УДК 336.082 **Технические науки**

Мешкова Е.В., Митрошина Е.В. *студентки 4 курса электротехнического факультета,*
Пермский национальный исследовательский политехнический университет

МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

Аннотация. В статье рассматриваются основные виды мошенничества, осуществляющиеся с помощью банковских карт. Также приводятся некоторые рекомендации для безопасного использования пластиковых карт.

Ключевые слова: пластиковая карта, банкомат, скимминг, фишинг, вишинг, траппинг.

Abstract. In an article discusses the main types of fraud carried out using credit cards. Also are some recommendations for safe use of plastic cards.

Keywords: plastic cards, automated teller machine (ATM), skimming, phishing, vishing, trapping.

В последнее время значительно возросла степень использования банковских карт, ведь пользоваться пластиковыми картами, как кредитными, так и дебетовыми, удобно. Так как нет необходимости всегда иметь с собой большого количества наличных денег, при этом средствами, хранящимися на картах, можно распоряжаться в любой момент. Однако пластиковые карты, являясь удобным способом доступа к денежным средствам на своем карточном счете, неизбежно становятся и объектом внимания злоумышленников, стремящихся похитить эти деньги [2].

В настоящее время специалисты выделяют несколько основных видов мошенничества с использованием пластиковых карт. Рассмотрим самые распространенные из них.

1. Скимминг. Этот вид карточного мошенничества заключается в создании так называемых «белых карт» или «карт-клонов». Для создания дубликатов карт используется специальное устройство – скиммер. Скиммер – это маленькая накладка, которую устанавливают или на сам банкомат, или на платежные терминалы - POS-терминал. Это устройство считывает секретную информацию с

магнитной ленты карты пользователя, а затем мошенники изготавливают дубликаты карт - кусочки пластика с магнитной полосой и нанесенной на нее украденной информацией. Чтобы узнать пин-код карты, монтируется скрытая камера или специальная накладка на клавиатуру на панели банкомата, которая запоминает набор цифр. После этого злоумышленники могут свободно пользоваться счетом настоящего владельца карты, которому в свою очередь будет очень сложно доказать свою непричастность к «левым» платежам [3].

2. Фишинг. Не менее популярный вид карточного мошенничества, который заключается в способности злоумышленника нелегальным способом вынудить держателя карт предоставить свои данные. Например, мошенники от имени банка рассылают электронные письма пользователям, в которых сообщают об изменениях, якобы производимых в системе безопасности. При этом злоумышленники просят доверчивых пользователей сообщить информацию о карте, а именно указать номер карты и ее ПИН-код, либо отправив ответное письмо, либо пройдя на сайт банка и заполнив соответствующую анкету. Однако ссылка, прикрепленная к письму, ведет на поддельный сайт, имитирующий работу настоящего, а не на ресурс банка.

3. Вишинг. Это вид мошенничества, который похож на такой вид мошенничества, как фишинг, только в этом случае используется телефон. Вишинг также позволяет красть у клиентов банков конфиденциальную информацию. Например, клиент получает звонок якобы от автоинформатора банка, который сообщает, что с карты пытались незаконно снять денежные средства. Злоумышленники просят перезвонить по указанному номеру. В свою очередь, данный номер является подставным, позвонив по которому ложный сотрудник службы безопасности попросить сообщить или ввести на клавиатуре телефона данные карты.

4. Траппинг. Суть этого способа состоит в установке на банкомат специального удерживающего карту устройства. Карта вам не возвращается (деньги вы получить, соответственно также не можете, пока не заберете карту). Пока вы едете в банк, к банкомату подходит мошенник и спокойно извлекает вашу карту, убирает устройство, вновь вставляет карту и опустошает счет. Заметим, что

в последнее время банки значительно усилили защиту банкоматов. Так банкоматы Сбербанка теперь блокируют карту, которую не вынули из банкомата в течение 45 секунд. А деньги из выдающего устройства не «выскочат», пока не будет изъята карта. Таким образом забыть карту в банкомате, что было обычным делом еще буквально полгода назад просто невозможно. Ну а приборы, задерживающие карты которые монтировали мошенники, теперь бесполезны. На «сбербанковских» банкоматах точно.

5. Фальшивые банкоматы. Любой человек может купить банкомат, для его последующей установки, обслуживания. Мошенники также могут купить банкомат, но для других целей. Они изменяют программную оболочку, удаляют из банкомата не нужные им функции, например выдача наличных, и устанавливают банкомат в общедоступном месте. Держатель карты при съеме наличных средств, вставляет карту, вводит пин-код, но при съеме средств, выходит ошибка «Операция временно недоступна». Держатель забирает карту, идёт в другой банкомат, а данные магнитной ленты и пин-код идут мошенникам, либо по линиям связи, либо на накопитель, который затем снимается.

Для того чтобы уберечь свои деньги на пластиковой карте, необходимо соблюдать правила безопасности. Ни в коем случае нельзя доверять свои карты другим лицам, оставлять их без присмотра. Так же необходимо запомнить ПИН-код для своей карты, а не оставлять его в легкодоступных местах, и тем более не записывать на самой карте, при этом никогда не стоит произносить его вслух даже работникам банка, выдавшего карту, и обслуживающему персоналу банкомата.

При оплате по безналичному расчету за оказанные услуги или товар необходимо видеть процесс оплаты, а именно, чтобы вашу карту пропустили через импринтер в вашем в присутствии, после чего нужно обязательно сохранить у себя чеки.

Следующим правилом безопасности в обращении с пластиковой картой является проверка движения денег на карточном счете, так ка существуют строго оговоренные сроки, в течении которых держатель карты может предпринять какое-либо действие. Особое внимание следует обратить на операции по счету, в которых использовалась карта.

И последний совет, который дают специалисты по безопасности банков своим клиентам – незамедлительно сообщайте в банк о потере или краже платежной карты, тем самым сократится вероятность пропажи средств с счета и облегчится поиск преступника.

Библиографический список

1. Василенко В. Пластиковые деньги. //Хозяйство и право – 2007. – 74 с.
2. Быстров Л.В., Воронин А.С., Гамольский А.Ю. Пластиковые карты. – М.: БДЦ-пресс, 2009. – 624 с.
3. Мирошкина О.В., Рубинштейн Т.Б. Пластиковые карты. – М.: Гелиос АРВ, 2007. – 416 с.