

Guide de Sécurité Numérique : Téléchargement et Navigation (Juin 2024)

1. Protection de la Connexion (VPN)

- Utilisez un VPN réputé avec une politique stricte de non-journalisation (no-logs).
- Activez systématiquement le 'Kill Switch' pour couper internet en cas de déconnexion du VPN.
- Privilégiez les serveurs situés dans des juridictions respectueuses de la vie privée.
- Vérifiez l'absence de fuites DNS via des outils en ligne avant de lancer vos transferts.

2. Sécurisation de l'Environnement Local

- Maintenez votre système d'exploitation et vos logiciels à jour pour corriger les failles de sécurité.
- Utilisez un antivirus actif avec une protection en temps réel et une analyse comportementale.
- Configurez un pare-feu (firewall) pour bloquer les connexions entrantes non sollicitées.
- Utilisez un compte utilisateur standard pour vos activités quotidiennes, et non un compte administrateur.

3. Bonnes Pratiques de Navigation et Téléchargement

- Installez une extension de navigateur pour bloquer les publicités et les scripts malveillants (ex: uBlock Origin).
- Vérifiez systématiquement les extensions de fichiers avant ouverture (.exe, .scr, .bat sont à proscrire).
- Analysez chaque fichier téléchargé avec un service multi-antivirus en ligne avant exécution.
- Privilégiez les sources communautaires vérifiées et évitez les sites aux publicités intrusives.

4. Hygiène Numérique Post-Téléchargement

- Videz régulièrement votre dossier de téléchargements pour éviter l'accumulation de fichiers inutilisés.
- Désactivez le partage automatique de fichiers après la fin de vos transferts.
- Effectuez des sauvegardes régulières de vos données sensibles sur un support externe déconnecté.
- Restez informé des menaces actuelles via des sites spécialisés en cybersécurité.