ГОСУДАРСТВО И ПРАВО, 2021, № 12, с. 181–185
STATE AND LAW, 2021, № 12, pp. 181–185

УДК 343.2
ББК 67.99 (5У) 8

О МЕРАХ ПО ПРОТИВОДЕЙСТВИЮ МОШЕННИЧЕСТВУ (НА ПРИМЕРЕ ФИШИНГА)

© 2021 г. А. Б. Сабырбаева

Академия МВД Республики Узбекистан, г. Ташкент

E-mail: a_sabyrbaeva@inbox.ru

Поступила в редакцию 27.11.2020 г.

Аннотация. В статье рассматриваются виды мошенничества в сфере платежных систем, а также с использованием информационно-коммуникационных технологий, с приведением примеров из практики и выводов для противодействия распространенных видов мошенничества, таких как фишинг и скимминг.

Ключевые слова: кибермошенничество, скимминг, фишинг, информационно-коммуникационные технологии, платежные системы, лжесайт, противодействие.

Цитирование: *Сабырбаева А.Б.* О мерах по противодействию мошенничеству (на примере фишинга) // Государство и право. 2021. № 12. С. 181–185.

DOI: 10.31857/S102694520017465-2

ON MEASURES TO COUNTER FRAUD (USING THE EXAMPLE OF PHISHING)

© 2021 A. B. Sabyrbaeva

Academy of MIA of the Republic of Uzbekistan, Tashkent

E-mail: a_sabyrbaeva@inbox.ru

Received 27.11.2020

Abstract. The article discusses types of fraud in the field of payment systems, as well as using information and communication technologies, with examples from practice and conclusions to counter common types of fraud, such as phishing and skimming.

Key words: cyber fraud, skimming, phishing, information and communication technologies, payment systems, false website, counter.

For citation: *Sabyrbaeva, A.B. (2021).* On measures to counter fraud (using the example of phishing) // Gosudarstvo i pravo=State and Law, No. 12, pp. 181–185.

Общеизвестно, безналичная система расчетов с использованием банковских платежных карт продолжает внедряться в нашу жизнь из-за удобства в применении, возможности быстро осуществить оплату услуг без очереди и бумажной волокиты. В мире выпущено более 1.5 млрд пластиковых карт. Каждый год мировой оборот составляет свыше 3 трлн долл. Карты принимаются более чем в 20 млн торговых организаций[1].

[1] См.: URL: https://www.kp.ru/guide/plastikovye-karty-bankov.html

Согласно статистике Центрального банка Республики Узбекистан, в 2019 г. было эмитировано на 14.8% больше пластиковых карт, т.е. 20.5 млн штук. Объем платежей, осуществленных только через платежные терминалы, за 2019 г. составил 71 млрд сум[2]. Наибольшее количество карт среди госбанков эмитировано Народным банком – 4 млн (рост на 7.5%), с участием иностранного капитала 879.2 тыс. (рост на 27.6%), частными банками: Ориент Финанс Банком – 252.4 тыс. (рост на 16.1%)[3].

Данный показатель указывает на востребованность у населения банковских карт в связи с легкостью и выгодой его использования в плане экономии временных и материальных затрат. Но при использовании их необходимо помнить о некоторых негативных последствиях. Сфера оказания банковских услуг, платежи с использованием пластиковых карт, в частности электронные, при таком обороте денежных средств все больше привлекают мошенников.

Несмотря на то что данный вид мошенничества появился в Республике Узбекистан сравнительно недавно, уже в 90-х годах XX в. были разработаны технологии, позволявшие выявлять факт совершения мошенничества. Один из первых разработчиков таких технологий – Falcon; другие ведущие программные решения для т.н. пластикового мошенничества включают Actimize, SAS, BAE Systems Detica и IBM.

Техника фишинга была подробно описана в 1987 г., а сам термин появился 2 января 1996 г. в новостной группе alt.online-service.America-Online сети Usenet, хотя возможно его более раннее упоминание в хакерском журнале 2600[4].

Преступления с использованием платежных карт требуют повышенного внимания, поскольку мошенники причиняют ущерб не только непосредственно пострадавшим, но в т.ч. кредитным организациям и государству, подрывая доверие к ним. Достаточно вспомнить ситуацию, связанную с шифровальщиками WannaCry и ExPetr, которые парализовали работы компьютерных систем. Суть данной атаки была в том, что пользователи, подвергшиеся вирусной атаке, получали предупреждение о выплате выкупа в криптовалюте, в противном случае восстановление файлов невозможно. Как правило, большинство пострадавших, боясь потери ценной информации на устройстве, производили оплату, но даже в этом случае код расшифровки не присылался.

Мошенничество можно разделить на следующие виды:

с использованием банкоматов (скимминг, банкомат-призрак, Ливанская петля, траппинг);

путем создания фиктивных сайтов и рассылки e-mail сообщений (фишинг);

с выуживанием кода пластиковой карты пострадавшего под видом перевода денежных средств (интернет-благотворительность);

мошеннические приложения (MasterCraft for Minecraft, Skins, Mods, Maps for Minecraft PE, Boys and Girls Skins);

с использованием виртуального (фишинг) или офлайн (скимминг) пространства;

не существующие пластиковые карты Card not present fraud – CNP (в Австралии такой вид мошенничества составил 85% от общего числа пластикового мошенничества с убытком около 500 млрд долл.[5]).

Существует еще много разновидностей пластикового мошенничества. Хотелось бы акцентировать внимание на наиболее распространенных из них.

К примеру, фишинг (англ. *phishing*, от *fishing* – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям[6].

По данным центра жалоб на интернет-преступления ФБР, мошеннические действия типа BEC привели к фактическим потерям в размере более 4.5 млрд долл., и они представляют собой глобальную проблему[7]. Опасность данных писем заключается в призыве незамедлительно ответить на сообщение или перейти по ссылке из-за якобы чрезвычайной срочности дела. Именно данная уловка используется в большинстве случаев самими фишерами. Об опасности данного нового мошенничества говорила Л.С. Хафизова[8], об одном из видов фишинга – Н.С. Юрочкин[9].

Нельзя согласиться с мнениями Р.Х. Хурсанова и А.У. Анорбоева[10] о том, что фишинг осуществляется путем передачи писем пользователям от кредитных организаций. Это одна из разновидностей фишинга, но отправители и адресаты могут быть разные.

В недавней фишинговой кампании группа 74 (также известная как Sofact, APT28, Fancy Bear) нацелилась на профессионалов в области кибербезопасности. Было написано электронное письмо, якобы связанное с конференцией Cyber Conflict U.S. Conference, вложение являлось документом, содержащим вредоносный макрос Visual Basic для приложений (VBA), который загружал и запускал разведывательное вредоносное программное обеспечение, называемое Seduploader[11]. А это уже более усовершенствованный вид фишинга, который имеет больший охват, несмотря на узкий круг пострадавших.

---

[2] См.: Статистический бюллетень Центрального банка Республики Узбекистан. 2019 год. С. 322.

[3] См.: URL: www.nuz.uz

[4] См.: URL: https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3#%D0%A0%D0%B0%D0%BD%D0%BD%D0%B8%D0%B9_%D1%84%D0%B8%D1%88%D0%B8%D0%BD%D0%B3_%D0%BD%D0%B0_AOL

[5] См.: *William Joley.* Common credit card frauds and how to avoid them. July 10, 2019. URL: https://www.savings.com.au/credit-cards/credit-card-fraud

[6] См.: URL: https://ru.wikipedia.org. Фишинг

[7] См.: URL: https://www.osp.ru/winitpro/2019/03/13054903

[8] См.: *Хафизова Л.С.* Уголовно-правовые и криминологические аспекты противодействия финансовому мошенничеству: автореф. дис. ... канд. юрид. наук. Н. Новгород, 2008.

[9] См.: *Юрочкин Н.С.* Кибермошенничество: характеристика, приемы и методы его совершения // Таврический науч. обозреватель www.tavr.science. 2016. № 12 (17). Ч. 2. С. 158.

[10] См.: *Хурсанов Р.Х., Анорбоев А.У.* Киберфирибгарлик жинояти: жиноий-ҳуқуқий ва криминологик тавсифи. Б. 306. Юридик фан ва ҳуқуқни қўллаш амалиётининг долзарб муаммолари мавзусидаги илмий-амалий конференция материаллари I жилд. Toshkent, 2020.

[11] См.: URL: https://www.osp.ru/winitpro/2019/03/13054903

С.А. Сторчак выделил некоторые виды антифишинговых технологий, таких как: IP-адрес, точки, слеши в URL, пустые якоря и т.д.[12]

В уголовных кодексах Российской Федерации, Испании, Италии, ФРГ, КНР, Швейцарии мошенничество с использованием платежных карт выступает в качестве квалифицирующего состава преступления. Учитывая, что в уголовном законодательстве нет квалифицирующего признака, предусматривающего ответственность за пластиковое мошенничество, предлагается *дополнить часть 3 ст. 168 УК Республики Узбекистан пунктом «г» – с «использованием платежных, поддельных карт или электронных средств платежа»*.

Многие государства не только усиливают уголовную ответственность за совершение такого вида мошенничества, но и применяют меры по их предотвращению. Это касается не только государства в целом, профилактика мошенничества проводится и в частном секторе. Так, многие компании проводят тренинги, семинары среди персонала с целью предотвратить фишинговые атаки на их компьютерные системы, т.к. атака и поражение одного компьютера может привести к сбою работы всей фирмы и принести огромный ущерб. Но эффективность данной практики как семинары и беседы с сотрудниками для того, чтобы они были бдительными и не нажимали на сомнительные ссылки, неизвестна. На сайте ООН опубликована статья «Остерегайтесь мошенников» с предупреждением о том, что мошенники, действуя от их имени, взимают плату за якобы трудоустройство, а также запрашивают номера и коды банковских карт.

Данный факт, что мошенники используют в своих интересах имена всемирных организаций, говорит о масштабе их деятельности. Многие организации, занимающиеся вопросами киберпреступности и борьбой с фишингом, остерегают от пользования «сомнительными» сайтами (не нажимать на ссылки, отправленные по электронной почте, и т.д.). Но как же определить, действительно ли эта ссылка сомнительна и есть угроза фишинговой атаки, ведь мошенники создают рассылки и лжевеб-сайты известных фирм с точностью до цветов и шрифта надписей. Так, к примеру, Яндекс отправляет своим зарегистрированным пользователям письма с предостережением от фишинговых атак мошенников с названием «Как отличить хорошие письма от писем мошенников». Однако в данном письме имеется лишь информация, что следует обратить внимание на внешний вид сайта. Хотя сами далее утверждают, что поддельные сайты часто выглядят как страницы реально существующих серверов. А в случае набора секретной информации злоумышленники получают доступ не только к почтовому ящику, но и к профилям в социальных сетях и интернет-банку. Хотя это и общеизвестный факт, но все же как сократить рост фишинговых атак и уберечь себя и свои накопления?

Для борьбы с фишингом А.А. Казыханов и И.Т. Байругин рекомендуют «проведение инструктажей со всем персоналом компании; использование защитного программного обеспечения; принцип доверия важной информации только квалифицированным сотрудникам»[13].

Национальный центр кибербезопасности Соединенного Королевства (NCSC)[14] указывает на ряд трудностей в ходе «антифишингового образования», в частности в связи с нарастающим количеством и объемом фишинговых угроз, а также необходимостью принятия мер по объединению технических средств защиты в виртуальном пространстве с повышением уровня осведомленности пользователей о распространенных видах фишинговых атак и способах информирования о них.

Так, получается повышение осведомленности пользователей это еще не залог успеха в борьбе с фишингом. Для изучения эффективности проведения профилактики, семинар-тренингов среди сотрудников, а также в целях изучения потенциального влияния на восприимчивость к фишингу ученые из Бристольского университета Э. Вильямс (Williams) и А. Джоинсон (Joinson) провели исследование, по результатам которого было выяснено, что «факторы относительно полученной эффективности защитной информации могут прямо влиять на будущее намерение на взаимодействие с данной информацией»[15], т.е. при установлении эффективности информации для защиты от фишинга пользователи склонны использовать ее в виртуальном пространстве.

Но не только эти меры могут защитить от фишинговой атаки. Согласно проведенному исследованию в большинстве случаев письма от мошенников, предлагающие перейти по ссылке на какой-то сайт, содержат бессмысленные наборы букв, цифр и символов. Официальный сайт банка или другого государственного учреждения, компании содержит название, которое имеет отношение к его деятельности.

Фишинговые атаки направлены на дезинформацию потенциального пострадавшего и побуждение перейти по ссылке, базируясь на таких человеческих качествах, как неосторожность, торопливость, невнимательность. Д.В. Бахтеев также считает, что «самая распространенная и опасная форма фишинга – рассылка пользователям интернет-банков электронных писем, содержащих уведомление о необходимости произвести какие-то действия с учетной записью и ссылку, внешне похожую на адрес входа в личный кабинет пользователя. В указанных способах интернет-мошенничества вместо прямого взлома защищенной системы (например, интернет-банка) мошенники используют уязвимость психологии пользователя, его невнимательность, индифферентное отношение к рутинным операциям, доверчивость, жажду наживы»[16].

На основании расследованных непосредственно самим автором уголовных дел касательно фишинга следует выделить несколько ключевых обстоятельств, в результате которых происходит виктимизация от фишинговых атак:

при наличии в фишинговых письмах аргументов с высоким качеством (более правдоподобные, соответствуют стилистике письма и манере написания «отправителя», соответствуют тематике ведения переписки);

---

[12] См.: *Сторчак С.А.* Обзор антифишинговых технологий // Проблемы науки. 2019. № 6 (42). С. 9–11.

[13] *Казыханов А.А., Байругин И.Т.* Фишинг, как проблема для специалистов отдела ИБ // Символ науки. 2016. № 10–2. С. 54.

[14] См.: NCSC Phishing Attacks: Defending Your Organisation. URL: https://www.ncsc.gov.uk/phishing (дата обращения: 10.07.2018).

[15] *Williams E.J., Joinson A.N.* Developing a measure of information seeking about phishing // Journal of Cybersecurity. 2020. Vol. 6. No. 1. P. 13.

[16] *Бахтеев Д.В.* О некоторых современных способах совершения мошенничества в отношении имущества физических лиц // Росс. право. 2016. № 3. С. 25.

если они пришли от источника с «высоким уровнем» доверия (друзья, начальство, коллеги, банк);

если жанр письма соответствует источнику (фоновые иллюстрации, шрифт, картинки, цвета, контраст, расположение письма, качество изображений, надписи);

если имеет место большой временной прессинг («СРОЧНО!», «НЕЗАМЕДЛИТЕЛЬНО», «ОЧЕНЬ ВАЖНО»).

Сообщения, используемые в фишинговых атаках, содержат по крайней мере некоторое ложное или противоречащее содержание, которое обычно может быть идентифицировано при достаточной систематической обработке. Существенным вкладом было исследование, проведенное Xin (Robert) Luo, Wei Zhang, Stephen Burd, Alessandro Seazzu[17], в котором было изучено влияние эвристической систематической модели обработки информации HSM, разработанной Чайкеном, на виктимизацию при фишинговых атаках. Они пришли к заключению, что концентрация на технологиях идентификации отправителей, а также обучении пользователей может способствовать привлечению внимания к выявлению поддельных и настоящих отправителей путем обучения специально ориентированным методам и навыкам.

Фишеры при попытке совершить фишинговую атаку на определенную организацию проводят исследование переписки, ведения дел, также изучают сотрудников, их увлечения по аккаунтам в социальных сетях. Целью является составление целевого фишингового письма, особенно данный метод применяется, когда в качестве пострадавшего выбирают самого руководителя, т.к. в отличие от простого сотрудника доступ к его данным может предоставить возможность получить более ценную информацию, которая впоследствии может принести большую прибыль. Поэтому необходимо быть осторожным при выкладывании частной информации, особенно о месте работы и обговаривать данный пункт (соблюдение конфиденциальности) при составлении договора при найме на работу.

Другая мера предосторожности для защиты в виртуальном пространстве – это необходимость включения функции оповещения о сомнительных или подозрительных сайтах, которая имеется в любом телефоне. Рекомендуется также не входить в такие сайты, даже если на этом сайте имеется необходимая информация или в ней объявлены невероятные скидки и акции по розыгрышу автомобиля или целого дома. Данные сайты служат для привлечения как можно большого количества людей для дальнейшего завладения информацией о пользователе или его банковских данных, в лучшем случае для проведения маркетинга или рекламы продукции.

К тому же, мало кто обращает внимание на аббревиатуры типа http и https. HTTP (Hypertext Transfer Protocol) – это протокол прикладного уровня передачи данных изначально – в виде гипертекстовых документов в формате HTML, используется для передачи произвольных данных[18].

Хотя большинство сайтов государственных учреждений, крупных компаний и в целом сайт организаций, осуществляющих легальную деятельность, начинаются с аббревиатуры www. либо https. Буква «S» в протоколе https означает слово «безопасный» (англ. *secure*). То есть данный сайт проверен на наличие опасности и является безопасным для использования, т.к. обеспечивает конфиденциальность информации путем ее шифрования. При использовании сторонних сайтов либо при поиске информации необходимо ориентироваться также и на такие нюансы безопасного интернета.

Данные правила являются далеко не исчерпывающими, но, поскольку мошенники всегда в поисках лазеек, чтобы обойти систему, осознав, что компьютер взломать труднее, они ориентируются на человеческий фактор (азарт, желание разбогатеть, получить скидку, выиграть в лотерее и т.д.) при фишинговых атаках. Поэтому необходимо соблюдать осторожность и обращать внимание на особенности и правила безопасного использования интернета во избежание траты денежных средств.

* * *

Исходя из вышеизложенного, автор сформулировал комплекс мер по противодействию одному из видов пластикового мошенничества – фишингу.

1. Дополнить часть 3 ст. 168 УК Республики Узбекистан пунктом «г» – с «использованием платежных, поддельных карт или электронных средств платежа».

2. Для защиты от фишинга отправлять пользователям только проверенную и доказавшую свою эффективность информацию.

3. В структуре и системе организации при найме на работу персонала проводить инструктаж по борьбе с кибермошенничеством и мерам противодействия фишингу, в случае фишинговой атаки на компанию сотрудник несет персональную ответственность за принесенные убытки.

4. Установление иерархии среди сотрудников, в соответствии с которой в зависимости от важности и конфиденциальности информации к каждой категории выдается допуск на ту или иную информацию, как в военных учреждениях.

5. Обращать внимание на аббревиатуры типа http и http**S**, где буква «S» (безопасный) указывает на предварительную проверку сайта на наличие опасности.

6. Выделены ключевые обстоятельства, в результате которых происходит виктимизация от фишинговых атак.

7. Обязательное включение функции оповещения о сомнительных или подозрительных сайтах, которая имеется в любом телефоне или компьютере.

Современные виды мошенничеств представляют большую опасность, нежели обычное мошенничество, в связи с тем, что предполагают создание преступной группы специалистов, владеющих компьютерными навыками, имеют более широкий круг пострадавших, в некоторых случаях имеют возможности, каналы для перенаправления денежных средств на зарубежные банковские счета, чтобы уклониться от ответственности. Поэтому усиление мер по их противодействию должно быть прерогативой правоохранительных органов.

[17] См.: *Xin (Robert) Luo, Wei Zhang, Stephen Burd, Alessandro Seazzu.* Investigating phishing victimization with the HeuristicSystematic Model: A theoretical framework and an exploration. Anderson School of Management, University of New Mexico, 1924 Las Lomas NE, MSC05 3090, Albuquerque, NM 87131, USA. URL: http://dx.doi.org/10.1016/j.cose.2012.12.003

[18] См.: URL: www.wikipedia.com; https://g.co/kgs/4PNRWv

СПИСОК ЛИТЕРАТУРЫ

1. *Бахтеев Д.В.* О некоторых современных способах совершения мошенничества в отношении имущества физических лиц // Росс. право. 2016. № 3. С. 25.
2. *Казыханов А.А., Байругин И.Т.* Фишинг, как проблема для специалистов отдела ИБ // Символ науки. 2016. № 10–2. С. 54.
3. *Сторчак С.А.* Обзор антифишинговых технологий // Проблемы науки. 2019. № 6 (42). С. 9–11.
4. *Хафизова Л.С.* Уголовно-правовые и криминологические аспекты противодействия финансовому мошенничеству: автореф. дис. ... канд. юрид. наук. Н. Новгород, 2008.
5. *Юрочкин Н.С.* Кибермошенничество: характеристика, приемы и методы его совершения // Таврический научный обозреватель www.tavr.science. 2016. № 12 (17). Ч. 2. С. 158.
6. *William Joley.* Common credit card frauds and how to avoid them. July 10, 2019. URL: https://www.savings.com.au/credit-cards/credit-card-fraud
7. *Williams E.J., Joinson A.N.* Developing a measure of information seeking about phishing // Journal of Cybersecurity. 2020. Vol. 6. No. 1. P. 13.
8. *Xin (Robert) Luo, Wei Zhang, Stephen Burd, Alessandro Seazzu.* Investigating phishing victimization with the HeuristicSystematic Model: A theoretical framework and an exploration. Anderson School of Management, University of New Mexico, 1924 Las Lomas NE, MSC05 3090, Albuquerque, NM 87131, USA. URL: http://dx.doi.org/10.1016/j.cose.2012.12.003
9. *Хурсанов Р.Х., Анорбоев А.У.* Киберфирибгарлик жинояти: жиноий-ҳуқуқий ва криминологик тавсифи. Б. 306. Юридик фан ва ҳуқуқни қўллаш амалиётининг долзарб муаммолари мавзусидаги илмий-амалий конференция материаллари I жилд. Toshkent, 2020.

REFERENCES

1. *Bakhteev D.V.* About some modern ways of committing fraud against the property of individuals // Russ. law. 2016. No. 3. P. 25 (in Russ.).
2. *Kazykhanov A.A., Bakhrushin I.T.* Phishing as a problem for specialists of the Information security Department // Symbol of Science. 2016. No. 10–2. P. 54 (in Russ.).
3. *Storchak S.A.* Review of anti-phishing technologies // Problems of Science. 2019. No. 6 (42). P. 9–11 (in Russ.).
4. *Khafizova L.S.* Criminal-legal and criminological aspects of countering financial fraud: abstract ... PhD in Law. N. Novgorod, 2008 (in Russ.).
5. *Yurochkin N.S.* Cyberbullying: characteristics, techniques and methods of its commission // The Tauride Scientific Observer www.tavr.science. 2016. No.12 (17). Part 2. P. 158 (in Russ.).
6. *William Joley.* Common credit card frauds and how to avoid them. July 10, 2019. URL: https://www.savings.com.au/credit-cards/credit-card-fraud
7. *Williams E.J., Joinson A.N.* Developing a measure of information seeking about phishing // Journal of Cybersecurity. 2020. Vol. 6. No. 1. P. 13.
8. *Xin (Robert) Luo, Wei Zhang, Stephen Burd, Alessandro Seazzu.* Investigating phishing victimization with the HeuristicSystematic Model: A theoretical framework and an exploration. Anderson School of Management, University of New Mexico, 1924 Las Lomas NE, MSC05 3090, Albuquerque, NM 87131, USA. URL: http://dx.doi.org/10.1016/j.cose.2012.12.003
9. *Khursanov R.H., Anorboev A.U.* Cyberfiribgarlik zhinoyati: zhinoy-xukukiy va criminologist tavsifi. B. 306. Yuridik fan vayukukni kyllash amaliyetining dolzarb muammolari mavzusidagi ilmiy-amaliy conference materiallari I zhild. Tashkent, 2020.

Сведения об авторе

САБЫРБАЕВА Айнура Бахыт кызы –
докторант Академии МВД Республики Узбекистан; 100197 Республика Узбекистан, г. Ташкент, ул. Интизор, д. 68

Authors' information

SABYRBAEVA Aynura B. kizi –
doctoral candidate of the Faculty of Postgraduate education of the Academy of MIA of the Republic of Uzbekistan; 68 Intizor str., 100197 Tashkent, Republic of Uzbekistan