Рафальская Евгения Игоревна
студентка
Тукова Екатерина Александровна
ассистент кафедры
ФГБОУ ВО «Уральский государственный
университет путей сообщения»
г. Екатеринбург, Свердловская область

СПОСОБЫ ЗАЩИТЫ ОТ НОВЫХ ВИДОВ МОШЕННИЧЕСТВА С БАНКОВСКИМИ КАРТАМИ

Аннотация: *в статье рассмотрены схемы мошенничества с банковскими картами в России. В работе также представлены способы защиты средств банковских карт, обозначены итоги конференции CyberCrimeCon за 2016–2017 гг., приведены несколько способов защиты от мошеннических операций с банковскими картами.*

Ключевые слова: *банковская карта, схемы мошенничества с банковскими картами, защита банковских карт, кибератаки, вредоносное программное обеспечение, скимминг, фишинг, доверительный метод.*

Не так давно клиенты банков перешли на пользование банковскими картами, именно этот переход поспособствовал появлению безналичного расчета, который в свою очередь упростил повседневную жизнь людей, но также и добавил появление ряда проблем. В настоящее время участились случаи краж денежных средств с банковских карт. Каждый раз злоумышленники придумывают всё новые способы похищение денег.

Банковская карта – это пластиковая карта, привязанная к одному или же нескольким расчётным счетам в банке. Применятся для оплаты товаров и услуг, в том числе через Интернет, а также снятия наличных.

Особое внимание мошенников к банковским картам привлек рост проводимых безналичных операций, которые проводились при помощи тех самых банковских карт. На данный момент существует более 10 методов мошенничества с

банковской картой. Рассмотрим некоторые схемы мошенничества с банковскими картами.

1. Вредоносное программное обеспечение (ПО) – это программное обеспечение, которое разрабатывается для получения несанкционированного доступа к информации устройств. Таким образом, хакеры проникают в смартфон и получают доступ к электронным кошелькам.

Наиболее приоритетными программными компонентами (плагинами) для эксплуатации уязвимостей являются: Java, Flash и InternetExplorer [3, с. 76]

2. Скимминг – кража данных карты при помощи специального считывающего устройства (скиммера). Мошенники копируют всю информацию с магнитной полосы карты (имя держателя, номер карты, срок окончания срока ее действия, CVV- и CVC-код), узнать ПИН-код можно с помощью мини-камеры или накладок на клавиатуру, установленных на банкоматах. Стать жертвой скимминга можно не только снимая наличные, но и оплачивая покупки в торговых точках [4].

3. Фишинг – это хищение персональных данных с помощью фишинговых сайтов: клиент переходит по ссылке на поддельный сайт платёжного сервиса, где ему предлагается ввести свои данные. Указав на таком сайте логин, пароль и любую другую конфиденциальную информацию, пользователь фактически предоставляет мошенникам доступ к своим средствам [2, с. 18–19].

4. Доверительный метод. Эта схема рассчитана на пользователей интернет-магазинов. Часто мошенники создают поддельные сайты или группы в социальных сетях, указывая в качестве оплаты электронные деньги. Оформляя заказ на подобных сайтах, клиент вносит предоплату и рискует остаться без покупки и без денежных средств.

5. Кибератаки в социальных сетях. Киберпреступники с помощью компьютерных программ взламывают аккаунты в социальных сетях и делают от чужого имени рассылки друзьям с подобным текстом: «Привет, можно тебе скинуть пароль от моей SIM-карты, на мой телефон почему-то не приходит». Пользователи социальных сетей соглашаются помочь своим знакомым и высылают номер

своего телефона и код из SMS-сообщения. Так мошенники узнают ПИН-коды у держателей карт различных банков и похищают денежные средства с их счетов.

Рост числа атак и сумм хищений является ярким индикатором финансовой активности киберпреступников, изменения их тактики и целей. Большая часть хакеров следует за деньгами. Если они находят новые, более высокооплачиваемые и безопасные способы заработка, то начинают инвестировать именно туда, создавая новые схемы проведения атак [5]

По данным ежегодной конференции CyberCrimeCon в период 2016–2017 г. было зафиксировано снижение рынка киберпреступлений в России и СНГ на 15% (таблица 1).

Таблица 1

Оценка рынка высокотехнологичных преступлений за 2015–2017 г.

Сегмент рынка в России и СНГ	Кол-во групп	Общее число успеш-ных атак в день	Средняя сумма од-ного хи-щения	Сколько воруют в день	Q2 2016-Q1 2017		Q2 2015-Q1 2016		Процент роста к прошлому году
					в RUB	в USD	в RUB	в USD	
Хищения в интер-нет-банкинге у юридических лиц с использованием вредоносных про-грамм.	3	2	1 250 000 р	2 500 000 р	622 500 000 р	$10 375 000	956 160 000 р	$16 774 737	–35%
Хищения в интер-нет-банкинге у физических лиц с использованием вредоносных про-грамм.	1	1	63 000 р	63 000 р	15 687 000 р	$261 450	6 424 200 р	$112 705	144%
Хищения у физи-ческих лиц с Android-тро-янами.	10	300	11 000 р	3 300 000 р	821 700 000 р	$13 695 000	348 600 000 р	$6 115 789	136%
Целевые атаки на банки	2	–	–	–	1 630 000 000 р	$27 166 667	2 500 000 000 р	$43 859 649	–35%
Фишинг	15	950	1 000 р	950 000 р	236 550 000 р	$942 500	–	–	–
Обналичивание похищаемых средств	–	–	–	2 638 350 р	1 390 449 150 р	$23 174 153	1 715 032 890 р	$30 088 296	–19%
Итог				6 813 000 р	4 716 886 150 р	$78 614 769	5 526 217 090 р	$96 951 177	–15%

По итогам конференции за 2016–2017 гг. наибольший прирост приходился на хищения у физических лиц с использованием вредоносных программ и составил 144%, на хищения у физических лиц с Android-троянами – 136%. Эта динамика говорит о том, что мошенники каждый раз придумывают новые и непохожие друг на друга вредоносные программы для мобильных устройств и компьютеров. Также в эти же годы был зафиксирован новый вид махинации – фишинг, с помощью которой в России и странах СНГ была украдена сумма в размере 236 550 000 руб.

В связи с участившимися случаями незаконного списания денежных средств с банковских карт ПАО «Сбербанк России» в 2017 году разработал полис страхования всех банковских карт, выпущенных банком и привязанных к счетам клиентов. Полис страхования позволяет защитить средства на банковских картах. Его можно оформить в любом отделении ПАО «Сбербанк России» всего за 790 рублей. Приобретая такой полис, клиенты банка, в случае наступления страхового случая, получат страховую выплату в установленном размере.

В современном мире схем мошенничества с банковскими картами очень много и с каждым годом их число растёт. Чтобы предотвратить незаконное списание денежных средств в таблице 2 предлагаются элементарные способы защиты.

Таблица 2

Способы защиты от мошеннических операций с банковскими картами

Вид мошенничества с банковскими картами	Предлагаемые способы защиты
1. Вредоносное ПО	– установка антивирусных программ на мобильные устройства, компьютеры; – не скачивать программы, приложения с подозрительных сайтов, непроверенных источников; – ни в коем случае не запускать незнакомые приложения, автоматически скаченные с интернета
2. Скимминг	– внимательно осмотреть банкомат перед тем, как вставить в него банковскую карту; – вводя PIN-код, прикройте клавиатуру от подсматривания

3. Фишинг	– внимательно осмотреть название сайта, на котором происходит покупка, в адресной строке; – использование привязки электронного кошелька к e-mail адресу
4. Доверительный метод, кибератаки в социальных сетях	– никому не передавать PIN-код из SMS-сообщения; – не стоит доверять группам, интернет-магазинам с подозрительно низкими ценами; – если все-таки хотите помочь другу, который обратился к Вам с просьбой в социальной сети, то обязательно свяжитесь с ним по мобильному телефону, чтобы убедиться в реальности его намерений

Любителям оплачивать покупки в интернет-магазинах стоит завести отдельную карту, на которую можно перекидывать небольшие суммы денежных средств для оплаты. Пользуясь современными пластиковыми картами нужно быть предельно осторожными при совершении каких-либо операций.

Список литературы

1. Воронин А.С. Мошенничество в платёжной сфере. Бизнес-энциклопедия. – М.: Интеллектуальная литература, 2016. – С.18–19.

2. Ревенков П.В. Финансовый мониторинг в условиях интернет-платежей. – КноРус, 2016. – 76 с.

3. Сбербанк России: официальный сайт [Электронный ресурс]. – Режим доступа: http://www.sberbank.ru/ru/person

4. Информационный портал GROPIB»Hi-TechCrimeTrends 2017» [Электронный ресурс]. – Режим доступа: https://www.group-ib.ru/

5. Катерова Ю.В. Новые виды мошенничества с платёжными картами в России [Электронный ресурс]. – Режим доступа: http://sci-article.ru/stat.php?i=1508854937 (дата обращения: 31.10.2017).