

cybersécurité

12 BONNES PRATIQUES

Comment protéger et préserver vos données et celles de l'entreprise ?



PROTÉGEZ VOTRE POSTE DE TRAVAIL

Verrouillez toujours votre session Windows, même pour peu de temps.



CRÉEZ DES MOTS DE PASSE COMPLEXES

Le mot de passe doit respecter la politique de sécurité de l'entreprise et être différent pour chacun des comptes. En cas de doute, changez le immédiatement.



PROTÉGEZ VOS DONNÉES SENSIBLES

Identifiez les données les plus sensibles et vérifiez régulièrement leur gestion.



EFFECTUEZ DES SAUVEGARDES RÉGULIÈRES

Assurez-vous régulièrement de la sauvegarde des données à des endroits différents.



RESTEZ VIGILANT EN OUVRANT LES PIÈCES JOINTES

Avant d'ouvrir une pièce jointe, vérifiez l'expéditeur et l'objet du mail. En cas de doute, transférez-le à votre service informatique.



METTEZ À JOUR RÉGULIÈREMENT LES APPAREILS ET LOGICIELS

Éteignez votre ordinateur régulièrement et acceptez les mises à jour proposées.



LIMITEZ LE BRANCHEMENT DE CLÉS USB OU DISQUES DURS EXTERNES À VOTRE ORDINATEUR

Privilégiez les services de transfert de fichiers en lieu et place des clés USB.



CLOISONNEZ BIEN LE PROFESSIONNEL DU PERSONNEL

Votre adresse professionnelle doit être utilisée uniquement à cet effet. Évitez de vous connecter à des sites publics avec ses identifiants professionnels.



NE TÉLÉCHARGEZ RIEN PAR SOI-MÊME

En cas de besoin d'une application ou d'un logiciel, contactez votre service informatique.



RESPECTEZ LES CONFIGURATIONS STANDARDS DE L'ENTREPRISE

Ne pas tenter de se connecter à un proxy inconnu de l'entreprise. Les manipulations visant à contourner les configurations standards sont à proscrire.



ADOPTÉZ ET ÉVOLUEZ AVEC LE BON ANTIVIRUS

L'antivirus protège votre ordinateur contre les virus, les malwares et les autres menaces en ligne. Optez pour un bon logiciel de sécurité et gardez le parfaitement à jour.



PROTÉGEZ VOS OUTILS MOBILES

Évitez les connexions aux bornes Wi-Fi publiques et gratuites. Ces connexions ne sont pas sécurisées. Ne téléchargez pas d'applications non officielles et n'exécutez pas d'applications inconnues. Priorisez une connexion via VPN.

Vous avez des questions ? Nous avons des solutions !