

Comment garantir la sécurité de votre organisation à l'intérieur comme à l'extérieur

Que vous travailliez à domicile ou dans un bureau, la sécurité de votre organisation doit être l'une de vos principales priorités. Même si ces deux environnements peuvent sembler très différents, vous pouvez prendre les mêmes précautions, que vous travailliez au bureau ou à la maison. Examinons quelques règles importantes en matière de cybersécurité, et la manière dont elles peuvent être appliquées au bureau et lorsque vous travaillez à domicile.

N'utilisez que des appareils sécurisés

- N'oubliez pas que la sécurité de votre appareil dépend des applications qui y sont exécutées. N'installez jamais une application ou un plug-in sans consulter au préalable votre service informatique.
- N'utilisez vos appareils qu'à des fins professionnelles. Si vous utilisez votre ordinateur personnel pour votre travail, nous vous recommandons de créer un compte utilisateur distinct avec un nom d'utilisateur et un mot de passe uniques.
- Au bureau, la sécurité du réseau est probablement gérée par votre service informatique. Pour sécuriser votre connexion Internet à domicile, utilisez un mot de passe complexe sur votre routeur. Si votre organisation offre un accès à un réseau privé virtuel (VPN), connectez-vous également à ce réseau.

Protégez votre espace de travail physique

- Au bureau, faites attention aux situations d'agglutinement (piggybacking) et de talonnage (tailgating). Un « piggybacker » est une personne qui prétend faire partie de votre organisation et qui vous suit dans une zone sécurisée sans utiliser de badge ni de code d'accès. Un « tailgater » est une personne qui attend que vous entriez ou sortiez d'une zone sécurisée pour se faufiler à l'intérieur pendant que la porte est encore ouverte. Méfiez-vous de toute personne que vous ne reconnaissez pas et n'hésitez pas à lui demander de décliner son identité.
- À la maison, aménagez-vous un espace de travail privé et confortable, où personne ne peut voir votre écran pendant que vous travaillez. Vous devez garder toutes les informations sensibles hors de vue de toute personne non autorisée, y compris votre partenaire, vos enfants et vos amis.
- Verrouillez toujours votre ordinateur lorsque vous quittez votre bureau. Si vous laissez votre ordinateur non verrouillé, n'importe qui peut l'utiliser pour accéder à des données sensibles, voler vos identifiants de connexion, ou même installer des programmes malveillants.

Réfléchissez avant de cliquer

- En aucun cas vous ne devez cliquer sur un lien ni télécharger une pièce jointe dans un e-mail reçu par surprise. Même si l'expéditeur semble appartenir à une organisation légitime, son adresse e-mail a peut-être été usurpée.
- Si un e-mail 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 l'e-mail. En accédant directement au site, vous avez la garantie de vous connecter au véritable site Web et non à un site factice.
- En cas de doute, appelez l'expéditeur de l'e-mail pour vous assurer que la demande, le lien ou la pièce jointe est légitime. N'appellez pas le numéro de téléphone indiqué dans l'e-mail car il peut s'agir d'un faux numéro.

