Astuces et conseils

Adoptez de bonnes habitudes de sécurité en ligne grâce à ces astuces et conseils. Cette partie a été élaborée en collaboration avec Get Safe Online (UK) et le ministère américain de la sécurité intérieure.

- Protégez votre ordinateur personnel (PC) et vos appareils portables
- Protégez vos informations personnelles et vos données d'identification
- Protégez vos informations professionnelles en dehors de votre entreprise
- Connectez-vous avec précaution
- Adoptez une attitude avisée en ligne

Protégez votre ordinateur personnel (PC) et vos appareils portables

PC

- Utilisez un pare-feu: les pare-feu protègent votre réseau contre les virus et les pirates informatiques.
- Installez un logiciel anti-virus: les logiciels anti-virus empêchent les infections virales de se propager dans votre ordinateur.
- Installez les dernières mises à jour de sécurité: assurez-vous que vos applications et votre système d'exploitation sont adaptés, sains et à jour.
- Arrêtez les logiciels espions: évitez d'ouvrir des courriels et des pièces jointes suspects afin d'empêcher des étrangers de s'introduire dans votre ordinateur.
- Effectuez régulièrement des sauvegardes: protégez vos données contre tout problème.

Ordinateurs portables

- Éteignez les connections sans fil lorsque vous ne les utilisez pas ou n'en avez pas besoin.
- Connectez régulièrement votre ordinateur portable à un réseau sécurisé afin de mettre à jour les mécanismes de sécurité.
- Faites une copie des informations stockées sur votre ordinateur portable
- Ne laissez pas votre ordinateur portable sans surveillance.

Clés USB

- Utilisez une clé USB cryptée.
- Mettez votre clé USB en mode «lecture seule» en utilisant le petit interrupteur réservé à cet effet; cela permettra d'éviter la transmission de virus. Certaines clés USB comprennent une commande qui permet un fonctionnement en mode «lecture seule»: ainsi, l'ordinateur hôte ne pourra écrire ou modifier les données présentes sur la clé.

- Contrôlez votre clé USB après avoir copié des fichiers à partir d'un ordinateur non sécurisé et/ou non autorisé pour éviter toute transmission de virus.
- Avant d'insérer votre clé USB dans l'ordinateur d'une autre personne, effacez tous les fichiers dont vous n'avez pas besoin dans le cadre de cette action.
- Faites une copie de sauvegarde des données stockées sur votre clé USB afin de les récupérer en cas de problème.
- Attachez votre clé USB à un porte-clés ou à un cordon afin d'éviter de la perdre: en effet, du fait de leur taille réduite, les clés USB se perdent ou se volent facilement. En outre, plus la capacité de stockage est élevée, plus le nombre de données risquant de faire l'objet d'un accès non autorisé est important. Une clé USB est généralement placée dans un sac, un sac à dos, une mallette d'ordinateur portable, une veste, la poche d'un pantalon, ou laissée sans surveillance sur le bureau. Le nombre de clés USB perdues, égarées, empruntées sans permission ou volées a récemment augmenté.

Téléphones portables et ordinateurs de poche

Les ordinateurs de poche, tels que les appareils de type Windows Mobile, Palm, iPhone, Android et Blackberry, donnent accès à des liens internet et sont capables de stocker de grandes quantités de données. Leur portabilité impose de les manipuler avec une très grande précaution.

- Éteignez les connections sans fil (c'est-à-dire Bluetooth et WLAN) lorsque vous ne les utilisez pas. La technologie Bluetooth permet à des dispositifs électroniques de communiquer entre eux via une connexion radio à basse fréquence.
- Ne laissez pas votre téléphone portable ou votre ordinateur de poche sans surveillance, cela pourrait conduire à une perte de données.
- Utilisez la fonction mot de passe afin d'empêcher le piratage à distance de votre téléphone intelligent.

Protégez vos informations personnelles et vos données d'identification

- **Utilisez un mot de passe sûr**: votre mot de passe est l'équivalent, sur l'internet, de la serrure et de la clé de votre maison. Les mots de passe constituent l'un des principaux moyens de défense; acquérir de bons réflexes dans ce domaine vous aidera à mieux protéger vos informations personnelles sensibles et vos données d'identification. Le mot de passe de votre ordinateur est la clé qui permet d'accéder à toutes les informations — professionnelles et personnelles — que vous avez stockées sur votre ordinateur et sur vos comptes en ligne. Utilisez un mot de passe sûr pour protéger vos données: il doit comporter un ensemble complexe de caractères et associer des lettres (majuscules et minuscules), des chiffres et des symboles. Plus votre mot de passe contient de caractères différents, plus il est difficile à deviner. N'utilisez pas d'informations personnelles, telles que votre nom, celui de vos enfants, des dates d'anniversaires, etc., que quelqu'un pourrait connaître ou obtenir

facilement, et essayez d'éviter les mots communs: certains pirates informatiques utilisent des programmes qui testent chaque mot du dictionnaire.

- **Modifiez votre mot de passe régulièrement**: si vous pensez que votre système a été atteint, modifiez immédiatement vos mots de passe.
- **Gardez votre mot de passe secret**: votre mot de passe est unique et ne doit être divulgué à personne. Lorsque cela est possible, essayez de mettre en place une stratégie vous permettant de mémoriser vos différents mots de passe. Si vous écrivez vos mots de passe quelque part, soyez prudent quant au lieu où vous stockez cette information. Ne laissez aucune trace écrite là où vous ne laisseriez pas les informations que vos mots de passe sont censés protéger.
- **Compte unique, mot de passe unique**: utilisez un mot de passe différent pour chaque compte en ligne auquel vous avez accès (ou au moins plusieurs mots de passe). Si vous utilisez le même mot de passe pour plusieurs comptes, un «agresseur» ayant réussi à accéder à l'un de vos comptes pourra faire de même pour tous les autres.
- **Sécurisez vos comptes**: de nombreux fournisseurs de comptes proposent d'autres solutions pour vérifier votre identité avant de vous autoriser à effectuer des opérations sur leur site.
- **Gérez votre présence en ligne**: lorsque cela est possible, définissez les paramètres de confidentialité et de sécurité sur les sites internet en fonction du niveau de partage d'informations qui vous convient. Il est préférable de limiter le nombre de personnes avec lesquelles vous partagez des informations.
- **Utilisez les réseaux sociaux avec prudence**: n'oubliez pas que les réseaux sociaux peuvent rassembler bon nombre des risques associés à la navigation en ligne: intimidation en ligne, divulgation de données privées, harcèlement électronique, accès des contenus ne convenant pas aux mineurs et, au niveau le plus extrême, manipulation psychologique en ligne et pédopornographie.

Protégez vos informations professionnelles en dehors de votre entreprise

- **Assurez-vous que les données sensibles sont en sécurité**: lorsque vous êtes en dehors de votre entreprise, assurez-vous à tout moment que vos informations sensibles et votre équipement sont en sécurité afin de prévenir un vol ou une perte. Lorsque vous vous trouvez dans des lieux publics en particulier, manipulez les informations avec précaution.
- **Ne divulguez pas d'informations professionnelles**: n'oubliez pas qu'une personne peut surprendre votre conversation. Ne portez pas les informations confidentielles de votre entreprise sur la place publique.
- **Méfiez-vous du «shoulder surfing» (espionnage par-dessus l'épaule)**: lorsque vous voyagez ou que vous travaillez à distance, méfiez-vous des personnes indiscrètes (qui suivent vos conversations par-dessus votre épaule).
- **Utilisez les services de courrier électronique de manière avertie**: lorsque vous utilisez un navigateur internet pour consulter vos courriers électroniques, veillez à être aussi prudent qu'avec une messagerie électronique de bureau. De plus, ce système comporte ses propres risques en matière de sécurité.

Connectez-vous avec précaution

- **Éteignez les connections sans fil lorsque vous ne les utilisez pas ou n'en avez pas besoin.**
- **Utilisez les bornes wifi avec bon sens**: lorsque vous utilisez des bornes wifi, limitez les opérations que vous effectuez et adaptez les paramètres de sécurité sur votre appareil afin de limiter l'accès à votre machine.
- **Protégez votre argent**: lorsque vous effectuez des opérations bancaires et des achats en ligne, assurez-vous que les sites sont sécurisés. Cherchez les adresses internet comportant le protocole «https://» ou «shttp://», ce qui signifie que le site prend des mesures supplémentaires afin de sécuriser vos données. Le protocole «http://» n'est pas sécurisé.
- **Stoppez les courriers indésirables**: les courriers indésirables constituent une menace pour la sécurité. N'ouvrez pas les courriels et les pièces jointes provenant d'expéditeurs inconnus.
- **En cas de doute, supprimez-les**: lorsque des liens dans des courriels, des messages, des tweets, ainsi que des publicités en ligne, semblent suspects, même si vous en connaissez la source, il est préférable de les supprimer ou, le cas échéant, de les marquer comme courrier indésirable.
- **Transférez le courriel si nécessaire.** Pensez à supprimer l'historique du message au préalable.
- **Naviguez sur l'internet avec prudence.**
- **Ne téléchargez aucun document ou matériel provenant de sources non fiables.**
- **Utilisez les ordinateurs publics avec précaution**: ne vous connectez à un ordinateur public que lorsque vous disposez d'une connexion cryptée (identifiée par un cadenas en bas à droite de la fenêtre de votre navigateur et par les lettres «https://» au début de l'adresse internet).
- **Utilisez les services de courrier électronique de sociétés fiables et réputées.**

Adoptez une attitude avisée en ligne

- **Tenez-vous au courant**: restez au fait des nouvelles manières de naviguer en ligne en toute sécurité: vérifiez les sites internet fiables pour obtenir les toutes dernières informations, partagez-les avec votre famille, vos amis et vos collègues, et encouragez-les à adopter une attitude avisée en ligne. Sécurisez votre navigateur.
- **Réfléchissez avant d'agir**: soyez prudent en ce qui concerne les communications qui vous proposent d'agir immédiatement, qui offrent quelque chose qui semble trop beau pour être vrai, ou qui vous demandent des informations personnelles.
- **Effectuez des sauvegardes**: protégez votre travail, votre musique, vos photos et autres données numériques en en faisant une copie électronique et en les stockant dans un endroit sûr.