Digitální identita a bezpečnost

Relevantní scénář únikové místnosti a zdroj projektu	• ER1 Porozumění AI • Využívání online ER11 a digitální bezpečnost • Pracovní list pro samoškolení: Etické otázky v digitálním podnikání
Cílová skupina a potřeby	**Věkové rozmezí:** 15–25 let **Velikost skupiny:** 3–6 účastníků **Předchozí znalosti nebo zkušenosti jsou vyžadovány:** Základní každodenní používání chytrých telefonů a sociálních médií
Délka trvání	60–75 minut
Cílové oblasti kompetencí	• Ochrana osobních údajů a soukromí • Porozumění digitální identitě a stopě • Etické rozhodování a bezpečné digitální chování
Cíle	• Identifikujte silná a slabá pravidla pro hesla. • Rozpoznávejte phishing a nebezpečné chování na internetu. • Identifikujte význam a dopad digitální stopy. • Dělejte etická rozhodnutí v realistických digitálních dilematech. • Používejte základní strategie ochrany soukromí.
Materiály a vybavení	• Tištěné listy hádanek (logická mřížka s hesly, screenshoty zpráv/příspěvků, karty scénářů)

	• Pera a papír nebo tabule na poznámky • Časovač nebo odpočítávací hodiny
Užitečné zdroje	• Thales - Pokyny ENISA pro ochranu identity a multifaktorovou autentizaci odolnou vůči phishingu • Evropská komise – Lepší internet pro děti • Zdarma simulátor phishingu – Zkusit mě vyvraždit, pokud můžeš
Nastavení	• Připravte 4 výzvové stanice s čísly, které označí pořadí, v jakém musí být provedeny. • Na každé stanoviště umístěte jednu hádanku. • Uspořádejte stoly tak, aby se týmy střídaly mezi stanovišti.
Krok za krokem instrukce	**Krok 1 – Úvod do příběhu (5 min)** Účastníci jsou informováni, že jejich účet na sociální síti byl kompromitován, hacknut a upraven. Musí ji zajistit a odstranit problematický obsah dříve, než dojde k nevratnému poškození. **Krok 2 – Stanice 1: Logická hádanka s heslem (15 min)** Účastníci řeší logickou mřížku, aby identifikovali nejsilnější heslo na základě pravidel (délka, symboly, jedinečnost) a zajistili účet pro přístup k dalšímu kroku. **Krok 3 – Stanice 2: Phishing nebo bezpečný (15 minut)** Účastníci analyzují zprávy a příspěvky a rozhodují, zda jsou bezpečné, nebezpečné nebo zahrnují phishing, aby identifikovali rizika a zablokovali potenciální hrozby před dalším postupem.

	Krok 4 – Stanice 3: Scénáře digitální stopy (10 min) Scénářové karty popisují typické online akce (nadměrné sdílení, debaty, e-mailové řetězce) a možné důsledky. Účastníci musí každou akci sladit s jejím dlouhodobým dopadem, aby odemkli další hádanku. **Krok 5 – Stanice 4: Etická dilemata (10 min)** Účastníci si musí v komplikovaných situacích vybrat mezi možnostmi (sdílení dat za účelem "pomoci" příteli, nahlášení nebo odhalení kyberšikany, zveřejnění či cenzura citlivého tématu). Každá volba vede k jiným výsledkům, které musí hráči zdůvodnit a zodpovědně zvládnout na základě všeho, co se naučili na předchozích stanicích. Jakmile prokáže, že rozumí, mohou přistupovat ke svému poškozenému účtu a cítit se bezpečně online.
Otázky k výslechu	• Které online chování mi přišlo "normální" a běžné, ale ve skutečnosti bylo riskantní? • Jak malé činy budují digitální stopu v průběhu času? Co to obnáší? • Byly etické volby vždy zřejmé? Proč ano nebo proč ne? Jaké by byly jejich důsledky? • Co byste změnili ve svých online návycích?
Hodnocení a hodnocení	• Pozorování skupinových rozhodnutí a kvalita reflexe a odůvodnění pro stanici 5 a debriefing • Kontrolní seznam sebehodnocení ("Dokážu rozpoznat phishing", "Vím, jak chránit svá data")

Varianty a adaptace	• **Mladší skupiny:** Méně scénářů, více vizuálních signálů, konkrétní a "černobílé" dilemata • **Neurodiverzní účastníci:** Jasné ikony, omezený text, strukturované volby, další nápovědy, flexibilní načasování • **Pokročilé skupiny:** Více protichůdných dilemat bez dokonalé odpovědi, podporují debatu a nuance
Tipy pro trenéry	• Vyhněte se moralizování; Soustřeďte se na důsledky a objektivní rizika, ne na soudy. • Podporujte diskusi a mediaci, když se účastníci neshodnou. • Udržujte scénáře realistické a blízké každodennímu digitálnímu životu účastníků. • Zdůrazněte, že bezpečnost je společná odpovědnost.
Reference a další literatura	• Agentura Evropské unie pro kybernetickou bezpečnost (ENISA). (2023). *Základy kybernetické bezpečnosti pro občany*. • Evropská komise. (2025). *DigComp 3.0: Evropský rámec digitálních kompetencí*.

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.

Kód projektu: 2023-2-LT02-KA220-YOU-000183156