

Родина Ю.В. Безопасность банковских карт. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей IX Междунар. научно-техн. конф. – Пенза: ПДЗ, 2009. – С. 141-143.

БЕЗОПАСНОСТЬ БАНКОВСКИХ КАРТ

Ю.В. Родина

Всероссийский заочный финансово-экономический институт,
г. Москва, Россия

В статье рассмотрены потери индустрии банковских карт от различных видов мошенничества. Приведены результаты исследований, связанных с безопасностью банковских карт. Рассмотрены условия, необходимые для решения проблем безопасности банковских карт.

Rodina Y.V. Security of banking cards.

The loss of banking cards' industry from different kinds of fraud is considered. The results of researches connected with the security of banking cards are given. The conditions, necessary for solving the problems of security of banking cards are considered.

В 2009 г., по прогнозам международной исследовательской компании Forrester [1], количество мировых онлайн-транзакций вырастет на 12,2%¹. Но при этом большинство покупок будет совершаться на фальшивых сайтах. Согласно данным корпорации электронных платежей CyberSource, количество мошеннических транзакций ежегодно возрастает на 20%.

По данным британской платежной ассоциации Арас¹ [2, 3], в первой половине 2008 г. потери индустрии, ставшие результатом мошенничества в сфере онлайн-банкинга, выросли на 185%. Они составили 21,4 млн. фунтов стерлингов по сравнению с 7,5 млн. фунтов стерлингов в этот же период 2007 г.

Количество случаев фишинга² выросло за последние два года вчетверо: с 5087 в первой половине 2006 г. до 20682 в первом полугодии 2008 г.

Банки все чаще не хотят возмещать убытки клиентам в случаях, если последние становятся жертвами фишинговых афер, так что клиентам приходится мириться с потерями. Банки утверждают, что клиенты, передающие свои данные на фишинговый вебсайт, проявляют халатность, что дает банку основания отказать в выплате возмещения.

Потери от мошенничества с банковскими картами за полгода возросли на 14% и составили 301,7 млн. фунтов. По данным Арас, более 40% из этой суммы – 121,2 млн. фунтов – потери в итоге мошенничества с картами за границей, в тех странах, которые еще не ввели чиповые карты.

Нарушения, совершаемые в пределах Великобритании, также увеличились на 17%. Потери за полгода составили 180,5 млн. фунтов. Мошенничество, совершаемое в магазинах, возросло более чем на четверть – до 47,4 млн. фунтов,

¹ Хотя такой прогноз в условиях финансового кризиса может быть не совсем достоверным. По данным [1] отмечается тенденция значительного уменьшения использования кредитных карт.

¹ Арас (Association for Payment Clearing Services APACS) – Ассоциация систем клиринговых платежей.

² Фишинг – преступление, основанное на принципах социальной инженерии (способе несанкционированного доступа к информации без использования технических средств, основан на использовании излишнего доверия людей), когда пользователи получают электронные сообщения, якобы отправляемые от имени банков, которые на самом деле отсылают пользователей на фальшивые веб-страницы, запрашивающие их банковские данные.

мошенничество с банкоматами увеличилось на 22%, после ежегодного снижения с 2004 г.

Рост числа случаев телефонного, сетевого и почтового мошенничества, когда карта не присутствует в процессе аферы, связан с увеличением количества людей, покупающих товары в режиме онлайн. К примеру, в период между 2001 и 2007 гг. этот тип мошенничества вырос на 204% по сравнению с 415%-ным увеличением количества транзакций по картам в процессе онлайн-шопинга. Мошенничество по этой схеме привело к потерям 161,9 млн. фунтов, что составляет почти половину прибылей всей индустрии.

Мошенничество с утерянными или украденными картами в первой половине 2008 г. практически не изменилось по сравнению с аналогичным периодом 2007 г. и составило 27,3 млн. фунтов.

В конце 2008 г. компания Cisco [4] опубликовала отчет «Cisco Annual Security Report», где отметила, что хотя целенаправленные фишинговые атаки составляют всего 1% от общего числа всех фишинговых схем, их число в будущем будет возрастать.

По информации лаборатории PandaLabs компании Panda Security³ [2] большинство новых вредоносных кодов (68%), выявленных в 2008 г., составляют Трояны, предназначение которых заключается в краже конфиденциальной информации, например, номеров банковских счетов, паролей и др.

Panda Security [2] провела оценку свыше 300 компаний, осуществляющих международные денежные переводы. Были тщательно исследованы более 1 500 компьютеров, и результаты оказались тревожными: на 30% из них были установлены устаревшие антивирусы, а 60% оказались инфицированы.

Компьютеры, не защищенные должным образом и часто используемые для посторонних целей (чаты, загрузки и т.д.), не могут гарантировать безопасность во время выполнения онлайн-транзакций. Это позволяет преступникам перехватывать авторизованные денежные переводы. В результате таких атак банковские данные отправителя перевода могут быть перехвачены киберпреступниками, и в этом случае открытый доступ к счетам жертвы будет обеспечен.

Помочь в решении проблемы безопасности банковских карт должен повсеместный переход на использование чиповых карт и внедрение стандарта PCI DSS⁴. Кроме того, многие банки проводят дополнительные мероприятия для повышения безопасности расчетов. Например, банк HSBC [4] представил технологию по мониторингу транзакций банковских карт на предмет выявления мошеннических операций. Транзакции клиентов будут в реальном времени проверяться на соответствие заранее определенным шаблонам нормального поведения при проведении операций с банковскими картами.

В мире используется огромное количество платежных карт. По данным Банка России [5] на 1 января 2008 г. только российские банки эмитировали 103,5 млн. банковских карт. На 1.10.2008 г. эта цифра составила уже 118,3 млн. Поэтому еще одним неизменным условием снижения случаев мошенничества с

³ Компания Panda Security – разработчик и провайдер решений для IT-безопасности.

⁴ Payment Card Industry Data Security Standard (PCI DSS) – стандарт защиты информации в индустрии платежных карт, разработанный международными платежными системами Visa и MasterCard, объединяет в себе требования ряда программ по защите информации. Распространяется на всех тех, кто передает, обрабатывает и хранит данные держателей карт.

использованием банковских карт является повышение осведомленности держателей карт в вопросах их безопасного использования.

Библиографический список

1. www.viruslab.ru
2. www.itsec.ru
3. www.moneynews.ru
4. www.xakep.ru
5. www.cbr.ru
6. www.bankir.ru