Scopri il phishing

Adattabile didatticamente per le seguenti materie:

Informatica/Scienze informatiche, Alfabetizzazione Mediatica, Educazione Civica, Economia, Lingua Inglese

Gruppo target	Studenti delle scuole secondarie superiori (età 15-18)
Argomenti	Riconoscimento di phishing/truffe online, cittadinanza digitale, linguaggio/tono persuasivo
Dimensione del gruppo	Una classe (20-25 studenti)
Pre- Requisiti e conoscenze pregresse	Alfabetizzazione digitale di base e esperienza nell'uso di Internet Familiarità con i social media e le piattaforme online Familiarità con l'uso di strumenti di intelligenza artificiale (ad esempio ChatGPT)
Obiettivi di apprendimento dal Curriculum DataPro	C.1 Gestione dell'identità ● Consapevolezza d'uso: interrogarsi regolarmente su come e dove utilizzare e condividere in modo sicuro le informazioni di identificazione personale. Comprendere i rischi associati alla condivisione dei dati personali. C4 Coontrollo validità delle informazioni e delle fonti ● Verifica delle fonti: prepararsii a consultare più fonti per verificare le informazioni, per riuscire a riconoscere e comprendere i diversi punti di vista o pregiudizi che si celano dietro determinate informazioni e fonti di dati. ● Riconoscimento dei pregiudizi: imparare a identificare i potenziali pregiudizi nelle informazioni, comprendendo che ogni fonte di dati può avere un pregiudizio intrinseco basato sulla sua origine o sul suo scopo.
Obiettivi di apprendimento specifici aggiuntivi	N/A
Durata	Singola lezione (circa 45 minuti; può essere abbreviata o prolungata a seconda delle necessità)

Requisiti tecnici	Computer/tablet con accesso a Internet per gli studenti (individuali o in coppia)
Materiali e strumenti di formazione da DataPro	Agente conversazionale DataPro Spot the Phish: Bank (strumento di apprendimento digitale)Spot the Phish: InstaPic (strumento di apprendimento digitale)
Materiali didattici specifici aggiuntivi	N/A
Suggerimenti per lo svolgimento di una lezione	**Introduzione al phishing (5 minuti)** • Discussione in classe: chiedete agli studenti di spiegare cosa sanno sul phishing e (facoltativo) di condividere eventuali esperienze personali relative alle minacce alla sicurezza online (ad esempio phishing, hacking, truffe). **Sessione pratica con strumenti di apprendimento digitale (15 minuti)** • Gli studenti completano individualmente entrambi gli strumenti di apprendimento digitale su come distinguere tra phishing ed e-mail/messaggi sui social media legittimi. **Scenario Data Pro Conversational Agent (20 minuti)** Presentate agli studenti un breve scenario realistico. Chiedete loro di utilizzare l'agente conversazionale DataPro per porre domande su come dovrebbero procedere nello scenario. Scenari suggeriti e possibili domande: • Ricevi un messaggio Whatsapp da un numero sconosciuto, che dice: “Ciao, sono tuo cugino! Ho cambiato numero! Puoi mandarmi 50 euro? Ti spiego dopo”. Come verifichi che sia davvero tuo cugino? Perché i truffatori si fingono nostri parenti o conoscenti? Cosa dovresti fare? • Ricevi un’e-mail dalla direzione scolastica, che ti chiede di effettuare il login e di aggiornare i tuoi dati nell’account studente, tramite un link. L’indirizzo e-mail è simile a questo: adminschool@gmail.com. Cosa controlli per prima cosa? L’indirizzo e-mail è affidabile? Chi potresti contattare per confermare l’autenticità dell’e-mail? • Mentre navighi sul Web, compare una schermata rossa con il messaggio: “Il tuo computer è stato infettato! Chiama immediatamente l’assistenza Microsoft all’ 123-456-789. Microsoft funziona in questo modo? Quali rischi comporta chiamare? Cosa dovresti fare, invece?

	Conclusione (5 minuti) • Chiedete agli studenti di scrivere una cosa utile che hanno imparato dal chatbot e di condividerla con la classe o in coppia


DATAPRO

Syllabus Data Pro
Scopri il phishing

WP2

Organizzazione	ProEduca z.s.
Progetto	DataPro
Livello di diffusione	Pubblico
Data di presentazione	Giugno 2025
Autori principali	Pippa Thompson | Lucie Brzáková

Co-funded by the European Union

Finanziato dall'Unione Europea. Le opinioni e i pareri espressi sono tuttavia esclusivamente quelli degli autori e non riflettono necessariamente quelli dell'Unione Europea o dell'Agenzia esecutiva per l'istruzione e la cultura (EACEA). Né l'Unione Europea né l'EACEA possono essere ritenute responsabili per essi.