INTERNET

Principaux risques et conseils pour les éviter

Qu'est-ce qu' « *Internet* » ?

Issu de la contraction des mots anglais « *Interconnected* » *(interconnecté) et « Network* » (réseau), Internet est un vaste réseau informatique mondial qui relie des millions d'ordinateurs, de serveurs et autres dispositifs, permettant le transfert de données à travers des protocoles de communication standardisés.

C'est un moyen d'accès à de multiples ressources, un canal de communication et un lieu d'échanges.

Les comportements à éviter :

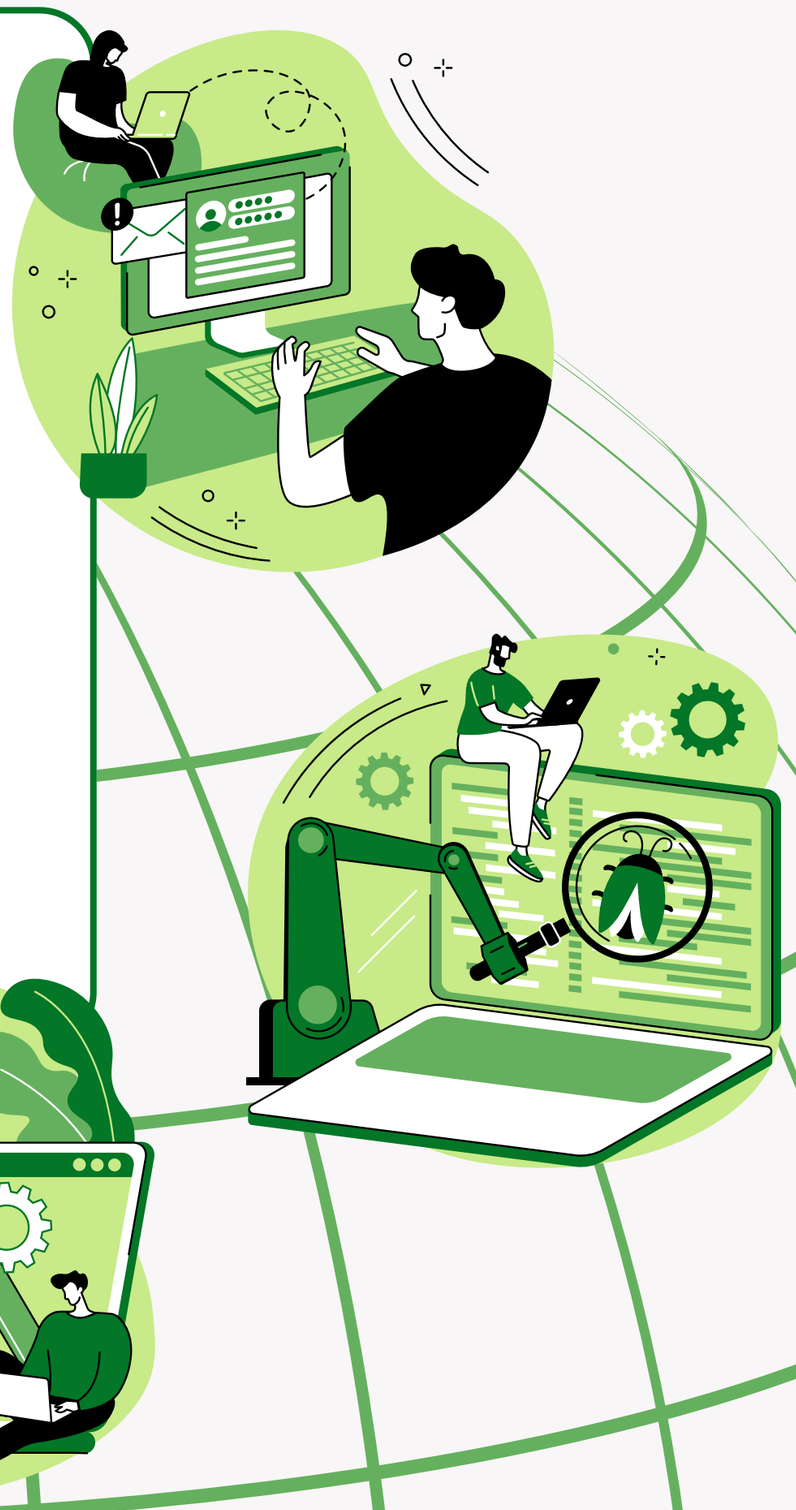
- Ne pas partager des données personnelles et/ou confidentielles
- Ne pas utiliser de réseaux WIFI publics ou inconnus
- Ne pas ouvrir de pièces jointes, ni de liens suspects
- Ne pas télécharger de fichiers, de logiciels, etc., à partir de sources inconnues ou non vérifiées

Pourquoi éviter ces comportements ?

Il existe une multitude de risques sur Internet, dont diverses arnaques et fraudes, qui souvent peuvent être évités ou du moins atténués en adoptant de bonnes pratiques. Parmi les risques les plus communs :

- Le hameçonnage (dit phishing),
- Les rançongiciels,
- Les faux supports techniques,
- Le piratage:
  - vol de données (y compris personnelles et/ou confidentielles),
  - vol d'identité,
- La collecte massive de données,
- La revente des données collectées à des tiers.

Pour plus d'information voir la fiche pratique « *Lexique du parfait hacker* »

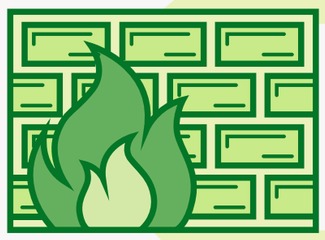


Quelles sont les bonnes pratiques sur Internet ?

Les 9 conseils à suivre pour se protéger sur Internet :

Sécuriser sa connexion Internet :

- activer un pare-feu
- chiffrer le réseaux wifi



Utiliser un VPN « *virtual private network* », dit réseau privé virtuel

Vérifier que le site web est sécurisé « *HTTPS* »

Mettre en place un antivirus et un logiciel anti-malware

Mettre à jour régulièrement le système d'exploitation et les logiciels ou applications du terminal (ordinateur, tablette, téléphone, etc.)

Vérifier et contrôler régulièrement les paramètres de confidentialité des applications et navigateurs Internet utilisés

Opter pour des mots de passe forts et uniques, comprenant au minimum 12 caractères, une majuscule, un caractère spécial et un chiffre

Opter pour l'authentification multifactorielle. La mise en place de plusieurs protocoles d'authentification permet en effet une meilleure sécurité en cas de tentative de piratage

Effectuer régulièrement des sauvegardes de ses données sur un ou plusieurs disque(s) dur(s) externe(s)