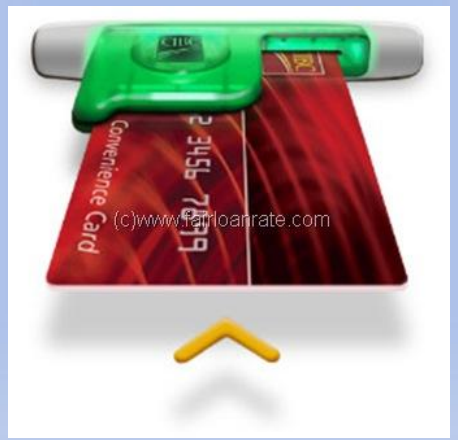
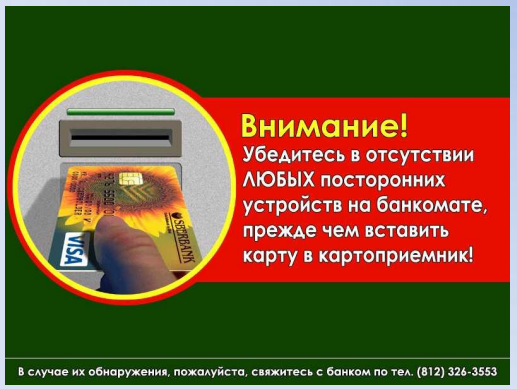
ОСТОРОЖНО!!!

Скимминг





2013 г.

СКИММИНГ – вид мошенничества с банковскими картами, при котором используется скиммер - инструмент для считывания, например, магнитной дорожки платёжной карты. При осуществлении данной мошеннической операции используется комплекс скимминговых устройств:

- Инструмент для считывания магнитной дорожки платёжной карты представляет собой устройство, устанавливаемое на картоприёмник банкомата или на картридер у входной двери в зону обслуживания клиентов в помещении банка. Представляет собой устройство со считывающей магнитной головкой, усилителем-преобразователем, памятью и переходником для подключения к компьютеру. Скиммеры могут быть портативными, миниатюрными.
- Миниатюрная видеокамера, устанавливаемая на банкомат и направляемая на клавиатуру ввода в виде козырька банкомата либо посторонних накладок, например, рекламных материалов. С помощью видеокамеры происходит наблюдение за набором пин-кода в целях его хищения.
- Фальш-клавиатура, которая может использоваться для хищения пин-кода карты вместо мини-видеокамеры. Фальш-клавиатура устанавливается поверх штатной клавиатуры банкомата таким образом, что при нажатии на её кнопки прилагаемые усилия передаются на кнопки настоящей клавиатуры. Однако в момент нажатия на кнопки происходит регистрация номеров кнопок и последовательность их нажатия.

Данные устройства питаются от автономных источников энергии — миниатюрных батарей электропитания, и, для затруднения обнаружения, как правило, изготавливаются и маскируются под цвет и форму банкомата.

Скиммеры могут накапливать украденную информацию о пластиковых картах, либо дистанционно передавать ее по радиоканалу злоумышленникам, находящимся поблизости.

Шимминг, представляет собой разновидность скимминга. В этом случае в картридер банкомата помещается электронное устройство (шиммер), позволяющее получить информацию о банковской карте. Толщина шиммера — порядка 0,2 мм. Внешнее определение использования шиммера крайне затруднено. В настоящий момент единственной действенной защитой от шимминга является использование чиповых пластиковых карт.

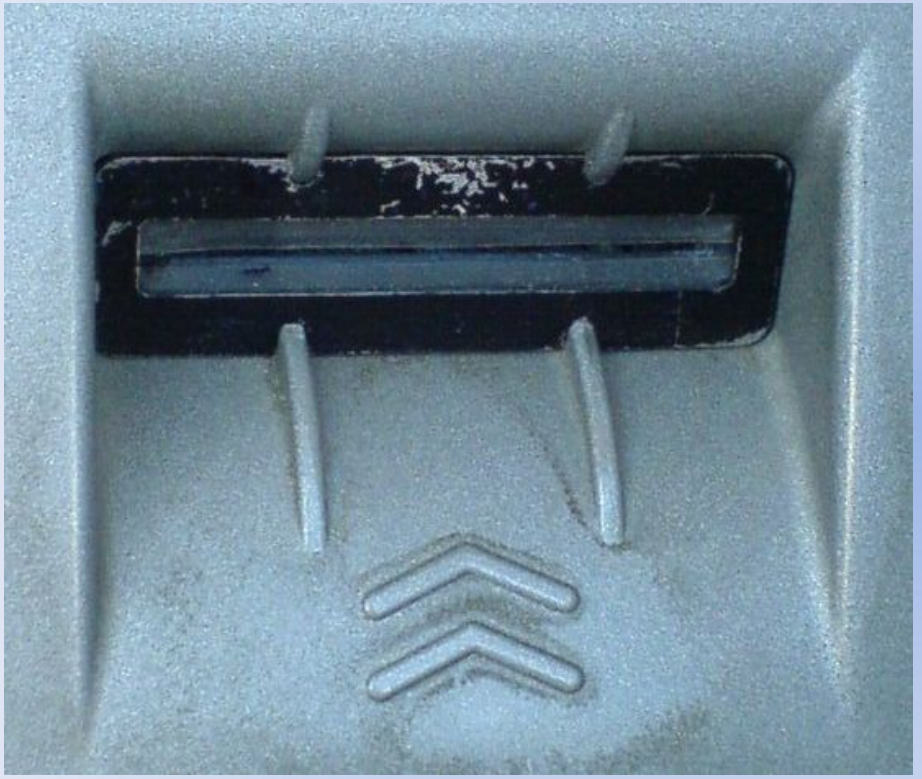
Вид банкомата

Картоприемник, в нормальном исполнении

Следы установки скиммера в банкомате

Вид скиммера, извлеченного из банкомата

Вид картоприемника банкомата



со скиммером и без него

Способ установки скиммера внутри банкомата под картоприемником через предварительно вырезанное отверстие, маскируемое рекламной наклейкой

Остатки клея, место установки видеокамеры

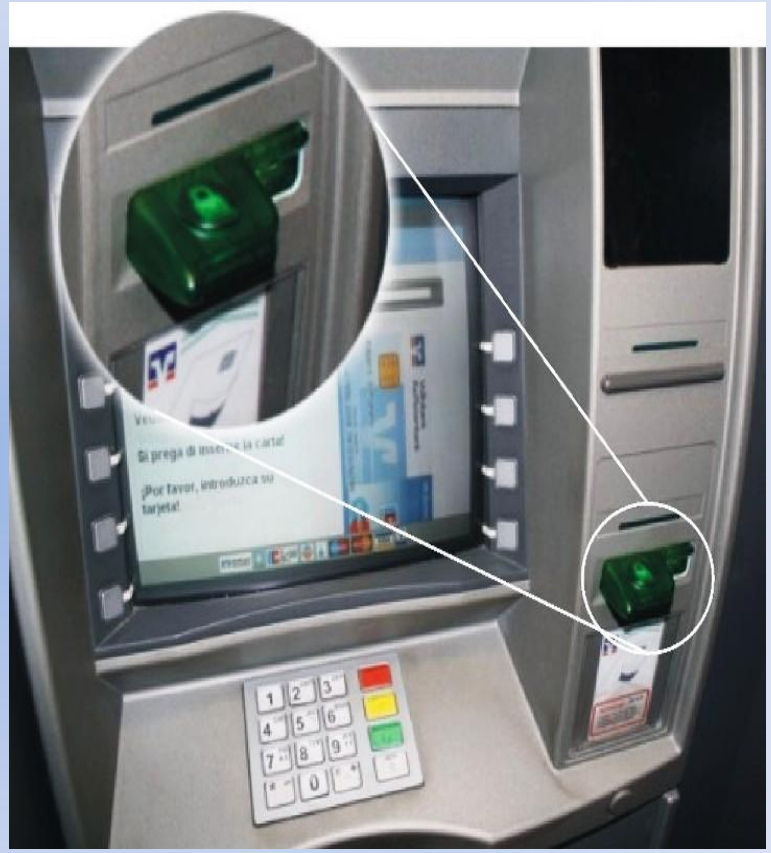
Накладка с видеокамерой

Замаскированное скимминговое оборудование

Накладка на клавиатуру

Поддельная полноформатная панель клавиатуры и накладка со скиммером

Антискиммингговая накладка



Поддельная антискимминговая накладка

Установка скиммера непосредственно на штатную антискимминговую

Нештатное оборудование, обнаруженное на банкомате NCR 6632 Западно-Сибирского банка (ноябрь 2012 г.)

Вид банкомата NCR 6632 в нормальном исполнении

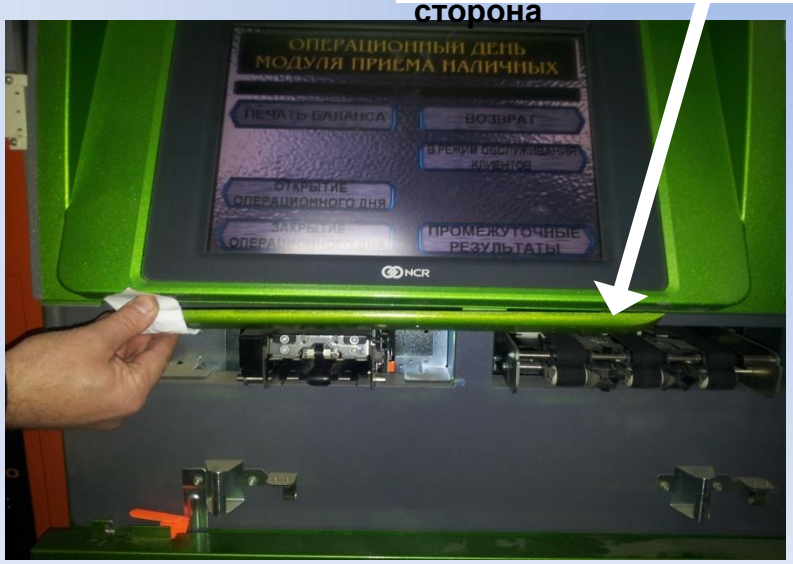
Вид банкомата NCR 6632 с нештатными накладками

Нештатное оборудование, обнаруженное на банкомате NCR 6632 Западно-Сибирского банка (ноябрь 2012 г.)

Нештатная накладка на картридер, выполненная в виде стандартной антискиминговой накладки

Внутренняя сторона нештатной накладки на картридер

Накладка с минивидеокамерой и её внутренняя сторона



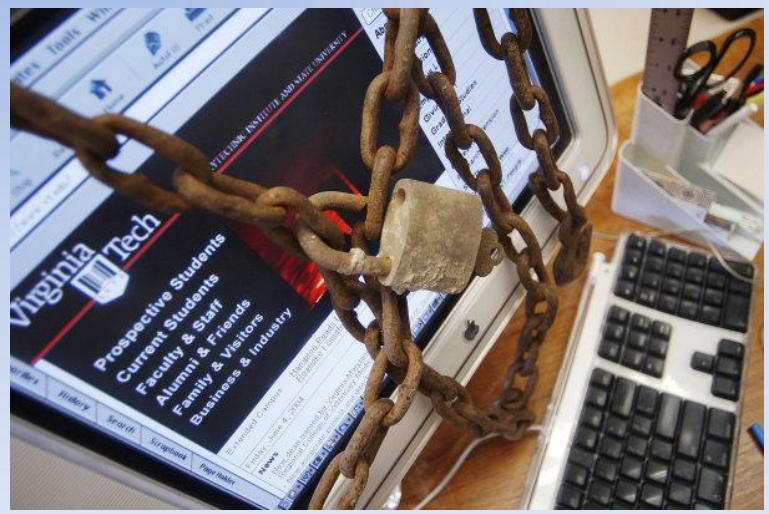
Видеокамера, замаскированная в буклетницу

Комплект скимминговой оборудования, вленный на ИПТ

Видеокамера для записи ПИН-кода вмонтирована в накладку на штатный выступ, в котором расположена камера купюроприемника.
Наличие камеры можно определить по небольшому отверстию с внутренней стороны выступа.

Устройство для копирования данных с магнитной полосы вмонтировано в накладку на внешнюю часть картоприемника.

Меры предосторожности



Старайтесь пользоваться банкоматом внутри банковских подразделений, в 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.

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.

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 оторвётся 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.

Смотрите внимательно на «козырёк» банкомата, на клавиатуру и картоприемник .

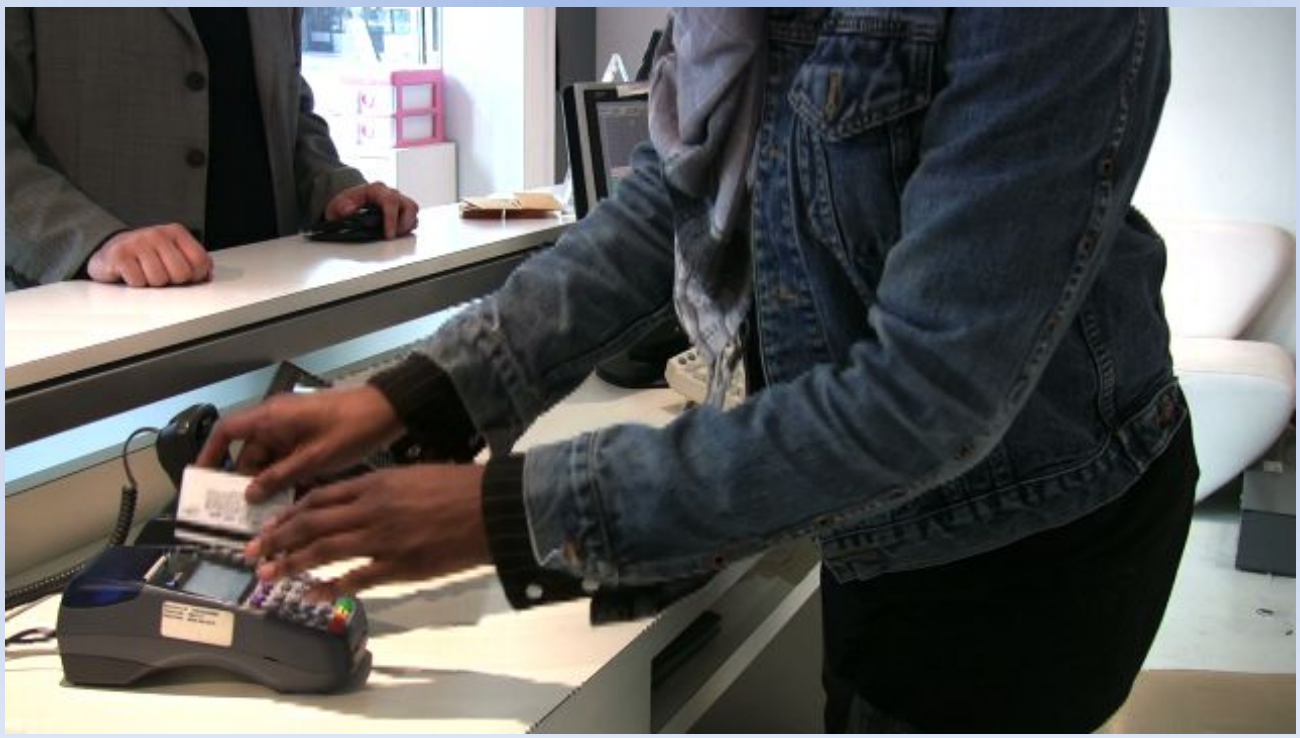
Не сообщайте свой пин-код никому, даже если человек представляется сотрудником банка

При наборе пин-кода убедитесь, что стоящий сзади Вас человек не может подсмотреть код через ваше плечо. Обязательно забирайте чеки. Регулярно проверяйте выписки по Вашему счету карты. Мошенники не всегда снимают деньги сразу.

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.



И помните, что лучшая защита в сохранении своих и чужих денег - это
конфедициальность , осторожность и внимательность
в совершении каких-либо действий.