Образовательный симулятор защиты личных данных

#TypeScript #FastAPI #Tailwind CSS / Material UI #PostgreSQL #Redis #Docker #WebSockets #React.js / Next.js

Интерактивный веб-симулятор для повышения цифровой грамотности и безопасности.

Пользователь попадает в среду, где ему необходимо выполнять повседневные задачи (работа с почтой, соцсетями), сталкиваясь с реальными сценариями кибератак. Задача пользователя — идентифицировать угрозу и применить правильный алгоритм защиты.

БАНК ЦЕНТР-ИНВЕСТ

О чём этот кейс?

В рамках данного кейса необходимо разработать платформу, которая решает проблему человеческого фактора как самого уязвимого звена в информационной безопасности. Решение представляет собой симулятор с нарративной составляющей.
В процессе прохождения сюжетных миссий (рабочий мессенджер, личная почта, настройка смартфона) система генерирует атаки: от самых примитивных (фишинговые письма) до сложных кейсов социальной инженерии с использованием дипфейков.

Целевой аудиторией являются пользователи, которые на ежедневной основе работают с информацией посредством рабочих мессенджеров, электронной почты, инструментами планирования задач, а также работают с конфиденциальными данными компании. Продукт может представлять собой desktop приложение или веб-приложение / мобильное приложение.

Основная его функция — в игровом стиле обучить пользователей идентифицировать кибер угрозы и применить правильный алгоритм защиты. Система производит обучение через действие: если пользователь ошибся, система не просто пишет «неправильно», а показывает пошаговую анимацию последствий взлома и обучает правильному алгоритму действий.

Важным компонентом станет рейтинговая система, позволяющая отслеживать процесс прохождения обучения

БАНК ЦЕНТР-ИНВЕСТ

Цель

Главная цель кейса — сформировать у пользователя устойчивые поведенческие паттерны безопасного поведения. Вместо скучных инструкций по информационной безопасности, создаем эмоциональный опыт. Когда студент «теряет» аккаунт в игре из-за того, что перешел по фишинговой ссылке, нейронные связи формируются глубже, чем при чтении текста. Решение должно обеспечить «индуктивный» метод обучения: от частных случаев (кликнул на ссылку -> получил вирус) к общим правилам (проверяй URL). Оценивается не просто количество пройденных тестов, а глубину понимания механик атак: различие между SPF, DKIM в письмах, распознавание поддельных сайтов и безопасное использование API.

Дополнительная цель — геймификация рейтингов. Внедрение системы лиг (новичок -> эксперт) и возможность получения верифицированного сертификата с QR-кодом повышает мотивацию. В перспективе платформа должна поддерживать API для импорта реальных кейсов атак, чтобы симулятор оставался актуальным перед лицом постоянно эволюционирующих угроз.

В рамках хакатона целью является создание рабочего прототипа, демонстрирующего выполнение ключевых задач и его потенциальную пользу для конечного пользователя.

БАНК ЦЕНТР-ИНВЕСТ

Основные задачи

- **Разработать нарративный сценарий (3+ уровней).** Создать логически связанные сюжетные линии (Офис, Дом, Общественный Wi-Fi), включающие не менее 5 типов атак (фишинг, скимминг, подбор пароля, соц. инженерия).

- **Создать модуль «Выбор действия».** Реализовать интерактивные карточки, где пользователь выбирает действие из 3-4 вариантов с валидацией выбора и системой подсказок при ошибке.

- **Реализовать модуль прогресса (геймификация).** Реализовать шкалу «Уровень безопасности» (HP) или «Репутация», которая снижается при ошибках и повышается при верных решениях.

- **Реализовать личный кабинет и отображение статистики.** Разработать экран с визуализацией прогресса (пройденные сценарии, процент успешных отражений атак, допущенные ошибки).

- **Реализованный интерфейс.** Обеспечить корректное отображение и полную функциональность на десктопе или на мобильных устройствах на ваш выбор.

БАНК ЦЕНТР-ИНВЕСТ

Требования к решению

- **Кроссплатформенность:** решение должно работать в стандартных веб-браузерах (Chrome, Yandex Browser). Если desktop, то на разных операционных системах (Windows, Linux). Это обеспечит максимальную доступность для пользователей.
- **Автономность:** решение должно быть самодостаточным. Запуск должен осуществляться одной командой (docker-compose up) или предоставлением ссылки на рабочий прототип (deploy).
- **Безопасность решения:** в ходе разработки запрещено использовать реальные вредоносные файлы (exe, скрипты-вандалы). Все угрозы должны быть симулированы на уровне интерфейса и текста.
- **Хранение данных:** данные о пользователях (логин, пароль, прогресс) должны храниться в базе данных. Пароли должны быть захэшированы.
- **Простой и минималистичный UI/UX:** интерфейс должен быть выполнен в стиле "легко научиться, трудно забыть".
- **Модульная архитектура:** код должен быть организован так, чтобы разные части программы (модуль сюжетов, рейтинг и пр.) были логически разделены. Это позволит в будущем легко дорабатывать и расширять продукт.
- **Безопасность и конфиденциальность:** поддержка протокола TLS 1.2/1.3.
- **Наличие рабочего прототипа** с демонстрацией его возможностей.
- **Ограничения** по языкам программирования, фреймворкам, библиотекам **отсутствуют**.
- **Документация:** обязательное наличие схемы базы данных (ER-диаграмма) и описание API (Swagger/OpenAPI или Postman-коллекция).

Входные данные

- **Актуальные базы уязвимостей:** CWE (Common Weakness Enumeration) — для описания последствий ошибок.
- **Реальные фишинговые сценарии:** APWG (Anti-Phishing Working Group) — для реалистичности сценариев.
- **Топ-10 угроз OWASP:** OWASP Top 10 — для объяснения пользователям, какие уязвимости эксплуатируют атакующие.
- **Дизайн-системы:** Material Design 3 или Human Interface Guidelines — для обеспечения высокого уровня UX.
- **Гайды по защите:** рекомендации Минцифры РФ и Лаборатории Касперского (раздел "Для пользователей").

БАНК ЦЕНТР-ИНВЕСТ

Критерии оценки

- Завершенность и работоспособность прототипа (презентация работающего модуля, веб- или мобильного-приложения). Реализованы все обязательные критерии (сценарии атак, упражнения).
- Простота и удобство интерфейса для управления. Отсутствие критических багов, ломающих логику прохождения.
- Чистота кода, наличие README и инструкции по запуску (Docker Compose).
- Наличие нарратива, эстетика интерфейса. Игра не должна выглядеть как «галочка» в тестировании. Важна скорость загрузки и интуитивность. Наличие пояснений «почему действие было опасным» после каждого шага. Отсутствие «слепых» кликов.
- Масштабируемость: возможность легко добавить новый сценарий атаки без переписывания ядра.
- Реализация рейтингов, системы сертификации и детального трекинга прогресса.
- Инновационность и креативность: привнесла ли команда в решение какие-то уникальные идеи, которых нет в стандартной постановке задачи, но которые могут быть очень полезны?
- Качество и понятность презентации.
- Для веб-приложение обязательна поддержка протокола TLS 1.2 +

БАНК ЦЕНТР-ИНВЕСТ

Рекомендации к презентации

- Описать только действительно реализованные возможности. Что не реализовано – предложить roadmap развития продукта.
- Указать стек использованных технологий. Если есть нестандартное/интересное применение технологий, то рассказать об этом подробнее.
- Описать кратко функционал (список функций).
- Продемонстрировать живой пример. Показать работу прототипа на реальном сценарии: «Есть данные. Моделируем атаку на данные. Показать, как защищаем данные от атаки».
- Демонстрация интерфейса. Показать экраны приложения. Продемонстрировать сюжетную линию, как совершается атака, как ее распознаем атаку и какие способы защиты используем и почему.
- Ссылка на реализованное решение (QR-код).

БАНК ЦЕНТР-ИНВЕСТ

Желаем успеха!

Сергей
Суховский

@SERGIO_SUKHOVSKIY

Руководитель
кредитных проектов

БАНК
ЦЕНТР-ИНВЕСТ