Checklist Sécurité 2025

Les 7 Points Essentiels pour Protéger vos Données au-delà du VPN

(Introduction) *Félicitations ! Vous avez compris qu'un VPN n'est qu'une des briques de votre forteresse numérique. Cette checklist est votre plan d'action pour construire les autres remparts. Cochez chaque case au fur et à mesure pour blinder votre sécurité en ligne et naviguer avec une réelle tranquillité d'esprit.*

Point n°1 : Gérez vos Mots de Passe comme un Pro

- **Pourquoi c'est crucial :** Un mot de passe faible ou réutilisé est la porte d'entrée la plus courante pour les pirates. Un VPN ne peut rien faire si quelqu'un se connecte à vos comptes avec votre propre mot de passe.
- **Votre Mission :**
    - ☐ **Installer un gestionnaire de mots de passe :** C'est un coffre-fort numérique qui crée et retient pour vous des mots de passe uniques et complexes pour chaque site. (Exemples : Bitwarden).
    - ☐ **Lancer un audit de vos mots de passe :** Utilisez la fonction d'audit de votre gestionnaire pour identifier et changer immédiatement tous les mots de passe faibles, dupliqués ou compromis.
    - ☐ **Utiliser des phrases de passe :** Pour votre mot de passe "maître" (celui du gestionnaire), utilisez une phrase longue, facile à retenir pour vous mais impossible à deviner (ex: "Quatre//Chevaliers+Bleus+Chantent*SurLeToit!").

Point n°2 : Activez l'Authentification à Deux Facteurs (2FA) PARTOUT

- **Pourquoi c'est crucial :** Le 2FA est votre filet de sécurité. Même si un pirate vole votre mot de passe, il ne pourra pas se connecter sans ce deuxième code temporaire qui n'arrive que sur votre téléphone.
- **Votre Mission :**
  - ☐ **Activer le 2FA** sur vos comptes les plus sensibles SANS EXCEPTION : e-mail principal, banque, réseaux sociaux, Amazon, etc.
  - ☐ **Privilégier une application d'authentification** (comme Google Authenticator, Authy, Microsoft Authenticator) plutôt que le SMS, qui est moins sécurisé.
  - ☐ **Sauvegarder vos codes de récupération 2FA** dans un endroit sûr (hors ligne ou dans votre gestionnaire de mots de passe).

Point n°3 : Appliquez les Mises à Jour sans Délai

- **Pourquoi c'est crucial :** Les mises à jour ne servent pas qu'à ajouter des fonctionnalités. Elles corrigent principalement des failles de sécurité critiques que les hackers exploitent activement.
- **Votre Mission :**
    - ☐ **Activer les mises à jour automatiques** sur votre système d'exploitation (Windows, macOS), votre smartphone (iOS, Android) et votre navigateur.
    - ☐ **Vérifier manuellement une fois par semaine** que vos applications les plus utilisées (Zoom, Office, etc.) sont bien à jour.

Point n°4 : Utilisez une Protection Antivirus Moderne

- **Pourquoi c'est crucial :** Un VPN chiffre votre connexion, mais il n'inspecte pas les fichiers que vous téléchargez. Un malware ou un ransomware peut infecter votre machine même avec un VPN activé.
- **Votre Mission :**
    - ☐ **S'assurer qu'un antivirus est actif et à jour.** L'outil intégré Microsoft Defender est aujourd'hui très performant sur Windows.
    - ☐ **Lancer une analyse complète du système** au moins une fois par mois.
    - ☐ **Activer la protection en temps réel** contre les ransomwares si votre solution le propose.

Point n°5 : Devenez un Détecteur de Phishing Humain

- **Pourquoi c'est crucial :** Le phishing (hameçonnage) est une attaque de manipulation. Aucun outil ne peut remplacer votre vigilance. Un VPN ne bloquera jamais un lien frauduleux sur lequel vous cliquez volontairement.
- **Votre Mission :**
    - ☐ **Toujours vérifier l'adresse de l'expéditeur** d'un e-mail suspect.
    - ☐ **Ne JAMAIS cliquer sur un lien dans un e-mail ou un SMS inattendu.** Passez votre souris sur le lien pour voir l'URL réelle, ou, mieux encore, allez directement sur le site officiel par vos propres moyens.
    - ☐ **Se méfier de tout message créant un sentiment d'urgence** ("Votre compte sera suspendu !", "Facture impayée !").

Point n°6 : Mettez en Place une Stratégie de Sauvegarde Robuste (3-2-1)

- **Pourquoi c'est crucial :** En cas d'attaque par ransomware ou de panne matérielle, une bonne sauvegarde est le seul moyen de récupérer vos données sans payer de rançon.
- **Votre Mission :**
    - ☐ **Appliquer la règle du "3-2-1" :** Avoir **3** copies de vos données importantes, sur **2** supports différents (ex: disque dur externe et Cloud), dont **1** copie hors site (pas chez vous).
    - ☐ **Configurer des sauvegardes automatiques** et régulières de vos fichiers les plus précieux.
    - ☐ **Tester la restauration** de vos sauvegardes une fois par an pour vous assurer qu'elles fonctionnent.

Point n°7 : Revoyez vos Outils du Quotidien : Pensez Confidentialité

- **Pourquoi c'est crucial :** Un VPN cache votre IP, mais votre navigateur et vos applications peuvent continuer à collecter une quantité énorme d'informations sur vous.
- **Votre Mission :**
    - ☐ **Utiliser un navigateur qui protège votre vie privée** par défaut (comme Brave ou Firefox avec des réglages stricts).
    - ☐ **Remplacer la recherche Google** par un moteur de recherche qui ne vous piste pas (comme DuckDuckGo ou Qwant).
    - ☐ **Revoir régulièrement les autorisations des applications** sur votre smartphone. Une application de météo a-t-elle vraiment besoin d'accéder à vos contacts ?

(Conclusion) *Bravo ! En parcourant cette liste, vous avez fait plus pour votre sécurité numérique que la plupart des gens. N'oubliez pas que la cybersécurité n'est pas une destination, mais un processus continu. Restez curieux, restez vigilant !*