Un clic. Une publication. Vous êtes compromis?

Les réseaux sociaux permettent d'échanger et de communiquer, mais pour les militaires et la défense, ils peuvent présenter des **risques importants pour la sécurité qui sont souvent négligés.** Le partage excessif d'information peut compromettre des missions, mettre des vies en danger et des informations sensibles.

Trois menaces importantes :

1 Compromission SECOP* et ciblage malveillant

Le partage en ligne de renseignements personnels ou professionnels expose les individus et l'organisation à des acteurs malveillants:

des services de renseignements hostiles, des cybercriminels ou d'autres adversaires exploitent ces informations au moyen de tactiques d'hameçonnage, d'ingénierie sociale ou de pièges de séduction.

**Sécurité des opérations*

Ex. : Un membre de la défense met à jour son profil LinkedIn pour y inclure son **RÔLE AU SEIN D'UNE UNITÉ DE CYBERINTELLIGENCE** et mentionne qu'il détient une « **AUTORISATION DE SÉCURITÉ TRÈS SECRET** ». Un individu exploite cette information pour rédiger un courriel d'hameçonnage convaincant, se faisant passer pour un fonctionnaire afin de soutirer des informations sensibles.

CONSEIL PRATIQUE

Évitez de partager des renseignements permettant de vous identifier. Lorsque vous partagez des éléments de votre CV, faites-le de manière sélective et utilisez les paramètres de confidentialité pour restreindre la visibilité de votre profil.

2 Partage de la géolocalisation

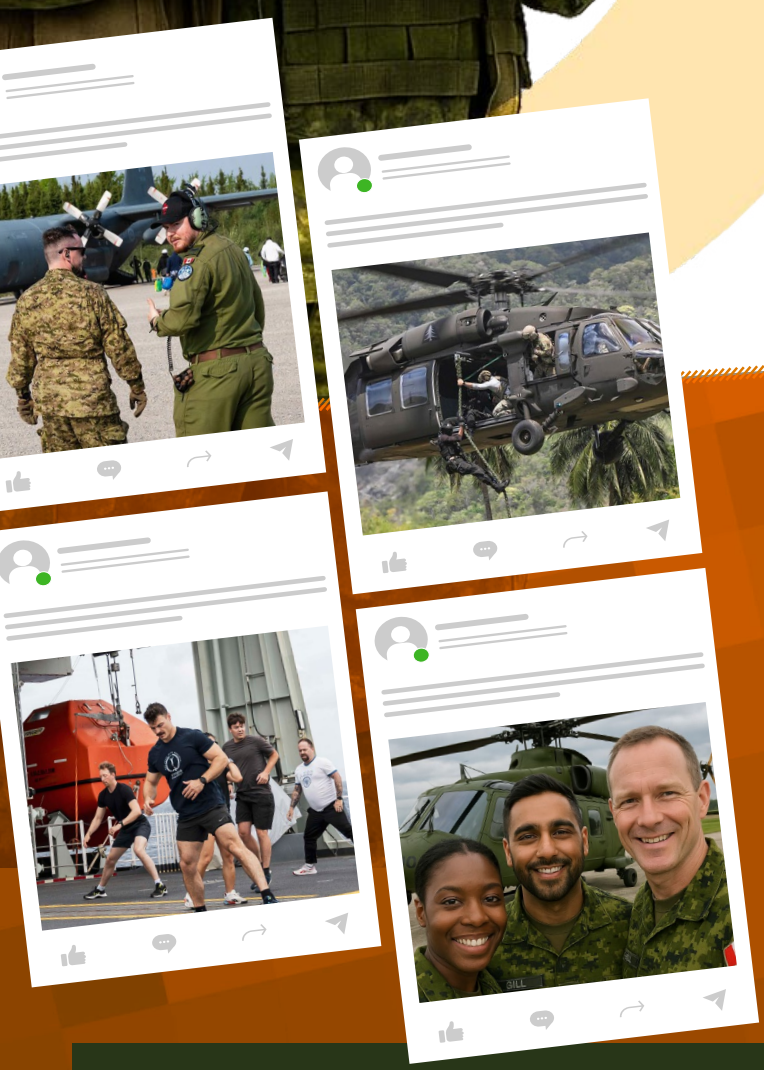
Fonctionnalités de géolocalisation :

- permettent le suivi en temps réel du personnel et des opérations
- représentent un risque accru pour les missions et le personnel en service dans les zones de conflit

Ex. : Un militaire **OUBLIE DE DÉSACTIVER LA GÉOLOCALISATION D'UNE APPLI. PENDANT UNE OPÉRATION SUR LE TERRAIN.** Cette négligence, qui peut sembler anodine, permet à l'adversaire de détecter la présence et les activités des troupes dans la zone.

CONSEIL PRATIQUE

Désactivez les services de localisation, évitez de publier des photos ou des vidéos géolocalisées et surveillez les arrière-plans susceptibles de révéler des emplacements stratégiques.



3 Métadonnées dans les photos

Les photos peuvent contenir des données sensibles cachées telles que l'heure, la date, des renseignements sur l'appareil et les coordonnées GPS, qui peuvent toutes être exploitées par des adversaires.

Ex. : Photo de groupe prise pendant une opération sans tenir compte de ce qui est visible à l'arrière-plan est partagée en ligne. Cette action semblait inoffensive, mais **ELLE A RÉVÉLÉ DE L'INFORMATION SENSIBLE ET DES MÉTADONNÉES : L'HEURE ET LE LIEU.**

CONSEIL PRATIQUE

Utilisez des outils pour supprimer les métadonnées des images et soyez attentif à votre environnement avant de les publier.

DGDSSIM-DGSDGIS @FORCES.GC.CA

- Ordonnances et directives de sécurité de la Défense nationale, Chapitre 17 : Sécurité et médias sociaux
- DOAD 6002-7, Utilisation des technologies des médias sociaux internes

2025/09