ФИШИНГ КАК НЕИЗУЧЕННОЕ КИБЕРПРЕСТУПЛЕНИЕ

PHISHING AS AN UNSTUDIED CYBER CRIME

УДК 343

Антонова Татьяна Сергеевна, курсант Московского Университета МВД России имени В.Я. Кикотя.

Смирнов Виталий Михайлович, кандидат технических наук, старший преподаватель кафедры информатики и математики Московского университета МВД имени В. Я. Кикотя.

Antonova T.S. tanaantonova290302@gmail.com

Smirnov V.M. smirnov.v.m002@gmail.com

Аннотация

С развитием информационного общества, появляются способы хищения персональных данных. В данной статье речь пойдет об одном из таких способов, как «Фишинг». На данный момент понятие «Фишинг» не упоминается в нормативно-правовых актах, а значит, встает вопрос о квалификации этого способа как преступления и посягательства на персональные данные.

Annotation

With the development of the information society, there are ways to steal personal data. This article will focus on one of such methods as "Phishing". At the moment, the concept of "Phishing" is not mentioned in regulatory legal acts, which means that the question arises of qualifying this method as a crime and infringement of personal data.

Ключевые слова: фишинг, безопасность, киберпреступления, Интернет, информация, персональные данные, защита личных данных, взлом, мошенничество, социальная инженерия.

Keywords: phishing, security, cybercrime, Internet, information, personal data, personal data protection, hacking, fraud, social engineering.

На сегодняшний день в России начинает увеличиваться рост преступлений с помощью информационных технологий. Почти 50 % преступлений в данной сфере приходятся на взлом пин-кодов банковских карт. Несмотря на то, что население призывают не разглашать реквизиты своих банковских карт, мошенники изобретают новые способы взлома систем, содержащих в себе реквизиты банковских карт и пин-кодов. Системы защиты от мошенничества далеко не всегда успевают адаптировать под новые методы взлома, по этой причине до сих пор и происходят преступления.

В 2020 году «аферисты в сетях» нанесли ущерб части населения России, которая пользуется банковскими картами, в размере, превышающем 74 миллиарда рублей. Большинство обманов происходит из-за невнимательного отношения пользователей в Интернете к своим данным. Одной из таких распространённых проблем является фишинг. Фишинг – это вид мошенничества в Интернете, цель которого украсть конфиденциальные данные пользователей.

Для этого злоумышленники используют массовую рассылку на электронную почту, в которых можно перейти на поддельные сайты. Одним из видом фишинга является создание похожих копий известных Интернет – магазинов, социальных сетей, где под различными предлогами получают реквизиты банковских карт и пароли от социальных сетей других пользователей, чтобы войти в свой аккаунт. Мошенник, получая доступ к логину и паролю осуществляют перевод денежных средств и тем самым совершают кражу. Также сюда можно отнести предложение избавится от кредита, купив на сайте жуликов дорогой товар по большой скидке. Фишинг в настоящее время очень

распространён, поэтому важно не реагировать на рассылки и не вводить свои конфиденциальные данные на непроверенных сайтах.

Этот вид мошенничества по своему составу не имеет причастности к преступлениям, которые предусмотрены в УК РФ, однако последствия данного правонарушения – УК РФ Статья 272. Неправомерный доступ к компьютерной информации, Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ. Из этого можно предположить, что фишинг является всего лишь инструментом в руках мошенника.

Одним из примеров проявления данного вида мошенничества можно выделить необычное киберпреступление, которые раскрыли сотрудники уголовного розыска вместе с отделом «К» УМВД России по Калининградской области. Потерпевший написал заявление в полицию о похищении аккаунта в игре в сети Интернет. Потерпевший объяснил, что в Интернете купил аккаунт от игры. Создание аккаунта бесплатное, он разъяснил, что игроку не приходится начинать играть с нуля – персонажи уже имеют высокий уровень, и какие-либо дополнения.

При совершении сделки не было ничего незаконного. Потерпевший заплатил 9 тысяч рублей. В течение месяца он захотел воспользоваться аккаунтом, но оказалось, что не может зайти на электронную почту. Злоумышленник изменил пароль.

Сотрудники в течение короткого срока установили, что к краже аккаунта причастен его бывший владелец. После сделки 27-летний мужчина восстановил доступ к электронной почте, на которую были зарегистрированы игры (по e-mail). Против мошенника возбудили уголовное дело по статье 272 УК РФ. Неправомерный доступ к компьютерной информации. Санкции статьи предусматривают штраф до двухсот тысяч рублей (200.000 р.) до года исправительных работ или лишение свободы до двух лет.

Так же существует еще один способ осуществления фишинга – социальная инженерия. Данное понятие было введено специалистами, связанные с обеспечением комплексной информационной безопасности. Особенностью

является то, что пользователи предоставляют свои данные добровольно. Преступник, зная психологические методы манипуляции, выведывает личные данные пользователя. С помощью такого вида фишинга злоумышленник может похитить конфиденциальную информацию многих людей, взломав администратора какой – либо фирмы. Поэтому на высокую должность больших фирм выбирают людей, наиболее подготовленных к соблюдению сохранности профессиональной тайны, но тем не менее, не подавая вид своей профессиональности.

Каждый может стать жертвой таких преступлений в Интернете. По этой причине стоит задаться вопросом: «Как же самостоятельно защитить свои данные от мошенников?»

От фишинга нет универсального способа защиты, кроме того, как внимательно следить за своими персональными данными. Простые способы обезопасить себя от данного вида мошенничества – не переходить на ссылки, которые пришли от незнакомых отправителей. Также на компьютер лучше установить антивирусную программу, которая способна блокировать опасные ссылки и вложения. К тому же, в сети Интернет лучше не разглашать личные данные в переписках даже с самыми близкими людьми, т.к. никто не защищен на все 100 процентов от взломов социальных сетей. Еще рекомендуется поставить на все социальные сети и почтовые ящики двухфакторную аутентификацию, позволяющую наиболее надежно обезопасить личные данные.

Подводя итог, можно сделать вывод, что ликвидировать фишинг почти невозможно, так как уловки мошенников приобретают новые формы. Способы защиты персональных данных и личной информации не успевают обогнать рост преступлений в этой сфере, что приводит к тому, что мошенники все чаще завладевают персональными данными. Поэтому пользователи Интернета должны иметь базовые знания, чтобы избежать утраты своих персональных данных. Также на данный момент нет компетентного законодательства для наказания таких мошенничских действий. Вопрос о информационной

безопасности выходит на новый уровень, так как защита информации и персональных данных несет очень важный характер.

Министерство внутренних дел Российской федерации делает все возможное, чтобы предотвратить или по крайней мере снизить уровень мошенничества в сети. Для этого существует ряд мер, а в первую очередь информирование населения о возможных способах хищения персональных данных. В Московском университете МВД имени В.Я. Кикотя есть факультет для подготовки сотрудников в сфере информационной безопасности, которые готовят высоко квалицированных специалистов в этой области, одним из главных направлений обучения этого факультета является предотвращение различных посягательств на персональные данные граждан.

Литература

1. Что такое фишинг? Описание и определение термина. URL// https://biznesprost.ru/fishing.html(дата обращения: 10.04 2021г.).
2. УК РФ Статья 272. Неправомерный доступ к компьютерной информации
3. УК РФ Статья 273. Создание, использование и распространение вредоносных компьютерных программ
4. Басараб М.А., Иванов И.П., Колесников А.В., Матвеев В.А. Обнаружение противоправной деятельности в киберпространстве на основе анализа социальных сетей: алгоритмы, методы и средства (обзор) // Вопросы кибербезопасности. 2016. Вып. 4 (17). С. 11–19
5. Штайгер А.А. «Социальная инженерия на примере фишинга» // Вестник современных исследований. 2018. Вып. 6.3 (21). С. 612-614
6. Гайфутдинов Р.Р. «К вопросу о типологии личности компьютерных преступников с учетом характера и мотивации их криминальной деятельности // Вопросы российского и международного права.» 2017. Т. 7. № 4А. С. 245–256 с

Literature

1. What is phishing? Description and definition of the term. URL// https://biznesprost.ru/fishing.html(accessed: 10.04 2021).

2. Criminal Code of the Russian Federation Article 272. Illegal access to computer information
3. Article 273 of the Criminal Code of the Russian Federation. Creation, use and distribution of malicious computer programs
4. Basarab M. A., Ivanov I. P., Kolesnikov A.V., Matveev V. A. Detection of illegal activity in cyberspace based on the analysis of social networks: algorithms, methods and tools (review). 2016. Issue 4 (17). pp. 11-19
5. Steiger A. A. "Social engineering on the example of phishing" / / Bulletin of modern Research. 2018. Issue 6.3 (21). pp. 612-614
6. Gaifutdinov R. R. "To the question of the typology of the personality of computer criminals taking into account the nature and motivation of their criminal activities / / Voprosy rossiyskogo i mezhdunarodnogo prava." 2017. Vol. no. 4A. pp. 245-256 p
7. Gaifutdinov R.R. "On the question of the typology of the personality of computer criminals, taking into account the nature and motivation of their criminal activity // Questions of Russian and international law." 2017. T. 7 No. 4A. P. 245-256