



CYBERSÉCURITÉ

Travailler en toute sécurité depuis son domicile

Nos domiciles sont devenus nos lieux de travail. Comment protégeons-nous nos systèmes et nos données contre les compromissions lorsque nous travaillons en dehors du bureau, en particulier depuis nos domiciles?

Comme les cybercriminels s'adaptent rapidement à une grande partie de la main-d'œuvre mondiale travaillant à distance, les foyers et la technologie utilisée par les employés sont devenus des cibles privilégiées. Il existe également des risques particuliers pour les données de l'entreprise lorsque les employés travaillent tous dans des environnements domestiques différents.

La cybersécurité est un partenariat. Votre entreprise a peut-être investi dans une technologie conçue pour sécuriser les systèmes et les données. Bien qu'il s'agisse d'une étape importante dans la protection contre d'éventuelles cyberattaques, vos employés jouent un rôle essentiel en tant que première ligne de défense.

Voici cinq étapes que les employés peuvent suivre pour sécuriser leur bureau à domicile et éviter la perte de données.

Cinq étapes pour sécuriser votre bureau à domicile



Sécurisez votre réseau domestique

- Modifiez le nom d'administrateur et le mot de passe par défaut de votre routeur réseau et de vos appareils Wi-Fi et assurez-vous qu'ils exécutent les dernières mises à jour du fabricant. Les employés peuvent appeler leur fournisseur d'accès à Internet pour obtenir des instructions sur la manière de procéder. Cette étape est essentielle, car les pirates informatiques connaissent les noms de réseau et les mots de passe par défaut de la plupart des fournisseurs.

- Pour joindre votre réseau Wi-Fi, vous devez disposer d'un mot de passe fort et utiliser le cryptage le plus récent (WPA2).
- Examinez les appareils qui se connectent à votre réseau (par exemple, les téléphones, les consoles de jeu, les lumières, les téléviseurs ou même votre voiture) et débranchez ceux qui ne sont pas nécessaires. Assurez-vous que les appareils qui restent connectés utilisent des mots de passe forts.
- Utilisez un réseau sans fil « invité » distinct pour vos amis.
- Si possible, ne « diffusez » pas le nom de votre réseau sans fil (SSID). Les employés peuvent contacter leur fournisseur d'accès à Internet pour déterminer comment modifier ce paramètre.

Contactez votre fournisseur de services ou le fabricant de l'équipement pour obtenir une aide supplémentaire – très souvent, les manuels d'entretien de l'équipement sont en ligne.



Sécurisez vos ordinateurs et appareils

- N'utilisez pas votre ordinateur professionnel pour des tâches personnelles inutiles.
- Conservez votre ordinateur de travail dans un endroit sûr et verrouillez-le (généralement WIN-L ou Ctrl-Alt-Supprimer et cliquez sur le verrou) avant de le laisser sans surveillance.
- Ne permettez pas à votre famille ou à vos amis d'utiliser votre ordinateur de travail ou tout autre appareil fourni par l'entreprise.



Sécurisez vos comptes personnels et vos mots de passe

- Utilisez des mots de passe forts et difficiles à deviner et même des phrases en guise de mot de passe lorsque c'est possible (par exemple, « Où est mon café? »).
- Utilisez des mots de passe différents pour chacun de vos comptes, services et appareils Internet.
- Ne répétez jamais les mots de passe entre les systèmes de l'entreprise et vos services et appareils personnels.
- Changez fréquemment les mots de passe.



Sécurisez vos renseignements personnels

- Sur les médias sociaux, n'affichez que ce que vous voulez que le public voie, et pensez aux renseignements permanents que vous pourriez involontairement partager sur vous-même ou votre famille.
- Ne soyez pas victime de la fraude cybernétique ([cliquez ici](#) pour de plus amples renseignements sur ce sujet).



Sécurisez et contrôlez ce que vous imprimez

- N'imprimez que ce dont vous avez besoin pour faire votre travail; dans la mesure du possible, évitez d'imprimer des renseignements commerciaux ou personnels sensibles.
- Ne transmettez pas les données de l'entreprise à des courriels personnels, même si ce n'est que pour les imprimer; les données de l'entreprise doivent toujours rester sur les appareils de l'entreprise.
- Tout document que vous imprimez et qui a trait au travail pourrait être retrouvé par quelqu'un et compromis si vous ne l'éliminez pas correctement. À moins que les documents que vous imprimez à partir de votre ordinateur professionnel ne soient des renseignements publics, déchiquetez-les à la maison ou conservez-les dans une boîte pour les éliminer plus tard en toute sécurité.

Visitez assurancevictor.ca pour en apprendre davantage.