



Identité et sécurité digitale

Scénario d'escape room pertinent & ressource de projet	• ER1 Comprendre l'IA • ER11 Exploitation en ligne et sécurité digitale • Feuille de travail d'auto-formation: Les questions éthiques dans l'entrepreneuriat numérique
Groupe cible & besoins	Tranche d'Âge: 15-25 Taille du Groupe: 3-6 participants Connaissance ou expérience requise au préalable: Utilisation journalière du téléphone et des réseaux sociaux
Durée	60–75 minutes
Zone de compétences cible	• Protéger les données personnelles et la vie privée • Comprendre l'identité et l'empreinte numérique • Prise de décision éthique et comportements numériques sûrs
Objectifs	• Identifier les règles de mots de passe forts et faibles. • Reconnaître le phishing et les comportements en ligne dangereux. • Identifier le sens et l'impact de l'empreinte numérique. • Prendre des décisions éthiques dans des dilemmes numériques réalistes. • Appliquez des stratégies de base pour la protection de la vie privée.



Matériel & équipement	• Feuilles de puzzle imprimées (grille logique de mot de passe, captures d'écran de messages/publications, cartes de scénario) • Stylos et papier ou tableau blanc pour les notes • Minuterie ou compte à rebours
Ressources utiles	• Thalès - ENISA Guidelines for Identity Protection and Phishing Resistant Multi-Factor Authentication (Lignes directrices de l'ENISA pour la protection de l'identité et l'authentification multi-acteurs résistant au phishing) • Commission Européenne – Better Internet for Kids (Meilleur internet pour les enfants) • Jeu de simulation de phishing gratuit – Phish me if you can (Phish moi si tu peux)
Mise en place	• Préparez 4 stations de défi, avec des chiffres pour indiquer l'ordre dans lequel elles doivent être effectuées. • Placez un puzzle à chaque station. • Organisez les tables pour que les équipes tournent entre les stations.
Instructions étape par étape	Etape 1 – Introduction à l'histoire (5 min) Les participants sont informés que leur compte sur une application de réseau social a été compromis, piraté et modifié. Ils doivent le sécuriser et supprimer le contenu problématique avant que des dommages irréversibles ne se produisent. Etape 2 – Station 1: Puzzle logique du mot de passe (15 min) Les participants résolvent une grille logique pour identifier le



	mot de passe le plus fort, en fonction des règles (longueur, symboles, unicité), et sécurisent le compte pour accéder à l'étape suivante. Etape 3 – Station 2: Phishing ou sécurisé (15 min) Les participants analysent les messages et les publications et décident s'ils sont sûrs, dangereux ou impliquent le phishing, afin d'identifier les risques et de bloquer les menaces potentielles pour ensuite aller de l'avant. Etape 4 – Station 3: Scénario d'empreintes numériques (10 min) Les cartes de scénario décrivent des actions en ligne typiques (partage excessif, débats, chaînes de courriels) et leurs conséquences potentielles. Les participants doivent faire correspondre chaque action à son impact à long terme pour débloquer le prochain puzzle. Etape 5 – Station 4: Dilemmes éthiques (10 min) Les participants doivent choisir entre différentes options dans des situations complexes (partager des données pour « aider » un ami, signaler ou exposer un cyberharceleur, publier ou censurer un sujet sensible). Chaque choix conduit à des résultats différents que les joueurs doivent justifier et naviguer de manière responsable en fonction de tout ce qu'ils ont appris dans les stations précédentes. Une fois qu'ils ont prouvé leur compréhension, ils peuvent accéder à leur compte corrompu et se sentir en sécurité en ligne.
Questions de débriefing	• Quels comportements en ligne semblaient « normaux » et courants mais étaient réellement risqués ?



	• Comment les petites actions construisent-elles une empreinte numérique au fil du temps ? Qu'est-ce que cela implique ? • Les choix éthiques étaient-ils toujours évidents ? Pourquoi ou pourquoi pas ? Quelles seraient leurs conséquences ? • Que changeriez-vous dans vos propres habitudes en ligne ?
Évaluation et Appréciation	• Observation des décisions de groupe et qualité de la réflexion et justifications pour la station 5 et debrief • Liste de contrôle d'auto-évaluation (« Je peux reconnaître le phishing », « Je sais comment protéger mes données »)
Variations & adaptation	• Jeunes groupes: Moins de scénarios, plus de repères visuels, des dilemmes concrets et « noir et blanc » • Participants neurodivergents: Des icônes claires, du texte réduit, des choix structurés, des indices supplémentaires, un timing flexible • Groupes avancés: Plus de dilemmes conflictuels sans réponse parfaite, encourager le débat et la nuance
Conseils du formateur	• Évitez de moraliser ; concentrez-vous sur les conséquences et les risques objectifs, pas sur le jugement. • Encourager la discussion et la médiation lorsque les participants sont en désaccord. • Gardez les scénarios réalistes et proches de la vie numérique quotidienne des participants. • Insister sur le fait que la sécurité est une responsabilité partagée.



**Références et
lectures
supplémentaires**

- European Union Agency for Cybersecurity (ENISA). (2023). [*Cybersecurity basics for citizens*](#).
- European Commission. (2025). [*DigComp 3.0: European Digital Competence Framework*](#).<https://publications.jrc.ec.europa.eu/repository/handle/JRC144121>
<https://publications.jrc.ec.europa.eu/repository/handle/JRC144121>



Cofinancé par
l'Union européenne



Financé par l'Union européenne. Les points de vue et avis exprimés n'engagent toutefois que leur(s) auteur(s) et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne sauraient en être tenues pour responsables.

Code du projet: 2023-2-LT02-KA220-YOU-000183156