Цифрова идентичност и безопасност

Подходящ сценарий за стая за бягство и ресурс за проекта	• ER1 Разбиране на изкуствения интелект • ER11 Онлайн експлоатация и дигитална безопасност • Работен лист за самообучение: Етични проблеми в дигиталното предприемачество
Целева група и нужди	**Възраст:** 15-25 години **Размер на групата:** 3-6 участници **Необходими предварителни знания или опит:** Основно ежедневно ползване на смартфони и социални медии
Времетраене	60–75 минути
Целеви области на компетентност	• Защита на личните данни и поверителността • Разбиране на дигиталната идентичност и дигиталния отпечатък • Етично вземане на решения и безопасно дигитално поведение
Цели	• Идентифицирайте правилата за силни и слаби пароли. • Разпознавайте фишинг и опасно онлайн поведение. • Определете значението и въздействието на дигиталния отпечатък.

	• Вземайте етични решения в реалистични дигитални дилеми. • Прилагайте основни стратегии за защита на поверителността.
Материали и оборудване	• Разпечатани листове с пъзели (мрежа с логика на пароли, екранни снимки на съобщения/публикации, карти със сценарии) • Химикалки и хартия или бяла дъска за бележки • Таймер или часовник за обратно броене
Полезни ресурси	• Thales - ENISA Guidelines for Identity Protection and Phishing Resistant Multi-Factor Authentication (Насоки на ENISA за защита на самоличността и многофакторно удостоверяване, устойчиво на фишинг) • Европейска комисия – Better Internet for Kids (По-добър интернет за деца) • Безплатна игра-симулатор на фишинг – Phish me if you can (Изпрати ми фишинг, ако можеш)
Подготовка	• Подгответе 4 станции с предизвикателства, с номера, указващи реда, в който трябва да бъдат решени. • Поставете по един пъзел на всяка станция. • Подредете масите така, че отборите да се редуват между станциите.

Инструкции стъпка по стъпка	**Стъпка 1 – Представяне на историята (5 мин)** На участниците се казва, че акаунтът им в приложение за социални медии е компрометиран, хакнат и променен. Те трябва да го защитят и да премахнат проблемното съдържание, преди да настъпят необратими щети. **Стъпка 2 – Станция 1: Логически пъзел с парола (15 мин)** Участниците решават логическа мрежа, за да идентифицират най-силната парола, въз основа на правила (дължина, символи, уникалност), и да защитят акаунта, за да получат достъп до следващата стъпка. **Стъпка 3 – Станция 2: Фишинг или безопасно (15 мин)** Участниците анализират съобщенията и публикациите и решават дали са безопасни, опасни или включват фишинг, за да идентифицират рискове и да блокират потенциални заплахи, преди да продължат напред. **Стъпка 4 – Станция 3: Сценарии за дигитален отпечатък (10 мин)** Картите със сценарии описват типични онлайн действия (прекомерно споделяне, дебати, вериги от имейли) и потенциални последици. Участниците трябва да съпоставят всяко действие с

	дългосрочното му въздействие, за да отключат следващия пъзел. **Стъпка 5 – Станция 4: Етични дилеми (10 мин.)** Участниците трябва да избират между опции в сложни ситуации (споделяне на данни, за да „помогнат“ на приятел, да докладват или разкрият кибертормоз, да публикуват или цензурират чувствителна тема). Всеки избор води до различни резултати, които играчите трябва да обосноват и да предприемат отговорни действия въз основа на всичко, което са научили в предишните станции. След като докажат разбирането си, те могат да получат достъп до корумпирания си акаунт и да се чувстват сигурни онлайн.
Въпроси за обсъждане	• Кои онлайн поведения са ви се стрували „нормални“ и често срещани, но всъщност са били рискови? • Как малките действия изграждат дигитален отпечатък с течение на времето? Какво е необходимо за това? Винаги ли етичните избори са били очевидни? Защо или защо не? Какви биха били техните последици? • Какво бихте променили в собствените си онлайн навици?

Оценяване и измерване на резултатите	• Наблюдение на груповите решения и качеството на размисъл и обосновки за станция 5 и обсъждане • Контролен списък за самооценка („Мога да разпозная фишинг“, „Знам как да защитя данните си“)
Вариации и адаптация	• **По-млади групи:** По-малко сценарии, повече визуални подсказки, конкретни и „черно-бели“ дилеми • **Невроразнообразни участници:** Ясни икони, намален текст, структурирани избори, допълнителни подсказки, гъвкаво време • **Напреднали групи:** Повече противоречиви дилеми без перфектен отговор, насърчаване на дебатите и нюансите
Съвети за треньори	• Избягвайте морализирането; фокусирайте се върху последствията и обективните рискове, а не върху осъждането. • Насърчавайте дискусиите и медиацията, когато участниците не са съгласни. • Поддържайте сценариите реалистични и близки до ежедневния дигитален живот на участниците. • Подчертайте, че безопасността е споделена отговорност.

Препратки и допълнителни четива	• Агенция на Европейския съюз за киберсигурност (ENISA). (2023). *Cybersecurity basics for citizens*. (Основи на киберсигурността за гражданите.) • Европейска комисия. (2025). *DigComp 3.0: European Digital Competence Framework*. (DigComp 3.0: Европейска рамка за цифрова компетентност.)

Съфинансирано от Европейския съюз

Финансирано от Европейския съюз. Изразените възгледи и мнения обаче са само на автора(ите) и не отразяват непременно тези на Европейския съюз или на Изпълнителната агенция за образование и култура (EACEA). Нито Европейският съюз, нито EACEA могат да бъдат държани отговорни за тях.

Код на проекта: 2023-2-LT02-KA220-YOU-000183156