нежели пользоваться сомнительными устройствами для получения наличных в «своём».