УДК 336.7

Мошенничество в сфере банковских карт

Татаринцев Игорь Александрович
Приамурский государственный университет им. Шолом-Алейхема
студент

Гребенникова Елена Юрьевна
Приамурский государственный университет им. Шолом-Алейхема
преподаватель юридических дисциплин промышленно-экономического факультета программ СПО

Лукьянова Людмила Васильевна
Приамурский государственный университет им. Шолом-Алейхема
к.п.н., директор промышленно-экономического факультета программ СПО

Аннотация
В данной статье рассмотрены новые способы мошенничества в сфере банковских карт в Российской Федерации. Представлены способы защиты средств банковских карт. Приведены итоги конференции CyberCrimeCon за 2016-2017 гг. Предложены способы защиты от мошенничества в сфере банковских карт.
Ключевые слова: мошенник, банковская карта, денежные средства.

Bank card fraud

Tatarintsev Igor Aleksandrovich
Sholom-Aleichem Priamursky State University
student

Grebennikova Elena Yurevna
Sholom-Aleichem Priamursky State University
teacher of legal disciplines of industrial and economic faculty of secondary vocational education

Lukyanova Lyudmila Vasilievna
Sholom-Aleichem Priamursky State University
Candidate of pedagogical sciences, director of industrial and economic faculty of secondary vocational education

Abstract
This article describes new methods of fraud with the bank cards in the Russian Federation. The methods of protection of the bank cards were summed up in the

conference named CyberCrimeCon in 2016-2017. The methods of protection against fraud in the field of Bank cards were proposed.
Key words: fraud, bank card, cash.

Появление в жизни российских граждан безналичных расчётов, а именно появление пластиковых банковских карт, которые упростили финансовые операции, привело к появлению нового вида мошенничества. В последнее время злоумышленники активно похищают средства с банковских карт.

Исходя из сказанного выше, тема мошенничества в сфере банковских карт является крайне актуальной на сегодняшний день.

Целью исследования является изучение новых способов мошенничества в сфере использования банковских карт.

Задачи исследования:

1) Раскрыть понятия способов мошенничества

2) Объяснить как избежать покушения на ваши финансовые средства

3) Отразить краткую статистику преступлений в данной сфере

Банковская карта-это персональный ключ к банковскому счёту, позволяет производить такие финансовые операции как: снять и положить средства на счёт, оплатить различные счета ,погасить кредит и д.р. Представляет собой небольшую пластиковый прямоугольник на котором отображены персональные данные владельца.

На сегодняшний день около 80% людей пользуется банковскими картами, растёт и количество безналичных операций совершаемых при помощи этих карт. Эти факты несомненно привлекают мошенников к совершению преступлений в данной сфере. Рассмотрим новые способы мошенничества.

1) Вредоносное программное обеспечение-это вредоносные приложения, которые считывают пароли и перехватывают СМС - сообщения с мобильных телефонов. Владельцы компьютеров и мобильных устройств часто различные приложения, в том числе и платёжные. Вредоносные программы часто маскируются, иногда обозначить их не остаётся возможным;

2) Скимминг - вид мошенничества, который осуществляется при помощи «скиммера» - приспособление для считывания магнитной дорожки с карты или имитатор клавиатуры банкомата внешне почти не отличимый, а также установленные злоумышленниками камеры наблюдения для получения пин - кода карты владельца;

3) Фишинг - это кража персональных данных.Происходит это следующим путём: при оплате чего-либо в интернете, клиент переходит на фальшивый сайт сервиса оплаты , где он должен ввести свои данные. После ввода данных пользователь передаёт личную информацию злоумышленникам, а те в свою очередь получают доступ к средствам пользователя;

4) Доверительный метод. Эта схема предусмотрена для пользователей онлайн магазинов. Всё происходит так: мошенники создают поддельные сайты или группы в соц.сетях, при этом они указывают электронный способ оплаты. Делая заказ на таких сайтах клиент вносит предоплату в следствии чего рискует остаться без покупки и денежных средств внесённых в качестве предоплаты;

5) Кибермошенничество в соц.сетях. Кибермошенники с помощью компьютерных программ взламываю учётные записи в социальных сетях и делают рассылки сообщений друзьям с подобным текстом: «Привет, скинь пожалуйста денег на карту, очень срочно, потом отдам», «Привет, я на твой номер скину пароль от восстановления e-mail, просто на мой не приходит». Далее друзья соглашаются помочь и выполняют просьбу мошенника. Так мошенники получают доступ к счетам и успешно похищают средства.

Согласно данным ежегодной конференции CyberCrimeCon «Тенденции развития преступлений в сфере высоких технологий» в период 2016-2017 гг. была зафиксирована следующая статистика (табл.1).

Таблица 1. Итоги конференции CiberCrimeCon

Способ мошенничества	**Число успешных атак в день**	**Средняя сумма одного хищения (руб.)**	**Сколько воруют в день (руб.)**	**Сумма похищенного в период 2016-2017 гг. (руб.)**
Хищение в интернет банкинге у юридических лиц с использованием вредоносных программ	2	1 250 000	2 500 000	622 500 000
Хищение в интернет банкинге у физических лиц с использованием вредонсных программ	1	63 000	63 000	15 687 000
Хищение у физических лиц с Android-троянами	300	11 000	3 300 000	821 700 000
Целевые атаки на банки	–	–	–	1 630 000 000
Фишинг	950	1000	950 000	236 550 000
Обналичивание похищаемых средств	–	–	2 638 350	1 390 449 150

Чтобы предотвратить хищение денежных средств с банковской карты предлагаются следующие способы защиты.

1) Вредоносное программное обеспечение:
- использование на своём устройстве антивирусных программ;
- не загружать программы с ненадёжных интернет - источников;
- не запускать незнакомые подозрительные программы автоматически скачанных с интернет - ресурсов;

2) Скимминг:
- тщательно осмотреть банковский терминал на предмет посторонних устройств перед тем как вставить карту;
- во время ввода пин-кода прикрывать клавиатуру рукой;

3) Фишинг:
- удостовериться в безопасности сайта;
- привязать электронный кошелёк к e-mail адресу

4) Доверительный метод:
- передавать никому пин-коды из СМС сообщений;
- перед отправкой другу денежных средств, убедиться в том, что вас просит именно ваш друг, а не мошенник;
- не стоит доверять интернет магазинам с очень низкими ценами.

В настоящее время существует достаточно много способов мошенничества хищения денежных средств, с банковских карт, чтобы не допустить этого, печального результата, необходимо использовать простые и достаточно эффективные способы защиты, предложенные нами.

Библиографический список

1. Воронин А.С. Мошенничество в платежной сфере. Бизнес-энциклопедия. М.: Центр исследований платежных систем и расчетов. Интеллектуальная Литература, 2016.
2. Ревенков П.В Финансовый мониторинг в условиях интернет-платежей. М.: КноРус, 2016. 76. с.
3. Информационный портал GROPIB «Hi-TechCrimeTrends 2017». URL: https://www.group-ib.ru/