Voici quelques conseils utiles destinés aux membres des réseaux sociaux:

- évaluez le contenu du ou des comptes que vous avez sur des réseaux sociaux et demandez-vous ce que vous inspire le fait que de parfaits inconnus puissent voir ce que vous y publiez;
- ne publiez pas de données privées, comme votre numéro de téléphone mobile, l'adresse de votre domicile, votre emploi du temps professionnel ou personnel etc., si vous ne voulez pas que n'importe qui puisse les utiliser pour vous trouver ou vous localiser, à tout moment du jour ou de la nuit;
- ne publiez rien qui soit susceptible de vous mettre dans l'embarras ou de nuire à l'image du SGC en tant qu'institution;
- utilisez les paramètres de confidentialité de votre compte de réseau social (il vous est possible d'ajuster ces paramètres pour contrôler qui peut avoir accès à vos données personnelles).

Enfin, vous pouvez toujours rechercher votre nom sur Google afin de voir de quelle manière on utilise votre nom ou votre identité. Si vous avez l'impression d'être la victime d'une usurpation d'identité, contactez immédiatement la police.

Pour en savoir plus sur les dangers des réseaux de socialisation en ligne, consultez le bulletin d'information de janvier 2012 consacré à la sensibilisation aux questions de sécurité (n° 4), disponible sur le site internet consacré à la sensibilisation aux questions de sécurité ("Security Awareness") sur Domus.

Vous pouvez également consulter la communication au personnel n° 88/11 "Principes généraux pour l'utilisation des "médias sociaux» par le personnel du SGC".

Graphisme et impression: DGA 3 - Services techniques de production - RS 079/2012 - Photos: Fotolia

Pour de plus amples questions ou commentaires, n'hésitez pas à contacter la Cellule de sensibilisation aux questions de sécurité à l'adresse suivante:

security.awareness@consilium.europa.eu

CONSILIUM

SURFER L'ESPRIT TRANQUILLE SUR LES RESEAUX SOCIAUX

Vous n'avez pas que des amis! Les sept erreurs fatales à ne pas commettre sur les réseaux sociaux

SECURITE SGC
SENSIBILISATION

Beaucoup d'internautes mentent sur leur identité!

N'OUBLIEZ PAS

Tout renseignement vous concernant peut être utilisé contre vous

Vous devez savoir que les réseaux sociaux sont surveillés par des harceleurs, des réseaux criminels ou des services de sécurité.

Comme il est impossible d'écarter toutes les menaces qui compromettent la sécurité des réseaux sociaux, soyez attentifs aux sept erreurs fatales à ne pas commettre. La cellule de sensibilisation à la sécurité a produit ce dépliant afin de vous aider à réduire sensiblement les risques qui pèsent tant sur votre vie privée que sur le SGC.

1 Mélanger vie privée et vie professionnelle

Cette erreur est étroitement liée à la première mais va au-delà de la simple divulgation de données du SGC. C'est le cas lorsqu'on utilise un réseau social à des fins tant professionnelles que de loisirs, le plus souvent sur Facebook, où notre cercle d'"amis" comprend des collègues, des membres de notre famille et des connaissances. Le problème, c'est que le langage que vous utilisez et les images que vous partagez avec vos amis et votre famille peuvent être tout à fait inappropriés sur le plan professionnel. N'oubliez pas que votre comportement en ligne peut nuire non seulement à votre propre image mais aussi à la réputation d'autrui.

2 Partager des informations liées au travail

En vous montrant trop bavard sur les réseaux sociaux à propos des travaux du SGC, vous risquez de dévoiler par inadvertance des informations sensibles sur le SGC, son personnel et son fonctionnement.
En outre, comme le montrent certains exemples concrets, des pirates informatiques (animés d'intentions criminelles ou travaillant pour des services de renseignements de pays tiers) pourraient utiliser des données obtenues sur vos sites de socialisation en ligne afin de programmer, à l'aide d'un réseau de machines zombies, des attaques contre le système de défense du SGC et en exploiter les failles pour accéder à des données ou à des informations sensibles.

3 Se défouler sur Twitter (ou Facebook/LinkedIn/Myspace)

Quand on se sent frustré au travail, à la suite d'un désaccord avec son supérieur hiérarchique par exemple, il peut s'avérer difficile de résister à l'envie de "se défouler" sur les réseaux sociaux. La colère est mauvaise conseillère.
Avant de laisser libre cours à votre fureur sur la toile, prenez garde à ce que vous allez dire et n'oubliez pas que vos lecteurs pourraient être bien plus nombreux que vous ne le pensiez de prime abord. Par conséquent, réfléchissez-y à deux fois avant de cliquer sur "publier", car votre diatribe pourrait rester dans le domaine public pendant des années.

4 Vouloir compter le plus grand nombre d'amis

Certains membres des réseaux sociaux ne pensent qu'à compter le plus grand nombre d'amis possible. Ce petit jeu peut sembler inoffensif ou, au pire, simplement agaçant. Mais lorsque la quantité prime la qualité, on peut facilement être amené à accepter dans son cercle d'"amis" un escroc, un usurpateur d'identité ou un agent de renseignements étranger.
Il est toujours conseillé de vous renseigner sur la personne qui cherche à entrer en contact avec vous. La connaissez-vous? Si ce n'est pas le cas, quel est son but? Vérifiez si le profil de cette personne est sécurisé. Si vous ne parvenez pas à trouver une liste de ses amis sur la toile, réfléchissez-y à deux fois avant d'accepter d'entrer en contact avec elle.

5 Opter pour la facilité lors du choix de son mot de passe

Une autre erreur fréquente est d'opter pour la facilité en choisissant pour vos réseaux sociaux des mots de passe que vous retiendrez le plus facilement. C'est le cas, par exemple, lorsque vous utilisez sur LinkedIn et Facebook le même mot de passe que celui que vous avez choisi pour votre compte bancaire en ligne ou votre ordinateur. Si une personne malintentionnée parvient à se procurer le mot de passe de votre réseau social, elle aura accès à tous vos autres comptes.
Utiliser le même mot de passe sur plusieurs sites revient à s'appuyer sur le maillon le plus faible d'une chaîne en pensant qu'il sera capable de supporter le même poids que les autres.

6 Avoir le clic facile (cliquer sur tout, en particulier sur Facebook)

Sur Facebook en particulier, les boîtes de messagerie débordent souvent de toutes sortes de demandes, qu'il s'agisse d'invitations à prendre un verre ou à soutenir une noble cause. Certains membres des réseaux sociaux n'hésitent pas une seconde avant de cliquer sur ces demandes. Malheureusement, les personnes malintentionnées le savent et vous enverront des liens qui semblent provenir d'amis légitimes. En cliquant sur ces liens, vous installerez un logiciel malveillant sur votre ordinateur.

7 Vous mettre vous-même ou les autres en danger

Tout ce qui a été dit ci-dessus nous amène à la septième erreur, sans doute la plus grave de toutes: en utilisant les réseaux de socialisation en ligne de manière inconsidérée, vous risquez de mettre des vies en danger. La vie d'un proche ou d'un collègue. Ou la vôtre.

L'objectif de cette brochure n'est pas de vous faire peur, mais de vous inciter à rester vigilant et prudent lorsque vous utilisez les réseaux sociaux