Scientific and Practical Cyber Security Journal (SPCSJ) 1(2):54-56
Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667

DANGERS OF USING BANK CARDS WITH CONTACTLESS PAYMENT TECHNOLOGY (PAYPASS, PAYWAVE AND OTHERS)

V.Ivanov, B,Horbatenko, V.Stopin

Kharkiv National University of Radio Electronics (NURE), «Computer science» faculty, department of «System engineering»

ABSTRACT:

Not so far ago, the world saw such a phenomenon as «contactless payments». Bank card, which has PayPass chip inside, proved to be comfortable in everyday using. There is no need to put the card into ATMs or terminals as well as to remember and enter PIN-code, to fill receipts and many other routine staff, which people do not like doing. Developers of this technology guarantee that cards with chip are totally secure and safe payment method, however, is it really so? In this article let's answer on this and some other questions about bank cards with a chip.

KEYWORDS: PayPass, payWave, cyber, security, theft, payment, visa, mastercard

Не так давно свет увидел такое явление, как «бесконтактные платежи». Банковская карта, в которую внедрен чип PayPass, показала себя удобной в использовании. Нет необходимости вставлять карту в банкомат или терминал, помнить и вводить PIN-код, заполнять чеки, и многие другие рутинные занятия, которые не нравятся людям в повседневной жизни. Разработчики данной технологии уверяют, что карта с чипом – абсолютно безопасное средство оплаты, однако, так ли это на самом деле? В этой статье ответим на этот и ряд других вопросах о банковских картах с чипами.

Данная статья несет исключительно ознакомительный характер, а также мероприятия, позволяющие противодействовать злоумышленникам. Никогда не пытайтесь повторить то, что описано в данной статье.

Бесконтактные банковские карты с технологией PayPass (или ее аналогами) используют технологию NFC для передачи данных, а NFC – это разновидность RFID. На карте с данной технологией находится чип и антенна, которые «отвечают» на запросы платежного терминала на радиочастоте 13,56 МГц. Существует множество стандартов бесконтактных

платежей, среди них: Visa payWave, MasterCard PayPass, American Express ExpressPay и так далее, но все они устроены похожим образом и не имеют кардинальных различий в структуре своей работы.

Расстояние, на котором данные карты функционируют и отправляют запросы, составляет около 3-5 см от считывающего устройства. То есть, приложив к терминалу карту на данном расстоянии, вы автоматически оплачиваете покупку без ввода пин-кода и каких-либо дополнительных проверок. Но стоит обратить внимание, что дополнительных проверок не последует, при условии, если не превышается лимит, установленный на сумму оплат посредством бесконтактного платежа. Для разных стран имеются собственные лимиты. Таким образом, в России, по умолчанию доступно ~85$, в Украине – ~38$, США – ~50$. Если указывать сумму для оплаты ниже обозначенного лимита, то никаких подтверждений не требуется.

Злоумышленник, желая заполучить чужие средства, может поступить следующим образом: происходит покупка фиктивной компании или фирмы на фиктивное лицо, обязательным условием является наличие расчетного счета в банке у этой компании. Каким образом это производиться в наше время, и какими средствами, в данной статье описано не будет, но знайте, что выполнить данный пункт очень легко [1]. Далее, злоумышленник приобретает беспроводное средство для проведения платежей (платежный терминал, эквайринг), имеющее доступ к сети, для проведения платежей. Это может быть, как мобильный интернет, так и любые другие средства, которые позволяют получить бесперебойный доступ к сети Интернет. Существует множество модификаций платежных терминалов, у которых усилена антенна передачи данных, более мощный сигнал связи и так далее.

Затем, злоумышленник отправляется в массовое скопление людей (например, торговый центр), где находятся его потенциальные жертвы. Сумма для оплаты в терминале программируется заранее. Злоумышленнику лишь остается положить терминал в тонкую сумку и приблизиться к месторасположению кредитной карты жертвы на расстояние до 5 см. Если карта находится достаточно близко к терминалу, то происходит списывание средств, о чем свидетельствует вибрация или специальный сигнал, что дает понять злоумышленнику, что операция прошла успешно.

Многие банковские системы не предусматривают защиты от повторных транзакций. Таким образом, недобросовестный человек может произвести несколько транзакций с небольшим промежутком времени. При этом, никаких дополнительных проверок или запросов PIN-кода не будет.

Как итог, необходимо обозначить, что использование карт с технологией бесконтактных платежей не является безопасным. Злоумышленник, в примечании к платежу, может написать что-либо непримечательное, обыденное для пользователя. Например, это может быть «обслуживание карты», при этом указывается небольшая сумма, чтобы тем самым не вызвать каких-либо недоразумений при проверке платежей. К сожалению, банковские системы не спешат исключать данные карты из общего пользования. Поэтому необходимо максимально обезопасить себя от возможных попыток списания средств [2]. Следующие советы помогут снизить вероятность списания личных средств с ваших карт без вашего ведома:

1) Храните бумажник в труднодоступных местах.
2) Создайте экранирование вокруг карты, например, обмотайте её фольгой. Она не пропустит сигнал терминала. Таким образом, злоумышленник не сможет выполнить запрос о снятии средств.
3) Приобретите специальный экранированный кошелек.
4) Будьте бдительны и обращайтесь в ваш банк при малейшем подозрении о несанкционированном списании средств.
5) Активируйте моментальное оповещение о транзакциях с вашей картой (смс оповещения, звонки и другое).
6) Измените максимальный лимит транзакции на минимально возможный и приемлемый для вас.
7) Избегайте близкого контакта с людьми имеющие тонкие сумки.
8) Поставьте обязательный ввод пин-кода, если это позволяет ваш банк.
9) Держите вашу кредитку в поле вашего зрения при оплате на кассе или где-то еще.

Данные советы не гарантируют полной безопасности, однако при их соблюдении вы значительно снижаете вероятность мошенничества и проведения несанкционированных платежей. По возможности исключите из использования подобные банковские карты. Не экономьте время, потраченное на подтверждение оплаты услуг, берегите личные средства.

Библиографический список:

1. Cybersecurity and Cyberwar: What Everyone Needs to Know® 1st Edition by P.W. Singer, Allan Friedman
2. Social Engineering: The Art of Human Hacking 1st Edition by Christopher Hadnagy, Paul Wilson