***Р У С С К И Й К А Р Т И Н Г*** .

Каким бы ты крутым кардером ни был, тебе все равно далеко до нашего родного правительства, Центрального банка и других российских банков.

Самая крупная кардерская акция была проведена 17 августа 1998 года.

Схема такова: Банки эмитируют (выпускают то бишь) свои собственные карты. Граждане открывают счета в банках и несут туда свои кровные. Через некоторое время правительство объявляет, что временно приостанавливает выплаты по внешним долгам и ценным бумагам, банки вслед за правительством объявляют, что временно приостанавливают операции по счетам и пластиковым картам. А, как известно, нет ничего более постоянного, чем временное... В результате банки получают твои денежки, а у тебя остается пара-тройка красивых сувениров в виде карточек с магнитной лентой и красивыми выдавленными на пластике буковками.

Так что чего же хакерам бояться, если на самом верху сидят такие крутые взломщики.

Всем бы такую крышу!

И снова кардинг. Российский опыт

Автор: Иван Говнофф

Много, много говорилось у нас о кардинге. А если взять Интернет, то там вообще каждый человек, сгенеривший себе номер кредитки, уже считает себя кардером. На самом деле, кардинг, это скорее наука, со своей спецификой, постоянными открытиями, построенная на изучении платежных систем разных государств. В этой статье мы попытаемся описать некоторые случаи мошенничества с расчетными (a.k.a. кредитными, пластиковыми) картами, специфические именно для России. Цель статьи - конечно же, сугубо профилактическая, показать, как несовершенны и небезопасны расчеты с использованием карт.

Для начала назовем вещи своими именами: воровство есть воровство и, как все воровство, - уголовно наказуемое. И хоть кража с использованием компьютера совсем не то же, что кража кошелька из сумки в магазине, нужно помнить, что это присвоение чужого, а, соответственно, при проигрыше в этой игре "кто умнее, милиция или я», тебя ждет тюрьма.

Первое, что говорят любые грамотные хакеры - нужно по возможности лучше разбираться в технологии функционирования платежной системы, использующей расчетные карты.

Немного истории. Почему возникли расчетные карты? Потому что людям удобно не ходить с крупной суммой денег, а использовать некий инструмент, позволяющий снимать со счета именно ту сумму, которую хочется потратить. Кроме того, уменьшится привлекательность грабежей: чужой картой воспользоваться трудно, так как ее блокируют по первому же звонку потерпевшего.

Немного технологии. Что происходит, когда ты совершаешь покупку по карте? Сначала продавец регистрирует параметры карты (номер, срок действия, иногда сверяет имя на карте с документом). Затем он обращается в центр обработки карт (так называемый процессинговый центр) за так называемой авторизацией транзакции. Как это выглядит: продавец сообщает, что он собирается совершить по данной карте транзакцию на сумму, скажем, $475. В ответ он либо получает так называемую авторизацию, либо отказ (возможны и другие варианты развития событий - например, приказ изъять карту). В данном случае авторизация - это просто число. Продавец регистрирует это число, и для него оно - гарантия того, что деньги он получит несмотря ни на что. При этом (почти всегда) требуемая сумма считается уже потраченной тобой, даже если ты вдруг решишь не совершать эту покупку. То есть эти деньги будут на твоем счету заморожены. Только в конце расчетного периода (обычно - 30 дней) ты снова сможешь распоряжаться этой суммой. Обращение в центр обработки карт может быть самым разнообразным - касса может сделать все сама или продавец может позвонить туда голосом. Это два крайних случая, возможно множество промежуточных вариантов. Все вышесказанное справедливо как для покупки по карте "живьем", так и для покупки через internet или по телефону/факсу. Подытожим. Важно понимать следующее:

1. Продавец обращается не в банк, выдавший карту, а в местный центр обработки карт. Банк, выдавший карту, может быть хоть в Парагвае. Центр обработки находится, как правило, в одном из местных банков.

2. Продавец не может узнать, сколько денег у тебя на счету. Он даже не может узнать, есть ли у тебя нужная ему сумма. Все, что он может, это попытаться получить авторизацию на нее.

3. Если продавец получил авторизацию на требуемую сумму, эта сумма на карточном счету замораживается. В случае легального использования карты это всего лишь мелкая неприятность, но становится проблемой при нелегальном использовании карты - уменьшается сумма, которую можно потратить, потому что аннулировать авторизацию - большой геморрой, и продавцы редко соглашаются это делать.

Начнем сначала. Где хакеры берут карты. Вариант с копанием в мусоре (по-английски это называется trashing от trash = мусор) - в местных условиях им не подходит. Вообще хакеры не любят связываться с картами местных банков - здесь у банков фашистские условия, игра не стоит свеч. Самый простой способ - это попросить друга в Америке "списать" у знакомого бармена/официантки/продавщицы несколько номеров и имен с чужих карт.

Второй распространенный способ - взламывают какой-нибудь internet site, где недоумки оставляют номера своих карт (правда, для этого надо либо самому быть компьютерным взломщиком, либо иметь друзей-взломщиков, причем настоящих, а не болтунов, которых 99%).

Или - самый распространенный способ, которым пользуются грамотные хакеры: они открывают собственный сайт в Интернете, чаще всего порно-сервер. Все это делается с заголовками типа «У нас самые большие сиськи во всем Интернете и всего за $5,95 на 3 месяца!». Оплату доступа, естественно, делают по карте. Самое удивительное - это то, что идиотов хватает, уж поверь! Правда, для этого нужно уметь делать internet-site'ы и как следует поработать.

В общем, главное в любом деле - думать и работать. Кстати, надо добавить, что из-за фантастических масштабов мошенничества многие организации, принимающие карты по телефону/факсу/internet'у (то есть не имеющие возможности лично удостовериться в том, что ты - действительно владелец карты), требуют какую-нибудь специальную личную информацию, которую мошенник знать не должен бы. Например, его почтовый индекс (zip code). Или девичью фамилию матери. Таких мест мошенники избегают.