COMMENT PROTÉGER VOS DONNÉES LORSQUE VOUS TRAVAILLEZ À DISTANCE

Que vous travailliez à la maison, dans un café ou tout simplement à distance, il est primordial que tous les professionnels, quel que soit leur secteur d'activité, adoptent des pratiques de cybersécurité solides. Cela contribue protéger les données confidentielles, autant personnelles que corporatives, des tentatives de vol.

1 Renforcez tous vos comptes utilisateurs

Assurez-vous de choisir des mots de passe solides (une combinaison de majuscules, de minuscules, de chiffres et de caractères spéciaux), et uniques à chaque compte. Pour un niveau de protection supplémentaire, activez l'authentification à deux facteurs pour tous vos comptes utilisateurs.

2 Utilisez un réseau privé virtuel (RPV)

Un RPV peut être utilisé pour sécuriser les connexions Internet et chiffrer les données partagées entre les appareils. Il permet aux employés de protéger les données individuelles et corporatives contre les cybercriminels, quel que soit le réseau Wi-Fi utilisé. Consultez votre gestionnaire ou votre service des TI pour obtenir des recommandations sur les logiciels compatibles ou des conseils pour leur installation.

3 Installez des logiciels pare-feux et antivirus

Bien que la plupart des systèmes d'exploitation soient équipés des mesures de sécurité de base, le fait d'optimiser les paramètres de vos logiciels pare-feux et antivirus permet d'améliorer votre niveau de protection contre les programmes malveillants et autres menaces. Consultez votre service des TI pour vous assurer que vos appareils sont munis de logiciels adéquats et à jour.

4 Protégez votre routeur sans fil domestique

Si vous travaillez régulièrement de la maison, une étape essentielle pour protéger les données échangées via votre réseau est de sécuriser votre routeur sans fil. Assurez-vous de changer votre mot de passe, en particulier s'il s'agit de l'original fourni par votre fournisseur de services Internet, et d'installer les plus récentes mises à jour de microprogrammes pour réduire les failles.

5 Effectuez les mises à jour de vos programmes et systèmes d'exploitation

Même si certains peuvent trouver le processus fastidieux, il est important d'effectuer régulièrement les mises à jour de vos applications et systèmes d'exploitation. Ces mises à jour comprennent souvent des correctifs de sécurité importants qui contribuent à supprimer des failles que les pirates ont pu exploiter par le passé.

6 Inspectez les messages entrants à la recherche d'éléments suspects

Tout comme vous le feriez au bureau, il est important d'être vigilant et attentif aux signes avant-coureurs communs d'une cybermenace. Inspectez chaque message entrant avec attention et évitez d'ouvrir des pièces jointes ou de cliquer sur des liens non sollicités, même s'ils semblent provenir d'un contact ou d'une organisation connu. Si vous êtes confronté à un courriel potentiellement malveillant, signalez-le immédiatement conformément aux politiques de votre organisation.