FORTRA

Terranova Security®

Co-présenté par Microsoft

Comment protéger vos données lorsque vous travaillez à distance

Que vous travailliez à domicile, dans un café, dans la salle de conférence d'un hôtel ou dans un autre lieu éloigné, tous les professionnels, quel que soit leur secteur d'activité, doivent observer de solides pratiques de cybersécurité. Cela permettra de protéger les données confidentielles, tant personnelles qu'organisationnelles, contre les tentatives de vol.

1

SÉCURISEZ LES COMPTES UTILISATEURS AVEC DES MOTS DE PASSE FORTS

Assurez-vous d'utiliser des mots de passe forts (une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux), ainsi que des mots de passe uniques pour chaque compte. Pour ajouter une couche de protection supplémentaire, activez l'authentification à deux facteurs pour ous vos comptes d'utilisateur.

UTILISEZ UN RÉSEAU PRIVÉ VIRTUEL (RPV)

Un RPV peut sécuriser les connexions Internet et chiffrer les données partagées entre les appareils, ce qui vous permet de garder les informations sensibles à l'abri des cybercriminels, quel que soit le réseau Wi-Fi utilisé. Demandez à votre responsable ou à votre service informatique de vous recommander des logiciels ou de vous guider dans le processus d'installation.

2

3

CONFIGUREZ DES COUPE-FEU ET DES ANTIVIRUS

Bien que la plupart des systèmes d'exploitation comprennent des protections de base, l'optimisation des paramètres de votre coupe-feu et de votre antivirus augmente votre niveau de protection contre les programmes malveillants et d'autres menaces. Assurez-vous que vos appareils sont équipés de logiciels adéquats et à jour, conformément à votre politique en matière de TI ou de télétravail.

SÉCURISEZ VOTRE ROUTEUR WI-FI À DOMICILE

Si vous travaillez régulièrement depuis chez vous, la sécurisation de votre routeur Wi-Fi est une étape essentielle qui contribuera à protéger les données échangées sur votre réseau. Veillez à changer votre mot de passe, surtout s'il s'agit du mot de passe d'origine fourni par votre fournisseur d'accès à Internet, et installez les dernières mises à jour du micrologiciel pour minimiser les vulnérabilités.

4

5

MAINTENEZ VOS PROGRAMMES ET VOTRE SYSTÈME D'EXPLOITATION À JOUR

La mise à jour de l'ensemble de vos applications et systèmes d'exploitation est essentielle pour sécuriser le télétravail. Lorsque vous voyez une mise à jour disponible, installez-la le plus rapidement possible, car elle contient souvent des correctifs de sécurité importants qui contribuent à éliminer les failles que les pirates pourraient exploiter.

INSPECTEZ LES MESSAGES ENTRANTS POUR DÉTECTER LES ÉLÉMENTS SUSPECTS

Comme vous le feriez au bureau, il est essentiel d'être vigilant et de prêter attention aux signaux d'alerte courants d'une cybermenace. Examinez attentivement chaque message entrant et évitez de cliquer sur des liens inattendus ou d'ouvrir des pièces jointes, même s'ils proviennent d'expéditeurs connus. Si vous êtes confronté à un courriel potentiellement malveillant, signalez-le immédiatement conformément aux politiques en vigueur dans votre organisation.

6