MES CONSEILS DE SÉCURITÉ INTERNET

1. **Éviter le compte administrateur lors de vos connexions routinières.**
2. **Avoir une véritable stratégie de sauvegarde (backups).**
3. **Utiliser le chiffrement pour les données importantes (fichiers zippés avec mot de passe, coffre VeraCrypt, …).**
4. **Effectuer des mises à jour régulières de tous vos programmes, du système d'exploitation et de l'antivirus. Préférer les mises à jour automatiques.**
5. **Vérifier et désactiver au besoin les programmes qui se lancent au démarrage de Windows (clic sur la barre des tâches puis sur le *Gestionnaire des tâches, onglet démarrage*).**
6. **Ne pas utiliser de mots de passe trop simples, les changer régulièrement (tous les six mois ou tous les ans) et créer des mots de passe différents pour tous les sites fréquentés.**
7. **Utiliser un gestionnaire de mots de passe (Dashlane, LastPass, KeePass). Éviter la gestion des mots de passe par le navigateur et le stockage des mots de passe dans le cloud.**
8. **Installer l'extension Privacy Badger (bloque les traqueurs).**
9. **Utiliser en cas de besoin des emails temporaires lorsque cela est autorisé par l'application web visitée.**
10. **Vérifier si votre adresse de courriel est compromise sur le site https://haveibeenpwned.com/**
11. **Utiliser un VPN payant pour éviter d'être suivi sur Internet. Le VPN permet encore de contourner des restrictions géographiques.**
12. **Avoir un antivirus à jour et un bon Firewall. En cas de doute : scanner le fichier suspect sur le site www.virustotal.com qui vérifie le fichier avec une pléthore d'antivirus différents.**
13. **Utiliser OSArmor (de la société *NoVirusThanks*) en plus de l'antivirus pour un blacklisting (règles comportementales) et un whitelisting (= création d'exclusions aux règles)**
14. **Utiliser un anti-keylogger (KeyScrambler ou Zemana AntiLogger) pour contrecarrer les enregistreurs de frappe.**
15. **Calculer le hash des fichiers téléchargés pour s'assurer qu'ils n'ont pas été modifiés depuis leur mise en ligne.**
16. **Si un fichier Office est téléchargé, rester par prudence en mode protégé.**
17. **Vérifier l'activité réseau avec TCPView pour s'assurer que votre ordinateur ne communique pas avec un bot.**
18. **Toujours afficher dans l'explorateur de fichiers les extensions connues afin de ne pas être trompé par la technique de la double extension ou par l'utilisation d'une icône usurpée.**
19. **Toujours vérifier le protocole des sites fréquentés : HTTPS est préférable à HTTP.**
20. **Toujours se méfier des emails non sollicités qui vous proposent de cliquer sur un lien pour résoudre un problème prétendument urgent : risque de phishing !**

© Max Grégoire