



Co-funded by
the European Union



REMCREAD

Empowering Refugee & Migrant Women
through Creative Methods and Digital Literacy

MODULE 3 : Sécurité et confidentialité en ligne

PLAN DE COURS

Financé par l'Union européenne. Les points de vue et opinions exprimés sont toutefois ceux des auteurs uniquement 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 peuvent en être tenus responsables.

Projet n° 2023-1-PL01-KA220-ADU-000156610

Site web du projet <https://www.remcreadwomen.eu/>



Module 3. Sécurité et confidentialité sur le web

Introduction

Le module « Sécurité et confidentialité en ligne » a été développé sous la forme d'une ressource interactive en ligne, disponible à l'adresse suivante : [Sécurité et confidentialité en ligne](#). Ces ressources peuvent être utilisées de différentes manières : comme présentation lors d'un cours en classe, dans le cadre d'un cours en ligne ou dans un format d'apprentissage mixte, combinant travail en ligne et hors ligne.

L'objectif du module est de sensibiliser les participants à la protection des données, à l'utilisation sûre des médias sociaux et à la minimisation des risques liés à l'activité en ligne. Le matériel guide les participants étape par étape, depuis la compréhension de l'essence même de la sécurité en ligne jusqu'à la publication consciente de contenu et la réponse aux violations de la vie privée, en passant par des compétences pratiques (notamment la création de mots de passe forts, la configuration des paramètres de confidentialité, l'utilisation de l'authentification à deux facteurs).

La structure du module repose sur un plan de cours qui comprend :

- une introduction à la sécurité et à la confidentialité,
- les risques associés aux réseaux sociaux (vol de données, hameçonnage, cyberharcèlement, usurpation d'identité, addiction),
- les principes de connexion sécurisée et d'utilisation des réseaux Wi-Fi publics,
- les conséquences de la publication de données personnelles, de photos et d'informations de localisation,
- une étude de cas et des exercices en groupe,
- un résumé et des ressources et outils supplémentaires.

Les ressources en ligne comprennent des vidéos, des graphiques, des liens vers des ressources externes et des exercices décrits qui peuvent être réalisés individuellement ou en groupe. Le guide fournit également des conseils sur la manière de mener des discussions et des études de cas afin d'impliquer les participants et de les aider à transférer les connaissances acquises à leurs propres expériences en ligne.

Grâce à son format flexible, le matériel peut être présenté en version complète (environ 120 minutes) ou en version abrégée, en fonction du temps dont dispose le groupe.

L'éducateur décide des éléments à inclure, en tenant compte des besoins et du niveau de compétence des participants.



Sécurité et confidentialité en ligne

Matrice des compétences en matière de sécurité numérique pour une personne active sur les réseaux sociaux

Domaine de compétence	Connaissances	Compétences	Attitudes
Gestion des mots de passe	- Principes pour créer des mots de passe forts - Le rôle des gestionnaires de mots de passe - L'importance de la double authentification	- Création et modification de mots de passe forts - Configuration de la 2FA sur différentes plateformes - Prise en charge du gestionnaire de mots de passe	- Veiller à utiliser des mots de passe différents pour chaque compte - Faire confiance aux outils de gestion des mots de passe - Faire preuve de prudence lors du partage de mots de passe
Sensibilisation au phishing et à l'ingénierie sociale	- Types d'attaques par hameçonnage - Techniques d'ingénierie sociale utilisées par les cybercriminels	- Reconnaître les messages et les sites suspects - Signaler le phishing - Protection des informations personnelles	- Approche critique des messages reçus - Prudence dans la fourniture de données - Vigilance face à des situations inhabituelles
Sécurité des appareils	- Le rôle des mises à jour du système - Importance des antivirus et des pare-feu - Menaces liées à l'accès physique aux appareils	- Installation et configuration d'un antivirus - Mise à jour régulière des logiciels - Sécurisation des appareils	- Mise à jour régulière des logiciels - Sensibilisation aux risques liés au manque de sécurité - Responsabilité vis-à-vis de ses propres appareils
Gestion des données et de la confidentialité	- Paramètres de confidentialité sur les plateformes - Protection des données - Réglementation RODO (RGPD)	- Configuration des paramètres de confidentialité - Limitation de la visibilité des informations personnelles - Partager des informations en toute sécurité	- Respect de votre vie privée et de celle des autres - Responsabilité relative aux données traitées - Sensibilisation juridique en matière de protection des données



Utilisation sécurisée des réseaux	- Les dangers des réseaux Wi-Fi publics - Caractéristiques et avantages de l'utilisation d'un VPN	- Configuration d'un VPN - Utilisation sécurisée des réseaux Wi-Fi - Éviter les connexions Internet à risque	- Précautions à prendre lors de l'utilisation de réseaux publics - Être proactif dans la sécurisation des connexions - Sensibilisation aux menaces en ligne
Gestion des comptes et du contenu	- Outils de surveillance des comptes - Rôle des politiques de confidentialité dans les médias sociaux	- Examen et analyse réguliers de l'activité des comptes - Publication sécurisée du contenu	- Responsabilité du contenu publié - Veiller au respect des politiques de confidentialité - Surveillance proactive des activités

Module 3. Sécurité et confidentialité sur le web

Résultats d'apprentissage :

Les participants à l'atelier :

- comprennent pourquoi la confidentialité et la sécurité en ligne sont importantes ;
- sont capables de créer des mots de passe forts et d'utiliser l'authentification à deux facteurs ;
- sont capables de définir des niveaux de confidentialité appropriés sur leurs profils sociaux ;
- sont conscients des risques liés à la publication de données personnelles, de photos et de lieux ;
- savent comment utiliser les réseaux Wi-Fi publics et les appareils inconnus en toute sécurité ;
- savent comment réagir en cas d'atteinte à la confidentialité ou de piratage de compte ;
- sont capables d'évaluer quels contenus peuvent être publiés en toute sécurité sur les réseaux sociaux.

Durée : 120 minutes

Activités	Objectif	Notes méthodologiques	Matériel	Temps	Autres ressources / lien vers les ressources
1. Introduction : Pourquoi la confidentialité en ligne est-elle importante ?	Sensibilisation aux risques en ligne et à leurs conséquences.	Brève introduction par le formateur + exemples concrets .	Contenu tiré de https://sites.google.com/view/securite-et-conf-remcread-fr - L'histoire de Magda, Christopher, exemples de coachs.	15 min	https://sites.google.com/view/securite-et-conf-remcread-fr

2. Mots de passe forts et authentification à deux facteurs	Les participants apprendront à créer des mots de passe forts et comprendront l'importance de l'authentification à deux facteurs.	Démonstration étape par étape Les séquences vidéo suggérées en anglais peuvent être traduites à l'aide des paramètres de YouTube. Le matériel suggéré sous forme de pages web peut être traduit dans n'importe quelle langue à l'aide d'un traducteur dans un navigateur tel que Chrome. Pour obtenir la meilleure traduction possible, il est recommandé d'utiliser la page préparée dans le cadre du projet en anglais.	Tableau blanc/tableau à feuilles mobiles, marqueur, applications mobiles	15 min	Instructions pour créer des mots de passe forts et configurer l'authentification à deux facteurs Comment protéger vos comptes Qu'est-ce que l'authentification à deux facteurs ? Qu'est-ce que l'authentification ? Authentification à deux facteurs 2FA : sécurisez votre vie numérique Qu'est-ce qu'un gestionnaire de mots de passe En ai-je besoin ?
3. Paramètres de confidentialité du profil	Les participants vérifient et modifient eux-mêmes les paramètres de leur compte.	Travail individuel avec téléphone/ordinateur portable + assistance du formateur.	Accès à Internet, instructions YouTube	20 min	Comment configurer la confidentialité sur Instagram

4. Partage éclairé de contenu	Les participants sont capables de distinguer les contenus qu'ils peuvent publier en toute sécurité.	Discussion guidée, analyse d'exemples.	Contenu provenant de https://sites.google.com/view/safety-and-privacy-remcread-en	15 min	Confidentialité et réseaux sociaux
5. Connexion sécurisée et utilisation du Wi-Fi	Les participants connaissent les risques associés au Wi-Fi public et savent comment les éviter.	Présentation + questions au groupe	Contenu tiré de https://sites.google.com/view/safety-and-privacy-remcread-en	15 min	Les bases de la cybersécurité - Informez-vous et protégez-vous
6. Que faire en cas d'atteinte à la vie privée ?	Les participants connaissent les mesures à prendre après le piratage d'un compte.	Discussion, analyse des procédures	Description des procédures (Facebook, Instagram, Twitter X)	15 min	https://help.instagram.com/
7. Étude de cas : Maria et la sécurité des femmes réfugiées	Réflexion sur la sécurité des utilisateurs vulnérables.	Travail de groupe + présentation des conclusions	Rapport de cas de Maria https://sites.google.com/view/securite-et-conf-remcread-fr	20 min	
8. Résumé et questions	Mise en évidence des principes clés et réponse aux préoccupations.	Questions ouvertes, recueil des conclusions		5 min	