УДК 004.056

Завадський Д.О., Кушніренко Н.І.

Національний університет «Одеська політехніка»

РОЗРОБКА НАВЧАЛЬНОГО ЗАСТОСУНКУ ДЛЯ ПРОТИДІЇ АТАКАМ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Вступ. Соціальна інженерія є потужним і дедалі більш актуальним чинником кіберзагроз: вона обминає технічні бар'єри, експлуатуючи людський фактор.Згідно з нещодавнім звітом, близько 74% інцидентів інформаційної безпеки пов'язані з людськими помилками, зокрема з використанням психологічних тактик соціальної інженерії [1].

Така статистика підкреслює вразливість організацій і користувачів перед цими атаками. Натомість більшість традиційних навчальних підходів – суто теоретичні курси чи періодичні перевірки за допомогою фішингових листів – не забезпечують глибокого засвоєння знань і практичних навичок. Тож зростає потреба в нових інтерактивних методах навчання, які долають пасивність і формалізм існуючих програм.

Мета: створення веб-застосунку, який у доступній та інтерактивній формі навчає користувачів розпізнавати атаки методами соціальної інженерії.

Основна частина

Ключовою ідеєю запропонованого підходу є додавання елементів гейміфікації в процес навчання - використання механізмів, властивих комп'ютерним іграм (бали, рівні, досягнення, рейтинги), для підвищення мотивації користувачів. Завдяки цьому навчальний процес набуває інтерактивного характеру: замість послідовного виконання інструкцій він перетворюється на динамічну гру, у якій кожне рішення має наслідки..

Застосунок побудовано за модульним принципом і включає кілька рівнів складності:

1. Базовий рівень - користувач знайомиться з основними типами атак: фішинг, смішинг, вішинг, бейтинґ, пре-текстинг. На цьому етапі система демонструє типові приклади обману й пояснює, як розпізнати ознаки маніпуляції.

2. Практичний рівень - користувач отримує завдання у вигляді реалістичних сценаріїв. Наприклад, на екрані з'являється фальшивий лист «від банку» або запит на оновлення паролю, і користувач повинен обрати, як діяти. Залежно від рішення система показує наслідок - успішне уникнення атаки чи умовну «втрату даних» користувача або організації де працює індивід.

3. Поглиблений рівень - тренування з підвищеною складністю, де потрібно аналізувати контекст, поведінку співрозмовника або структуру вебсторінки. Такі завдання розвивають критичне мислення та вчать оцінювати інформацію більш комплексно, та позитивно сприяють на критичне мислення.

Окрім навчальних сценаріїв, у програмі реалізовано систему миттєвого зворотного зв'язку. Після кожної відповіді користувач бачить коротке пояснення - чому обране рішення було правильним або помилковим, які маніпулятивні прийоми застосував зловмисник і як їх розпізнати у майбутньому.

Важливим компонентом стала адаптивність навчання. Застосунок відстежує успішність користувача і автоматично змінює рівень складності наступних завдань. Якщо учасник впевнено проходить базові тести, система пропонує складніші ситуації, що вимагають детальнішого аналізу; якщо ж він робить багато помилок - надає підказки та додаткові приклади.

Такий підхід дозволяє навчатися у власному темпі, що особливо корисно для користувачів з різним рівнем цифрової компетентності. Ще однією перевагою є простота доступу. Застосунок є веборієнтованим - для роботи не потрібно встановлювати додаткове програмне забезпечення. Він адаптований для мобільних пристроїв і персональних комп'ютерів, що робить його універсальним інструментом для освітніх установ, компаній або індивідуального користування [2].

Технічна реалізація проєкту базується на використанні мови програмування JavaScript, що забезпечує високу продуктивність, гнучкість та масштабованість системи. За візуальне відображення використано HTML.

Психологічна складова - одна з головних переваг розробки. Кожен сценарій не лише навчає, а й пояснює, які емоційні тригери використовуються у конкретній атаці: довіра до авторитету, страх, терміновість, співчуття чи цікавість. Таким чином, користувач не просто запам'ятовує набір правил, а розуміє логіку дій зловмисника, що дозволить у подальшому бути більш уважним.

Інтерфейс застосунку створено з урахуванням принципів когнітивної ергономіки: мінімалістичний дизайн, інтуїтивна навігація, короткі інструкції, чітка візуалізація ризиків. Завдяки цьому навчання не перевантажує користувача інформацією, а натомість сприяє концентрації на суті завдання.

Висновок. Запропонований веб-застосунок спрямований на посилення цифрової безпеки користувачів шляхом інтерактивного навчання. Він допомагає практично закріпити навички розпізнавання соціально-інженерних атак і виробити алгоритми реагування на них. Поєднання теоретичних пояснень, ігрових тренінгів та регулярного тестування знань робить навчання ефективнішим. [3]. Завдяки такому комплексному підходу - інтерактивна практика плюс акцент на психологічних механізмах атак - користувачі краще підготовлені і менш схильні до помилок. Таким чином інтерактивне навчання з практичними симуляціями і психологічною обізнаністю сприяє суттєвому підвищенню загального рівня кібербезпеки.

Перелік використаних джерел.

1. Verizon Data Breach Investigations Report 2024. Verizon Enterprise, 2024. 98 p. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 11.10.2025).

2. ISO/IEC 27032:2023 Cybersecurity Guidelines. International Organization for Standardization, Geneva, 2023. 65 p..

3. Gartner Research. The Impact of Gamified Cybersecurity Training on Employee Awareness, 2024. 12 p. DOI: https://doi.org/10.1016/gartner.cybersec.2024.0415.