УДК 343.72:657

КАК НЕ СТАТЬ ЖЕРТВОЙ КАРТОЧНЫХ МОШЕННИКОВ. ЛИЧНЫЙ ОПЫТ

Исаева В.В., студентка 5 курса экономического факультета
***Научный руководитель – Банникова Е.В., кандидат экономических наук*, доцент**
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: «*карточное» мошенничество, пластиковая карта, мошенники, платежные карты, скимминг, фишинг, вишинг, траппинг.*

В статье описываются наиболее часто встречающиеся способы мошенничества в сфере пластиковых карт, а именно: скимминг, фишинг, вишинг, траппинг. Также приведен пример из личного опыта.

Быстрое развитие современных технологий в сфере электронных платежных систем освобождает граждан от необходимости держать при себе наличные денежные средства. Тем не менее, наряду с удобством безналичного расчета вероятность стать жертвой мошенника увеличивается.

Мошенники придумывают все новые изощренные способы кражи денежных средств с банковских карт. Мощным оружием, в сфере информационных технологий, оказывается их опыт. Преступники совершенствуют как собственные технологии, так и психологические способы, чтобы «раскусить» обладателя заветной пластиковой карточки. Происходит постоянное соревнование между средствами защиты, которые создаются по заказу кредитных организаций, и средствами незаконного доступа к денежным средствам, которые изобретаются правонарушителями. К самым часто встречающимся можно отнести: с помощью мобильных телефонов, через сеть «Интернет», мобильный банк и другие.

Рассмотрим более подробно некоторые способы. Например, скимминг, принцип работы данного вида «карточного» мошенничества заключается в похищении реквизитов пластиковой карты с помощью скиммер. Данное устройство снимет данные карты с магнитной полосы, а мини-камера или прозрачная пленка, расположенная на панели набора ПИН-кода, способствует мошенникам получить код доступа к банковской карте. В результате проведенной операции мошенник получает все необходимые данные для создания «карты-клона», что позволит похищать денежные средства с банковского счета потерпевшего.

Фишинг, данный вид мошенничества заключается в создании поддельного сайта банка, моделировать работу настоящего. Затем мошенники делают рассылку электронных писем, спам-сообщений клиентам кредитной организации, заманивая их на поддельный сайт, где требуют указать сведения о карте, а конкретно: номер карты, ПИН-код. К примеру, преступники от имени банка рассылают сообщения о том, что в системе банка, который обслуживает это лицо, будут выполняться корректировки, из-за чего требуют сказать данные карты (номер, ПИН-код) либо пройти по ссылке «обозначенной ниже» и заполнить анкету. В результате лицо, переходя по ссылке, попадает на поддельный сайт банка и указывает данные карты. Соответственно информация попадает в руки мошенников.

Вишинг, данный способ обмана является аналогом фишинга, средством совершения аферы является телефон. К примеру, клиент получает звонок от «работника» службы безопасности банка, который сообщает о попытке незаконного списания денежных средств со счета. Подставной сотрудник просит перезвонить по указанному им сотовому телефону, что и делает жертва. Соответственно указанный номер является подставным, позвонив по которому потерпевшего требуют сказать данные своей карты либо отправить SMS-сообщение с информацией о карте.

Траппинг, механизмом работы этого способа обмана является установление специального удерживающего платежную карту устройства на банкомат. Соответственно, человек вставляет карту в банкомат, она теряется. Пока жертва едет в отделение банка, к банкомату подходит злоумышленник как ни в чем не бывало убирает устройство, забирает карту, опустошая при всем этом ваш банковский счет.

Для подтверждения актуальности и серьёзности проблемы мошенничества с банковскими картами приведу пример из личного опыта. Летом прошлого года мною было выставлено на сайт «Авито» объявление о продаже определённой продукции собственного приготовления. В скором времени со мной связались, якобы, представители кафе и предложили стать их постоянным поставщиком. Так называемые покупатели, пообещали выкупить крупную партию моей продукции в начале недели, осуществив предоплату в половину стоимости, а оставшуюся часть суммы перечислить после поставки продукции в конце недели.

После того, как я согласилась, покупатели попросили предоставить им все данные с моей банковской карты, якобы, для того чтобы внести её реквизиты в базу данных кафе. Затем, представители кафе, пояснили, что на привязанный к карте номер телефона начнут посту-

пать коды, которые будет необходимо сообщать им. На этом моменте я должна была проявить осторожность и предусмотрительность. Однако, они говорили настолько убедительно, грамотно и чётко, что у меня и мысли не возникло, что передо мной самые настоящие мошенники, которые пользуются моей наивностью и доверием.

Следовательно, называя код регистрации, я сама лично предоставила им возможность доступа в мой «Сбербанк Онлайн». Далее мне на телефон стали поступать смс-сообщения, в которых говорилось о пополнении моего счёта на суммы в 300 руб. Однако, вход в мой личный кабинет «Сбербанк Онлайн» был заблокирован. Как оказалось, мошенники похитили все имеющиеся на моей банковской карте денежные средства в сумме около 6000 руб. Через несколько минут мы поняли, что произошло и перезвонили им. В результате непродолжительного разговора мошенники в грубой форме дали понять, что украденная сумма - для них не деньги, и чтобы мы не беспокоили их.

Сотрудники Сбербанка направили меня обратиться в правоохранительные органы и дали пояснение, что такие случаи сейчас часто происходят и практически каждый день к ним обращаются люди, пострадавшие от подобных действий. Но обратившись в полицию, мне дали понять, что вернуть денежные средства - это очень трудозатратно и вряд ли кто-то за это дело возьмётся. В возбуждении дела мне не отказали, но предупредили, что, так как я обучаюсь в другой области, сумма денежных средств, потраченных на дорогу за время расследования может превысить сумму похищенных средств и нет никаких гарантий, что похищенное удастся вернуть. Таким образом, я решила не подавать заявление и смириться со случившимся.

Подводя итоги данной статьи, можно сделать вывод, что существует немало способов мошенничества с использованием платежных карт. Мошенники, изобретая новые способы вымогательства, ловко адаптируются к ходу прогресса. Обладателям пластиковых карт необходимо проявлять осторожность при пользовании различных банкоматов, услуг в сети «Интернет», внимательно заполнять анкеты на различных сайтах, не отвечать на подозрительные звонки и смс.

Библиографический список:

1. Мешкова, Е. В. Мошенничество с банковскими картами / Е. В. Мешкова, Е. В. Митрошина // Контентус. - 2016. - № 8. - С. 117-120.
2. Танасейчук, Я. В. Мошенничество с использованием пластиковых карт / Я. В. Танасейчук // Право: современные тенденции : материалы V Международ-

ной научной конференции. – Краснодар : Новация, 2018. - С. 57-62.
3. Хамзина, О. И. Методы фальсификации финансовой отчетности / О. И. Хамзина, Е. В. Банникова, С. В. Андреев // Экономика и предпринимательство. - 2017. - № 8-4 (85). - С. 1066-1070.
4. Климушкина, Н. Е. Порядок и правила создания резерва по сомнительным долгам в налоговом учете / Н. Е. Климушкина, Л. М. Прохорова // Наука и образование в XXI веке : материалы Международной научно-практической конференции. – Ульяновск, 2013. - С. 41-43.
5. Банникова, Е. В. Внутренний аудит в системе экономической безопасности / Е. В. Банникова, О. И. Хамзина, А. А. Навасардян // Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения : материалы Национальной научно-практической конференции. - Ульяновск : УлГАУ, 2019. - С. 225-229.

HOW NOT TO BECOME A VICTIM OF CARD SCAMMERS. PERSONAL EXPERIENCE

Isaeva V. V.

Keywords: *«card» fraud, plastic card, scammers, payment cards, skimming, phishing, vishing, trapping.*

The article describes the most common methods of fraud in the field of plastic cards, namely: skimming, phishing, vishing, trapping. An example from personal experience is also given.