Conseils de sécurité en matière de réseautage social

Le réseautage social est populaire, mais il comporte des risques liés à la sécurité pour vous et pour le Ministère étant donné la nature même des sites de réseautage social. Veuillez lire les conseils de sécurité qui suivent afin de vous assurer que, lorsque vous accédez à Internet, vous n'exposez pas le Ministère, vos contacts ou vous-même à des risques.

Qu'est-ce que le réseautage social?

Le réseautage social en ligne est le prolongement du réseautage social traditionnel, à cette différence qu'il s'effectue sur Internet. Dans les sites réservés exclusivement aux contacts sociaux, vous pouvez nouer des liens d'amitié ou établir des relations amoureuses. Dans les sites réservés aux affaires et à des intérêts spéciaux, vous pouvez établir des contacts d'affaires et obtenir de l'information. Dans votre propre blogue ou site Web, vous pouvez mettre d'autres internautes au courant de vos travaux et de vos activités personnelles.

Les sites de réseautage social vous encouragent à fournir énormément de renseignements sur vous-même et offrent certains moyens de communication (par exemple, les salons de clavardage et la messagerie instantanée), lesquels vous permettent d'entrer en contact avec d'autres internautes. Dans certains sites, vous pouvez naviguer à la recherche de personnes, alors que dans d'autres, vous devez être « présenté » à des gens par l'entremise d'une connaissance commune.

Pourquoi divulguer autant de renseignements?

Lorsque vous dévoilez des renseignements en ligne, qu'il s'agisse d'une promotion ou de votre calendrier de déplacements pour affaires, il se peut que vous fournissiez plus de détails que si vous vous adressiez à quelqu'un de vive voix. En outre, vous n'avez sans doute pas envisagé la possibilité que l'information soit utilisée à des fins non légitimes, ou encore l'incidence de toute utilisation à des fins non légitimes pour vous, les autres ou le Ministère. Voici d'autres raisons pour lesquelles nous avons tendance à divulguer beaucoup de renseignements en ligne :

- Internet donne aux gens un sentiment d'anonymat.
- L'absence d'interaction physique avec les autres donne un faux sentiment de sécurité.
- Nous diffusons de l'information à l'intention des amis ou de la famille, en oubliant que d'autres pourraient en prendre connaissance – même des criminels ou des employeurs éventuels.
- Nous voulons impressionner des amis ou des associés éventuels en fournissant des renseignements sur nous-mêmes ou en mentionnant le nom de nos connaissances, et nous oublions que nous dévoilons trop de renseignements qui pourraient être utilisés par d'autres internautes.

- Nous ne tenons pas compte des répercussions, sur le plan juridique ou de la sécurité, liées à la diffusion d'information sur nous-mêmes, les autres ou le Ministère (dans l'immédiat ou dans l'avenir).
- Nous oublions que l'information est permanente et que nous ne pouvons jamais l'éliminer complètement du domaine public.

Quelles sont les répercussions sur le plan de la sécurité?

La plupart des internautes qui accèdent à ces sites ne constituent pas une menace. Cependant, les internautes malveillants sont attirés par les sites de réseautage social en raison de la grande quantité de renseignements personnels de nature délicate et de la facilité d'accès à l'information propre aux utilisateurs.

Les internautes peuvent recueillir de l'information à la pièce et lancer une attaque d'ingénierie sociale. Autrement dit, ils peuvent usurper votre identité ou faire du tort au Ministère ou à quelqu'un au sein du Ministère. Il est vrai qu'il est normalement impossible de se livrer à des pratiques malveillantes lorsqu'on dispose uniquement du nom de quelqu'un. Cependant, si un internaute connaît votre nom, votre adresse, un numéro de téléphone cellulaire et votre date de naissance, il peut être en mesure de convaincre quelqu'un qu'il a le droit d'accéder à vos données personnelles ou financières. Si vous ajoutez votre numéro d'assurance sociale à cette liste, cette personne pourrait être en mesure d'ouvrir un compte bancaire ou de faire une demande de carte de crédit en votre nom.

Si vous photographiez quelqu'un au travail dans un lieu secret ou dans un secteur à accès restreint, et que vous diffusez cette photo sur Internet, vous pourriez divulguer des renseignements qui ne sont pas considérés du « domaine publique » à propos de cette personne ou de cet emplacement. N'oubliez pas que plus un utilisateur malveillant dispose de renseignements sur vous, votre travail, vos contacts, ou le Ministère, plus il est facile pour celui-ci de profiter de vous, de quelque chose que vous possédez ou connaissez, ou encore de quelqu'un que vous connaissez. On a fait état de personnes mobilisées pour surveiller des sites de réseautage social afin de recueillir de l'information servant à des attaques terroristes soupçonnées. Les sites faisant l'objet de surveillance renfermaient des photos de gens, de lieux et d'armes. Bon nombre de militaires et d'employés des Services extérieurs ont reçu l'ordre de retirer ces informations du réseau Internet.

Sept conseils en matière de sécurité :

1. **Limitez l'information personnelle que vous diffusez** – Ne diffusez pas d'information concernant votre lieu de travail ou votre calendrier de projets. Encouragez vos collègues et amis à ne pas diffuser d'information sur vous. Ne publiez pas de photographies ou de contenu vidéo de votre lieu de travail.
2. **N'oubliez pas qu'Internet est une ressource publique** – Diffusez uniquement l'information que vous êtes à l'aise de partager ou que vous êtes autorisé à communiquer en fonction de votre cote de sécurité. Ne l'oubliez jamais lorsque vous créez votre profil dans les blogues ou les forums. Des gens que vous n'avez jamais rencontrés peuvent accéder à votre page Web. Lorsque vous tenez un journal en ligne ou un blogue, ne le rédigez pas de la même façon qu'un journal personnel; attendez-vous à ce n'importe qui puisse en lire le contenu.

3. **Méfiez-vous des étrangers** – Internet facilite la tâche des gens qui cherchent à se présenter sous un faux jour face aux autres, qu'il s'agisse de leur identité ou de leurs motifs. Envisagez la possibilité de restreindre le nombre de personnes qui sont autorisées à vous contacter sur ces sites. Si vous communiquez avec des étrangers, faites preuve de vigilance lorsqu'il s'agit de divulguer de l'information.
4. **Soyez sceptique** – Ne croyez pas tout ce que vous lisez en ligne. Les gens peuvent publier des informations fausses ou trompeuses sur différents sujets, y compris leur propre identité. En outre, méfiez-vous des dispositifs de sécurité des sites de réseautage social. Les cas d'atteinte à la sécurité sont rarement rendus publics. Peu importe le niveau de sécurité apparent des sites, il est possible d'en exploiter les failles.
5. **Vérification des politiques sur la protection des renseignements personnels** – Certains sites partagent de l'information avec d'autres entreprises, notamment les adresses de courriel, ce qui peut entraîner une augmentation du pourriel (spam). Prenez soin de lire la politique sur la protection des renseignements personnels des sites que vous visitez afin d'éviter de faire en sorte que vos collègues et amis ne soient la cible de pourriel.
6. **Faites preuve de vigilance lorsque vous diffusez de l'information** – De plus en plus de renseignements personnels sont disponibles en ligne. Peu importe ce que vous décidez de révéler, vous devez prendre conscience que vous en faites la diffusion à l'échelle mondiale. Lorsque vous fournissez des détails sur vous-même ou sur les autres, ou que vous diffusez des images ou du contenu vidéo, vous donnez peut-être à des pirates suffisamment d'informations pour leur permettre de lancer une attaque d'ingénierie sociale.
7. **Sachez que vous ne pouvez pas reprendre l'information diffusée** – N'oubliez pas que lorsque vous diffusez de l'information en ligne, vous ne pouvez pas la reprendre. Même si vous l'éliminez du site, l'information diffusée peut avoir été enregistrée ou conservée dans la mémoire cache d'un ordinateur quelque part. **PENSEZ** avant de diffuser de l'information sur Internet! Demandez-vous quelle est la valeur de cette information aujourd'hui et tenez compte du fait que toute information diffusée maintenant pourrait être du domaine public pour toujours!