

Будьте осторожны - СКИММИНГ

Нет ни одного застрахованного человека от кражи или потери банковской карты. Однажды и вы можете оказаться в числе тех, с чьих карточек испарились деньги. В России еще не особо высок уровень по карточному мошенничеству. Это потому что в нашей стране граждане еще не особо доверяют картам и используют их только для снятия наличных. Тем не менее, численность владельцев банковских карт постепенно растет, и закономерно, что этот сегмент привлекает все более пристальное внимание преступников.

С магнитной полосы банковской карты при помощи специального устройства считывается содержащаяся на ней информация. Как правило, оно прикреплено к слоту, который принимает карту в банкомате. Одновременно с помощью мини-видеокамеры или специальной наклейки на клавиатуру фиксируется PIN-код. Часто такие устройства оснащены автономными портативными передатчиками, способными транслировать украденные данные на расстояние до 200 метров. Такие устройства называют «скиммерами».

В дальнейшем записанные с магнитной полосы данные мошенники эмбоссируют (наносят) на свои пластиковые заготовки. Чаще всего этим занимаются группы профессиональных мошенников, которые передают данные вашей карты за границу, где их сообщники изготавливают дубликат карты и снимают ваши деньги, причем от момента считывания информации с вашей карты до момента снятия с нее денег мошенниками проходит всего полчаса. Вернуть деньги после такого способа мошенничества практически невозможно.

Злоумышленники прибегают к различным ухищрениям для того, чтобы замаскировать прикрепленные к банкомату считывающие устройства. Дизайн скиммингового оборудования подбирается таким способом, чтобы у потерпевшего не возникло мысли о наличии накладок.

Вот так выглядят наклейки на банкоматы:





Иногда злоумышленники монтируют миниатюрную видеокамеру на самом банкомате либо в непосредственной близости от него для того, чтобы фиксировать, какой ПИН-код набирает потерпевший.

Пример монтажа видеокамеры представлен на следующих иллюстрациях:



Участились случаи использования скимминговых устройств в торговых точках нечестными на руку продавцами и официантами. Потерпевший передает карту для оплаты, продавец при помощи миниатюрного устройства считывает данные магнитной полосы, а при помощи наклейки на клавиатуру ПОС-терминала — ПИН-код карты. Наиболее часто такие продавцы встречаются в местах массового скопления туристов. На иллюстрации изображен один из видов миниатюрного скиммингового устройства:



Для того, чтобы минимизировать шансы стать жертвой высокотехнологичных преступников, необходимо внимательнее относиться и к своей банковской карте, и к местам, где Вы ей расплачиваетесь и стараться следовать следующим советам:

- Старайтесь пользоваться банкоматом внутри банковских отделений, хорошо просматриваемых помещениях и.т.д. Мошенники редко ставят свои устройства на банкоматах, которые могут находиться под наблюдением, часто посещаются банковскими или инкассаторскими службами. Какой смысл устанавливать дорогостоящее оборудование, если его могут снять в тот же день.
- Старайтесь снимать деньги в одних и тех же банкоматах и хорошенько запомните его внешний вид. Как правило, любые изменения банкоматов никак не затрагивают его внешний вид. Если Вы заметили «новую деталь» на банкомате – не пользуйтесь таким банкоматом.
- Не стесняйтесь попробовать оторвать с банкомата все подозрительные детали вокруг щели для карточек, постучать по клавиатуре. Если какие-то элементы отваливаются или прикреплены не очень хорошо - ни в коем случае не пользуйтесь банкоматом. Помните, что это самый надежный способ избежать скимминга.
- Ни один банк никогда не повесит на свой банкомат оповещение о том, что инструкция по использованию, выводимая на экран, была изменена.
- Не используйте устройства, которые требуют ввода пин-кода для доступа в помещение, где расположен банкомат.
- Выработайте в себе привычку внимательно смотреть на прорезь для карты. Если Вам кажется, что в районе этой прорези присутствуют выступающие элементы, либо рамка прорези заметно выступает, можно попробовать легонько пошатать её пальцами. Если это накладка, она оторвется или будет шататься.
- Никогда не вставляйте карту в прорезь с усилием. Если чувствуете, что банкомат работает не как обычно, нажмите клавишу отмены и заберите Вашу банковскую карту.
- Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой в банкоматах.
- Если при проведении операций с банковской картой в банкомате банкомат не возвращает банковскую карту, следует позвонить в кредитную организацию по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, а также следует обратиться в кредитную организацию - эмитент банковской карты (кредитную организацию, выдавшую банковскую карту), которая не была возвращена банкоматом, и далее следовать инструкциям сотрудника кредитной организации.
- Смотрите внимательно на «козырёк» банкомата.
- Не сообщайте свой пин-код никому, даже если человек представляется сотрудником вашего банка.
- При наборе пин-кода убедитесь, что стоящий сзади Вас человек не может подсмотреть код через ваше плечо. Лучше всего для снятия денег использовать банкомат, у которого есть выпуклое зеркало. Тогда Вы сможете видеть, что происходит за Вашей спиной.
- Обязательно забирайте чеки и ведите учет операций, вы могли сравнить чеки из банкоматов с ежемесячной выпиской. Регулярно проверяйте выписки по Вашему счету карты. Мошенники не всегда снимают деньги сразу.
- Вы можете обратиться в банк за установлением ежедневного или ежемесячного лимита расходования по Вашей карточке.
- Подключите услугу «SMS-информирования по операциям с использованием банковской карты». С помощью данной услуги можно контролировать состояние своего счета банковской карты и вовремя заметить посторонние списания.
- Не используйте банковские карты в организациях торговли и услуг, не вызывающих доверия.
- Требуйте проведения операций с банковской картой только в Вашем присутствии. Это необходимо в целях снижения риска неправомерного получения Ваших персональных данных, указанных на банковской карте.
- В случае если при попытке оплаты банковской картой имела место "неуспешная" операция, следует сохранить один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.

Если Вы заметили несанкционированные операции с использованием Вашей карты или её реквизитов, необходимо выполнить следующие действия:

- Незамедлительно сообщить в Службу клиентской поддержки по круглосуточным телефонам **+7 (495) 139-43-04** и заблокировать карту.
- Оформить в Банке заявление о факте неправомерного использования Вашей карты.
- Оформить в банке заявление по оспариваемым операциям.
- Оформить в Банке заявление о перевыпуске карты с новым номером и новым пин-кодом.