Appareils connectés

Vérifiez les paramètres de vos appareils :

Faites un NIP fort, avec des chiffres aléatoires.
Vérifiez vos paramètres de localisation : votre historique de trajets est souvent conservé automatiquement, mais on peut vider cet historique.

Utilisez un cache caméra :

La caméra d'un ordinateur peut être piratée pour filmer à votre insu, même quand vous ne l'utilisez pas. Pensez à la masquer!

Vérifiez si vos photos sont sauvegardées dans votre appareil ou dans le nuage :

Si vos photos sont en ligne, protégez-les avec un identifiant unique et un mot de passe fort. Placez vos photos intimes dans un dossier séparé et protégé par un mot de passe fort.

Utilisez un Réseau Privé Virtuel (RPV) :

En masquant votre adresse IP, le RVP (ou VPN en anglais) vous permet de garder votre emplacement secret.

Comptes en lignes

Choisissez un mot de passe robuste :

Au moins 8 caractères, des lettres majuscules, des lettres minuscules, des caractères spéciaux et des chiffres.
Si besoin, changez l'adresse courriel de connexion à vos comptes.

Vérifiez les paramètres de vos comptes en ligne :

Pensez à tous vos comptes : courriel, comptes bancaires, sites d'achat, comptes de loisirs (Netflix, Apple TV, etc.)
Vérifiez vos paramètres de localisation : par exemple, l'historique de vos emplacements est souvent conservé automatiquement, mais on peut vider cet historique.

Désactivez l'enregistrement automatique de vos informations personnelles :

La plupart des comptes en ligne sauvegardent votre adresse, vos informations de paiement et votre historique de navigation. Vérifiez ces paramètres si vous ne voulez pas les utiliser.

ENSEMBLE CONTRE l'intimidation

Avec la participation financière de :

Québec

CDEACF

WWW.CYBERINTIMIDATION.INFO

Comptes de réseaux sociaux

Choisissez un mot de passe robuste :

Au moins 8 caractères, des lettres majuscules, des lettres minuscules, des caractères spéciaux et des chiffres.
Si besoin, changez l'adresse courriel de connexion à vos comptes.

Vérifiez les paramètres de vos comptes de réseaux sociaux :

Confidentialité, localisation, géolocalisation, options de partage (public ou privé).

Désactivez la géolocalisation sur vos comptes de réseaux sociaux :

Certains réseaux sociaux proposent de vous localiser en temps réel et d'afficher votre localisation aux autres usagères et usagers. Si vous ne souhaitez pas être localisable en temps réel.

Publiez le moins d'informations personnelles ou corporatives possibles :

Gardez secrètes votre adresse courriel, votre destination de vacances, votre adresse postale, etc.

En cas d'attaque

Ces conseils ont été élaborés avec la clinique de cybercriminalité de l'UdeM.

- **Essayez de vous entourer de personnes de confiance pour ne pas vivre cette épreuve seule.**
- **Adressez-vous aux ressources d'accompagnement, d'aide psychologique ou juridique qui sont dans votre région.**
- **Bloquez les profils qui envoient des contenus agressifs, ou limitez les interactions.**
- **Signalez les personnes malveillantes et leurs agressions auprès du réseau social ou de la plateforme.**
- **Gardez une trace des agressions reçues (ex: photo, sauvegarde de la page, une capture d'écran, avec la date et l'heure de publication) :**
  Elles pourront servir de preuve en cas de dénonciation aux autorités.
- **Pour limiter l'impact des propos diffamatoires sur votre réputation :**
  Prévenez vos proches ou vos contacts professionnels si des informations jugées diffamatoires sont diffusées à votre sujet afin de les informer et d'obtenir de l'aide.
- **Gardez une trace de vos partages :**
  Conservez un historique de ce que vous avez partagé et avec qui.

ENSEMBLE CONTRE l'intimidation

Avec la participation financière de : Québec

CDEACF

WWW.CYBERINTIMIDATION.INFO