



Guide du bon usage des Médias Sociaux



Tube



Les médias sociaux font aujourd'hui partie de notre quotidien, on y échange des informations, on se renseigne, on s'y exprime...

En tant que militaire, nous les utilisons pour communiquer avec nos proches lorsque nous partons en opération. Nos familles partagent leur intérêt pour nos activités militaires ou postent des informations liées à notre vie familiale bousculée par notre départ en opération.

Nous alimentons nos pages personnelles pour retracer notre parcours à la Défense. Parce que notre métier, c'est une partie importante de notre quotidien. Et on apprécie de le partager avec notre entourage.

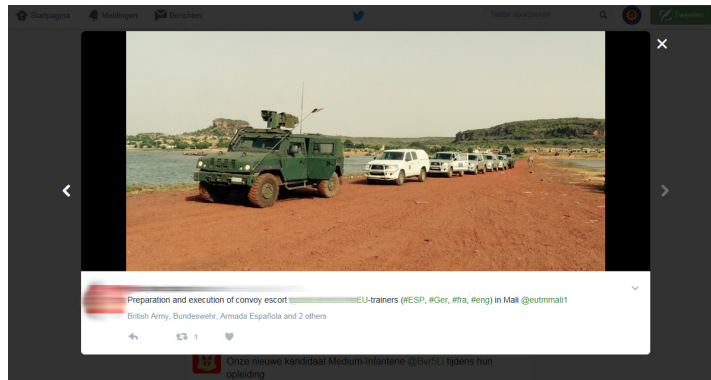
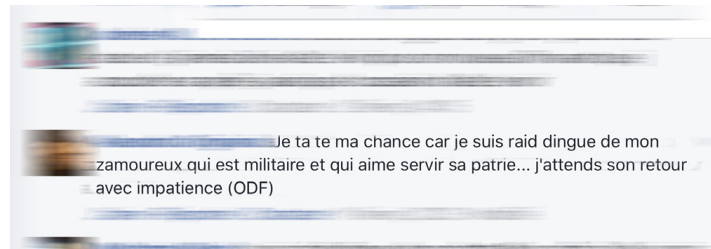
Mais tous ces comportements sont-ils entièrement sécurisés?
Quels risques encourons-nous en partageant ces informations?
Dans quelle mesure peuvent-elles être utilisées contre nous?

Exemples

Nous publions trop de contenus qui nous trahissent, notre entourage aussi: des informations sur notre mission, un incident impliquant nos capacités en opération, la préparation, le dispositif d'un convoi qui se prépare à partir...



Two belgian army armoured vehicle MPPV Dingo 2 overturns on side in Afghanistan Defense News



Généralités

Une information publiée sur internet n'est jamais anodine, ni confidentielle.

Dans les conflits modernes, nos « ennemis » scannent régulièrement le web (réseaux sociaux, blogs, forums, sites personnels...) à la recherche d'informations sensibles et aussi pour détecter les faiblesses de la Défense.

Cette collecte permanente est susceptible de vous nuire directement ainsi qu'à votre entourage et à la Défense. En tant que personnel militaire, il convient donc d'être extrêmement vigilant.

Nous reprendrons dans cette brochure 4 conseils pour éviter de divulguer des informations qui peuvent être utilisées contre vous. Il en va de la sécurité de la Défense, de votre propre sécurité mais aussi de celle de votre famille.

Conseil 1

Je maîtrise mes contenus

Je ne publie aucune information classifiée sur une opération en cours ou planifiée: dates, lieux et horaires de patrouilles, nature des missions, objectifs, règles d'engagement...

En opération, je ne publie jamais de contenu laissant visible un arrière-plan montrant un bâtiment, du matériel classifié ou tout élément sensible (badge, nominette, plan, localisation...).

Je ne fais aucun tagging nominatif de mes collègues sur des contenus à caractère militaire.

Je reste discret sur ma fonction, j'évite de trop détailler mes missions sur les réseaux sociaux.

Je garde à l'esprit que toute information publiée sur ma fonction et mes activités à la Défense peut être utilisée contre moi et/ou ma famille et mettre en péril le bon déroulement d'une opération.

Même dans ma vie privée, je reste un membre de la Défense pour la communauté.

Lors de toute publication ou commentaire je respecte les valeurs d'intégrité et de loyauté que m'impose mon statut.

J'évite toute attitude nuisible à l'image de la Défense.

Conseil 2

Je contrôle mes paramètres de confidentialité

En opération, je désactive la fonction de géolocalisation de mes applications et j'éteins le GPS de mon smartphone, s'il n'est pas nécessaire à l'opération.

Je limite l'accessibilité de mon profil à des personnes que je connais personnellement.

Je fais attention à ce qui est publié en mode public.

Je désactive le tagging automatique pour ne pas être identifié à mon insu sur des contenus.

Bien communiquer sur les médias sociaux c'est aussi en maîtriser les outils de confidentialité et éviter que des informations ne soient publiées à mon insu.

Conseil 3

J'en parle à mon entourage

Je sensibilise ma famille et mes amis aux risques encourus.

Je leur demande de respecter ces règles, notamment à propos des lieux où je suis, des dates de retour et de manœuvres...

Plus mon entourage publie en ligne du contenu sur mes activités à la Défense, plus celui-ci dévoile inconsciemment des données qui peuvent être utilisées contre moi, ma famille ou mes amis.

Conseil 4

Je pense Cybersécurité

De manière générale, je protège mon ordinateur et les appareils connectés et je ne laisse aucune porte d'entrée aux cybercriminels.

Mes mots de passe sont-ils sécurisés?
Suis-je protégé contre les virus?

Peut-on pénétrer dans le système de mon ordinateur?

Je teste la protection de mes appareils sur safeonweb.be et je suis les recommandations d'usage.

Conseils généraux

Avant publication, envisagez que vos lecteurs ne sont peut-être pas tous bienveillants. Les amis de vos amis ne sont pas forcément vos amis. En tant que personnel de la Défense, un manque de réserve quant à ses opinions, croyances religieuses, politiques ou philosophiques ou un manque de respect vis-à-vis de la Défense peut rapidement se retourner contre vous.

Faites toujours preuve de bon sens et posez-vous les bonnes questions avant de partager des informations sur les médias sociaux.

Même l'uniforme au vestiaire, je reste toujours un militaire.

Ne vous laissez pas séduire aveuglément par les nouvelles fonctionnalités (live streaming, Snapchat) et appliquez toujours les principes de précaution à ces nouvelles technologies.

De nouvelles technologies et applications arrivent régulièrement et je continue à appliquer les mêmes principes de prudence.

Il faut avoir en permanence à l'esprit que certains services offerts par les médias sociaux (mailing, VoIP...) ne garantissent pas une sécurité comparable aux services offerts par la Défense.

Il est donc fortement recommandé de ne pas les utiliser lors de contacts professionnels.

Les nouvelles technologies nous proposent des objets connectés. Dans certains domaines ils offrent une réelle plus-value. Il faut garder à l'esprit que ces technologies collectent bien plus d'informations que nous l'imaginons et que ces informations peuvent être indûment partagées via les médias sociaux.

J'applique les précautions de ma vie réelle dans ma vie numérique.

Je m'informe correctement sur les lois, les règlements et directives qui encadrent mon expression et je les respecte aussi sur les nouveaux médias.

Communication des unités



Je ne communique pas d'initiative au nom de mon unité ou de la Défense. Seul le porte-parole, le service de presse de la Défense ou des personnes mandatées y sont autorisés.

Lorsqu'une unité souhaite créer des interactions via les médias sociaux, elle doit en avertir préalablement son référent à la Communication (DELCOM) et désigner l'éditeur responsable (en principe le chef de corps).

Les contenus doivent traiter de sujets qui restent au niveau de l'unité et de ses activités. Ceux-ci doivent veiller en permanence à la bonne image et à la réputation de la Défense, en respectant les règles de sécurité liées aux opérations.

L'éditeur responsable veille au respect de l'ensemble des directives, lois, règlements concernés par une action de communication. Il doit également fournir les capacités nécessaires (L'utilisation du média est généralement gratuite, mais une telle activité nécessite également beaucoup de temps, de ressources et de personnel).

Besoin d'un conseil? La DG StratCom peut être consultée à tout moment. Dès que cela est possible l'utilisation d'une charte est très fortement conseillée.

Proposition de charte à l'attention des utilisateurs:

Cette page est la page officielle de <nom de l'institution>. Les messages et informations partagés et/ou échangés par les internautes reflètent leur opinion personnelle et non la position officielle de <nom de l'institution>. Nous attirons votre attention sur le respect de la vie privée et la réglementation relative aux droits d'auteurs.

Nous nous réservons le droit de supprimer toute intervention dont le contenu serait notamment:

- à caractère injurieux, diffamatoire, insultant ou grossier ;
- à caractère raciste, xénophobe, révisionniste, négationniste ;
- à caractère discriminatoire, en raison du sexe ou de l'orientation sexuelle, de la religion, de l'origine ethnique ;
- à caractère pornographique ou obscène ;
- à caractère publicitaire, commercial ou de parrainage à l'exception d'accords conclus entre le <nom de l'institution> et des tiers ;
- à caractère insultant envers l'institution et/ou les personnes y travaillant.

Le non-respect de ces règles peut entraîner l'exclusion de cette page.



Points de contacts

Vous constatez un incident qui peut nuire à la sécurité de la Défense ou de son personnel: contactez l'officier de sécurité de votre unité.

Vous êtes victime d'un acte malveillant (usurpation d'identité, piratage de vos données...) contactez la computer crime unit de la police fédérale à l'adresse web: <https://www.ecops.be/> et rapportez à votre officier de sécurité.

En cas de harcèlement: contactez la personne de confiance de votre unité.

Pour une information élargie: <http://infosec.mil.intra>

