Научная статья
УДК 343.9
EDN SRVHGS
DOI 10.17150/2411-6262.2022.13(2).36

А.Н. Завьялов
Иркутский юридический институт (филиал) Университета прокуратуры Российской Федерации, г. Иркутск, Российская Федерация, zavyalov.61@bk.ru

ИНТЕРНЕТ-МОШЕННИЧЕСТВО (ФИШИНГ): ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ И ПРЕДУПРЕЖДЕНИЯ

АННОТАЦИЯ. Интернет-технологии сегодня настолько распространены, что в буквальном смысле охватывают практически все сферы жизнедеятельности. Однако, из-за роста интернет-технологий возрастают и угрозы безопасности для систем и сетей. Одной из таких серьезных угроз является «фишинг», при котором злоумышленники пытаются незаконными способами получить учетные данные пользователей. Фишинг — это один из способов мошенничества, целью которого является формирование поддельного сайта, неправомерное получение паролей, номеров банковских счетов и т.д. для получения конфиденциальной информации пользователей. Данный вид мошенничества становится все более актуальным, и объясняется это тем, что от преступников требуется минимальное количество затрат, так как инструменты, которыми пользуются лица в противоправных целях относительно доступны и понятны. Целью данной работы является изучение особенностей фишинговых атак, а также анализ средств и методов противодействия этим противоправным деяниям. В статье рассмотрены существующие формы противодействия фишинговым атакам, а также проанализированы меры, направленные на выявление и пресечение таких противоправных деяний. Анализ судебно-следственной практики показал, что в настоящее время государству необходимо обеспечить правоохранительные органы наиболее современными техническими средствами, программным обеспечением, высококвалифицированными специалистами для успешной борьбы с новыми вызовами в киберпространстве в условиях цифровой экономики.

КЛЮЧЕВЫЕ СЛОВА. Мошенничество, фишинг, интернет, фишинговые атаки, интернет-технологии, интернет-мошенничество.

ИНФОРМАЦИЯ О СТАТЬЕ. Дата поступления 5 апреля 2022 г.; дата принятия к печати 25 мая 2022 г.; дата онлайн-размещения 10 июня 2022 г.

Original article

A.N. Zavyalov
Irkutsk Law Institute (Branch) University of the Prosecutor's Office of the Russian Federation, Irkutsk, Russian Federation, zavyalov.61@bk.ru

INTERNET SCAM (PHISHING): ISSUES OF COUNTERACTION AND PREVENTION

ABSTRACT. Internet technologies are so common today that they literally extend over almost all areas of life. However, due to the ongoing growth of Internet technologies, security threats to systems and networks are also rising. One of these serious threats is «phishing», in which attackers try to illicitly obtain user credentials. Phishing is a fraudulent practice, the purpose of which is to create a fake website, illicitly asking for passwords, bank account numbers, etc. to induce users to reveal confidential information. This type of scam is increasingly gaining in popularity, since fraudsters incur a minimum amount of expenses, and the tools used by them for illegal purposes are relatively accessible and easy to use. The purpose of this

study is to examine common features of phishing attacks, as well as to analyze means and methods of countering these wrongdoings. The article looks into the existing ways of countering phishing attacks and analyzes measures aimed at identifying and suppressing such crimes. The analysis of judicial and investigative practice has shown that in the current state the government needs to provide law enforcement agencies with cutting-edge technical equipment, software, and highly qualified staff in order to successfully overcome new challenges in cyberspace in the context of the digital economy.

KEYWORDS. Scams, phishing, internet, phishing attacks, internet technologies, internet scams.

ARTICLE INFO. Received April 4, 2022; accepted May 25, 2022; available online June 10, 2022.

Противоправные деяния, совершаемые с использованием информационно-телекоммуникационных технологий (далее — ИТТ) на сегодняшний день набирают стремительные обороты. Современные реалии таковы, что подавляющее большинство противоправных деяний так или иначе связаны с техническим прогрессом и возможностями глобальной сети Интернет. Так, Президент Российской Федерации В.В. Путин на расширенном заседании коллегии МВД России 17 февраля 2022 г. отметил: «...кибертехнологии развиваются стремительно, возникают новые риски, и нужно их предупреждать, не позволять преступникам паразитировать на технологическом прогрессе, в связи с чем необходимо действовать на опережение...»[1].

Очевидно, что противоправные деяния, совершаемые с использованием цифровых технологий, являются крайне актуальной проблемой и несут в себе серьезную угрозу национальной безопасности Российской Федерации[2].

Современный период трансформации экономики способствует усилению интеграционных процессов между коммерческой деятельностью и цифровыми технологиями [1, с. 223]. Разнообразие преступной деятельности с использованием ИТТ достигло масштабных размеров, однако особым образом считаем целесообразным акцентировать внимание на таком противоправном явлении как фишинг. На сегодняшний день, проблема мошенничества при помощи сетевых и иных технологий стоит весьма остро [2, с. 31]. В настоящее время фишинг — это один из способов мошенничества, целью которого является формирование поддельного сайта, неправомерное получение паролей, номеров банковских счетов и т.д. для получения конфиденциальной информации пользователей. Данный вид мошенничества становится все более актуальным, и объясняется это тем, что от преступников требуется минимальное количество затрат, так как инструменты, которыми пользуются лица в противоправных целях относительно доступны и понятны. В этой связи популярность фишинга постоянно растет, а методы, которыми пользуются в преступных целях непрерывно совершенствуются и модернизируются.

За последние несколько лет количество фишинговых афер резко возросло, что представляет огромную угрозу для глобальной безопасности в Интернете. Сегодня фишинговая атака является одной из наиболее распространенных и серьезных угроз в Интернете, ведь она направлена на попытки незаконного завладения личными или финансовыми учетными данными пользователя с помощью вредоносных программ или социальной инженерии.

---

[1] Выступление Президента Российской Федерации В.В. Путина на расширенном заседании коллегии МВД России 17 февраля 2022 г. URL: http://www.kremlin.ru/events/president/news/67795 (дата обращения: 21.04.2022).

[2] О Стратегии национальной безопасности Российской Федерации : Указ Президента РФ от 2 июля 2021 г. № 400 // СПС «Консультант плюс».

Фишинг — это форма кражи личных данных, которая происходит, когда вредоносный веб-сайт выдает себя за законный, чтобы получить конфиденциальную информацию, такую как пароли, данные учетной записи или номера кредитных карт. Хотя существует несколько антифишинговых программ и методов для обнаружения потенциальных попыток фишинга в электронных письмах и обнаружения фишингового контента на веб-сайтах, фишеры придумывают новые и гибридные методы, чтобы обойти доступное программное обеспечение и методы.

Фишинг — это метод обмана, который использует комбинацию социальной инженерии и технологий для сбора конфиденциальной и личной информации, такой как пароли и данные кредитных карт, выдавая себя за заслуживающего доверия человека или бизнес в электронном сообщении. Фишинг использует поддельные электронные письма, которые выглядят подлинными и якобы поступают из законных источников, таких как финансовые учреждения, сайты электронной коммерции и т.д., чтобы пользователи переходили на мошеннические веб-сайты по ссылкам, указанным в фишинговом письме. Мошеннические веб-сайты предназначены для имитации внешнего вида веб-страницы реальной компании.

Фишинговые злоумышленники обманывают пользователей, используя различные тактики социальной инженерии, такие как угрозы приостановить действие учетных записей пользователей, если они не завершат процесс обновления учетной записи, не предоставят другую информацию для проверки своих учетных записей или по каким-либо другим причинам, чтобы заставить пользователей посещать их поддельные веб-страницы.

Почему так важно решать проблему фишинга? Фишинговые атаки затрагивают миллионы пользователей Интернета и являются огромным финансовым бременем для бизнеса и жертв фишинга. Информация, предоставленная поддельным веб-сайтам, приводит к прямым убыткам, в связи с чем фишинг стал серьезной угрозой как для пользователей, так и для бизнеса.

За последние несколько лет большое внимание уделялось вопросу безопасности и конфиденциальности.

Стоит отметить, что цифровой прогресс работает в обе стороны: совершенствуются как законные способы и методы развития, так и модернизируется преступное общество. В условиях современной реальности очевидно, что вычислять поддельные сайты с каждым днем становится все сложнее, их адреса все больше похоже на подлинные, при этом в некоторых случаях они находят контакт даже с защищенным соединением HTTPS, а если говорить о использовании сайтов через мобильные устройства, то здесь риск столкнуться с фишинговым сайтов еще больше увеличивается ввиду технических особенностей смартфонов.

Компании и банки стараются бороться с действиями злоумышленников [3, с. 299]. Конечно, при работе с сайтами в корпоративной среде риск столкнуться с фишингом крайне невелик, ввиду ограничения нецелевого использования, а также применения различных встроенных инструментов в используемый браузер. Однако такие меры являются базовыми и в редких случаях гарантируют безопасность персональных данных. Очевидно, что необходимо прибегать к использованию внешних ресурсов, применять комплексный подход, который будет включать в себя комбинацию действий: от технических инструментов, до проведения организационных мероприятий по защите сайтов.

В рамках противодействия преступности в рассматриваемой области, а также осуществления надзора за реализацией нацпроекта «Цифровая экономика» в Генеральной прокуратуре Российской Федерации создан отдел по надзору за исполнением законодательства в ИТ-сфере.

Анализ статистических данных показал, что наиболее частым фишинговым атакам подвергаются официальные сайты Пенсионного фонда и Фонда социального страхования. Данный факт обусловлен тем, что указанные сайты работали без соблюдения условий безопасности, в частности, установлено отсутствие нормативных правовых актов, позволяющих определять актуальные угрозы безопасности данных. Очевидно, что такие фишинговые сайты имеют огромные возможности по получению личных данных граждан Российской Федерации и борьба с их созданием и использованием должна вестись на достаточно серьезном уровне. Крайне актуально здесь применять все возможные меры профилактики, предупреждение этих деяний должно стать первостепенной задачей, в этой связи созданный специальный отдел по надзору за исполнением законодательства в ИТ-сфере станет одной из мер по контролю за внедрением искусственного интеллекта, целью которого является обеспечение защиты и хранения информации.

Еще одной мерой по борьбе с фишинговыми сайтами стало предложение Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, которое заключается в объединении Единого портала государственных и муниципальных услуг с государственной биометрической системой, что позволит также повысить безопасность пользователей сайтов государственных органов. По словам ведомства, биометрия является наилучшей защитной системой в данном случае. Кроме того, Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации в настоящее время занимается созданием единой системы по борьбе с кибератаками, которая будет включать в себя возможности поиска фишинговых сайтов, а также функции автоматизированной обработки на признаки мошенничества в сфере ИТТ и поиск мер по блокировки вредоносных программ, сайтов и т.д.

Кроме того, регулярными проверками занимается и Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее — Роскомнадзор), направленными на защиту и обработку персональных данных.

Многообразие фишинговых атак показывает, что существует огромное число средств, позволяющих получить от пользователя сети Интернет любую конфиденциальную информацию [4, с. 612].

Безусловно, чем больше технологически развита страна, чем больше используются современные инфокоммуникационные технологии — тем выше риск, а, соответственно, меры безопасности должны работать на опережение. Современная преступность, являясь неотъемлемой частью общественных отношений, все больше приобретает характерные черты высокотехнологического процесса [5, с. 132]. В этой связи трудно не согласиться с высказыванием О.П. Грибунова, который отметил, что в настоящее время без современных технологий процесс противодействия противоправным деяниям уже практически невозможен [6, с. 11].

Очевидно, что противодействие фишинговым атакам должно проводится на всех уровнях, здесь должна вестись совместная работа организаций, различных государственных структур, правоохранительных органов, граждан. Борьбу с данным видом мошенничества можно осуществлять только с применением комплексного подхода. Однако, очевидно, что защита своих персональных данных во многом зависит от пользователя, от его умения критически анализировать поток информации [7, с. 198]. Таким образом, здесь важны и меры профилактики, заключающиеся в информировании граждан о существующих угрозах и о мерах по защите своих персональных данных, и систематические проверки по соблюдению законодательства в сфере информационно-телекоммуникационных технологий.

В результате рассмотрения судебной практики мы пришли к выводу о том, что чаще всего фишинг неочевиден: неизвестны данные о конкретном лице, ко-

торое совершило преступление, известен лишь факт совершения преступления. Проведение оперативно-розыскных мероприятий и следственных действий при расследовании фишинга осложняется тем, что часть получаемых при их производстве данных добывается из источников виртуальной информации (компьютер потерпевшего или преступника, удаленный локальный сервер, сеть Интернет и т.д.) [8, с. 371].

Исходя из всего вышесказанного, можно сделать вывод о том, что проблема фишинга на сегодняшний день особенно актуальна в современном Российском киберпространстве. Не существует универсального средства борьбы с фишингом. Злоумышленники постоянно увеличивают свой арсенал и находят новые способы обхода технических средств защиты. Однако специалисты информационной безопасности продолжают создавать новое программное обеспечение, чтобы снизить шанс успешного проведения атаки. Помимо этого, сейчас также идет активная борьба со злоумышленниками на законодательном уровне. Однако уровень квалификации и опыт следственных органов в расследовании подобных преступлений пока остается на невысоком уровне [9, с. 90].

Следовательно, государству необходимо обеспечить правоохранительные органы наиболее современными техническими средствами, программным обеспечением, высококвалифицированными специалистами для успешной борьбы с новыми вызовами в киберпространстве в условиях цифровой экономики [10, с. 772].

Подводя итог, хочется отметить, что борьба с преступностью играет важную роль в формировании и поддержании устойчивого правового государства. Соблюдение должного уровня правопорядка и законности — одна из приоритетных задач современного общества [11, с. 188]. Анализ преступности показал, что информационно-телекоммуникационные технологии постепенно становятся неотъемлемой частью практически любой сферы деятельности, что напрямую ставит вопрос о необходимости повышения роли информационной безопасности. При этом такой вид преступной деятельности является крайне специфичным, и положительный исход по делу во многом зависит от качества проведения предварительного следствия [12, с. 32].

Обеспечение безопасности в сфере информационного поля, пространства, информационных ресурсов и информационных систем в настоящее время является одной из приоритетных задач, эти вопросы представляют собой крайне актуальную область исследования и требуют постоянного развития и совершенствования.

Список использованной литературы

1. Тимофеев С.В. Информационное обеспечение противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий / С.В. Тимофеев. — EDN GRWGZD // Известия Тульского государственного университета. Экономические и юридические науки. — 2021. — № 1. — С. 132–137.

2. Грибунов О.П. К вопросу о противодействии экстремизму на объектах транспорта / О.П. Грибунов. — EDN SIQRWN // Вестник Восточно-Сибирского института МВД России. — 2013. — № 3 (66). — С. 9–16.

3. Енин В.М. Фишинг как угроза нового поколения / В.М. Енин, И.А. Матющенко. — EDN MMIRXB // International Journal of Advanced Studies in Computer Engineering. — 2021. — № 2. — С. 31–37.

4. Шерстяных А.С. Фишинг как инструмент социальной инженерии / А.С. Шерстяных. — EDN FGWHYV // Актуальные проблемы борьбы с преступностью: вопросы теории и практики : материалы XXV междунар. науч.-практ. конф. — Красноярск, 2022. — С. 299–301.

5. Штайгер А.А. Социальная инженерия на примере фишинга / А.А. Штайгер. — EDN XUROQP // Вестник современных исследований. — 2018. — № 6.3 (21). — С. 612–614.

6. Юсупов М.Ю. Фишинг как угроза конфиденциальности в сети / М.Ю. Юсупов, А.О. Путилов. — EDN BSZNZY // E-Scio. — 2021. — № 10 (61). — С. 223–232.

7. Парфенюк В.Е. Основные элементы криминалистической характеристики фишинга / В.Е. Парфенюк. — EDN IWXLKV // Вопросы современной науки: проблемы, тенденции и перспективы : материалы III Междунар. науч.-практ. конф. — Новокузнецк, 2019. — С. 369–372.

8. Баев Н.И. Феномен фишинга в современном российском киберпространстве / Н.И. Баев. — EDN DCMLSH // Инновационные научные исследования. — 2021. — № 11-2 (13). — С. 89–95.

9. Крюкова И.В. Фишинг как вид интернет-мошенничества / И.В. Крюкова, Э.Н. Алимамедов. — EDN AVQUPN // Наукосфера. — 2021. — № 2-2. — С. 196–201.

10. Жиронкин Д.С. Фишинг как инструмент современной киберпреступности в условиях цифровой экономики / Д.С. Жиронкин, Д.Г. Нарышкин // Следственная деятельность: проблемы, их решение, перспективы развития : материалы III Всерос. молодежной науч.-практ. конф. — Москва, 2020. — С. 769–772.

11. Малыхина Е.А. Структура и содержание криминалистической характеристики хищений комплектующих деталей объектов железнодорожного транспорта и ее значение для частной методики расследования / Е.А. Малыхина. — EDN DIENJE // Вестник Восточно-Сибирского института МВД России. — 2019. — № 1 (88). — С. 188–200.

12. Грибунов О.П. Отдельные вопросы тактики допроса при расследовании взяточничества / О.П. Грибунов, Е.А. Малыхина. — EDN NLRCOO // Научный дайджест Восточно-Сибирского института МВД России. — 2020. — № 4 (7). — С. 28–32.

References

1. Timofeev S.V. Information Support for Countering Crimes Committed with the Use of Information and Telecommunication Technologies. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki = Izvestiya of the Tula State University. Economic and legal sciences*, 2021, no. 1, pp. 132–137. (In Russian). EDN: GRWGZD.

2. Gribunov O.P. On the Question of Combating Extremism on Transport. *Vestnik Vostochno-Sibirskogo instituta MVD Rossii = Vestnik of the Eastern Siberia Institute of the Ministry of the Interior of the Russian Federation*, 2021, no. 1, pp. 132–137. (In Russian). EDN: SIQRWN.

3. Enin V.M., Matyushchenko I.A. Phishing as a New Generation Threat. *International Journal of Advanced Studies in Computer Engineering*, 2021, no. 2, pp. 31–37. (In Russian). EDN: MMIRXB.

4. Sherstyanykh A.S. Phishing as a Tool of Social Engineering. *Actual Problems of Fighting Crime: Issues of Theory and Practice. Materials of the XXV International Scientific and Practical Conference*. Krasnoyarsk, 2022, pp. 299–301. (In Russian). EDN: FGWHYV.

5. Shtaiger A.A. Social Engineering on the Example of Phishing. *Vestnik sovremennykh issledovanii = Bulletin of Modern Studies*, 2018, no. 6.3, pp. 612–614. (In Russian). EDN: XUROQP.

6. Yusupov M.Yu., Putilov A.O. Phishing as a Security Threat of Confidential Data Online. *E-Scio*, 2021, no. 10, pp. 223–232. (In Russian). EDN: BSZNZY.

7. Parfenyuk V.E. Major Elements of Criminal Characteristics of Phishing. *Issues of Modern Science: Problems, Trends and Prospects. Materials of the III International Scientific and Practical Conference*. Novokuznetsk, 2019, pp. 369–372. (In Russian). EDN: IWXLKV.

8. Baev N.I. The Phenomenon of Fishing in Modern Russian Cyberspace. *Innovatsionnye nauchnye issledovaniya = Innovative Scientific Research*, 2021, no. 11-2, pp. 89–95. (In Russian). EDN: DCMLSH.

9. Kryukova I.V., Alimamedov E.N. Phishing as a Type of Internet Fraud. *Naukosfera*, 2021, no. 2-2, pp. 196–201. (In Russian). EDN: AVQUPN.

10. Zhironkin D.S., Naryshkin D.G. *Phishing as a Tool of Modern Cybercriminals in the Context of the Digital Economy. Materials of III All-Russian youth research conference*. Moscow, 2020, pp. 769–772. (In Russian).

11. Malykhina E.A. Structure and Content of the Criminalistic Characteristics of Thefts of the Component Parts of the Railway Transport Objects and Its Value for the Specific Investigation Methodology. *Vestnik Vostochno-Sibirskogo instituta MVD Rossii = Vestnik of the Eastern Siberia Institute of the Ministry of the Interior of the Russian Federation*, 2019, no. 1, pp. 188–200. (In Russian). EDN: DIENJE.

12. Gribunov O.P., Malykhina E.A. Separate Issues in Interrogation Tactics in Investigating Bribery. *Nauchnyi daidzhest Vostochno-Sibirskogo instituta MVD Rossii = Scientific Digest of East-Siberian Institute of the Ministry of Internal Affairs of the Russian Federation*, 2020, no. 4, pp. 28–32. (In Russian). EDN: NLRCOO.

Информация об авторе

Завьялов Александр Николаевич — кандидат педагогических наук, доцент, кафедра общегуманитарных и социально-экономических дисциплин, Иркутский юридический институт (филиал) Университета прокуратуры Российской Федерации, г. Иркутск, Российская Федерация, zavyalov.61@bk.ru, https://orcid.org/0000-0001-9261-2570.

Author

Aleksandr N. Zavyalov — PhD in Pedagogical Sciences, Associate Professor. Department of General Humanitarian and Socio-Economic Disciplines, Irkutsk Law Institute (Branch) of the University of the Prosecutor's Office of the Russian Federation, Irkutsk, Russian Federation, zavyalov.61@bk.ru, https://orcid.org/0000-0001-9261-2570.

Для цитирования

Завьялов А.Н. Интернет-мошенничество (фишинг): проблемы противодействия и предупреждения / А.Н. Завьялов. — DOI 10.17150/2411-6262.2022.13(2).36. — EDN SRVHGS // Baikal Research Journal. — 2022. — Т. 13, № 2.

For Citation

Zavyalov A.N. Internet Scam (Phishing): Issues of Counteraction and Prevention. *Baikal Research Journal*, 2022, vol. 13, no. 2. (In Russian). EDN: SRVHGS. DOI: 10.17150/2411-6262.2022.13(2).36.