УДК 004.45

ФИШИНГОВЫЕ АТАКИ И СПОСОБЫ ЗАЩИТЫ В ЦИФРОВОМ МИРЕ

Фур М.А., студент гр. ИБт-231, II курс
Научный руководитель: Дементьева Ю.С., преподаватель
Кузбасский государственный технический университет
имени Т.Ф. Горбачева
г. Кемерово

Фишинг, как вид киберпреступления, представляет собой одну из наиболее распространенных угроз в современном цифровом обществе. Согласно отчету «Лаборатории Касперского» [1] около 47% всех писем в мире были спамом, многие из которых скорее всего были фишинговыми. Около 60 тысяч ссылок в мессенджере Telegram были фишинговыми. Он используется мошенниками различных направлений и формирует важную проблему для пользователей интернета. В связи с этим появляется актуальный вопрос: «Как защититься от фишинга?» Целью данной работы является изучение методов защиты от фишинга, а также разработка эффективного решения для предотвращения подобных угроз.

Для реализации поставленной цели были обозначены следующие задачи:

1. Определить понятие фишинга.
2. Изучить методы защиты от фишинга.
3. Создать собственное решение проблемы.

Для выполнения данной работы был определён ряд этапов, включающих исследование проблемы фишинга и разработки решений по защите от данного вида киберпреступлений.

Первым этапом стало исследование теоретических материалов, связанных с фишингом. На данном этапе были собраны данные о различных формах фишинга, о его принципах и механизмах работы, а также о том, как мошенники используют различные тактики для того, чтобы заманить пользователей на фальшивые сайты или заставить их передать личную информацию.

После сбора теоретических сведений был проведён анализ методов защиты от фишинга. На данном этапе работы было рассмотрено множество существующих решений и технологий, направленных на выявление и предотвращение фишинговых атак. Включая как программные решения, так и обучающие программы, которые помогают пользователям распознавать фишинг. Основной задачей было оценить их эффективность и выявить возможные слабые места в существующих решениях.

Завершающим этапом работы стала разработка и создание собственного средства защиты от фишинга. Это решение было направлено на создание программы, которая могла бы эффективно проверять веб-сайты на наличие

признаков фишинга, опираясь на данные о достоверных веб-ресурсах. Программа была разработана на языке C# и прошла этап тестирования на различных примерах сайтов.

Было сформировано краткое определение [2]. Фишинг представляет собой вид мошенничества, который направлен на получение доступа к личной информации пользователя обманным путем. То есть, мошенник вынуждает вас совершить действие, позволяющее ему получить доступ к вашему устройству, учетным записям или персональным данным. Преступник может выдать себя за кого-то другого или представить фальшивый информационный ресурс как настоящий.

Часто фишинговые сообщения приходят по электронной почте, через телефонные звонки или текстовые сообщения, что приводит пользователя на фальшивые сайты [2], адрес которых слегка изменён, но выглядит почти идентично оригинальному. В случае с телефонными звонками или сообщениями, мошенник использует социальную инженерию, чтобы создать доверие и заставить жертву следовать его инструкциям.

Фишинг может также быть целенаправленным, когда мошенники нацелены на конкретные компании или организации. В таком случае они атакуют определённых людей или группы, чтобы получить доступ к внутренним системам и выудить большие объёмы данных, а возможно, даже финансовые средства.

Изучив материалы по фишингу, был сформирован один из самых распространённых сценариев [3]:

1. Мошенник отправляет вам письмо или сообщение от вашего коллеги или друга, с просьбой или причиной перейти на веб-сайт, ссылку на который он оставляет в сообщении.
2. После перехода на сайт вас просят зарегистрироваться или войти в аккаунт, если это подделка какого-либо известного ресурса.
3. После этого к вашим личным данным, банковским картам, личным данным получает доступ мошенник.

Часто фишинг действует совместно с другими преступными действиями в пространстве сети Интернет, например: сталкинга, социальной инженерии, хакинга. Например, в социальных сетях фишинг может быть связан с взломом аккаунта друга, который затем используется для рассылки фишинговых сообщений, призывающих перейти на сайт и, например, проголосовать или получить какой-то выигрыш.

Конкретизируем что именно пытаются сделать мошенники посредством фишинга [4]:

1. Получить конфиденциальные данные, такие как: данные банковских карт, номера телефона, персональные данные с целью последующего шантажа или внесения в базы данных мошенников.
2. Получить доступ к вашим учётным записям, чтобы рассылать фишинг уже от вашего лица.
3. Убедить вас добровольно перевести деньги, передать ценности.

4. Заражение вашего устройства вредоносным программным обеспечением.

Любой человек может стать жертвой фишинга, однако чаще всего цель мошенников — неопытные пользователи, особенно пожилые люди.

Кратко выделим типы фишинга [3][4], чтобы позже сформулировать предписания для защиты себя от фишинга:

1. Почтовый фишинг — на почту отправляют письмо с просьбой перейти по ссылке на фишинговый сайт, дополнительно придумав ложную причину, почему вы должны так поступить.
2. Подделка доменного имени — взаимосвязано с прошлым. Но здесь злоумышленник меняет доменное имя компании, совсем немного, чтобы оно было похоже на оригинал.
3. Голосовой фишинг (вишинг) — вам звонит мошенник, выдавая себя за реального человека, например сотрудника компании или родственника. Вынуждая совершать определённые действия, нацеленные на передачу денежных средств мошенникам.
4. SMS-фишинг (смишинг) — так же, как и в случае вишинга, мошенники выступают от имени реально существующего человека или компании. В таком сообщении обычно содержится ссылка или телефонный номер, которыми вам предлагают воспользоваться. Пользователи мессенджеров тоже рискуют оказаться жертвами такой атаки.
5. Фишинг в соцсетях — Мошенник создаёт страницу или заполучает доступ к странице реального человека, от его лица совершая правонарушения. Зачастую мошенник просит помощи, по трудной жизненной ситуации.
6. Клон-фишинг — мошенники копируют уже полученные вами письма и заменяют их содержимое на вредоносное ПО.

Это далеко не все виды фишинга, но они являются наиболее распространёнными.

Зная основные виды фишинга, можно выделить основные правила для защиты от фишинга:

1) Не отвечать на незнакомые номера и сообщения незнакомцев.
2) Перепроверять информацию, особенно в случае, если это ссылки на вебсайты.
3) Не доверять подозрительным людям, собеседникам в интернете. Даже несмотря на их щедрость, или выгодные предложения.
4) Установите антивирусное ПО для почтового ящика и ваших устройств.
5) Перепроверять ссылки перед их использованием, чтобы убедиться в их подлинности.

В ходе многолетнего использования интернет-ресурсов и анализа существующих методов защиты пользователей от фишинга, можно прийти к выводу, что не существует универсального и абсолютно точного способа проверки вебсайта на фишинговую активность. Имеющиеся решения в основном проверяют сайт на наличие в базе данных фишинга, либо блокирует его полностью, если там есть хоть какое-то подозрение на фишинг.

В связи с этим была поставлена цель разработать альтернативное решение, способное выполнять проверку веб-ресурсов по иной методике. В рамках исследования было предложено создание программного обеспечения на языке C#, которое осуществляет анализ веб-сайтов, сравнивая их с базой данных официальных ресурсов. Такой подход позволяет минимизировать вероятность ложных срабатываний и одновременно снизить риск взаимодействия пользователя с потенциально опасными веб-сайтами.

Разработанное программное обеспечение представляет собой приложение с графическим интерфейсом, предназначенное для удобной работы пользователя с системой проверки. Внешний вид пользовательского интерфейса программы представлен на рисунке 1.

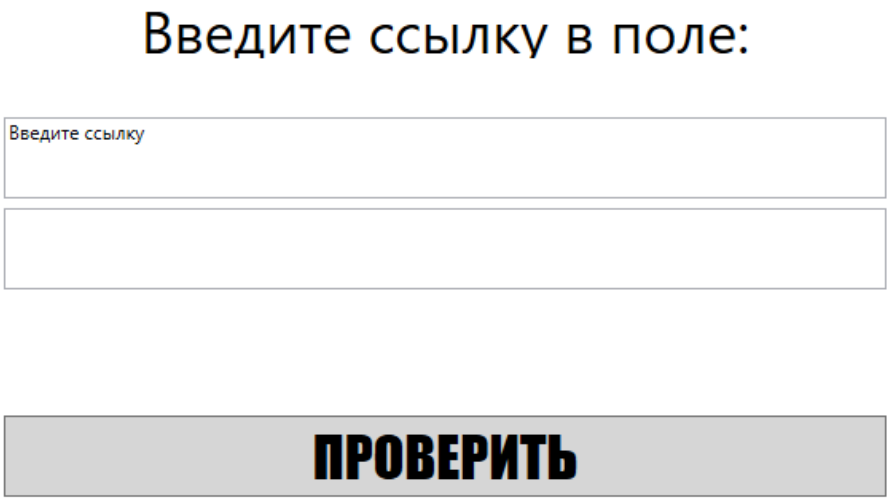

Рисунок 1 – Интерфейс приложения

Разработанное программное обеспечение обладает интуитивно понятным интерфейсом, позволяющим пользователям легко проверить веб-ресурс на наличие фишинговых признаков. Для проведения анализа пользователь вводит URL-адрес веб-сайта в специальное текстовое поле, расположенное в верхней части окна программы. В качестве примера можно рассмотреть проверку официального сайта КузГТУ (Рисунок 2).

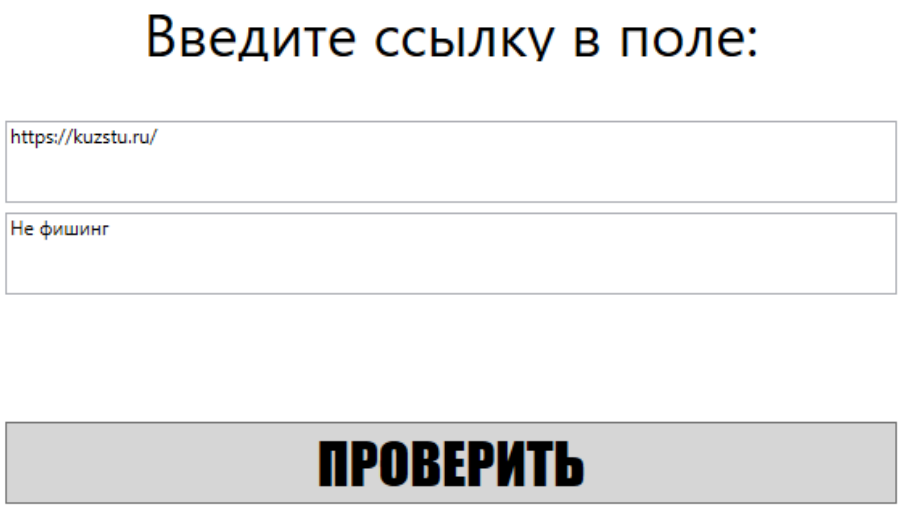

Рисунок 2 – Проверка настоящего сайта

После ввода ссылки и нажатия кнопки «Проверить» программа анализирует введенный URL, сверяя его с базой данных официальных сайтов. Если сайт присутствует в этой базе, программа выводит сообщение, информирующее пользователя о том, что данный ресурс не является фишинговым.

Для демонстрации работы программы можно проверить несуществующий домен, который гипотетически может быть использован злоумышленниками для получения данных студентов и преподавателей (Рисунок 3).

При вводе подобного URL-адреса и нажатии кнопки «Проверить» программа анализирует его наличие в базе официальных сайтов. Поскольку данный ресурс не зарегистрирован в списке доверенных доменов, система уведомляет пользователя о возможной угрозе. Это позволяет заблаговременно выявлять потенциально опасные веб-страницы, тем самым снижая риск утечки конфиденциальной информации.

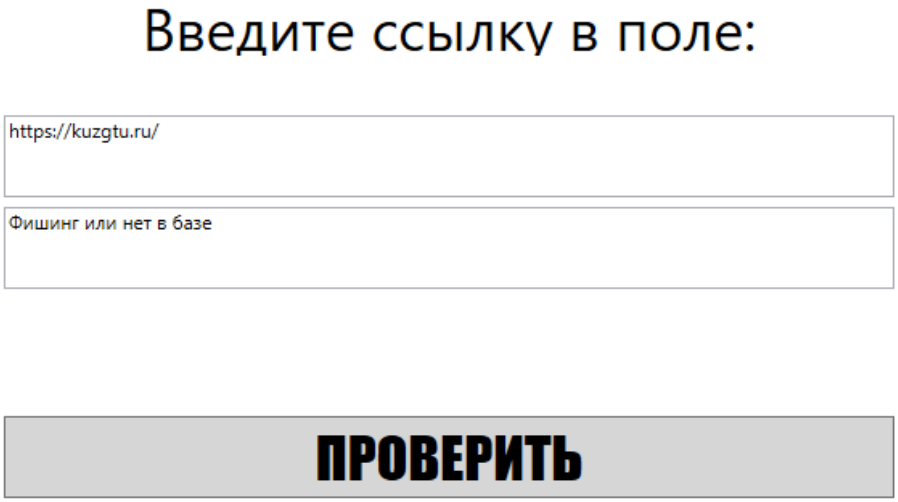

Рисунок 3 – Фишинговый сайт

В настоящее время программа находится в стадии доработки. В планах разработчиков — реализация возможности добавления пользовательских сайтов в базу данных программы, что позволит расширить функционал и повысить уровень защиты.

Кроме того, в перспективе рассматривается перенос программы в формат расширения для браузеров. Это обеспечит пользователям автоматический анализ посещаемых сайтов в реальном времени, минимизируя риск взаимодействия с фишинговыми ресурсами. Такой подход сделает работу в интернете более безопасной, предупреждая попытки мошенничества на ранних этапах.

Подводя итог, следует отметить, что фишинг является серьезной угрозой для современного общества, который затрагивает пользователей всех возрастов, однако особенно уязвимым остается старшее поколение. В условиях постоянного развития киберугроз крайне важно не только применять существующие методы защиты, но и разрабатывать новые, актуальные решения, способные эффективно противостоять мошенническим схемам.

Одним из ключевых направлений борьбы с фишингом является просвещение населения. Проведение тематических классных часов и информационных кампаний позволит повысить уровень осведомленности пользователей о киберугрозах и методах защиты. Только при активном взаимодействии разработчиков, специалистов по кибербезопасности и самих пользователей можно снизить уровень фишинга в обществе, обеспечив защиту персональных данных и финансовых средств.

Список литературы:

1. Куликова Т., Свистунова О., Ковтун А., Шимко И., Деденок Р. Спам и фишинг в 2023 году / Куликова Т., Свистунова О., Ковтун А., Шимко И., Деденок Р. [Электронный ресурс] // SECURELIST : [сайт]. — URL: 1. https://securelist.ru/spam-phishing-report-2023/109104/ (дата обращения: 24.03.2025).
2. Фишинг / [Электронный ресурс] // Ру-вики : [сайт]. — URL: https://ru.ruwiki.ru/wiki/Фишинг (дата обращения: 22.03.2025).
3. NATHAN COPPINGER, Varonis Systems Полное руководство по фишинговым атакам / NATHAN COPPINGER, Varonis Systems [Электронный ресурс] // Habr : [сайт]. — URL: https://habr.com/ru/companies/varonis/articles/544140/ (дата обращения: 22.03.2025).
4. Фишинговые письма: как их распознать и не стать их жертвой / [Электронный ресурс] // kaspersky : [сайт]. — URL: https://www.kaspersky.ru/resource-center/preemptive-safety/phishing-prevention-tips (дата обращения: 22.03.2025).