

Rozpoznávání phishingu, podvodů a sociálního inženýrství online

Začlenění do školních předmětů – Informatika, Výchova k bezpečnosti

Cílová skupina	Střední škola
Velikost skupiny	Minimálně 10 studentů, maximálně 30 studentů
Požadavky na předchozí znalosti	(Pro učitele) Připravte příklady phishingových zpráv (e-mail, SMS, zprávy v messengerech). Připravte příklady bezpečných a nebezpečných webových stránek.
Výukové cíle z kurikula DataPro	A.2 Bezpečnostní opatření Rozpoznávat nebezpečné e-maily, SMS zprávy a odkazy. Osvojit si základní pravidla bezpečného používání internetu. Naučit se využívat bezpečnostní filtry a aktualizace systému. A.3 Kritické hodnocení Rozvíjet schopnosti kritického hodnocení informací nalezených online. Rozpoznávat manipulativní pokusy a nepravdivé zprávy. B.1 Uznávání svobody Porozumět tomu, že ochrana soukromí umožňuje bezpečné používání internetu. Uvědomit si rizika spojená se ztrátou kontroly nad osobními údaji. C.1 Správa identit Naučit se vytvářet silná a jedinečná hesla. Rozvíjet povědomí o ochraně přihlašovacích údajů a osobních dat. Porozumět významu dvoufaktorového ověřování.
Další specifické výukové cíle	Rozvoj digitálních kompetencí. Rozvoj schopnosti týmové spolupráce. Zlepšení analytického a kritického myšlení.



	Rozvoj odpovědnosti za vlastní chování online.
Časový rámec	3 různé varianty lekcí v délce 45 minut Dodatečný čas na domácí úkol v rámci třetí metodiky je 30 minut.
Technické požadavky	Notebooky nebo tablety s připojením k internetu Projektor Materiály s příklady phishingových zpráv
Výukové materiály a nástroje z project DataPro	Odhal falešnou zprávu: InstaPik (aktivita Interacty) Odhal falešnou zprávu: Česká banka (aktivita Interacty) DataPro AI Assistant
Další specifické výukové materiály	
Návrhy na strukturu lekce / metodický postup	Návrh 1 • Úvodní diskuse: s jakými hrozbami se mohou uživatelé internetu setkat. • Učitel představí příklady phishingových zpráv a falešných webových stránek. • Studenti pracují ve dvojicích, analyzují příklady a identifikují znaky podvodu. • Společná diskuse a vytvoření seznamu pravidel bezpečného chování online. Návrh 2 • Krátké zopakování pravidel online bezpečnosti. • Praktické cvičení: studenti dostanou modelové situace a rozhodují, jak reagovat. Tyto scénáře lze vytvořit pomocí nástroje DataPro AI Assistant. • Diskuse: proč kyberzločinci používají manipulaci a na jaké emoce cílí. • Učitel představí způsoby hlášení podvodů a správné reakce na incidenty. Návrh 3 • Skupinový projekt: vytvoření plakátu nebo infografiky „Jak se nenechat podvést online?“ • Prezentace projektů studentů. • Shrnutí nejdůležitějších pravidel bezpečnosti. Domácí úkol



	Studenti připraví krátký seznam pravidel bezpečného používání internetu pro mladší studenty nebo členy rodiny.
--	--



DataPro Sylabi | Work Package 2

Kontaktní osoba | Joanna Bać
Instituce | CWEP
E-mailová adresa | joanna.bac@cwep.eu
Telefonní číslo | +48 17 853 66 72

Projekt | DataPro
Úroveň šíření | Veřejná
Datum | prosinec 2024 – únor 2025
Autoři | Joanna Bać



**Spolufinancováno
Evropskou unií**

Financováno Evropskou unií. Názory vyjádřené jsou názory autora a neodráží nutně oficiální stanovisko Evropské unie či Evropské výkonné agentury pro vzdělávání a kulturu (EACEA). Evropská unie ani EACEA za vyjádřené názory nenese odpovědnost.