УДК 004 **DOI: 10.34670/AR.2020.26.78.042**

Мошенничество с банковскими картами: экономические аспекты

Шабаев Магомед Баймарзович

Студент,
Чеченский государственный университет,
364049, Российская Федерация, Грозный, ул. Кирова, 47;
e-mail: lashabaev95@gmail.com

Джангаров Ахмед Идрисович

Ассистент,
кафедра программирования и инфокоммуникационных технологий,
Чеченский государственный университет,
364049, Российская Федерация, Грозный, ул. Кирова, 47;
e-mail: dzhangarov1995@gmail.com

Аннотация

Банковские карты – отличная альтернатива наличным средствам. С их помощью можно оплачивать покупки в магазине и расплачиваться в Интернете. Однако при этом есть большой риск столкнуться с мошенничеством, начиная от кражи карты и пин-кода к ней и заканчивая хакерскими уловками. В данной статье рассматриваются основные схемы мошенничества с банковскими картами, а также способы защиты от них. Авторы отмечают, что сегодня мошенничество с банковскими картами становится все более распространенным явлением. Схемы для обмана постоянно совершенствуются, становятся все более изощренными, а жертв подобного вида преступлений становится все больше. Используя данные схемы, мошенники получают доступ к персональным данным и похищают чужие деньги. На законодательном уровне предпринят ряд мер, направленных на предупреждение и борьбу с подобного рода мошенничеством. Однако стоит помнить о том, что собственная безопасность является ответственностью в первую очередь самого гражданина.

Для цитирования в научных исследованиях

Шабаев М.Б., Джангаров А.И. Мошенничество с банковскими картами: экономические аспекты // Экономика: вчера, сегодня, завтра. 2020. Том 10. № 9А. С. 377-382. DOI: 10.34670/AR.2020.26.78.042

Ключевые слова

Банковские карты, мошенничество, Интернет, обман в сети.

Введение

В наш технологический век у человека есть очень много возможностей, в том числе по распоряжению своими денежными средствам. Люди чаще держат деньги на банковских картах, так как в таком случае очень удобно совершать покупки в оффлайн- и онлайн-магазинах и легко контролировать свои расходы, регулярно проверяя детализацию операций. Данное явление стало настолько привычным, что мало кто задумывается о безопасности своих личных данных и денежных средств. Это и привлекает и мошенников, желающих завладеть чужими деньгами. Схемы для обмана постоянно совершенствуются, становятся все более изощренными, а жертв подобного вида преступлений становится все больше. Способы разные, но во всех схемах есть общие признаки: манипулируют чувствами людей, нагнетают страх и заставляют действовать быстро. Используя данные схемы, мошенники получают доступ к персональным данным и похищают чужие деньги.

Основная часть

Рассмотрим наиболее часто встречающиеся схемы мошенничества с банковскими картами.

1) Кража карты. Такой способ используют только в том случае, когда злоумышленникам известен пин-код карты. Узнав пин-код, они разными путями воруют карту и обналичивают ее. Поэтому, совершая оплату или снятие наличных в банкомате, желательно руками загораживать пин-код. А еще лучше снимать деньги в банкомате при отсутствии посторонних людей.
2) Через Интернет. Это самый распространенный способ. Уже придумано множество схем, посредством которых мошенники через Интернет могут завладеть деньгами с банковской карты (рисунок 1). Наиболее распространенные среди них – фейковые сайты известных магазинов. Создаются сайты с аналогичным дизайном и адресом сайта, разница может быть в одной букве. Покупатель заходит на сайт, не подозревая ни о чем, и совершает покупку. В результате деньги за покупку переходят на счет мошенников. Также мошенники завладевают и данными вашей карты. Другой способ – это создание интернет-магазина. Чтобы привлечь покупателей, они выставляют явно заниженный ценник. Разумеется, никакого товара нет, это всего лишь приманка.

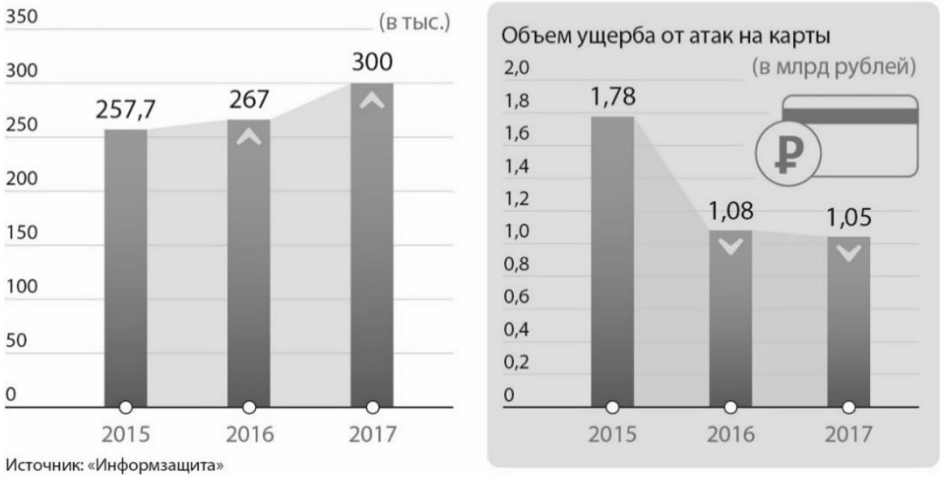

Рисунок 1 - Рост краж с банковских карт в количественном и денежном выражении

3) Мошенники на «Авито» и других досках объявлений. При использовании сайта или приложения «Авито» стоит обращать внимание на следующие моменты. Продавец может попросить внести предоплату за товар без предварительного осмотра покупателем. К счастью, сейчас это встречается крайне редко, потому что администрация сайта держит под контролем подобные сделки. Кроме того, может запрашиваться пин-код при покупке товара. На такую аферу попадаются как продавцы, так и покупатели. Злоумышленники под любым предлогом пытаются узнать номер карты с пин-кодом от нее, чтобы провести оплату через сторонние ресурсы. Этот факт должен насторожить. Соответственно, от совершения сделки в целях безопасности стоит отказаться. Также нельзя сообщать никому CVC (CVV) код, расположенный на обороте карты.
4) Мошенничество с банкоматом. Мошенники научились обманывать и банкомат. В разъем для банковской карты вставляется листовой пластик или кусочек фотопленки так, чтобы карта проникла вовнутрь, а вот обратно не вышла. Пока владелец карты находится в растерянности, один из мошенников под видом обычного прохожего пытается отвлечь его, предлагая обратиться в банк либо позвонить в службу поддержки, а цель другого, рядом стоящего мошенника заключается в том, чтобы запомнить пин-код, извлечь карту и снять с нее наличные.

Фальшивая накладка устанавливается как на клавиатуру банкомата, так и в отверстие для приема карты и позволяет считывать данные с самой карты и пин-код, вводимый на подложной клавиатуре. Затем на основании этих данных изготавливается дубликат карты, при помощи которой злоумышленники снимают деньги.

Нужно быть особенно внимательным, когда отдаешь банковскую карту продавцу или официанту, следить за движениями его рук. Проводя карту один раз через терминал, проходит платеж, а при проведении второй раз может считываться информация, которую злоумышленники используют в своих целях.

Также проявлять осторожность нужно и обладателям бесконтактных карт (тех, которые прикладываются к терминалу без ввода пин-кода). Используются они для оплаты покупки на сумму не более нескольких тысяч рублей. Мошенникам достаточно будет приблизиться и аккуратно поднести небольшой переносной терминал к карте, которая находится во внешнем кармане брюк или сумки и списать с нее деньги.

Списывание денег при помощи смс-сообщений или через телефон. В случае потери или кражи смартфона злоумышленники получают доступ к счетам. На телефон жертвы приходит смс-уведомление как будто от банка, где сказано, что банковская карта заблокирована и, чтобы разблокировать ее, необходимо позвонить по указанному номеру. На самом деле такие сообщения отсылают не сотрудники банка, а мошенники. И если позвонить, то они попытаются разузнать всю нужную им информацию: номер карты, пин-код, срок действия и секретный код (слово). Эти данные они потом будут использовать в личных целях.

Как защититься от мошенников? Никому никогда нельзя называть платежную информацию о банковской карте, особенно пин-код и CVC (CVV) код. Его не имеют право спрашивать даже сотрудники банков. Желательно подключить смс-уведомления, это позволит получать оперативную информацию о зачислении и списании средств со счета, что в конечном итоге может повлиять на судьбу денег на карте.

Что делать жертве, пострадавшей от мошенников? При первом же обнаружении того, что с карты пропали деньги, действовать нужно незамедлительно. Но для начала необходимо

выяснить, на самом ли деле произошло незаконное списание. Возможно, кто-то из членов семьи воспользовался картой или же деньги могли списаться в счет задолженности судебными приставами. После этого следует обратиться по телефону горячей линии банка, рассказать о случившемся и попросить заблокировать карту. Далее необходимо лично обратиться в банковское учреждение и написать заявление о несогласии с проведенными транзакциями. В некоторых ситуациях банки могут отказать в процедуре транзакции. В таком случае придется обратиться с заявлением в прокуратуру.

Заключение

Сегодня мошенничество с банковскими картами становится все более распространенным явлением. Схемы для обмана постоянно совершенствуются, становятся все более изощренными, а жертв подобного вида преступлений становится все больше. Используя данные схемы, мошенники получают доступ к персональным данным и похищают чужие деньги. Тот факт, что телефоны стали неотъемлемой частью жизни современного общества, играет мошенникам на руку. На законодательном уровне предпринят ряд мер, направленных на предупреждение и борьбу с подобного рода мошенничеством. Однако стоит помнить о том, что собственная безопасность является ответственностью в первую очередь самого гражданина.

Библиография

1. Белоножко Е.С., Чеджемов Г.А. Мошенничество в сети Интернет // Наука XXI века: актуальные направления развития. 2017. № 1-1. С. 86.
2. Виды мошенничества в Интернете и с банковскими картами. URL: https://www.nwab.ru/static/single/-rus-common-materials41618_154419-/material41618_154537.
3. Гладкий А. Мошенничество в Интернете. Методы удаленного выманивания денег, и как не стать жертвой злоумышленников. М., 2018. 899 с.
4. Магомедов И.А., Мурзаев Х.А., Золкин А.Л. Киберграмотность как одна из главных дисциплин, необходимых в современное время. 2020. С. 1011-1015.
5. Мурзаев Х.А., Магомедов И.А. Технология NFC и способы ее применения // Сборник научных статей по итогам международной научной конференции «Приоритетные направления инновационной деятельности в промышленности». Казань, 2020. С. 144-146.
6. Осипенко А.Л. Сетевая компьютерная преступность теория и практика борьбы. Омск, 2009. 480 с.
7. Романов С.А. Мошенничество в России. 1000 способов как уберечься от аферистов. М., 2018. 320 с.
8. Схемы мошенничества. URL: https://www.sngb.ru/cards-schemas.
9. Черных В.В. Проблемы расследования мошенничества, совершенного с использованием банковских карт, и пути их решения // Вестник Таганрогского института управления и экономики. 2018. № 1 (27). С. 123-126.
10. Шейнов В.П. Как защититься от обмана и мошенничества. М.: Харвест, 2019. 464 с.
11. Омшанова Э.А., Щёголева К.Е. Программные инструменты стимулирования ипотечного кредитования // Финансовые рынки и банки. 2020. № 3. С 83 – 86.
12. Кокорев А.С. Глобализация и актуальные проблемы современной региональной экономики // Московский экономический журнал. 2020. № 4. С. 14.
13. Бабаева Н.М., Карачун И.А. Финансовый рынок в Беларуси и Узбекистане // Журнал Белорусского государственного университета. Экономика. 2019. № 2. С. 37 – 47.

Bank card fraud: economics aspects

Magomed B. Shabaev

Student,
Chechen State University,
364049, 47 Kirova st., Grozny, Russian Federation;
e-mail: lashabaev95@gmail.com

Akhmed I. Dzhangarov

Assistant,
Department of programming and infocommunication technologies,
Chechen State University,
364049, 47 Kirova st., Grozny, Russian Federation;
e-mail: dzhangarov1995@gmail.com

Abstract

Bank cards are a great alternative to cash. With their help, we can pay for purchases in the store and pay on the Internet. People often keep their money on bank cards, since in this case it is very convenient to make purchases in offline and online stores and it is easy to control their expenses by regularly checking the details of their operations. However, at the same time, there is a great risk of being faced with fraud, ranging from theft of the card and pin-code to it and ending with hacker tricks. This article discusses the main schemes of fraud with bank cards, as well as ways to protect against them. The authors note that today, fraud with bank cards is becoming more common. Fraud schemes are constantly being improved, becoming more sophisticated, and the number of victims of this type of crime is becoming more and more. Using these schemes, fraudsters gain access to personal data and steal other people's money. At the legislative level, a number of measures have been taken to prevent and combat this kind of fraud. However, it is worth remembering that personal safety is the responsibility of the citizen himself, first of all principle.

For citation

Shabaev M.B., Dzhangarov A.I. (2020) Moshennichestvo s bankovskimi kartami: ekonomicheskie aspekti [Bank card fraud: economics aspects]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 10 (9A), pp. 377-382. DOI: 10.34670/AR.2020.26.78.042

Keywords

Bank cards, fraud, Internet, Internet deception.

References

1. Belonozhko E.S., Chedzhemov G.A. (2017) Moshennichestvo v seti Internet [Fraud on the Internet]. *Nauka XXI veka: aktual'nye napravleniya razvitiya* [Science of the XXI century: current directions of development], 1-1, p. 86.
2. Chernykh V.V. (2018) Problemy rassledovaniya moshennichestva, sovershennogo s ispol'zovaniem bankovskikh kart, i puti ikh resheniya [Problems of investigation of fraud committed using bank cards and ways to solve them]. *Vestnik*

Taganrogskogo instituta upravleniya i ekonomiki [Bulletin of the Taganrog Institute of Management and Economics], 1 (27), pp. 123-126.
3. Gladkii A. (2018) *Moshennichestvo v Internete. Metody udalennogo vymani-vaniya deneg, i kak ne stat' zhertvoi zloumyshlennikov* [Internet fraud. Methods for extorting money remotely, and how not to become a victim of cybercriminals]. Moscow.
4. Magomedov I.A., Murzaev Kh.A., Zolkin A.L. (2020) *Kibergramotnost' kak od-na iz glavnykh distsiplin, neobkhodimykh v sovremennoe vremya* [Cyber literacy as one of the main disciplines required in modern times], pp. 1011-1015.
5. Murzaev Kh.A., Magomedov I.A. (2020) Tekhnologiya NFC i sposoby ee primene-niya [NFC technology and methods of its application]. In: *Sbornik nauchnykh statei po itogam mezhdunarodnoi nauchnoi kon-ferentsii "Prioritetnye napravleniya innovatsionnoi deyatel'nosti v promyshlennosti"* [Proc. Int. Conf. "Priority areas of innovation in industry"]. Kazan', pp. 144-146.
6. Osipenko A.L. (2009) *Setevaya komp'yuternaya prestupnost' teoriya i praktika bor'by* [Network computer crime theory and practice of struggle]. Omsk.
7. Romanov S.A. (2018) *Moshennichestvo v Rossii. 1000 sposobov kak uberech'sya ot aferistov* [Fraud in Russia. 1000 ways to protect yourself from swindlers]. Moscow.
8. Sheinov V.P. (2019) *Kak zashchitit'sya ot obmana i moshennichestva* [How to protect yourself from deception and fraud]. Moscow: Kharvest Publ.
9. *Skhemy moshennichestva* [Fraud schemes]. Available at: https://www.sngb.ru/cards-schemas [Accessed 17/11/2020].
10. *Vidy moshennichestva v Internete i s bankovskimi kartami* [Types of fraud on the Internet and with bank cards]. Available at: https://www.nwab.ru/static/single/-rus-common-materials41618_154419-/material41618_154537 [Accessed 17/11/2020].
11. Asanova E. A., Shchegolev, K. E. Software tools in order to stimulate mortgage lending // Financial markets and banks. 2020. No. 3. P. 83-86.
12. Kokorev A. S. Globalization and actual problems of modern regional economy // Moscow Economic Journal. 2020. No. 4. P. 14.
13. Babaeva N. M., Karachun I. A. Financial market in Belarus and Uzbekistan / / Journal of the Belarusian State University. Economy. 2019. No. 2. P. 37 – 47.