MES 21 CONSEILS DE SÉCURITÉ CYBER

1. **Éviter le compte administrateur lors de vos connexions routinières avec Windows et Mac.**
2. **Avoir une véritable stratégie de sauvegarde (les backups en local sont préférables).**
3. **Utiliser le chiffrement pour les données importantes (fichiers zippés avec mot de passe, coffres VeraCrypt, et surtout Cryptomator). Cryptomator est cloud-friendly et SSD-friendly !**
4. **Effectuer des mises à jour régulières de tous vos programmes, du système d'exploitation et de l'indispensable antivirus. Préférer les mises à jour automatiques.**
5. **Vérifier et désactiver au besoin les programmes qui se lancent au démarrage de Windows avec le Gestionnaire des tâches (Task Manager) ou mieux, avec Autoruns (Sysinternals).**
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 (KeePass, Dashlane, LastPass). 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 des courriels temporaires (lorsque cela est autorisé) ou mieux : des alias de messagerie (Firefox Relay) pour éviter de communiquer votre véritable adresse électronique.**
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 et vous protège des réseaux Wi-Fi publics.**
12. **En cas de doute avec un exécutable : 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 définir des règles comportementales (blacklisting). On peut créer des exclusions à ces règles (whitelisting).**
14. **Utiliser un anti-keylogger (comme KeyScrambler) pour contrecarrer les enregistreurs de frappe de type logiciel.**
15. **Lorsque le site officiel le fournit, 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 (avec ou sans macro) est téléchargé, rester par prudence en mode protégé.**
17. **Vérifier l'activité réseau avec TCPView (*Sysinternals* de Microsoft) ou CurrPorts (*NirSoft* de Nir Sofer) 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. **Pour bloquer les outils offensifs (comme Kon-Boot) qui bypassent l'authentification : activer BitLocker (qui chiffre le disque) ou créer un mot de passe UEFI (et bloquer l'USB boot). Activer Secure Boot est un plus (pour stopper les binaires non signés au démarrage).**
21. **Toujours se méfier des courriels non sollicités qui vous proposent de cliquer sur un lien pour résoudre un problème prétendument urgent : risque de phishing (hameçonnage) !**