УДК 004.056.5

АНАЛИЗ ПРОБЛЕМЫ ФИШИНГА В ЦИФРОВОМ ПРОСТРАНСТВЕ

Тарасова Ю.А.

ООО «Антифишинг», Санкт-Петербург, e-mail: tarasovayuliya00@gmail.com

Современное общество все больше полагается на информационные технологии и цифровые решения, однако это сопряжено с рядом проблем и угроз, которые могут возникнуть в цифровом пространстве. Одна из таких проблем – фишинг, который представляет угрозу для конфиденциальности и безопасности личных данных. Фишинг осуществляется через социальную инженерию и может привести к краже личной информации, финансовым потерям и другим негативным последствиям. Для борьбы с фишингом важно понимать его основные аспекты и разработать соответствующие меры предотвращения. В данной статье проводится всесторонний анализ проблемы фишинга в цифровом пространстве современного общества. Исследование включает систематизацию информации о различных типах фишинга, наиболее распространенных уязвимостях и рекомендации по укреплению кибербезопасности. Для обеспечения безопасности в цифровом пространстве необходимо постоянно быть внимательным и внедрять эффективные меры защиты. Материалы данной статьи представляют ценность как для обычных пользователей программного обеспечения, так и для IT-специалистов, которые занимаются защитой информации и разработкой безопасных систем. В современном цифровом мире осознание рисков, связанных с фишингом, и применение соответствующих мер безопасности являются неотъемлемой частью успешной деятельности в онлайн-среде.

Ключевые слова: фишинг, цифровое пространство, информационные технологии, интернет-мошенничество, защита информации

ANALYSIS OF THE PROBLEM OF PHISHING IN THE DIGITAL SPACE

Tarasova I.A

LLC «Antiphishing», Saint-Petersburg, e-mail: tarasovayuliya00@gmail.com

Modern society increasingly relies on information technology and digital solutions; however, this is accompanied by a range of problems and threats that can arise in the digital space. One such problem is phishing, which poses a threat to the confidentiality and security of personal data. Phishing is carried out through social engineering and can lead to the theft of personal information, financial losses, and other negative consequences. To combat phishing, it is important to understand its key aspects and develop corresponding prevention measures. This article provides a comprehensive analysis of the phishing problem in the digital space of modern society. The research includes the systematization of information on various types of phishing, the most common vulnerabilities, and recommendations for strengthening cybersecurity. Ensuring security in the digital space requires constant vigilance and the implementation of effective protection measures. The materials in this article are valuable for both regular software users and IT specialists involved in information security and the development of secure systems. In the modern digital world, awareness of the risks associated with phishing and the application of appropriate security measures are integral parts of successful online activity.

Keywords: phishing, digital space, information technology, Internet fraud, information protection

Информационные технологии непрерывно разрабатываются, совершенствуются и приникают во все как бытовые, так и профессиональные сферы жизнедеятельности человека. Именно информационные технологии способны значительно повысить эффективность и оптимизировать выполнение рутинных задач. В связи с этим их использование наблюдается практически во всех сферах человеческой жизнедеятельности. Однако вместе с рядом преимуществ использование информационных технологий и нахождение человека в цифровом пространстве несут и ряд угроз [1].

Так, на сегодняшний день особенно актуализируются проблемы информационной безопасности со стороны технических аспектов, а также наблюдается значительное увеличение различных фишинговых атак. Если в первом случае ведутся активные работы по разработке эффективных решений, обеспечивающих информационную безопасность, то второе является относительно новым направлением в сфере информационных технологий. При этом фишинг наиболее характерен для пользователей, использующих информационные технологии в бытовой сфере.

Представленная статья посвящена анализу проблем фишинга в современном цифровом пространстве. В рамках работы предпринимаются попытки по выявлению наиболее актуальных проблем, а также способов и методов противодействия фишинговым атакам.

Результаты исследования и их обсуждение

Цифровое пространство играет ключевую роль в современном обществе, а его развитие находится в центре внимания как государств, так и бизнес-сектора. Эта актуальность обусловлена рядом факторов. Во-первых, цифровизация облегчает до-

ступ к информации, образованию и услугам, улучшая качество жизни. Во-вторых, она способствует экономическому росту и инновациям, что важно для конкурентоспособности стран и компаний. В-третьих, цифровое пространство становится средой для социальных взаимодействий, и оно влияет на формирование общественного мнения и культуры [2].

Однако развитие цифрового пространства сопровождается рядом проблем. Важной из них является цифровое неравенство, когда не все граждане имеют равный доступ к цифровым ресурсам и технологиям. Также существуют риски в области кибербезопасности, связанные с хакерскими атаками, утечками данных и кибершпионажем. Подрыв общественной приватности и рост влияния больших технологических корпораций вызывают обеспокоенность вопросами этики и регулирования [3].

Для обычных пользователей существует несколько основных проблем, связанных с цифровым пространством:

– кибербезопасность и конфиденциальность данных. Пользователи подвергаются риску взлома аккаунтов, утечки личных данных и кибермошенничества. Недостаточная осведомленность и небрежное обращение с личной информацией могут привести к серьезным последствиям;

– цифровое неравенство. Не все пользователи имеют равный доступ к высокоскоростному Интернету и цифровым устройствам. Это создает неравенство в доступе к образованию, информации и возможностям;

– социальные и психологические аспекты. Цифровое пространство может оказывать негативное воздействие на психическое состояние и социальные отношения пользователей. Проблемы вроде интернет-зависимости, кибербуллинга и потери личной связи могут возникнуть из-за чрезмерного использования онлайн-платформ;

– дезинформация и фейковые новости. Интернет является источником огромного объема информации, и пользователи могут столкнуться с дезинформацией, фейковыми новостями и манипуляциями. Это может вызвать принятие неверных решений и формирование неправильных взглядов;

– управление временем и продуктивность. Цифровые устройства и социальные медиа могут отвлекать пользователей от важных задач и уменьшать продуктивность. Необходимость балансировать время онлайн и офлайн может быть вызовом.

При этом одной из наиболее актуальных и серьезных проблем в современном цифровом пространстве является фишинг. На рисунке 1 представлен принцип реализации угрозы, связанных с фишингом [4].

Эта киберугроза состоит в том, что злоумышленники, выдающие себя за доверенные организации или доверенных лиц, пытаются обмануть пользователей и получить доступ к их личным данным, финансовым средствам или конфиденциальной информации. Актуальность фишинга обусловлена несколькими факторами. Во-первых, в мире существует множество служб, банков и онлайн-платформ, и пользователи регулярно взаимодействуют с ними через электронную почту, социальные сети и мессенджеры. Это создает идеальные условия для злоумышленников, чтобы выдать себя за такие организации и заполучить доверие пользователей.

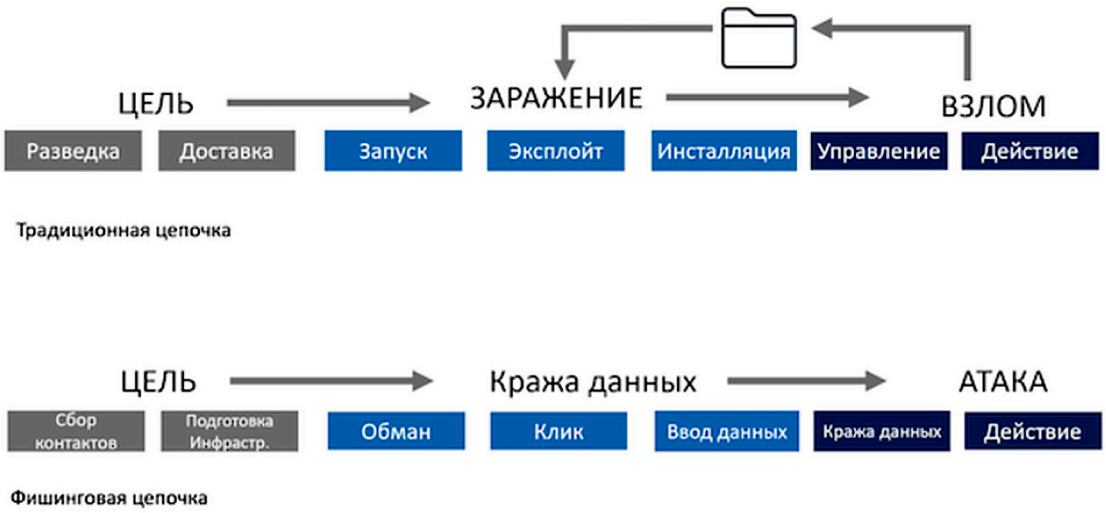

Рис. 1. Цепочка работы (жизненного цикла) фишинга

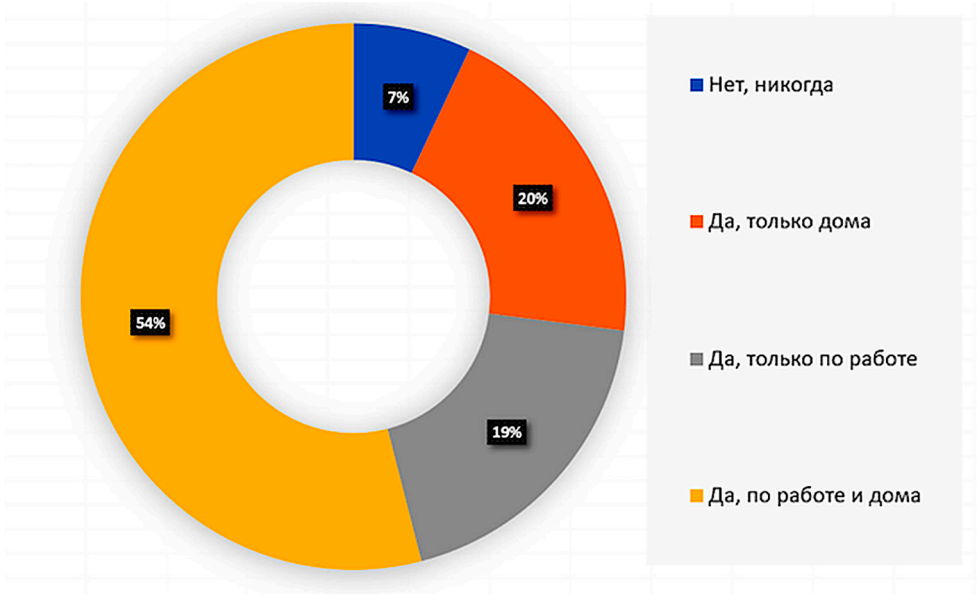

Рис. 2. Результаты опроса о столкновении с фишингом

Также важно отметить, что с данной угрозой сталкивались много людей, активно использующих средства информационных технологий. Это подтверждается многочисленными исследованиями и опросами пользователей. На рисунке 2 представлен результат опроса одной из организаций на предмет сталкивания с фишингом (задаваемый вопрос: «Сталкивались ли вы когда-нибудь с фишингом, и где?»).

При этом можно выделить целое множество видов фишинга, которые используются мошенниками на сегодняшний день.

Почтовый (E-mail) фишинг. Злоумышленники отправляют фальшивые электронные письма, в которых выдают себя за легитимные организации, банки или сервисы. Целью является убедить получателя перейти по поддельной ссылке и ввести личные данные, такие как пароли или номера кредитных карт. Почтовый фишинг часто использует тактику социальной инженерии, которая заключается в манипуляции человеческими эмоциями и психологией, чтобы заставить получателя действовать без раздумий. Злоумышленники могут создавать срочность или угрозу, чтобы подтолкнуть пользователей к принятию моментальных действий.

Социальный фишинг. Этот тип фишинга основан на манипуляции межличностными отношениями. Злоумышленники могут использовать социальные сети, чтобы выдать себя за знакомых или коллег и попросить жертву предоставить конфиденциальную информацию.

Сайтовый (Web) фишинг. Злоумышленники создают фальшивые веб-сайты, имитирующие настоящие, и маскируют их под легитимные ресурсы. Пользователи, переходя на такие сайты, могут случайно предоставить свои данные мошенникам. Злоумышленники могут использовать поддельные URL-адреса, которые похожи на оригинальные, чтобы пользователи не заметили разницы. Например, они могут заменить одну букву на похожую или добавить дополнительные символы в адрес сайта. Когда пользователи посещают фальшивый веб-сайт, злоумышленники могут попросить их ввести личные данные: учетные данные для входа в личные кабинеты, номера кредитных карт и другую персональную информацию.

Смс-фишинг (SMiShing). Злоумышленники отправляют фальшивые текстовые сообщения с просьбами или уведомлениями, которые могут включать вредоносные ссылки или просьбы о предоставлении личной информации.

Внутренний (Internal) фишинг. Этот вид фишинга направлен на сотрудников организации. Злоумышленники могут выдавать себя за коллег и пытаться получить доступ к корпоративным системам или конфиденциальной информации. Целью внутреннего фишинга является получение конфиденциальной информации, такой как логины, пароли, данные кредитных карт, секреты компании или другие чувствительные данные. Злоумышленники могут попросить сотрудников предоставить эти данные, обманув их с помощью поддельных запросов или предлогов, таких как проверка безопасности аккаунта или обновление информации.

Спиритический (Vishing). Здесь фишеры используют голосовую связь, обманывая пользователей по телефону. Они могут представляться сотрудниками банков или государственных организаций и запрашивать личные данные [5].

Проблема фишинга заключается в том, что он может привести к серьезным последствиям. Пользователи, попавшиеся на «удочку фишера», могут потерять свои деньги, стать жертвами кражи личных данных или страдать от кибермошенничества. Более того, фишинг может использоваться для распространения вредоносного программного обеспечения и атак на корпоративные сети. Для борьбы с фишингом необходимо проведение мероприятий для образования и повышения осведомленности пользователей, чтобы последние могли распознавать подозрительные сообщения и ссылки. Также важно, чтобы организации усиливали свои меры безопасности в целях предотвращения подобных атак и регулярно информировали пользователей о существующих угрозах.

Для борьбы с фишингом существуют различные методы и инструменты. Во-первых, важную роль играют образование и повышение осведомленности пользователей о фишинге. Регулярное обучение сотрудников и общественности в целом тому, как распознавать подозрительные электронные сообщения, веб-сайты и запросы на предоставление информации, может значительно снизить вероятность попадания в ловушку. Во-вторых, технологические средства также помогают в борьбе с фишингом. Это включает в себя антивирусные программы, фильтры для электронной почты, антифишинговые расширения для браузеров и системы мониторинга сетевой активности. Эти инструменты могут помочь автоматически обнаруживать и блокировать фишинговые атаки [6].

Кроме этого, организации могут внедрять политики безопасности, требующие двухфакторную аутентификацию и защиту данных, чтобы усилить защиту от фишинга. Такие меры способствуют минимизации риска утечки конфиденциальной информации. Совместное использование образования, технологических средств и правил безопасности помогает снизить уровень успешных фишинговых атак и обеспечивает более надежную защиту от этого вида мошенничества.

Также существуют и программные инструменты, предназначенные для борьбы с фишингом. Далее представлены основные из них:

– антивирусные программы и антифишинговые модули. Многие антивирусные программы включают в свой состав антифишинговые модули. Они могут блокировать доступ к вредоносным веб-сайтам и предупреждать о подозрительных ссылках в электронных письмах;

– фильтры электронной почты. Электронные почтовые клиенты и почтовые серверы могут быть настроены на автоматическое фильтрование и блокирование писем, содержащих подозрительные ссылки или вложения;

– браузерные расширения и плагины. Существуют расширения и плагины для популярных веб-браузеров, которые предупреждают о потенциально опасных сайтах и помогают распознавать фишинговые атаки;

– системы обнаружения вторжений (IDS). Некоторые IDS имеют специальные сигнатуры для обнаружения характерных признаков фишинговых атак, что позволяет своевременно реагировать на подобные инциденты;

– системы предотвращения утечек данных (DLP). DLP-системы могут помочь в обнаружении и блокировании передачи конфиденциальной информации вне организации, что способствует предотвращению фишинговых атак;

– системы мониторинга сетевой активности. Они могут обнаруживать аномалии и подозрительную активность в сети, включая попытки перенаправления трафика на фишинговые сайты [7].

Итак, проблема фишинга прочно вошла в жизнь современного человека, ведущего активный образ жизни в цифровом пространстве. Решение данной проблемы требует использования множества методов и инструментов. Средства борьбы с фишингом должны быть комплексными и включать как технические инструменты, так и обучающие мероприятия, специализированные под возрастные группы [8].

Заключение

Таким образом, основной целью представленной статьи являлось выполнение анализа по проблеме фишинга в цифровом пространстве современного общества. В рамках работы проведено комплексное исследование и представлены результаты по таким вопросам, как актуальность защиты пользователя в цифровой среде, основные угрозы, возникающие при использовании цифровых и информационных технологий. Подробно рассмотрены ключевые аспекты возникновения фишинговых атак, их жизненного цикла, методов и видов проведения. Отдельное внимание было уделено анализу инструментов для защиты от фишинговых атак и их предотвращения.

В заключение необходимо отметить, что фишинг является сложной и актуальной проблемой в современном цифровом мире. Злоумышленники постоянно совершенствуют свои методы, создавая обманные веб-сайты и электронные сообщения, которые могут выглядеть практически неотличимыми от легитимных. Эта форма мошенничества может обусловить серьезные последствия, включая утечку конфиденциальных данных и финансовые потери. Именно поэтому борьба с данным видом угрозы в цифровом пространстве требует постоянного внимания, образования пользователей и использования передовых технологических решений.

Список литературы

1. Завьялов А.Н. Интернет-мошенничество (фишинг): проблемы противодействия и предупреждения // Baikal Research Journal. 2022. №2. С. 36-42.

2. Архипова А.Б., Нечаев Д.А. Технология формирования интегрированной антифишинговой системы в цифровом обществе // Вестник СибГУТИ. 2023. № 2. С. 93-103.

3. Александров А.Г., Петухов А.Ю., Данильян А.С. Анализ угроз информационной безопасности при использовании фишинговых сайтов // Юристъ – Правоведъ. 2022. № 4 (103). С. 156-161.

4. Ревенков П.В., Ошманкевич К.Р., Бердюгин А.А. Фишинговые схемы в банковской сфере: рекомендации пользователям интернета по защите и разработка задач регулирования // Финансы: теория и практика. 2021. № 6. С. 212-226.

5. Селюк А.С. Защита персональных данных в цифровом пространстве // Вестник Университета имени О.Е. Кутафина. 2023. № 2 (102). С. 110-119.

6. Курлов Е.Г. Актуальные проблемы регулирования экономических отношений в условиях цифровизации финансового рынка // Научные междисциплинарные исследования. 2020. № 1. С. 21-35.

7. Антонова Т.С., Смирнов В.М. Фишинг как неизученное киберпреступление // StudNet. 2021. № 6. С. 69-75.

8. Гончарова М.Н., Перевалов А.М., Геймбихнер В.Р. Интернет-мошенничество как угроза экономической безопасности // Умная цифровая экономика. 2022. № 2. С. 116-121.