УДК 343.721
DOI: 10.26140/anie-2020-0902-0078

К ВОПРОСУ О МЕТОДАХ ЗАЩИТЫ ОТ ФИНАНСОВОГО КИБЕРМОШЕННИЧЕСТВА

© 2020

AuthorID: 736254
SPIN: 9502-6593
ResearcherID: V-1952-2018
ORCID: 0000-0002-7273-1852

Мальцева Светлана Михайловна, кандидат философских наук,
доцент кафедры философии и теологии

AuthorID: 1051665
SPIN: 5347-0851
ResearcherID: V-5218-2018
ORCID: 0000-0002-6629-0667

Строганов Дмитрий Александрович, старший преподаватель кафедры
Всеобщей истории, классических дисциплин и права
Кокорин Александр Романович, студент
Куликова Анастасия Антоновна, студент

Нижегородский государственный педагогический университет им. К. Минина
(603005, Россия, Нижний Новгород, Ульянова, 1, e-mail: cool.kulikova-anastasiya2001@yandex.ru)

Аннотация. В статье предлагается общий обзор финансовых киберпреступлений. Рассмотрены правовые последствия совершения киберпреступлений в разных странах. Указаны основные правила, позволяющие пользователям сети Интернет и банковских карт снизить риск остаться обманутыми кибермошенниками. Новизна исследования**:** формирование классификации существующих методов защиты от финансового кибермошенничества. Классификация осуществлена по нескольким основаниям: источник получаемых заведомо ложных и/или вредоносных данных, психологическая устойчивость потенциальных жертв, использование безналичных денег, физическое взаимодействие с объектами повышенного внимания мошенников. На основе данных проведенного среди студентов опроса отмечено, что большая часть из ни х уже имеет опыт столкновения с финансовым мошенничество в интернете. Полученные в результате исследования знания могут быть использованы держателями банковских карт и пользователями сети Интернет с целью защиты собственных денежных средств от мошенников, а также преподавателями школ на уроках по основам безопасности жизнедеятельности для повышения уровня знаний учащихся в области киберпространства.

Ключевые слова: кибермошенничество, кибермошенник, пластиковая карта, скимминг, фишинг, социальная инженерия, сеть Интернет, схема обмана, правовые последствия, правила предосторожности.

ON THE ISSUE OF METHODS OF PROTECTION AGAINST FINANCIAL CYBER FRAUD

© 2020

Maltseva Svetlana Mikhailovna, Candidate of Philosophy, Associate Professor
of the Department of Philosophy and Theology
Stroganov Dmitry Alexandrovich, senior lecturer of the Department
of universal history, classical disciplines and law
Kokorin Aleksandr Romanovich. student
Kulikova Anastasia Antonovna, student

Minin Nizhny Novgorod State Pedagogical University
(603005, Russia, Nizhny Novgorod, Ulyanov St., 1, e-mail: cool.kulikova-anastasiya2001@yandex.ru)

Abstract. The article offers a General overview of financial cybercrimes. The legal consequences of cybercrime in different countries are considered. The basic rules that allow users of the Internet and Bank cards to reduce the risk of being cheated by cybercriminals are specified. Novelty of the research: formation of a classification of existing methods of protection against financial cyber fraud. The classification was carried out on several grounds: the source of the deliberately false and/or malicious data received, the psychological stability of potential victims, the use of non-cash money, and physical interaction with the objects of increased attention of fraudsters. Based on data from a survey conducted among students, it was noted that most of them have already experienced financial fraud on the Internet. The knowledge obtained as a result of the research can be used by Bank card holders and Internet users to protect their own funds from fraud, as well as by school teachers in classes on the basics of life safety to improve the level of knowledge of students in the field of cyberspace.

Keywords: cybercrime, cybercrime, plastic card, skimming, phishing, social engineering, Internet, fraud scheme, legal consequences, precautionary rules.

ВВЕДЕНИЕ

Постановка проблемы. На сегодняшний день сеть Интернет и информационные технологии в «неправильных» руках могут стать настоящим оружием. Виртуальное пространство таит в себе немало опасностей, поэтому даже продвинутый пользователь может стать жертвой так называемого кибермошенника. Портрет злоумышленника сильно отличается от классического представления образа преступника [1]. Чаще всего это человек, который ранее не был судим, он хорошо образован и имеет глубокие познания в информационно-телекоммуникационной сфере. Среда, в которой совершаются противоправные действия, также имеет свои особенности. Интернет-пространство позволяет совершать анонимные действия оперативно и безопасно. Зачастую жертва и кибермошенник могут быть разделены сотнями или даже тысячами километров.

МЕТОДОЛОГИЯ

Формирование целей статьи. Классифицировать существующие методы защиты от финансового кибермошенничества.

Используемые в исследовании методы, методики и технологии. Исходя из цели, в работе были поставлены следующие *задачи исследования***: о**писать существующие виды финансового кибермошенничества и классифицировать методы защиты от него; проанализировать и сравнить правовые последствия кибермошенничества в разных странах. Также использован интернет-опрос студентов, проверяющий знания о возможностях и угрозах киберпространства.

Изложение основного материала исследования с полным обоснованием полученных научных результатов.

Число схем, с помощью которых можно обмануть пользователя глобальной сети, весьма велико. Одной из первых схем обмана стали так называемые «Нигерийские» письма, в которых незнакомец просит о помощи в переводе крупной суммы денег, а взамен обещает солидное вознаграждение, но для начала необходимо перевести небольшое количество средств на указанный счёт для оплаты банковских расходов [2, С. 284]. Схожа с «Нигерийскими» письмами схема под названием «Лотерея». Разница состоит лишь в том, что пользователю сообщают о большом выигрыше, а для его получения необходимо оплатить соответствующие расходы [2, С. 285; 3]. В обоих случаях после перевода денежных средств никакого вознаграждения и выигрыша пользователь не получает. Ещё один вид обмана скрывается в схеме, называемой «Подружка». С жертвой знакомится представитель противоположного пола, желающий поскорее встретиться с возлюбленным. Однако в скорее оказывается, что незнакомцу не хватает денег на билет, оформление визы и так далее. Жертву просят помочь, а после перевода денег на указанный счёт злоумышленник исчезает [2, С. 285]. Данные схемы дают представление только о незначительной части существующих на сегодняшний день методов обмана [4, 5, 6].

Часто жертвами финансовых кибермошенников становятся держатели банковских карт. Наиболее популярная схема у преступников – это скимминг, то есть изготовление поддельной банковской карты на основании украденных у владельца данных. Хищение происходит с помощью специальных устройств, считывающих информацию с магнитной полосы карты, во время использования банкомата. ПИН-код узнаётся по накладке на клавиатуру или при помощи видеокамер [7, С. 157]. Ещё один пример – это фишинг. Данная схема базируется на хищении персональных данных держателя банковской карты с помощью поддельных банковских сайтов [8, С. 1281]. Как и в случае мошенничества в сети Интернет, данные примеры являются лишь малой частью всего обилия преступных схем.

Следует отметить, что среди всех видов финансового кибермошенничества наиболее продуктивным является социальная инженерия. Она направлена на получение персональных данных под разными предлогами, часто с согласия самой жертвы. При этом злоумышленник заявляет о необходимости совершения каких-либо экстренных или неотложных действий, вводящих жертву в заблуждение [9].

Появление нового вида мошенничества привело к необходимости борьбы с ним. В результате в законодательствах многих стран появились определения, описывающие данное преступление, и статьи, предусматривающие наказание за его совершение. Так, например, в США первый закон о мошенничестве с использованием компьютеров был принят ещё в 1984 году. С того времени он неоднократно дополнялся. Санкциями за данный вид преступления являются денежные штрафы и лишение свободы [10]. Отметим, что в настоящий момент Конгресс США считает необходимым уравнять киберпреступления с преступлениями, происходящими в не виртуальной среде, по степени их общественной опасности. В законодательстве Германии компьютерное мошенничество охватывается одним понятием, включающим множество разновидностей данного преступления. Пойманному злоумышленнику может грозить до трёх лет лишения свободы. В Японии существует собственная классификация киберпреступлений, состоящая из проникновения в компьютеры и преступлений, связанных с использованием сети Интернет. Понятие «компьютерное мошенничество» относится к первой классификации, а понятие «мошенничество» - ко второй. Наказание за киберпреступления в Японии очень сурово – лишение свободы на срок до 10 лет [11].

В Уголовном кодексе Российской Федерации не существует норм, связанных с «компьютерным мошенничеством». Постановление Пленума Верховного суда СССР от 5.09.1986 г. №11 «По делам о хищении личной собственности» описывает главный признак мошенничества – добровольность передачи потерпевшим имущества или права на имущество виновному под влиянием обмана или злоупотребления доверием. Однако в случае с «компьютерным мошенничество» добровольность, как главный признак, отсутствует, поскольку потерпевший может ничего не знать о передаче имущества или права на имущество в момент этой передачи, и вообще не желать её. В то же время нельзя ввести статью с названием «Компьютерное мошенничество», так как понятие «мошенничество» имеет обязательный волевой признак, а в законодательной практике один термин должен иметь одно определение [12, 13].

В российском законодательстве деяния, связанные с мошенничеством, регулируются 159 и 272 статьями УК РФ, в малой степени защищающими обманутых киберпреступниками. Санкциями за данный вид преступления могут служить штраф в размере до 500 тысяч рублей, исправительные работы на срок до 2-х лет, ограничение или лишение свободы на срок до 3-х лет.

Сравнивая законодательства представленных стран, можно сделать вывод, что в России правовое регулирование киберпреступности на данный момент не соответствует реалиям жизни. Существует потребность в доработке и внесении изменений в действующее законодательство.

Число видов кибермошенничества на сегодняшний день велико, но существуют определённые правила, позволяющие снизить риск остаться обманутым. Эти правила можно проклассифицировать.

Первое основание для классификации – это источник получаемых заведомо ложных и/или вредоносных данных. Отсюда следуют некоторые правила предосторожности. Во-первых, файлы, полученные из сети Интернет, необходимо проверять при помощи антивируса. Особенно те, которые получены от неизвестных отправителей. Во-вторых, необходимо быть осторожным при переходе по неизвестным ссылка и всегда проверять их правильность. В-третьих, не следует заполнять анкеты и формы, полученные из неизвестных источников. Персональные данные можно оставлять только на защищённых сайтах. И, наконец, при получении писем по электронной почте необходимо обращать внимание на число адресатов, так как крупные организации не занимаются рассылкой, если необходимо узнать личные данные клиента [14].

Второе основание для классификации – это психологическая устойчивость потенциальных жертв. Чтобы не остаться обманутым, необходимо придерживаться определённых правил. Во-первых, в любой ситуации необходимо сохранять спокойствие, не принимать необдуманных решений, а всю полученную информацию проверять у официальных представителей организаций, поскольку один из методов работы мошенников заключается во введении жертвы в стрессовое состояние. Во-вторых, в случае каких-либо технических неполадок, возникающих при использовании сети Интернет или банковской карты, не нужно сообщать конфиденциальную информацию незнакомым лицам, даже если они хотят помочь. В подобных ситуациях следует обращаться в службу поддержки [15, 16].

Третье основание для классификации – это использование безналичных денег. Исходя из этого, следует придерживаться определённых правил. Во-первых, кроме основной банковской карты необходимо иметь дополнительную, которая будет служить для совершения покупок в сети Интернет. На неё следует переводить такое количество денег, которое необходимо для совершения покупки. Во-вторых, помимо материальных карт, следует иметь виртуальные, предоставляемые различными платёжными системами. В-третьих, следует установить ограничение на количество средств, которые можно пе-

ревести за один раз с одной карты на другую.

Четвёртое основание для классификации – это физическое взаимодействие с объектами повышенного внимания мошенников. На основании данной классификации существуют определённые правила предосторожности. Во-первых, необходимо проводить постоянный мониторинг состояния собственных счетов и отслеживать проводимые операции на предмет наличия посторонних действий, не совершаемых владельцем счёта. Во-вторых, информацию, содержащую секретные сведения, например, ПИН-код банковской карты, необходимо хранить в тайне. И, наконец, пользоваться нужно только теми банкоматами и терминалами, которые установлены в отделениях банка или в крупных магазинах.

В ходе исследования в декабре 2019 года среди студентов вузов был проведён интернет-опрос на тему «Киберпространство: возможности и угрозы». В опросе приняло участие 90 человек. Данная группа была выбрана потому, что период раннего студенчества – это время, на которое часто приходится самостоятельное планирования своего бюджета, большей свободы от родительского контроля, но все еще редко кто из студентов имеет самостоятельный заработок [17, 18]. Вопросы и ответы были следующими: «Как часто Вы пользуетесь Интернетом?» - 100% ответили «Каждый день»; «Вам приходилось оставаться финансово обманутым вследствие собственной доверчивости в сети Интернет?» - 66,7% ответили «Нет», 33,3% ответили «Да, приходилось»; «Приходилось ли Вам сталкиваться с подозрительными сообщениями на электронной почте?» - 88,9% ответили «Да», 11,1% ответили «Нет»; «Есть ли у Вас банковская карта?» - 88,9% ответили «Да», 11,1% ответили «Нет»; «Чему вы отдаёте предпочтение: наличным деньгам или оплате по карте?» - 66,7% ответили «Банковская карта», 33,3% ответили «Наличность»; «Знакомы ли вы с правилами защиты от финансового кибермошенничества?» - 66,7% ответили «Да», 22,2% ответили «Нет», 11,1% ответили «Впервые слышу».

Таким образом, можно сделать вывод о том, что подавляющее большинство студентов не только регулярно пользуется интернет-пространством, но и совершает в нем некоторые финансовые операции, зачастую предпочитая такую форму традиционной оплате наличными средствами. Практически все сталкивались с подозрительной финансовой информацией в сети и две трети пострадали, но лишь чуть больше половины опрошенных имеют представление о том, как можно себя обезопасить.

ВЫВОДЫ

Выводы исследования. Жизнь современного человека практически невозможно представить без доступа в Интернет. Ежедневно каждый пользователь глобальной сети получает большое количество информации, которая, к сожалению, не всегда является достоверной, а зачастую наносит вред. Именно поэтому каждому человеку следует проявлять бдительность во время нахождения в виртуальном пространстве. Безналичные расчёты так прочно вошли в повседневную жизнь, что уже трудно представить, как обойтись без банковской карты. Однако при её использовании следует учитывать риск остаться жертвой преступной схемы [19-22]. И всё же, несмотря на обилие подстерегающих каждый день опасностей, при соблюдении определённых правил безопасности вероятность остаться обманутым значительно снижается, что позволяет сохранить не только денежные средства, но и психологическое здоровье.

СПИСОК ЛИТЕРАТУРЫ:

1. Буряк В.В. Цифровая экономика, хактивизм и кибербезопасность: монография. Симферополь: ИП Зуева Т. В., 2019. 140 с.

2. Бураева Л.А. О вопросах противодействия кибератакам, совершаемым в интернет-пространстве на современном этапе // Пробелы экономики и юридической практики. 2018. №3. С. 284-286.

3. Гальченко А.С. Особенности мотивационной структуры гражданской активности подростков с разным статусом гражданской идентичности // Вестник Мининского университета. 2019. № 3 (28). С. 8.

4. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. дис. ... канд. юр. наук: 12.08.08 – уголовное право и криминология; уголовно-исполнительное право. Владивосток, 2005. 28 с.

5. Бабаева А.В., Крашенинников А.А. Антропологическое измерение пространства современного города // Вестник Мининского университета. 2019. Т.7 № 2 (27). С. 14.

6. Строганов Д.А. Проблема герметических сообществ в контексте исторической антропологии // Вестник Мининского университета. 2016. № 1-2 (14). С. 28.

7. Юрочкин Н.С. Кибермошенничество: характеристика, приёмы и методы его совершения. //Таврический научный обозреватель. 2016. №12. С. 156-159.

8. Гришина Е.А. Риски в платежных системах: мошеннические схемы в мире банковских карт // Финансы и кредит. 2018. №6. С. 1280-1291.

9. Бураева Л.А. Актуальные проблемы защиты информации в коммуникационных системах на современном этапе // Научные исследования: теория, методика и практика: сборник материалов II Международной научно-практической конференции (9 ноября 2017). Чебоксары: ЦНС «Интерактив плюс», 2017. С. 211-213.

10. Гундерич Г.А. Состояние киберпреступности // Научный вестник Крыма. 2018. №4. С. 1-9.

11. Барчуков В.К. Терминология мошенничества в сфере компьютерной информации // Пробелы в российском законодательстве. Юридический журнал. 2017. №4. С. 163-165.

12. Шхагансоев З.Л., Бураева Л.А. Киберпреступность и киберконфликты в современной России // Пробелы в российском законодательстве. Юридический журнал. 2018. №3. С. 48-50.

13. Балашова Е.С., Богачева А.В., Мальцева С.М. «Философия» как мировоззренческая основа правового сознания студента вуза // Современные исследования социальных проблем. 2019. Т. 11. № 2-2. С. 74-78.

14. Кудрявцева Ю.В. Инновационные финансовые технологии и операционные риски в сфере дистанционного банковского обслуживания // Финансовая аналитика: проблемы и решения. №6. С. 647-662.

15. Ширманов А.О., Сизов Р.С., Булганина С.В. Вирусный маркетинг как инновационный инструмент продвижения продукции // Инновационные технологии управления: сборник статей по материалам II Всероссийской научно-практической конференции. Нижегородский государственный педагогический университет им. К.Минина. 2015. С. 125-127.

16. Воронкова А.А., Мальцева С.М., Никанорова В.С. К вопросу о методах психологического воздействия рекламы на потребителя // Инновационная экономика: перспективы развития и совершенствования. 2019. № 1 (35). С. 28-33

17. Богачева А.В., Мальцева С.М., Лужкова Е.А. Влияние семейного климата на развитие личности современного студента // Инновационная экономика: перспективы развития и совершенствования. 2019. № 5 (39). С. 11-17.

18. Воронкова А.А., Кашина О.П. Проблема формирования языковой личности и духовной зрелости современных российских предпринимателей // Фундаментальные исследования. 2015. № 2-15. С. 3417-3421

19. Изотов Д.С., Быкова Н.Н. Виды мошенничества с банковскими картами // Вестник НГИЭИ. 2015. № 3 (46). С. 49-53.

20. Чесноков М.В. Непосредственный объект мошенничества в сфере кредитования // Балтийский гуманитарный журнал. 2016. Т. 5. № 3 (16). С. 285-288.

21. Грязнова Е.В., Треушников И.А., Мальцева С.М. Тревожные тенденции в системе российского образования: анализ мнений ученых и педагогов // Перспективы науки и образования. 2019. № 2 (38). С. 47-57.

22. Мальцева С.М., Булганина А.Е., Булганина С.В., Белоусова К.В. Социологическое исследование выявления предпочтений молодежи по трудоустройству // Наука и бизнес: пути развития. 2019. № 3 (93). С. 89-92.

Статья поступила в редакцию 13.02.2020
Статья принята к публикации 27.05.2020