Фишинг: Угроза в Цифровом Пространстве

Выполнил: студент НБИБД-01-24
Ошкодер Сергей Александрович

Преподаватель: Кулябов Дмитрий Сергеевич, профессор кафедры прикладной информатики и теории вероятностей

Организация: Российский университет дружбы народов имени Патриса Лумумбы

О Докладчике

Студент НБИБД-01-24

Специализация: Бизнес-информатика

Интересы: Кибербезопасность, криптография, защита данных, IT-архитектура предприятия

Цель работы: Исследование методов фишинга и разработка эффективных мер противодействия для обеспечения безопасности пользователей в цифровой среде.

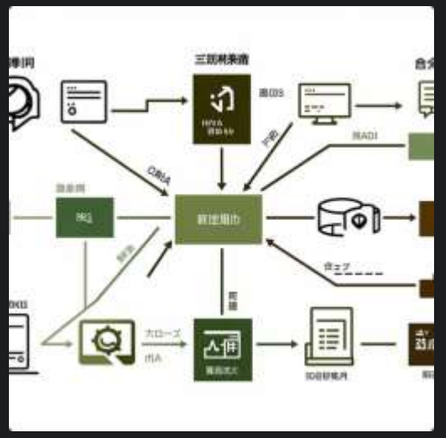
Вводная Часть: Актуальность. Проблемы Фишинга

Быстрый Рост Киберугроз

Фишинг остается одним из наиболее распространенных и изощренных методов кибератак, адаптируясь к новым технологиям и уловкам.

Уязвимость Пользователей

Недостаточная осведомленность пользователей делает их легкой мишенью для мошенников, приводя к значительным финансовым и репутационным потерям.



Масштаб Ущерба

Ежегодно миллионы людей и организаций по всему миру страдают от фишинговых атак, что подчеркивает критическую необходимость в эффективных решениях.

Типовой сценарий атаки

01

Убедительное сообщение

Жертве отправляют сообщение с 'срочной' причиной действовать

02

Перейти по ссылке

Злоумышленник направляет на поддельный сайт

03

Открыть вложение или сообщить код

Запрос конфиденциальной информации или кода подтверждения

04

Техники обхода защиты

Поддельные страницы входа, перехват сессий, прокси-страницы, выманивание одноразовых кодов

Часто используемые методы

- Поддельные страницы входа (очень похожи на настоящие)
- Техники обхода двухфакторной аутентификации
- Перехват сессий
- Прокси-страницы
- Выманивание одноразовых кодов

Цель и Предмет Исследования

Цель Работы

Комплексно изучить фишинг как угрозу:

- **Выделить ключевые виды и механизмы атак**
- **Разработать обоснованный комплекс мер защиты, привязанный к этапам атаки**

Классификация Фишинга и Контрмеры

Классификация фишинга помогает подобрать специфические контрмеры для каждого типа фишинга:

Против Поддельных Доменов и Писем	Против Поддельных Страниц Входа	Против Вредоносных Вложений
DMARC	FIDO2 и Подтверждение Устройства	**Применяем песочницы (sandbox)**

Этапы Фишинговой Атаки

Фишинговая атака проходит в 6 этапов:

01

Разведка

02

Подготовка

03

Доставка

04

Вовлечение

05

Компрометация

06

Закрепление и Монетизация

Предлагаемое Решение: Комплексная Программа Противодействия

Ключевой вывод: фишинг сочетает психологические и технические компоненты, поэтому одиночные меры защиты неэффективны.

Почему одиночные меры недостаточны?

Программа противодействия включает:

- **Технические Меры**
- **Организационные Меры**
- **Оперативные Меры**
- **Психологическая Подготовка**

Ключевой Принцип Решения:

Эффективность достигается только через комбинацию мер на всех этапах атаки — от разведки до монетизации. Каждая мера дополняет другую, создавая многоуровневую защиту (defense in depth).

Перспективы и Прогнозы

Перспективные Направления Развития Защиты от Фишинга

В среднесрочной перспективе стоит обратить внимание на следующие технологии и подходы:

Искусственный Интеллект и Машинное Обучение

Предиктивный анализ фишинговых атак и автоматическое обнаружение новых паттернов

Биометрическая Аутентификация

Дополнительный слой защиты на основе уникальных биологических характеристик

Блокчейн-Технологии

Подтверждение подлинности электронных документов и цифровых подписей

SOAR-Системы

Автоматизация реагирования на инциденты (Security Orchestration, Automation and Response)

Стандарты Безопасной Аутентификации

Развитие WebAuthn 2.0 и других современных протоколов

Прогноз Развития Угроз

Ожидается, что злоумышленники будут:

Социальная Инженерия в Мессенджерах

Активнее использовать подделку личности в мессенджерах и социальных сетях

Целевые Атаки (Spear Phishing)

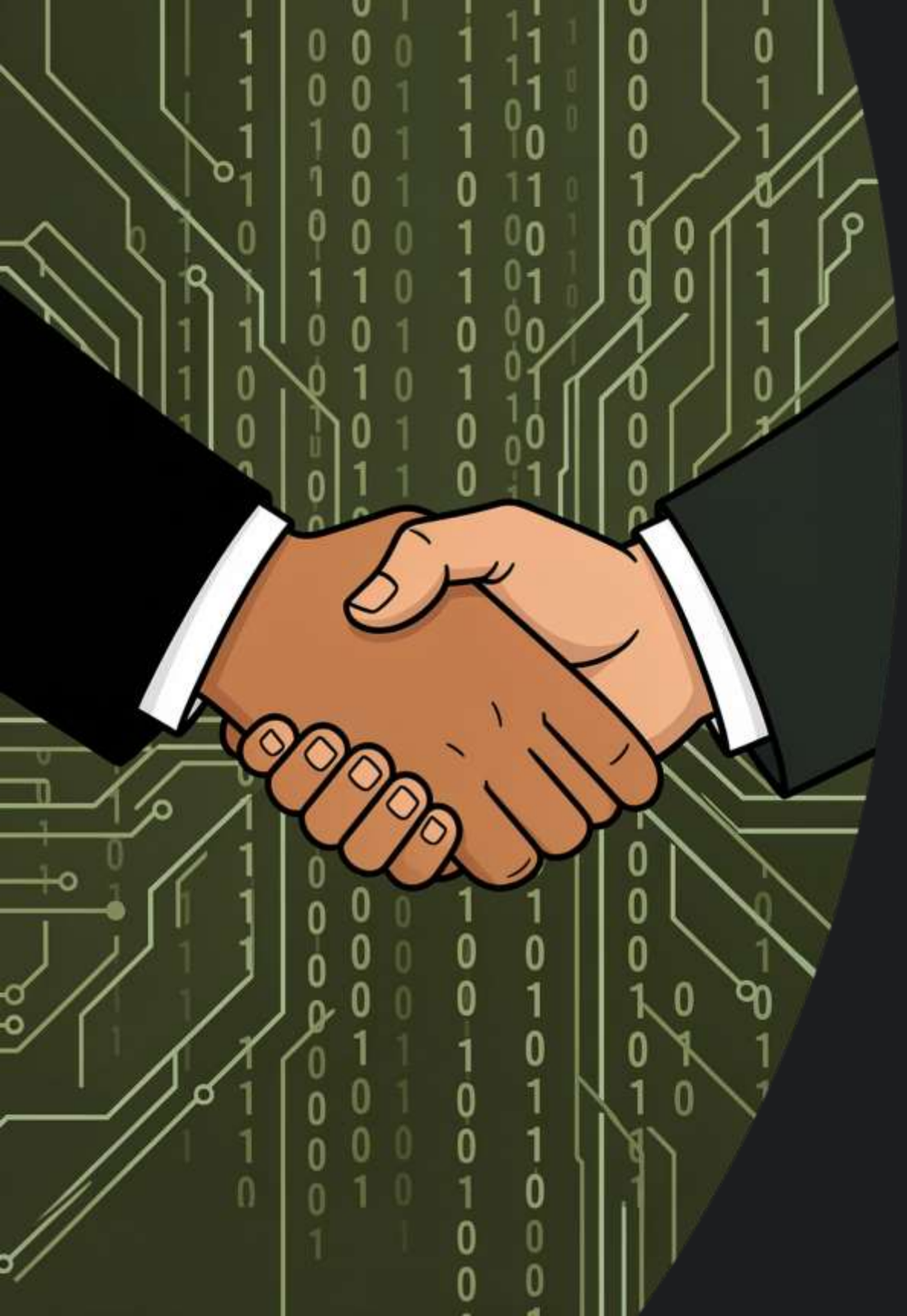
Применять персонализированные атаки с глубоким анализом целевой аудитории

Эксплуатация Уязвимостей

Использовать уязвимости в популярных сервисах и приложениях

Комбинированные Атаки

Комбинировать фишинг с распространением вредоносного ПО и другими видами атак



Заключение и Выводы

Фишинг Эволюционирует

Необходимость постоянной адаптации к новым угрозам.

Комплексный Подход

Сочетание технологий и обучения — ключ к успеху.

Человеческий Фактор

Критическая роль осведомленности и пользователей.

Моё исследование подтверждает, что только активные и многоаспектные стратегии могут обеспечить надежную защиту от фишинга в современном цифровом мире.