INFORSUD TECHNOLOGIES
Solutions et impulsions pour l'avenir

USAGES PRO/PERSO
10 bonnes pratiques !

Avec le développement des appareils mobiles et d'internet, les collaborateurs peuvent travailler de n'importe où.
La frontière entre la sphère professionnelle et personnelle s'estompe.

1 UTILISEZ DES MOTS DE PASSE DIFFÉRENTS

Si vous ne le faîtes pas et qu'un des services auquel vous accédez se fait pirater, le vol de votre mot de passe permettra à une personne malveillante d'accéder à tous vos autres services y compris les plus critiques (banque, messagerie, réseaux sociaux…).

2 NE MÉLANGEZ PAS VOTRE MESSAGERIE PROFESSIONNELLE OU D'ÉLU AVEC VOTRE MESSAGERIE PERSONNELLE

L'utilisation de votre messagerie professionnelle à des fins personnelles et vice versa peut avoir comme conséquences de voir des informations confidentielles de votre organisation échapper vers des contacts personnels qui pourraient en faire un mauvais usage et inversement.

3 UTILISEZ INTERNET AU TRAVAIL DE MANIÈRE RESPONSABLE

L'utilisation d'Internet à des fins personnelles peut être tolérée mais elle peut mettre en cause les données de votre organisation, en cas de téléchargement de contenu malveillant à votre insu par exemple. Modérez votre connexion professionnelle à un usage personnel.

4 N'UTILISEZ PAS DE SERVICES DE STOCKAGE EN LIGNE PERSONNEL À DES FINS PROFESSIONNELLES

Les services de stockage en ligne souvent gratuits pour les particuliers ne présentent pas un niveau de sécurité renforcée. Pour les besoins des entreprises, il existe des solutions professionnelles et sécurisées.

5 FAITES LES MISES À JOUR DE SÉCURITÉ DE VOS ÉQUIPEMENTS

Il est important d'installer sans tarder les mises à jour dès qu'elles sont publiées. Elles corrigent souvent des failles de sécurité qui pourraient être exploitées par des cybercriminels.

6 UTILISEZ UNE SOLUTION DE SÉCURITÉ CONTRE LES VIRUS ET AUTRES ATTAQUES

Veillez à installer des solutions anti-virus sur vos équipements professionnels (si c'est de votre responsabilité) mais aussi personnels, et tenez-les à jour.

7 N'INSTALLEZ DES APPLICATIONS QUE DEPUIS LES SITES OFFICIELS

Seuls les sites officiels vous permettent de vous assurer que les applications installées ne sont pas piégées par un virus qui permettrait à un cybercriminel de prendre le contrôle de votre équipement.

8 MÉFIEZ-VOUS DES SUPPORTS USB

Vous trouvez ou on vous offre une clé USB, partez du principe qu'elle est piégée. Ne la branchez sur aucun de vos équipements informatiques.

9 ÉVITEZ LES RÉSEAUX WI-FI PUBLICS OU PARTAGÉS

L'accès à ces réseaux, même avec un mot de passe, peut être contrôlé par des cybercriminels qui interceptent vos connexions et récupèrent vos données confidentielles personnelles ou professionnelles.

10 SOYEZ VIGILANT.E SUR LES RÉSEAUX SOCIAUX

Quand vous parlez de la vie de votre structure (ambiance, nouveaux projets…) sur les réseaux sociaux, même si vos propos ne sont pas négatifs, vous ne contrôlez pas la rediffusion ou l'interprétation de vos relations.

inforsud-technologies.com 0 811 349 609

« Cybermalveillance.gouv.fr – Données originales téléchargées sur Cybermalveillance.gouv.fr, publié le 11/2019. »