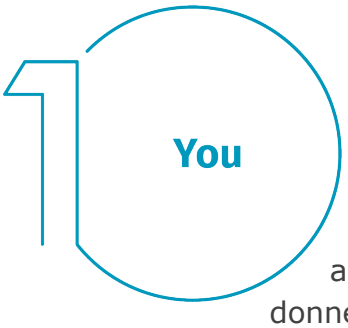
Les 5 principales étapes pour travailler en toute sécurité à domicile

Nous savons qu'il est peut-être nouveau pour vous de travailler de la maison, voire même accablant de s'ajuster à ce nouvel environnement. Un de nos objectifs est de vous permettre de travailler de façon aussi sécuritaire que possible à partir de la maison. Ci-dessous sont données cinq étapes simples pour travailler de façon sécuritaire. La bonne nouvelle est que toutes ces étapes aideront non seulement à rendre votre travail sécuritaire, mais elles contribueront aussi à assurer la cybersécurité de votre famille et la vôtre, à la maison.



Vous : Tout d'abord, la technologie seule ne peut vous protéger adéquatement – vous êtes la meilleure défense. Les cybercriminels ont compris que la meilleure façon d'obtenir ce qu'ils veulent est de vous cibler personnellement, plutôt que de viser votre ordinateur ou autres appareils. S'ils veulent votre mot de passe, vos données de travail ou contrôler votre ordinateur, ils tenteront de vous pousser à les leur donner, en créant un sentiment d'urgence. Par exemple, ils peuvent vous appeler en usurpant l'identité d'un agent du soutien technique et prétendre que votre ordinateur est infecté. Ou ils vous envoient un courriel avertissant qu'un colis ne peut être livré, pour que vous cliquiez sur un lien malicieux. Les indicateurs les plus connus d'attaques d'ingénierie sociale comprennent :

- Une personne qui fait naître un sentiment d'urgence extrême, par la peur, l'intimidation, une crise, ou un délai important. Les cybercriminels savent créer des messages persuasifs qui semblent venir d'organisations de confiance, telles que des banques, un gouvernement ou un organisme international.

- La pression de contourner ou d'ignorer les politiques et procédures de sécurité, ou une offre qui semble trop alléchante pour être vraie (non, vous n'avez pas gagné la loterie!)
- Un message qui semble venir d'un collègue, mais dans lequel le ton ou les propos tenus ne leur ressemblent pas.

Voilà pourquoi la meilleure défense contre ces attaques, c’est vous.

Maison Réseau : Presque tous les réseaux privés commencent avec un réseau sans fil (souvent appelé Wi-Fi). Ce réseau vous permet de connecter tous vos appareils à Internet. La plupart des réseaux sans fil domestiques sont contrôlés par votre routeur Internet, ou par un point d'accès sans fil séparé. Les deux fonctionnent de la même façon : en diffusant des signaux sans fil auxquels des appareils de la maison se connectent. Ce qui signifie qu'une connexion sans fil sécurisée est une protection clé pour votre maison. Nous recommandons les étapes suivantes pour la rendre sécuritaire :

- Changez le mot de passe qui contrôle votre réseau sans fil fourni par défaut pour le routeur. Le compte de l'administrateur est ce qui vous permet de configurer les réglages pour votre réseau sans fil.
- Assurez-vous que seules les personnes en qui vous avez confiance peuvent se connecter à votre réseau sans fil. Pour y arriver, appliquez des mesures de sécurité appropriées. Tout d'abord, exigez qu'un mot de passe soit requis pour se connecter à votre réseau sans fil, et qu'une fois connecté, les activités d'une personne en ligne soient chiffrées.
- Assurez-vous que le mot de passe requis pour se connecter à votre réseau sans fil est fort et différent de celui fourni par l'administrateur. N'oubliez pas que vous n'avez qu'à entrer le mot de passe une seule fois pour chaque appareil, puisque ceux-ci enregistrent ce mot de passe.

Vous ignorez comment exécuter ces étapes? Demandez à votre fournisseur de services Internet, consultez leur site web, lisez les documents fournis avec votre outil d'accès sans fil, ou consultez le site web du marchand distributeur.

Les mots de passe : Lorsqu'un site vous demande de créer un mot de passe : créez-en un fort, plus il comprend de caractères plus il sera fort. L'utilisation d'une phrase de passe est une des façons les plus simples de s'assurer que vous utilisez un mot de passe fort. Une phrase de passe n'est rien d'autre qu'un mot de passe composé de plusieurs mots, tels que « *abeille miel bourbon.* » L'utilisation d'une phrase de passe unique signifie d'en utiliser une différente pour chaque appareil ou chaque compte en ligne. Ainsi, si une de vos phrases de passe est compromise, tous vos autres comptes et appareils sont toujours protégés. Est-il trop difficile de mémoriser toutes ces phrases de passe?

Utilisez un gestionnaire de mots de passe, qui est un logiciel spécialisé qui stocke toutes vos phrases de passe de façon sécuritaire dans un format chiffré (et qui comporte aussi d'autres caractéristiques importantes). Enfin, activez la vérification en deux étapes (aussi appelé authentification à deux facteurs) autant que possible. Elle utilise votre mot de passe, mais ajoute aussi une deuxième étape, tel qu'un code qui vous est envoyé par téléphone ou une appli qui génère le code pour vous. La vérification en deux étapes est probablement l'étape la plus importante à prendre pour protéger vos comptes en ligne et elle est beaucoup plus simple que vous pourriez l'imaginer.

Mises à jour : Assurez-vous que chacun de vos ordinateurs, appareils mobiles, programmes et applis sont à jour avec la plus récente version de logiciel. Les cybercriminels cherchent continuellement de nouvelles failles dans les logiciels que vous utilisez pour vos appareils. Lorsqu'ils découvrent des failles, ils utilisent des programmes spéciaux pour les exploiter et pour les pirater dans les appareils que vous utilisez. En même temps, les entreprises qui ont créé ces logiciels pour vos appareils travaillent sans cesse pour y remédier en diffusant des mises à jour. En vous assurant d'installer rapidement les mises à jour sur ces appareils, vous compliquez la tâche à quiconque cherche à les pirater. Pour demeurer à jour, activez simplement la mise à jour automatique autant que possible. Cette règle s'applique sur presque toute technologie connectée à un réseau, y compris non seulement vos appareils de travail, mais aussi votre téléviseur, moniteur pour bébé, caméra de sécurité, routeur à la maison, console de jeux vidéo ou même votre voiture.

Enfants / Invités : Ce dont vous n'avez pas à vous inquiéter au travail ce sont les enfants, invités ou autres membres de la famille qui utiliseraient votre portable de travail ou autres appareils de travail. Assurez-vous que votre famille et vos amis comprennent qu'ils ne peuvent utiliser vos appareils de travail, parce qu'ils pourraient accidentellement effacer ou modifier de l'information, ou, au pire, infecter accidentellement l'appareil.