

Règles de navigation sécurisée

7 bonnes pratiques essentielles pour naviguer en toute sécurité sur Internet

1 Navigateurs sécurisés et à jour

Utilisez des navigateurs reconnus et activez les mises à jour automatiques.

3 Évitez les sites suspects

Ne cliquez pas sur des pop-ups inattendus ou des liens provenant de sources non vérifiées.

5 Effacez régulièrement les cookies

Nettoyez périodiquement les cookies et le cache du navigateur.

7 Ne pas enregistrer les mots de passe

Évitez d'enregistrer les mots de passe dans le navigateur. Utilisez un gestionnaire de mots de passe sécurisé.

2 Limiter les extensions

Installez uniquement les extensions officielles et limitez leur nombre.

4 Vérifiez le protocole HTTPS

L'adresse du site web doit commencer par : <https://>

6 Mode privé

Utilisez le mode de navigation privée pour des connexions nécessitant de la confidentialité.

Outils de vérification des sites web

Google Transparency Report

Offre des informations sur la sécurité d'un site, signalant les sites potentiellement malveillants.

- ✓ Détection des sites malveillants
- ✓ Suivi des tentatives de phishing
- ✓ Rapports de sécurité réguliers

Mozilla Observatory

Outil qui teste la configuration de sécurité d'un site web et fournit des recommandations.

- ✓ Analyse des paramètres de sécurité
- ✓ Recommandations pour améliorer la robustesse
- ✓ Note de sécurité interactive

Whois Lookup

Permet de vérifier l'origine et les informations d'enregistrement d'un site web.

- ✓ Identification des sites frauduleux
- ✓ Vérification de l'authenticité du propriétaire
- ✓ Consultation des dates d'enregistrement

Règles essentielles de téléchargement

7 règles fondamentales pour garantir la sécurité lors des téléchargements

1 Sources officielles

Téléchargez exclusivement depuis les sites officiels des fabricants, les App Stores ou le Microsoft Store.

3 Analyse préalable

Scannez exclusivement les fichiers téléchargés avec un antivirus avant de les ouvrir.

5 Lecture des commentaires

Avant d'installer un logiciel libre, consultez les commentaires et les évaluations des autres utilisateurs.

7 Actifs antivirus et antimalware

Assurez-vous qu'un antivirus et un antimalware sont constamment actifs et à jour sur l'appareil.

2 Éviter les liens suspects

Ne jamais télécharger à partir de liens trouvés dans des forums non vérifiés ou des courriels non sollicités.

4 Vérification des extensions

Soyez vigilant face aux extensions de fichiers potentiellement dangereuses telles que .exe, .bat ou .scr.

6 Mises à jour régulières

Maintenez tous les logiciels à jour pour bénéficier des correctifs de sécurité et prévenir les vulnérabilités.

Outils d'analyse et de protection

Virus Total

Permet d'analyser un fichier ou un lien suspect en utilisant plusieurs moteurs antivirus pour détecter les menaces cachées.

Antivirus/Antimalware

Des solutions comme Windows Defender, Bitdefender ou Malwarebytes sont essentielles pour la détection et la suppression des menaces.

Any.run

Offre la possibilité d'analyser le comportement d'un fichier dans un environnement isolé (**sandbox**) pour détecter des activités malveillantes.

Ninite.com

Une plateforme sécurisée qui permet d'installer et de mettre à jour plusieurs logiciels populaires sans les adwares ou barres d'outils indésirables.