Votre sûreté et sécurité en ligne: conseils de sécurité

Le Bureau des Affaires éducatives et culturelles du Département d'État des États-Unis prend très au sérieux votre sûreté et votre sécurité en ligne. Quand vous utilisez les réseaux sociaux, le courriel, ou Internet, rappelez-vous les **conseils de sécurité** suivants **:**

1. Ne diffusez jamais de coordonnées privées. Ne listez jamais votre adresse courriel ou votre numéro de téléphone dans un espace public, comme votre page de profil, un blog, des forums, ou une légende de photo.

2. Si vous faites partie d'un réseau social, faites très attention à vos limites de renseignements personnels, qui vous permettent de décider combien d'information personnelle vous souhaitez révéler, et à qui.

3. Faites très attention à ce que vous publiez sur un réseau social. Avant d'afficher des photos, des vidéos, ou un texte, demandez-vous si vous seriez embarrassé que votre famille ou votre employeur le voient.

4. Avant d'ajouter un widget (une application qui peut être partagée électroniquement avec d'autres) à votre profil, demandez-vous si vous voulez que les créateurs de ce widget puissent accéder à votre profil et aux informations sur votre activité sur le réseau social. Rappelez-vous que ce réseau n'a généralement pas de contrôle sur ces widgets, et restez donc prudents pour les utiliser.

5. Signalez tout abus des conditions d'utilisation d'un site Internet aux administrateurs du site. Tout site Internet or réseau social sérieux disposera d'un moyen vous permettant de le faire.

6. Le courriel peut servir pour diffuser un logiciel malveillant ou obtenir des renseignements personnels pour commettre une fraude. Afin de vous protéger, ainsi que les ordinateurs dont vous vous servez, respectez les recommandations suivantes:

- Méfiez-vous des courriels ou appels téléphoniques non sollicités qui vous demandent des renseignements personnels. Si un ou une inconnu(e) affirme appartenir à une organisation légitime, essayez de vérifier directement son identité auprès de cette organisation.

- Ne communiquez jamais d'information personnelle ou financière (numéro de carte de crédit, numéros d'identification personnels (PIN) et autres numéros d'identification) en réponse à des courriels ou des appels téléphoniques que vous n'avez pas demandés.

- N'envoyez aucune information personnelle ou financière par Internet avant de vérifier la sécurité du site Internet. (les adresses Internet sûres commencent par "https://")

- Faites attention à l'adresse d'un site Internet, située en haut de l'écran. Les sites internet malveillants peuvent paraître identiques à un site légitime, mais l'adresse peut comporter une variation dans l'orthographe ou un domaine différent (par ex., ".com" vs. ".net").

- Protégez votre ordinateur et ceux que vous utilisez en scannant contre les virus tous les supports d'information amovibles, comme les clés USB, les CD, ou les DVD, avant d'ouvrir les fichiers qu'ils contiennent et en scannant tous les fichiers joints que vous recevez par courriel avant de les ouvrir.

- N'acceptez et n'ouvrez aucun fichier exécutable (indiqué par un nom de fichier finissant en ".exe") que vous recevez par courriel. Ce type de fichier peut être dangereux.