

DataPro · Plán lekce: Nothing to Hide

Tematická skupina C – Opatření na ochranu údajů

Co mohu konkrétně udělat? | 5.–8. ročník | přibližně 90 minut

Předmět	Informatika, mediální výchova, společenské vědy
Délka	2 vyučovací hodiny po 45 minutách nebo jeden 90minutový blok
Prezentace	Dostupná na: https://www.datapro.education/datapro-webgames/ v části „Class Material“
Doplňkové materiály	Pracovní list k phishingu, DataPro Chatbot / DataPro Assistant pro doplňující úkoly, Kahoot: https://www.datapro.education/tools/
Příprava před lekcí	Učitel si předem prostuduje Průvodce hrou pro učitele, dostupný na: https://www.datapro.education/datapro-webgames/
Předchozí znalosti	Lekce navazuje na tematické skupiny A a B, ale lze ji využít také samostatně.
Odkaz na hru	https://dataprogames.ph-freiburg.de/nothing-to-hide/

Výukové cíle

Po dokončení lekce žáci dokážou:

- vytvořit silné a snadno zapamatovatelné heslo nebo přístupovou frázi a vysvětlit, proč je bezpečnější než krátké nebo předvídatelné heslo (C.2);
- vysvětlit princip **dvoufázového ověřování (2FA)** a uvést příklady druhého ověřovacího kroku, například kód zasláný na telefon nebo ověřovací aplikaci (C.2);
- rozpoznat typické znaky phishingu a základní taktiky sociálního inženýrství (C.4);
- správně reagovat na podezřelé zprávy nebo odkazy: **neklikat, neodpovídat, ověřit odesílatele a podezřelý obsah nahlásit** (C.4);
- samostatně vyhledávat a ověřovat informace k tématu digitální bezpečnosti a využít nástroj DataPro k vytvoření jednoduchého výukového nebo kvízového materiálu (C.5).

Struktura lekce

Čas	Fáze / cíl	Průběh lekce	Snímek / materiály
10 min	Úvod Zmapování dosavadních znalostí a návyků	Položte žákům otázku: Co už dnes děláte pro svou bezpečnost na internetu? Odpovědi zapisujte na tabuli a společně je rozdělte na běžně používaná opatření a věci, na které se často zapomíná. Zdůrazněte, že cílem lekce není „být dokonale v bezpečí“,	Bez prezentace – společná úvodní diskuse.

		ale umět rozpoznat riziko a vědomě volit bezpečnější postup.	
25 min	Hesla a dvoufázové ověřování <i>Posílení zabezpečení účtů</i>	Snímek 2: Proveďte se žáky aktivitu zaměřenou na tvorbu silného hesla nebo přístupové fráze. Diskutujte o tom, proč jsou krátká, osobní nebo snadno předvídatelná hesla riziková. Snímek 3: Vysvětlete princip dvoufázového ověřování (2FA) a tři základní typy ověřovacích faktorů: něco, co znám; něco, co mám; něco, čím jsem. Společně uveďte příklady. Na závěr položte otázku: Proč nemusí ani silné heslo samo o sobě stačit?	Snímek 2: Hesla + aktivita. Snímek 3: Dvoufázové ověřování (2FA).
20 min	Phishing a sociální inženýrství <i>Rozpoznávání podezřelých zpráv a pokusů o manipulaci</i>	Snímek 4: Vysvětlete, co je phishing a jak fungují základní taktiky sociálního inženýrství. Snímek 5: Společně analyzujte několik příkladů. Ptejte se: Co je na zprávě podezřelé? Co se nás odesílatel snaží přimět udělat? Jak bychom mohli zprávu ověřit? Poté žáci pracují s pracovním listem k phishingu a vyhledávají typické varovné signály v ukázkových zprávách.	Snímek 4: Phishing a sociální inženýrství. Snímek 5: Příklady k diskusi. Pracovní list k phishingu: https://www.datapro.education/tools/
25 min	Hra: Nothing to Hide <i>Uplatnění ochranných opatření v modelových situacích</i>	Před zahájením hry zadejte žákům pozorovací úkol: Která bezpečnostní opatření ve hře pomáhají? Ve kterých situacích vzniká riziko? Kde byste se rozhodli jinak než postava ve hře? Žáci si mohou poznamenat jedno rozhodnutí, které považovali za zvlášť důležité nebo překvapivé. Pokud hru hráli již v předchozí lekci, mohou porovnat své současné rozhodování s předchozí zkušeností.	Nothing to Hide: https://dataprogames.ph-freiburg.de/nothing-to-hide/
20 min	Přenos znalostí: Vytvořte vlastní kvízovou otázku <i>Upevnění a sdílení získaných znalostí</i>	Snímek 6: Každý žák nebo dvojice si vybere jedno téma z lekce – například silná hesla, 2FA, phishing nebo bezpečné ověřování zpráv – a pomocí DataPro Chatbota vytvoří	Snímek 6: Kvízový úkol a pokyny. DataPro Chatbot: https://datapro.cyber-geiger.com

		krátkou kvízovou otázku. Nejprve společně projděte pokyny uvedené na snímku. Žáci si poté otázky vzájemně vymění, odpovědi porovnají a u nejasností společně vysvětlí správné řešení.	
--	--	---	--

Poznámky

- Prezentace obsahuje celkem 7 snímků. Snímek 2 obsahuje kompletní aktivitu zaměřenou na tvorbu bezpečných hesel, včetně příkladů.
- Snímek 6 obsahuje podrobné pokyny k vytvoření zadání pro DataPro Chatbot. Doporučujeme je před zahájením aktivity projít společně se žáky a ujistit se, že zadání rozumějí.
- Aktivita s tvorbou kvízových otázek na snímku 6 je vhodná také pro práci ve dvojicích.
- Příklady phishingových zpráv ze snímku 5 žákům před aktivitou podrobně nevysvětľujte. Nechte je nejprve samostatně rozpoznat podezřelé prvky a formulovat, podle čeho je identifikovali.
- Tematická skupina C je vhodným zakončením celé série lekcí. Pokud žáci hráli Nothing to Hide již v tematické skupině A, lze porovnat jejich současná rozhodnutí a výsledky s první zkušeností a diskutovat o tom, zda se jejich přístup k ochraně dat a digitální bezpečnosti změnil.

Hodnocení

- Vzájemné ověření kvízových otázek: žáci si ve dvojicích vymění otázky vytvořené v rámci aktivity ze snímku 6, odpoví na ně a následně společně zkontrolují a vysvětlí správné řešení.
- Kahoot kvíz zaměřený na ochranná opatření je dostupný na: <https://www.datapro.education/tools/>
- Pokud žáci hráli hru Nothing to Hide již v tematické skupině A, porovnejte výsledky z obou hraní. Zaměřte se nejen na počet bodů, ale také na otázky: Rozhodovali jste se tentokrát jinak? Která rizika jste nyní rozpoznali dříve? Co ovlivnilo vaše rozhodování?

Projekt	DataPro – Erasmus+
Institutce	Pädagogische Hochschule Freiburg
Autor/ka	Renata Säuberli
Datum	Červen 2026