https://www.modscires.pro/index.php/msr/article/view/be4-218-012
DOI: 10.30889/2523-4692.2018-04-03-012

PHISHING - ONE OF THE MOST CURRENT MODERN METHODS OF FRAUD USING BANK CARDS

ФИШИНГ – ОДИН ИЗ АКТУАЛЬНЫХ СОВРЕМЕННЫХ СПОСОБОВ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ.

Lamonova A.O. / Ламонова А.О.
Student / студент
Law School of the Far Eastern Federal University
Юридическая школа Дальневосточного федерального университета

Аннотация. *В статье автор рассматривает один из современных способов мошенничества с использованием банковских карт – фишинг, который представляет собой сетевой вид мошенничества, при котором технически подкованные мошенники выманивают у людей конфиденциальную информацию. Перед банком стоит основная задача - обеспечить безопасность операций клиентов и контролировать операции по счетам с целью выявления случаев мошенничества. В статье проводится анализ 30 приостановленных уголовных дел данной категории по п.1 ч.1 208 УПК РФ (лицо, подлежащее привлечению в качестве обвиняемого, не установлено) за период с октября 2017 года по апрель 2018 года.*

Ключевые слова: *преступление, мошенничество, банковская карта, фишинг, интернет-сайт.*

Мошенничество - одно из сложных для раскрываемости преступление, которое характеризуется запутанностью, заранее обдуманной витиеватой схемой.

Один из более актуальных способов - мошенничество, совершаемое с помощью банковских карт. Банковские карты стали универсальным платежным инструментом, позволяющим проводить финансовые операции без участия наличных денежных средств. Мошенничество с банковскими картами набирает обороты, поскольку мошенники каждый раз придумывают новые схемы и махинации, целью которых является снятие денег с банковской карты [1].

Способов совершения мошенничества с использованием банковских карт различное множество (скимминг, фишинг, шиминг и.т.д.) [2], с которыми необходимо активно бороться, минимизировать совершение таких преступлений, повышать эффективность расследования.

Фишинг («рыбалка», «ловить на удочку», «выуживание») является одним из современных способов мошенничества с использованием банковских карт. Смысл этого способа состоит в том, что на электронную почту с мошеннических интернет-сайтов или телефон жертвы приходит сообщение с просьбой указать данные банковской карты. Фишинг представляет собой сетевой вид мошенничества, при котором технически подкованные мошенники выманивают у людей конфиденциальную информацию. Это может осуществляться при помощи спама, почтовых и мгновенных сообщений, вредоносных интернет-сайтов, но ни один банк не будет рассылать такого рода предложения с целью получения личных данных владельцев карты. Пользователь полагает, что переходит на официальный сайт банка, однако, фактически перенаправляется на подставной сайт, который является по внешнему виду идентичным с официальным сайтом. Пользователь вводит на

подставном сайте: регистрационное имя, PIN - код, тем самым давая фишерам ключ к своим денежным средствам. Подобный фишинговый сайт очень сложно обнаружить без специальных навыков. Поддельные сайты - одно из направлений современного фишинга. Существует такие разновидности фишинга, как вишинг (фишинг посредством звонков пользователям) и смишинг (фишинг посредством сообщений) [3].

Фишинг - как один из современных способов мошенничества, нашел свое отражение в работах Н.Н. Быковой, Д.С. Изотова, Ф.Т. Байрушина, А.А. Казыханова, С.С. Хачатурова. В большинстве случаев предложения авторов сводятся к тому, что клиенты банка должны быть сами бдительны и внимательны при пользовании банковской карты, разработаны рекомендации для владельцев карт, которые могут обезопасить от указанного преступного посягательства.

Количество фишеров возрастает, также увеличивается рост совершаемых ими преступлений. Существует ряд проблем, связанных с обнаружением, расследованием, предотвращением фишинга.

Владельцы карт, пострадавшие от указанного вида мошенничества, обращаются с заявлением в полицию, анализ уголовных дел показал, что в большинстве случаев дела приостановлены по п.1 ч.1 208 УПК РФ (лицо, подлежащее привлечению в качестве обвиняемого, не установлено).

Подтверждением сказанному является анализ 30 приостановленных уголовных дел за период с октября 2017 года по апрель 2018 года.

Во всех случаях были возбуждены уголовные дела в отношении неустановленных лиц по признакам преступления, предусмотренного ч.1 ст.159 УК РФ. В тридцати случаях было вынесено постановление о признании лица потерпевшим.

В комплекс первоначальных следственных мероприятий входили следующие:

1. Допрос потерпевшего.

2. Вынесение постановления с ходатайством перед судьей о получении разрешения на проведение оперативно-розыскного мероприятия - наведение справок, направленное на получение с ПАО «ВТБ»/ ПАО «Сбербанк» сведений о собственнике банковской карты, схемы движения денежных средств по счету, в случае перевода денежных средств на счета или номера операторов сотовой связи, с указанием данных лиц на которых зарегистрированы данные счета (номера).

3. Вынесение постановления о разрешении на проведение оперативно-розыскного мероприятия - наведение справок путем получения в сотовых компаниях сведений о соединении абонентского номера с указанием IMEI и адресов базовых станций.

Установлено, что преступления были совершены путем создания поддельных сайтов банка схожих с официальными сайтами. В 18 из 30 дел была совершена подделка сайта ПАО «ВТБ», в 12 случаях сайта ПАО «Сбербанк». Во всех случаях в телефоне у потерпевшего отображалось, что происходит обновление, в этот момент происходило совершение

мошеннических действий.

В 21 из 30 случаях потерпевшие указали, что поняли, что с ними были совершены мошеннические действия сразу после наступления негативных последствий, когда обнаружили снятие денежных средств с карты. В остальных девяти случаях пояснили, что не понимают, когда и как был осуществлен несанкционированный доступ к его данным.

27 потерпевших из 30 незамедлительно обратились на горячую линию банка. 23 потерпевших обратились с претензией в банк по поводу списания денежных средств путем мошеннических действий. Согласно ФЗ «О национальной платежной системе» у банка существует обязанность возвращать денежные средства клиенту, который заявил о несанкционированном списании средств с его личной платежной карты, а уже после проводить свое собственное расследование того, по чьей вине это произошло [4]. Во всех случаях банк в ответ на претензию указывал, что операции были совершены с использованием личного кабинета клиента, у банка не было оснований полагать, что действия исходят не от клиента. Анализ результатов внутреннего расследования позволяет сделать вывод о том, что в отношении клиента были совершены мошеннические действия неустановленным лицом, получившим доступ к личным данным. Банк не несет ответственность за ущерб, возникший вследствие несанкционированного использования третьими лицами идентификаторов и средств подтверждения клиента, если такое использование стало возможным не по вине банка.

Трое из тридцати потерпевших незамедлительно обратились с заявлением в полицию, минуя обращение в банк. 6 потерпевших обратились с заявлением на следующий день после совершения мошеннических действий. Долгое обращение с заявлением в правоохранительные органы, затрудняет расследование указанных дел. Также созданные поддельные сайты являются сайтами-однодневками, которые перестают существовать после совершения мошеннических действий.

Владельцы карт, у которых были списаны денежные средства с банковской карты путем мошеннических действий, вынуждены обращаться в порядке гражданского судопроизводства с указанием ответчиком соответствующий банк, в связи с тем, что дела по указанной категории приостановлены по п.1 ч.1 208 УПК РФ (лицо, подлежащее привлечению в качестве обвиняемого, не установлено). Клиенты банка полагают, что система безопасности банка не обеспечивает должного уровня защиты, не срабатывает должным образом. Анализ 25 гражданских дел данной категории в период с января 2017 года по апрель 2018 года показал, что суд приходит к выводу, что банк не нарушал правил обслуживания банковских карт и производил перечисление денежных средств со счета истца в соответствии с установленным порядком предоставления услуги в рамках заключенного с истцом договора, полагая, что поручения о перечислении денежных средств исходят от клиента.

Подтверждением сказанному является анализ судебных решений по указанной категории дел. Решением Южно-Сахалинского городского суда от 11.10.2017 года Сергееву Д.А. было отказано в удовлетворении исковых

требований о взыскании денежных средств с ВТБ 24 (публичное акционерное общество). Сергеев Д.А. в исковом заявлении указал, что 01.02.2016г. зашел на сайт банка, который оказался поддельным, телефон истца был заражен вирусом. Сергеевым Д.А. была произведена авторизация посредством ввода уникального номера клиента и пароля [5].

Злоумышленники специально заражают вирусом, который, проникая в телефон, начинает работать на мошенников. Он заменяет окно мобильного банкинга фишинговым, то есть поддельным, а владелец телефона вводит туда свои данные, ничего не подозревая. Вирус отправляет их мошенникам, которые затем незаконно получают доступ к карточному счету клиента [6].

На основании анализа приостановленных уголовных дел по п.1 ч.1 208 УПК РФ (лицо, подлежащее привлечению в качестве обвиняемого, не установлено), гражданских дел, сделан вывод, что фишинг как один из современных способов мошенничества является одним из чаще встречающихся, во всех случаях лицо, совершившее преступление не было установлено. Клиенты банка, у которых были списаны денежные средства с банковской карты путем совершения указанного способа мошенничества, не вернули похищенные денежные средства вышеприведенными способами.

Проведённое исследование убедительно свидетельствует о том, что существуют проблемы с расследованием указанной категории дел, с должной работой системы безопасности банка.

Необходимо совершенствовать работу системы безопасности банков. В настоящее время состояние защиты банка от мошеннических посягательств находится на низком уровне. Необходимо разработать специальную программу с целью выявления мошеннических операций, механизмы воздействия на них. Более быстро реагировать на подозрительную подборку паролей при входе в такие приложения как «Сбербанк онлайн». У каждого банка имеется свой официальный сайт, банку необходимо самостоятельно отслеживать появление аналогичных интернет-сайтов и сообщать в соответствующие органы в целях предотвращения совершения преступлений, т.к. из анализа 30 приостановленных уголовных дел следует, что мошенники создают практически идентичные сайты и клиент, вводя данные карты, делает их доступными для мошенника.

Литература:

1. Завидов Б.Д. О понятии мошенничества и его видоизменениях в уголовном праве России. // Российский следователь. 2016. №2. С. 20–28

2. Ларичев В.Д, Спирин Г.М. Коммерческое мошенничество в России. Способы совершения. Методы защиты. М.: «Экзамен», 2015.С.187

3. Фролова О.Ю. Современный рынок российских банковских продуктов// Балтийский гуманитарный журнал. 2014 № 3. С. 93-96

4. О национальной платежной системе: Федеральный закон: принят Государственной Думой 27.06.2011 № 161-ФЗ// Доступ из справ. - правовой системы «КонсультантПлюс». (по состоянию на 18.07.2017)

5. URL: http://u-sahalinsky.sah.sudrf.ru/ (дата обращения 09.04.2018)

6. Ивлева Г.И., Тишина В.Н. Анализ рынка банковских катр России // Молодой ученый. 2013. № 12. С.309

Abstract. *In the article the author considers one of the modern methods of fraud using bank cards - phishing, which is a network type of fraud, in which technically savvy scammers lure people with confidential information. The main task before the bank is to ensure the security of customer transactions and to control transactions on accounts in order to detect fraud. The article analyzes 30 suspended criminal cases of this category under point 1 of article 208 of the Code of Criminal Procedure of the Russian Federation (the person to be charged as an accused has not been established) for the period from October 2017 to April 2018.*

Keywords: *crime, fraud, bank card, phishing, Internet site.*

References:

1. Zavidov B.D. On the concept of fraud and its modifications in the criminal law of. // The Russian investigator. 2016. №2. Pp. 20-28

2. Larichev V.D., Spirin G.M. Commercial fraud in Russia. Ways to commit. Methods of protection. M .: "Exam", 2015.S.187

3. Frolova O.Yu. The modern market of Russian banking products // The Baltic Humanities Journal. 2014 No. 3. P. 93-96

4. On the national payment system: Federal Law: adopted by the State Duma on 27.06.2011 № 161-FZ // Access from the reference. - legal system "ConsultantPlus". (as of July 18, 2017)

5. URL: http://u-sahalinsky.sah.sudrf.ru/ (reference date is April 9, 2018)

6. Ivleva GI, Tishina V.N. Analysis of the Russian banking market market // Young Scientist. 2013. No. 12. P.309