



Assurer la sécurité de votre organisation au bureau comme à l'extérieur

Que vous travailliez à la maison ou au bureau, la sécurité de votre organisation doit être l'une de vos priorités. Bien que ces lieux de travail soient passablement différents, vous pouvez prendre les mêmes précautions en matière de sécurité. Examinons quelques règles importantes en matière de cybersécurité et la manière de les appliquer lorsque vous travaillez au bureau ou à la maison.

Utilisez seulement des appareils sûrs

- N'oubliez pas que la sécurité de votre appareil dépend essentiellement de celle des applications installées sur celui-ci. N'installez jamais d'application ou de module d'extension sans en parler avec le service des TI.
- Utilisez vos appareils seulement pour le travail. Si vous utilisez votre ordinateur personnel pour le travail, nous vous recommandons de créer un compte d'utilisateur distinct avec un nom d'utilisateur et un mot de passe différents.
- Au bureau, la sécurité du réseau est probablement gérée par le service des TI. Pour assurer la sécurité de votre connexion Internet à la maison, utilisez un mot de passe complexe pour votre routeur. Si votre organisation offre l'accès à un réseau privé virtuel (RPV), connectez-vous également à celui-ci.

Protégez votre espace de travail physique

- Au bureau, méfiez-vous de l'accès à califourchon et du talonnage. L'accès à califourchon désigne une situation dans laquelle une personne prétend faire partie de votre organisation et vous suit dans une zone sécurisée sans badge ni code d'accès. Le talonnage est défini comme une personne attendant que vous entriez ou sortiez d'une zone sécurisée pour ensuite s'y faufiler alors que la porte est ouverte. Méfiez-vous de toute personne que vous ne reconnaissez pas et n'hésitez pas à demander une pièce d'identité.
- À la maison, établissez votre espace de travail dans un endroit privé et confortable à l'abri du regard des autres. Vous devez garder toutes les informations sensibles hors de la vue de toute personne non autorisée, y compris vos partenaires, vos enfants et vos amis.
- Verrouillez toujours votre ordinateur lorsque vous vous absentez de votre bureau. Si vous laissez votre ordinateur déverrouillé, n'importe qui peut l'utiliser pour accéder à des données sensibles, voler vos identifiants de connexion ou même installer un logiciel malicieux.

Réfléchissez avant de cliquer

- Ne cliquez jamais sur un lien et ne téléchargez jamais une pièce jointe d'un courriel auquel vous ne vous attendiez pas. Même si l'expéditeur semble appartenir à une organisation légitime, l'adresse de courriel pourrait être fausse.
- Lorsqu'un courriel vous demande de vous connecter à un compte ou à un service en ligne, accédez à ce service par le biais de votre navigateur. Ne cliquez jamais sur le lien inclus dans le courriel. En accédant directement au site, vous vous assurez de vous connecter au vrai site Web et non à un site similaire.
- En cas de doute, appelez l'expéditeur du courriel pour vous assurer de l'authenticité de la demande, du lien ou de la pièce jointe. N'appellez pas le numéro inscrit dans le courriel, car il pourrait s'agir d'un faux numéro.

