

PROTÉGER LES INFORMATIONS PERSONNELLES ET FINANCIÈRES

16+

SUJET : Apprentissage numérique, éducation du consommateur

SUJET DU COURS : Comment protéger les informations personnelles et financières en ligne

DURÉE : 60 minutes

OBJECTIFS D'APPRENTISSAGE :

Objectifs principaux du cours :

Apprendre aux élèves l'importance de la protection des informations personnelles et financières en ligne, comprendre les menaces potentielles, et apprendre des stratégies efficaces pour qu'ils se protègent des fraudes en ligne et de l'usurpation de l'identité.

Compétences que les élèves vont acquérir :

- Savoir des menaces de cybersécurité importantes (i.e. hameçonnage, logiciel malveillant, violations de données).
- Capacité à reconnaître des activités, courriels, et sites web suspects.
- Sensibilisation aux pratiques en ligne sécurisées quand on partage des informations personnelles ou financières.

MATÉRIAUX/RESSOURCES NECESSAIRES :

Module 5 (<https://www.digi-civis.eu/e-learning>); un projecteur et un ordinateur pour la présentation, Internet, des exemples de courriels d'hameçonnage, faux sites web.

MÉTHODES/TECHNIQUES:

- Petits groupes de discussions
- Réflexion personnelle et auto-évaluation
- Discussion en classe et feedback
- Exercice de jeu de rôle

APERÇU DU PLAN DU COURS :

PRÉPARATION :

- Préparez les diapositives de la présentation à partir du MODULE 5 de DIGI-CIVIS.
- Sélectionnez des exemples de courriels d'hameçonnage, de sites web frauduleux, et des sites sécurisés à montrer pendant le cours.
- Créez des feuilles de travail qui guident les élèves à la création de mots de passe forts et à l'identification des tentatives d'hameçonnage.

MISE EN OEUVRE :

- Introduction aux menaces en ligne (10 minutes) : Expliquez les menaces en lignes courantes (hameçonnage, logiciel malveillant, violations de données), et pourquoi il est important de protéger ses informations personnelles et financières.
- Reconnaître des attaques d'hameçonnage (10 minutes) : Montrez des exemples de courriels d'hameçonnages et de sites web frauduleux. Discuter des signes d'alerte comme des URL suspects et des demandes urgentes d'informations.
- Meilleures pratiques pour se protéger (15 minutes) : Apprenez-leur la création de mots de passe forts, l'utilisation de la double authentification, et éviter les Wi-Fi publics pour des transactions sensibles. Démontrez comment vérifier la sécurité d'un site web (i.e. « https », icône de cadenas).
- Activité manuelle « Création de mots de passe forts » (10 minutes) : Guidez les élèves dans la création de mots de passe sécurisés, et montrez comment évaluer leur puissance.
- Discussion sur une étude de cas (10 minutes) : Revue des données réelles, montrant son impact et comment de meilleures pratiques de sécurité auraient pu empêcher cela.
- Réflexion (5 minutes) : Les élèves identifient un pas qu'ils prendront pour améliorer leur propre sécurité en ligne.

POUR EN SAVOIR PLUS :

EU OP, [Shopping online within EU](#)

[EU E-Commerce Report 2023](#)

[DMA scheme](#)

[Be safe out there](#)

ANNEXES :

[Data Protection in EU \(Video\)](#)

[Financial literacy \(video\)](#)

DEVOIRS :

Les élèves doivent réaliser un audit de sécurité de leurs propres comptes en ligne, écrire une réflexion d'une page sur ce qu'ils ont trouvé et quelles actions ils ont prises pour améliorer leur sécurité en ligne.

ÉVALUATION :

Passez en revue les devoirs des élèves pour voir leur capacité à appliquer les principes de sécurité en ligne.