LES BONNES PRATIQUES DE CYBERSECURITE

La prévention commence avec vous !

1. Choisir avec soin ses mots de passe

Proscrivez la date de naissance de votre enfant ou le nom de votre animal de compagnie... Un bon mot de passe doit être complexe et unique pour chaque compte (nombre de caractères minimum, usage de majuscules, minuscules, chiffres, caractères spéciaux...).
Différenciez vos mots de passe personnels et professionnels.
Evidemment ils doivent rester secrets...

2. Faire ses mises à jour

Faites régulièrement les mises à jour poussées par votre système d'exploitation : logiciels, pilotes..

3. Rester vigilant sur les mails

Les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, pièces jointes piégées, etc.).
Soyez attentif à l'adresse mail de votre expéditeur, son orthographe et l'objet.

4. Vérifier la sécurité du WI-FI

L'aspect simple et pratique du Wi-Fi en fait une technologie très utilisée et pas toujours sécurisée. Il ne faut pas oublier qu'un Wi-Fi mal sécurisé peut permettre à des tiers d'intercepter vos données et votre connexion Wi-Fi à votre insu pour réaliser des opérations malveillantes...
Evitez au maximum les Wi-Fi publics (hotels, aéroports...) et préférez le partage de connexion 4G de votre téléphone.

CES BONNES PRATIQUES S'APPLIQUENT AUTANT SUR VOTRE ORDINATEUR QUE SUR VOTRE SMARTPHONE.

EASY SERVICE INFORMATIQUE

5. Sauvegarder ses données

Pour la sécurité de vos données, il est vivement conseillé d'effectuer des sauvegardes régulières. Vous pourrez alors en disposer en cas de dysfonctionnement de votre ordinateur. En général votre entreprise dispose d'espaces de stockage sécurisés et sauvegardés, veillez à y stocker vos données.

6. Disposer d'un antivirus à jour

Votre antivirus est votre premier allié en termes de sécurité informatique. Vous devez absolument disposer d'un antivirus à jour afin de limiter les risques.

7 Télécharger prudemment

Le téléchargement de données sur internet est un gros vecteur de malware en tout genre. Veillez à proscrire les sites illégaux ou suspects et à ne télécharger que depuis des sites officiels (Adobe, Google, Microsoft, Apple...).
Evitez les sites non sécurisés : symbolisés par un cadenas barré à gauche de l'URL. Cela signifie qu'ils sont considérés comme potentiellement dangereux par votre navigateur.

8. Séparer les usages persos des usages pros

Ne faites jamais suivre vos mails professionnels sur des messageries personnelles. Les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, smatphone, etc.) personnels et professionnels.

9. Crypter ses données

Vos clés USB, vos ordinateurs portables, vos disques durs externes doivent être cryptés pour éviter toute perte ou vol de données.

10. Prendre conscience des conséquences

De plus en plus d'entreprises, de toutes tailles, sont touchées par la cybercriminalité. Ces actes de cyber-malveillance ont des conséquences désastreuses pouvant aller jusqu'à la faillite.

CES BONNES PRATIQUES S'APPLIQUENT AUTANT SUR VOTRE ORDINATEUR QUE SUR VOTRE SMARTPHONE.

EASY SERVICE INFORMATIQUE