ARRÊTEZ | RÉFLÉCHISSEZ | BRANCHEZ-VOUS®

CONSEILS ET ASTUCES

Conservez votre ordinateur propre et à jour

- Actualisez votre logiciel de sécurité: l'utilisation des toutes dernières versions du logiciel de sécurité, dunavigateur Web et du système d'exploitation constitue la meilleure défense contre les virus, les logiciels malveillants et autres menaces en ligne.

- Automatisez les mises à jour des logiciels: de nombreux logiciels se connectent et installent automatiquement leur mise à jour pour se protéger contre les risques connus. Activez les mises à jour automatiques si vous disposez de cette option.

- Protégez tous les périphériques connectés à Internet. Les ordinateurs, les téléphones intelligents, les consoles de jeux et autres périphériques activés sur le Web doivent également être protégés contre les virus et les logiciels malveillants.

- Clé et lecteur: les périphériques USB et les autres types de périphériques externes peuvent être contaminés par des virus ou logiciels malveillants. Utilisez votre logiciel de sécurité pour les analyser.

Protégez vos informations personnelles

- Sécurisez vos comptes: exigez une protection au-delà des mots de passe. De nombreux fournisseurs de comptes proposent désormais plusieurs méthodes de vérification de votre identité avant la poursuite de toute activité sur le site concerné.

- Créez des mots de passe complexes et forts: la combinaison de lettres majuscules et minuscules avec des chiffres et des symboles renforce la sécurité de vos mots de passe.

- Un mot de passe unique pour chaque compte: un mot de passe distinct et propre à chaque compte permet de contrecarrer la criminalité en ligne.

- Écrivez votre mot de passe et conservez-le en lieu sûr: il est facile d'oublier un mot de passe. Conservez la liste de vos mots de passe dans un lieu sûr et éloigné de l'ordinateur.

- Soyez maître de votre présence en ligne: lorsque ces options sont proposées, réglez les paramètres de confidentialité et de sécurité sur les sites Web en fonction du niveau de confort souhaité pour le partage d'informations. Choisissez avec qui vous souhaitez partager vos informations.

Created by the National Cyber Security Alliance

CONSEILS ET ASTUCES

ARRÊTEZ | RÉFLÉCHISSEZ | BRANCHEZ-VOUS®

Soyez prudent lorsque vous êtes en ligne

- En cas de doute, supprimez le message reçu: les cybercriminels attaquent votre ordinateur par l'intermédiaire de liens dans des courriels, en utilisant Twitter, des billets de blog ou de la publicité en ligne. Lorsqu'une information vous paraît suspecte, et même si vous en connaissez la provenance, il est recommandé de la supprimer ou, le cas échéant, de la marquer comme courrier indésirable.

- Méfiez-vous des points d'accès Wi-Fi: limitez le type d'activités effectué et réglez les paramètres de sécurité sur votre périphérique afin de restreindre l'accès à votre ordinateur.

- Protégez vos finances: lorsque vous effectuez des opérations bancaires ou des achats, vérifiez que les sites sont sécurisés. Recherchez les adresses Web commençant par "https://" ou "shttp://", ce qui signifie que le site a pris des mesures de sécurité supplémentaires pour protéger vos informations. "Http://" n'est pas une adresse sécurisée.

Soyez attentif sur le Web

- Soyez à jour. Restez au fait des nouvelles méthodes de sécurité en ligne. Consultez les sites Web approuvés pour obtenir leurs toutes dernières informations, puis partagez vos découvertes avec vos amis, votre famille et vos collègues, en les encourageant à être prudents sur le Web.

- Réfléchissez avant d'agir: méfiez-vous des communications qui exigent de vous une action immédiate, proposent des produits trop beaux pour être vrais, ou sollicitent vos informations personnelles.

- Effectuez des sauvegardes: protégez votre travail, votre musique, vos photos et toute autre information numérique, en créant une copie électronique que vous conserverez en lieu sûr.

Soyez un bon internaute

- Plus de sécurité pour vous et donc pour les autres: ce que vous faites en ligne a un impact sur tous, à la maison, au bureau et partout dans le monde. La pratique de bonnes habitudes en ligne avantage la communauté numérique dans son ensemble.

- Ne publiez pas d'informations sur les autres s'ils n'en publient pas sur vous.

- Aidez les autorités à lutter contre la criminalité en ligne: signalez un vol financier ou d'identité, ou toute autre forme de criminalité cybernétique à la police.

Adoptez l'approche Arrêtez. Réfléchissez. Branchez-vous. et encouragez les autres à la suivre.

Created by the National Cyber Security Alliance