Conseils de cybersécurité pour vous protéger contre les cyberattaques

- **Sauvegarde des données** : les sauvegardes peuvent aider dans plusieurs situations.
Elles minimiseront les dommages causés si un cybercriminel supprime ou modifie les données de votre système et atténuera les effets d'une attaque de ransomware.

- **Contrôle de l'accès au système** : vous pouvez également réduire le risque de cyberattaques en faisant preuve de rigueur au niveau de l'accès au système, notamment en révoquant l'accès dès qu'une personne quitte l'entreprise et en mettant en place un contrôle d'accès strict basé sur les rôles.

- **Obtenez une assistance professionnelle** : grâce à un outil de surveillance de la sécurité tel qu'une solution SIEM.

- **Authentification multifacteur :** l'utilisation de l'authentification multifacteur permet d'empêcher les pirates d'accéder à votre réseau ou à vos appareils s'ils ont réussi à mettre la main sur vos mots de passe. Cette précaution est particulièrement importante pour les entreprises, au niveau desquelles un risque élevé de phishing par emails existe.

- **Sensibilisez et formez ses employés** : assurez-vous que vos employés soient conscients de l'importance de la cybersécurité et de la manière d'éviter les cyberattaques, notamment les risques liés aux malwares et au phishing.

La CCI de la Drôme propose une formation « Réferent en cybersécurité» pour savoir prévenir, identifier et analyser les problèmes de cybersécurité

- **Mettre à jour les systèmes** : quel que soit le système ou le programme que vous utilisez, il doit toujours être mis à jour. Cette précaution vous permettra de tirer parti des derniers correctifs de sécurité qui traiteront les vulnérabilités connues.

- **Utilisez des pares-feu et un antivirus** : tous les appareils connectés au réseau de votre entreprise doivent disposer d'un logiciel antivirus et d'un pare-feu opérationnels. Cette précaution offrira une couche de protection supplémentaire en détectant les malwares et en atténuant les autres risques.

Source logpoint.com

- **Effectuer un test d'intrusion par des organismes certifiés** pour vérifier votre sécurité comme avec le programme de l'ENE (Espace Numérique Entreprise) intitulé « Cybersécurité» à découvrir ici !

En fonction de ce diagnostic des préconisations et des actions correctives sont faites afin de corriger les dysfonctionnements, les failles de votre système informatique.

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

Est-ce que vous utilisez la même clé pour toutes les serrures chez vous ? Bah non !
Alors, pourquoi utiliser sur tous vos comptes le même mot de passe par facilité ?
C'est ce genre de conseils que l'Agence nationale de sécurité des systèmes d'information (ANSSI) délivre sur son site internet à destination des particuliers, des entreprises et des institutions. Il recèle une masse d'informations pratiques et pédagogiques parfois sous forme de fiches.

En plus de sa mission de cybervigilance, l'ANSSI délivre des agréments à des entreprises susceptibles d'intervenir pour assister celles qui viennent d'être attaquées ou pour les aider à renforcer leurs défenses afin de s'en prémunir.

Depuis février 2021, un label Expert Cyber liste ces prestataires de confiance.

Le site gouvernemental de sensibilisation aux bonnes pratiques numériques cybermalveillance.gouv.fr permet de signaler des faits mais il sert aussi à proposer une assistance en ligne et à mettre en relation les victimes avec des professionnels.