К уже традиционным видам карточного мошенничества постепенно добавляются усовершенствованные виды несанкционированного снятия денег с пластика.

По оценкам банкиров, удельный вес убытков от мошенничества в Сети пока не превышает нескольких процентов в общем объеме потерь от липовых операций. Но размер ущерба от этого вида мошенничества ежегодно возрастает в несколько раз. За последнее время жулики изрядно поднаторели и в краже персональных данных клиентов с серверов интернет-магазинов, развлекательных и игровых сайтов. К примеру, аферисты нередко занимаются технической "доработкой" сайтов интернет-магазинов. Над формой для отправки реквизитов карты они размещают собственную форму. В результате клиент вводит персональные данные в липовое окно и отправляет их мошенникам. "Другая схема, получившая распространение, - регистрация сайтов-клонов, созданных специально для сбора данных. Мошенники создают сайт, абсолютно идентичный тому, на котором совершаются покупки. Отличие можно заметить лишь по незначительным изменениям в названии сайта (в адресной строке браузера), замене слешей точками, подмене букв и т.д. Клиенты заходят на сайт-клон и оставляют там свои персональные данные, которые потом уходят к злоумышленникам", - рассказывает в.и.о. председателя правления Конверсбанка Вениамин Лебедев.

Но чаще всего клиенты становятся жертвами испытанного временем фишинга (получение конфиденциальных данных с помощью рассылки поддельных сообщений от лица банков, провайдеров, платежных систем и пр.). "Одна из последних атак, с которой мы столкнулись, проводилась через украинские сайты поиска работы. На них размещались объявления о возможности легкого заработка в Интернете. Для этого необходимо было зарегистрироваться на определенном сайте, ввести данные карты (номер, срок действия, CVV2-код). Для большего доверия мошенники даже ставили логотип Portmone.com и ссылались на нас как на партнеров", - рассказывает Юлия Кащенко, маркетинг- и PR-менеджер Межбанковской системы электронной доставки и оплаты счетов Portmone.com.

Отдельный вид мошенничества, который сейчас набирает обороты, - всевозможные вирусы, "трояны" и "черви", ворующие информацию из банкоматов, платежных терминалов и даже персональных компьютеров. Самое масштабное мошенничество такого рода недавно было зафиксировано в соседней России, где вирус поразил терминалы одной из крупнейших российских платежных систем - Qiwi.

Чтобы защититься от мошенников, банкиры советуют использовать для расчетов в Интернете так называемые виртуальные карты с ограниченной суммой на счету. "Мы рекомендуем вносить на такую карту только сумму, необходимую для оплаты покупки или услуги через Интернет. Причем лучше всего это делать непосредственно перед проведением планируемой трансакции", - советует Юлия Морозова, директор департамента развития карточного бизнеса VAB Банка.

Но львиная доля убытков от мошенничества с пластиком по-прежнему приходится на испытанные временем трюки, такие как подделка карт (skimming) с помощью кражи персональных данных клиентов через специальные устройства на банкоматах или терминалах. "В течение последнего квартала буквально раз в неделю (а то и чаще)

фиксируется снятие с банкоматов специальных накладок, которые применяются для считывания информации с магнитной полосы карты, и компрометация (получение третьим лицом информации) ПИН-кода с использованием видеокамеры или поддельной клавиатуры для ввода кода", - рассказал "k:" директор Украинской межбанковской ассоциации членов платежных систем "ЕМА" Александр Карпов. Банкиры сталкиваются и со случаями более изощренного мошенничества, один из которых установка в торговых центрах фальшивых банкоматов. "Очень важно обращать внимание на внешний вид банкомата, наличие в нем неестественных, "наложенных" деталей и устройств. Если есть хоть малейшее сомнение - пользование банкоматом недопустимо", - предупреждает Оксана Лаговская, директор департамента карточного бек-офиса главного операционного управления Правэкс-Банка.

Еще одной масштабной аферой, вошедшей в топ-пять в прошлом году, стала атака жуликов на зарубежные банки. "Украина была задействована для обналичивания украденных мошенниками средств с использованием платежных технологий. При этом злоумышленники использовали примитивную схему, где в обналичивании участвуют платежные карты украинских банков-эмитентов, оформленные на подставных лиц. Так, ряд граждан Украины умышленно и за вознаграждение оформляют на себя платежную карту, которую передают для использования мошенникам", - рассказывает Сергей Досенко, заместитель директора департамента экономической безопасности Альфа-Банка (Украина).

Источник: http://smi.liga.net