БЕЗОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ БАНКОМАТОВ И ТЕРМИНАЛОВ

Светличный В.А., Онищенко Ю.Н.

Харьковский национальный университет внутренних дел, Харьков, Украина

В работе рассмотрены вопросы безопасного использования банкоматов и терминалов при осуществлении финансовых транзакций. Показаны наиболее распространенные типы оборудования, используемые мошенниками для установки в банкоматы и терминалы. Сформированы правила безопасности при использовании пластиковых банковских карт.

Ключевые слова: *банкомат, ATM - Automated Teller Machine, терминал, банковская платежная карта, скимминг, скиммер, шиммер, ПИН - код, диспенсер, картридер, ActivEdge, компьютер, смартфон, Secure Revolving System*

Введение

На сегодняшний день постоянно используется множество различных высокотехнологичных устройств: компьютеров, смартфонов, банковских платежных карт, терминалов, банкоматов и т.д. Любой банкомат (или ATM - Automated Teller Machine) представляет собой компьютер, совмещенный с сейфом. Компьютер, как правило, оснащен устройством ввода, дисплеем, картридером (устройством для чтения данных с пластиковой карты), презентером (для выдачи кэша) и чековым/журнальным принтером. Самым важным устройством в банкомате является диспенсер - устройство, предназначенное для выдачи/получения денежных купюр, проверки их подлинности и сортировки.

Постоянно появляются новые модели, программы и сервисы. Все это делает нашу жизнь удобнее, но требует определенных навыков и знаний. К сожалению, одновременно с развитием таких устройств появляются виды мошенничества, которые позволяют присвоить денежные средства граждан. Чтобы не поддаться на уловки злоумышленников, достаточно знать, как они действуют, и соблюдать правила безопасного использования устройств.

Основной текст

Целью работы является формирование рекомендаций и правил для безопасного использования в банкоматах и терминалах платежных карт с магнитной полосой.

Аналитические исследования, проведенные в 2016 году экспертами американской компании Visa Inc., показали, что лидерами среди незаконных операций с банковскими картами являются скимминг и online - мошенничество.

Скимминг (от англ. skim - снимать сливки) - создание копии магнитной полосы для изготовления клона карты пользователя с помощью специализированных накладных или вставляемых внутрь картридера устройств, которые соответственно называются скиммер или шиммер. Именно такие устройства мошенники чаще всего устанавливают на терминалы и банкоматы. Скимминг представляет собой накладку на картридер и содержит электронику, предназначенную для считывания данных магнитной полосы и хранения или передачи этих данных по радиоканалу. Выглядеть скиммер может как угодно, и держатель карты крайне редко может его распознать, тем более что обычно скиммер маскируется под штатную накладку на картридер конкретной модели банкомата. Тем более что внешний вид различных банкоматов настолько различается, что подозрений по поводу накладок не возникает. Практически всегда скимминговое устройство комплектуется накладкой на клавиатуру или миниатюрной беспроводной камерой. Это необходимо злоумышленникам для того, чтобы узнать ПИН-код карты.

По принципу действия скиммер и шиммер не отличаются друг от друга. Однако, в шимминге вместо традиционной относительно громоздкой накладки на картридер банкомата, используется очень тонкая, гибкая плата, устанавливаемая внутрь картридера банкомата. Шиммер «подсаживается» с помощью специальной карты-носителя: ее просовывают в щель банкомата, где тонкий шиммер присоединяется к контактам, считывающим данные с карт, после чего карта-носитель удаляется. Далее все работает, как и при традиционном скимминге, то есть пользователь банковской карты вставляет в картридер банкомата карту, где шиммер считывают все необходимые данные, которые затем используются злоумышленниками для производства карт-дубликатов и снятия с их помощью денежных средств. Единственное, но очень важное отличие шимминга от скимминга состоит в том, что нет заметных демаскирующих внешних признаков того, что в банкомате установлен шиммер. Все дело в том, что толщина шиммера не должна превышать 0,1 мм, в противном случае он будет мешать пластиковым картам. Это в два раза толще средней толщины человеческого волоса.

Активизация защитных мер против скимминга на Западе способствует тому, что злоумышленники ищут новые рынки и приходят, в том числе и в Украину. Несмотря на то, что банки-эквайеры (банки собственники банкоматов) многое делают для того, чтобы злоумышленникам становилось с каждым годом все сложнее воровать деньги с пластиковых карт. А именно: регулярный осмотр банкоматов на наличие скиммеров; установка прозрачных антискимминговых накладок и система блокировки скомпрометированных карт, работа которой заключается в том, что если хотя бы от одного пользователя банковской карты поступала информация об обнаружении скиммерных накладок, то блокируются все карты, которые прошли через этот банкомат за определенный период времени,

например за сутки. Однако, последний способ очень неудобен, так как пользователям карт приходится ехать в банк для получения новых карт, поскольку их старые были заблокированы. Значительно результативнее, технические решения активного и проактивного типа.

Активное техническое решение подразумевает установку небольших генераторов электромагнитных помех, устанавливаемых внутрь банкомата вблизи картридера. Их излучение выводит из строя или блокирует работу радиомодулей скиммеров и шиммеров, но при этом и стоит значительно дороже, чем прозрачные антискимминговые накладки.

Более целесообразно использовать технические решения, позволяющие фиксировать предметы, оставленные на поверхности банкомата. В основе этих технологий лежит компьютерный анализ видеоданных и систематизирование информации, получаемой от штатных и дополнительно установленных камер видеонаблюдения. Кроме контроля монтажа скиммеров и последующего блокирования работы банкомата или терминала, видеоаналитика позволяет обеспечивать безопасность сотрудников банков. Так, при инкассации банкомата просчитывается скорость движения людей в зоне наблюдения, и в случае нападения на инкассаторов срабатывает экстренное оповещение полиции и центра наблюдения службы безопасности банка.

Системы проактивной защиты рассчитаны на усложнение работы картридера, либо на обнаружение каких-либо несанкционированных действий с банкоматом. Еще в 2013 году компания MB Telecom (Румыния) представила механизм защитной поворотной системы (Secure Revolving System, SRS), который работает по следующей схеме: сначала пользователь вставляет карту в банкомат длинной стороной, так, что магнитная полоса располагается параллельно стенке банкомата, после чего механизм поворачивает карту на 90°, чтобы считать информацию с магнитной полосы. В 2014 году известная компания - производитель банкоматов Diebold объявила о разработке собственного картридера ActivEdge, в котором считывающая информацию с магнитной полосы головка двигается перпендикулярно традиционному направлению размещения карты в картридере. Предлагаемое решение позволило сделать установку скиммера бессмысленным. Такое устройство решает основную задачу антискимминга - оно принципиально не дает возможность считать информацию с магнитной полосы пользовательской карты.

Более дешевые проактивные технические решения предполагают установку современных систем охранной сигнализации на базе вибрационных и электромагнитных датчиков. Вибрационные датчики позволяют зафиксировать собственно процесс установки скиммера, а электромагнитные датчики выявляют шиммеры внутри картридера. Если система получает подозрительные показания датчиков, работа банкомата блокируется, и отправляется сигнал в службу безопасности банка.

Выбор системы безопасности банкомата остается за банкирами, а пользователям банковских карт остается на свой страх и риск выполнять финансовые транзакции с банковскими картами.

Выводы

Для владельцев банковских платежных карт с магнитной полосой разработано огромное количество различных инструкций и правил безопасности. Приведем основные из них:

1. При проведении операций с банковской картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д.

2. Обращайте внимание на картридер и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по заранее сохраненным в своем мобильном телефоне номерам банка.

3. В случае некорректной работы банкомата - если он долгое время находится в режиме ожидания или невольно перезагружается - откажитесь от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.

4. Никогда не поддавайтесь помощи и советам посторонних лиц при проведении операций с банковской карты в банкоматах. Свяжитесь с Вашим банком - он обязан предоставить консультационные услуги по работе с картой.

5. Подключите СМС-банкинг и отслеживайте все операции с картой.

6. Если картой воспользовались мошенники, заблокируйте ее и напишите заявление в банк об опротестовании транзакций.

7. В торговых точках, ресторанах и кафе все действия с Вашей картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты с помощью специальных устройств и использовать их в дальнейшем для изготовления клона карты.

Главное - не стоит использовать пластиковую карту для накопления. Это платежное средство, и правильнее всего держать на нем лишь ту сумму, которая необходима для текущих расходов.