Доклад на тему “Фишинг”

Преподаватель Кулябов Дмитрий Сергеевич, д.ф.-м.н, профессор кафедры теории вероятностей и кибербезопасности

Азарцова Вероника Валерьевна

2026-02-20

Содержание

Список иллюстраций

Список таблиц

0.1 Объект и предмет исследования

- Обьект исследования - фишинг.
- Предмет исследования - методы защиты от фишинга в сфере информационной безопасности.

0.2 Актуальность

Фишинг (Phishing) - вид интернет-мошенничества, подразумевающий получение доступа к конфедициальным данным пользователя путём массовых рассылок от имени известных брендов или компаний и в некоторых случаях созданием поддельных сайтов.

Этот вид угрозы информационной безопасности как никогда актуален с развитием искусственного интеллекта, который способствует развитию новых, всё более реалистичных, методов фишинга. В настоящее время каждому студенту нужно глубоко понимать принцип работы фишинга, в целях того чтобы не стать его жертвой, и впоследствии обезопасить разрабатываемые продукты от него.

0.3 Цели и задачи

- Изучить различные методы фишинга и методы противодействия им.
- Проинформировать студентов с помощью полученной информации в форме доклада.

0.4 Материалы и методы

- Исследование проводится методом анализа литературных источников и научных статей на тему доклада.

0.5 Содержание исследования

0.5.1 Анализ угрозы

В основе фишинга - происходит от английского fishing, рыбалка - лежит попытка обмануть пользователя, внедрив ему необоснованное чувство безопасности, притворяясь официальным источником - известным сайтом, брендом, коллегой или знакомым.

Не смотря на то, что угроза фишинга далеко не новая, она нне теряет актуальность последние 10 лет и аналитики прогнозируют рост цены сферы защиты от фишинга на экономическом рынке (рис. 1).

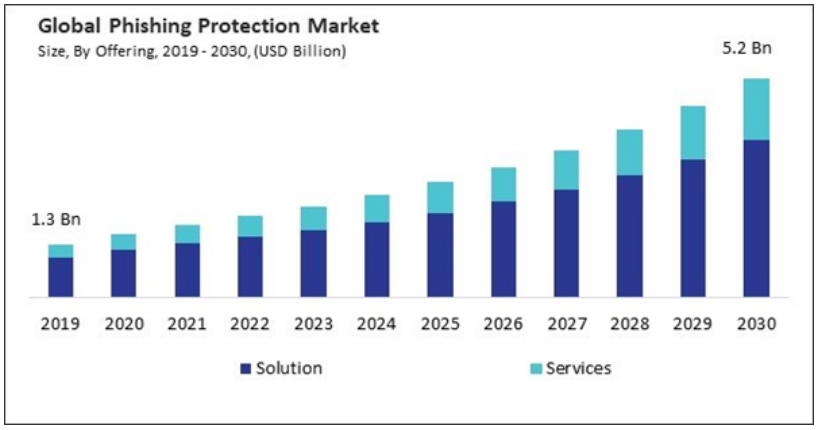

Рисунок 1: Статистика фишинга 2017-2024

В процессе исследования я выяснила, что существует пять наиболее распространненых методов фишинга (рис. 2):

- Bulk Phishing (Массовый фишинг) - массовая рассылга фишинговых писем целям без отбора.

- Spear Phishing (Фишинг «На копье») - Фишинг, направленный на специально отобранную цель - одного человека или компанию.
- Whaling («Китобойный» фишинг) - Фишинг, направленный на руководителя компании.
- Vishing, Voice Phishing - Фишинг, выполненный с помощью голосовых звонков.
- Smishing, SMS Phishing - Фишинг, выполненный через СМС или другие виды мгновенных текстовых сообщений.

Рисунок 2: Виды фишинга

0.5.2 Методы противодействия

После изучения документации на тему фишинга, я выяснила, что при существовании многих методов борьбы с фишингом, самый эффективных подход к защите от него для разработчика или управляющего компании многосторонний (рис. 3) и включает в себя все следующие действия:

1. Усложнить доступ мошшеников к пользователям

- Ограничить количество личной информации, такой как личный адрес электронной почты, номер телефона, физический адрес и другие, в открытом доступе, до минимум необходимой контактной информации.

2. Научить пользователей идентифицировать и отправлять жалобы на фишинг

- Изучить процессы, которые может мимикрировать фишинг: вход в систему с помощью логина, переход по незнакомым ссылкам.
- Провести нужный тренинг, обьясняющий различные методы фишинга и привести найденные уязвимости в пример.
- Ввести возможность жалоб на подозрительные входящие сообщения и убедиться что жалобы проверяются быстро.

3. Защититься от последствий фишинговых аттак

- Ввести методы защиты системы после получения мошенниками одного вида авторизации путем ввода мультифакторной авторизации.
- Убедиться, что пользователи вовремя обновляют браузеры и систему, и ввести использование прокси.
- Следовать современным рекомендациям производителей по защите устройств от вирусов.

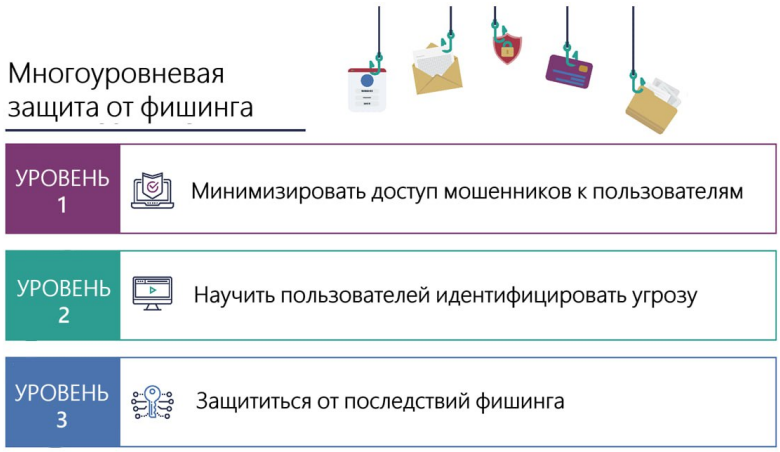

Рисунок 3: Мультисторонний подход к защите от фишинга

0.5.3 Аспект искусственного интеллекта

Нововведение в сфере фишинга - искусственный интеллект. Традиционный фишинг может выявляться по многим причинам, например, ошибки в грамматике отправителя, минимальных отличиях сайта от официального и выход за рамки контекста общения. С начала 2025, по статистике организаций кибер-безопасности (рис. 4) чаще и чаще большие языковые модели искуственного интеллекта успешно помогают мошенникам обходить все эти проблемы, создавая грамматически правильные сообщения, идеально подстроенные под информацию, собранную с общедоступных источников на лююбом языке, а также создавая реалистичные копии сайтов за минуты.

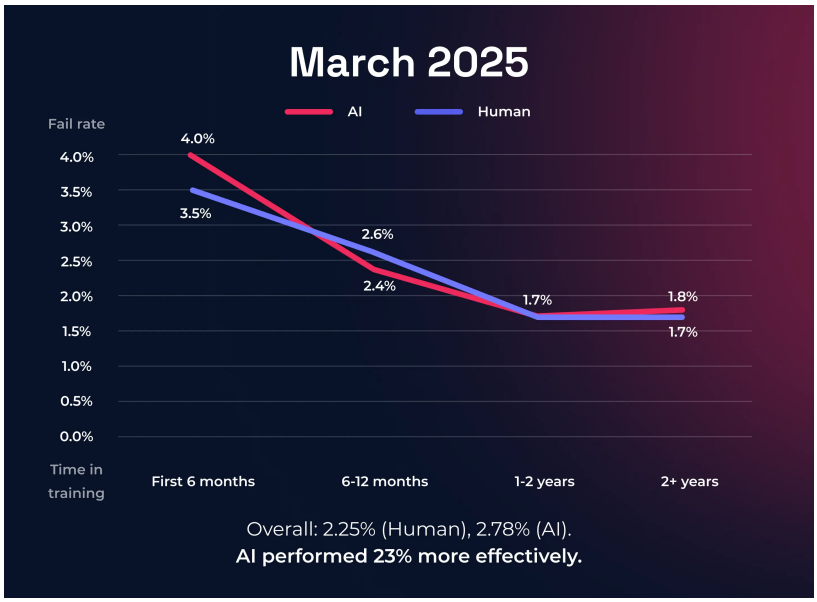

Рисунок 4: Статистика, март 2025, эффективность через фишинга ИИ

В противовес этому, в современной информационной безопасности искусственный интеллект активно используется для выявления фишинговых атак до того как они попадут к получателю, с помощью незаметных человеку маркеров поведения или синтаксиса.

Для защиты от новых развивающихся видов атак, нужно следить за последними новостями и применять не только традиционные, но и новые методы защиты.

0.6 Результаты

В результате исследования я:

- Изучила самый оптимальный многосторонний подход к защите от фишинговых атак.
- Изучила новые виды атак, использующие искусственный интеллект и требующие современных методов защиты.
- Преподнесла информацию в понятном виде, подготовившись проинформировать студентов о данной теме.

Список литературы

National Cyber Security Center, UK - «Phishing attacks: defending your organisation»

ru.wikipedia.org - «Фишинг»

www.checkpoint.com - “How AI Phishing Attacks Became A Threat in 2025

ibm.com, Matthew Kosinski, Staff Editor - «What is Phishing?»