Cybersécurité

Sécuriser son ordinateur et protéger ses données

CONSEILLER NUMÉRIQUE

Les comptes utilisateurs

Limitez les risques avec des comptes adaptés

Compte Administrateur

Usage restreint et ponctuel

- Installation/désinstallation de logiciels et mises à jour système
- Modification des paramètres critiques de l'ordinateur
- Doit être protégé par une authentification forte (mot de passe, code PIN...)
- À utiliser uniquement pour les tâches administratives, jamais pour naviguer

Compte Standard

Usage quotidien

- Navigation web, bureautique, lecture d'emails et multimédia
- Réduit l'impact des logiciels malveillants (droits limités)
- Empêche l'installation accidentelle de programmes indésirables
- Principe du moindre privilège : juste les droits nécessaires

L'antivirus : Un seul suffit !

N'installez jamais deux antivirus

- Conflits entre les antivirus
- Ralentissement de l'ordinateur
- Faux positifs et alertes incohérentes
- Protection moins efficace
- Instabilité du système

Les antivirus payants

Utiles pour leurs fonctionnalités étendues :

- VPN inclus,
- Gestionnaire de mots de passe,
- Contrôle parental avancé,
- Protection bancaire spécifique.

Microsoft Defender

- Inclus nativement dans Windows
- Suffisant pour un usage quotidien
- Protection en temps réel
- Excellents taux de détection
- Protection anti-ransomware
- Protection contre les sites et fichiers malveillants (virus, phishing, etc)
- Pare-feu intégré
- Mise à jour automatique

Comparez les antivirus

av-comparatives.org

Les applications

Téléchargez et utilisez vos logiciels en toute sécurité

Sources Officielles

Téléchargez toujours vos logiciels depuis le site officiel de l'éditeur.

Évitez les plateformes tierces qui repackagent les installateurs.

Mises à jour Automatiques

Activez les mises à jour automatiques pour votre système d'exploitation et vos applications afin de corriger les failles de sécurité dès leur découverte.

Analyse Préventive

Scannez systématiquement tout fichier téléchargé avec votre antivirus.

En cas de doute, utilisez un outil en ligne comme VirusTotal avant l'exécution.

Vigilance

Bannissez les logiciels piratés (cracks) vecteurs de malwares.

Lors de l'installation, décochez les offres optionnelles (bundles) souvent indésirables.

Les navigateurs

Protégez votre vie privée en ligne

Recommandés

Confidentialité par défaut

- Firefox : Open-source et modulaire
- LibreWolf : Version durcie de Firefox
- Brave : Bloqueur de publicités intégré
- Tor Browser : Confidentialité et anonymat

Performance vs. confidentialité

Collecte intensive de donnée

- Google Chrome : Le géant de la collecte à but publicitaire
- Microsoft Edge : Télémétries techniques et d'usage.

Pour séparer vos usages vous pouvez utiliser deux navigateurs.

Les moteurs de recherche

Alternatives respectueuses de votre vie privée pour échapper au profilage publicitaire

DuckDuckGo

- Moteur de recherche américain
- Résultats issus de sources tel que Yahoo, Bing et de son propre index
- N'enregistre ni l'adresse IP, ni les cookies, ni les données des utilisateurs

Mojeek

- Moteur britannique indépendant
- Index 100% autonome
- Confidentialité et absence de suivi

Qwant

- Moteur de recherche français
- Résultats issus de Bing et de son propre index
- Développe avec Ecosia un index européen commun

Swisscows

- Moteur de recherche suisse
- Dispose de son propre index de recherche tout en s’appuyant sur Bing et Brave Search
- Sans contenus violents et pornographiques

Les mots de passe

Des mots de passe robustes et uniques

Les règles d'or

- **15 caractères minimum**
- **Complexité variée**
  Mélangez majuscules, minuscules, chiffres et caractères spéciaux (ex: T7#pL9@mX2!vE4*).
- **Un mot de passe unique par service.**
- **À bannir impérativement**
  Dates de naissance, noms d'animaux, "azerty", "123456" ou mots du dictionnaire seuls.

Testez vos mots de passe

Combien de temps faut-il à un cybercriminel pour le trouver ?

https://fantomapp.fr

La solution : Les gestionnaires

Utilisez un coffre-fort numérique sécurisé pour générer et stocker vos mots de passe.

bitwarden

KeePassXC

La messagerie électronique

Une messagerie sécurisée et organisée

Choix du fournisseur

Évitez les adresses liées à votre FAI (Orange, SFR...) pour ne pas être bloqué en cas de changement.

Privilégiez des services sécurisés comme ProtonMail, Tutanota, Infomaniak ou Mailo.

Vigilance avec les pièces jointes

Soyez alerte face aux fichiers suspects et aux extensions doubles (ex: fichier.txt.exe).

N'ouvrez jamais une pièce jointe inattendue sans vérification préalable.

Gestion par "Alias"

Protégez votre adresse principale en utilisant des alias pour vos inscriptions et newsletters. Cela permet de séparer les usages (pro/perso) et de filtrer le spam.

Vérification des liens

Les liens raccourcis peuvent masquer des sites malveillants.

Utilisez un outil comme **unshorten.it** pour révéler la destination réelle avant de cliquer.

Sauvegarder ses données

Ne perdez jamais vos documents importants

La stratégie 3-2-1

3 Copies totales
Conservez toujours 3 exemplaires de vos fichiers : 1 original et 2 sauvegardes.

2 Supports différents
Diversifiez les technologies pour réduire les risques (ex: Disque dur externe + Cloud).

1 Copie hors site
Une sauvegarde doit être physiquement ailleurs (Cloud ou disque chez un proche) contre le vol/incendie.

Quoi sauvegarder ?

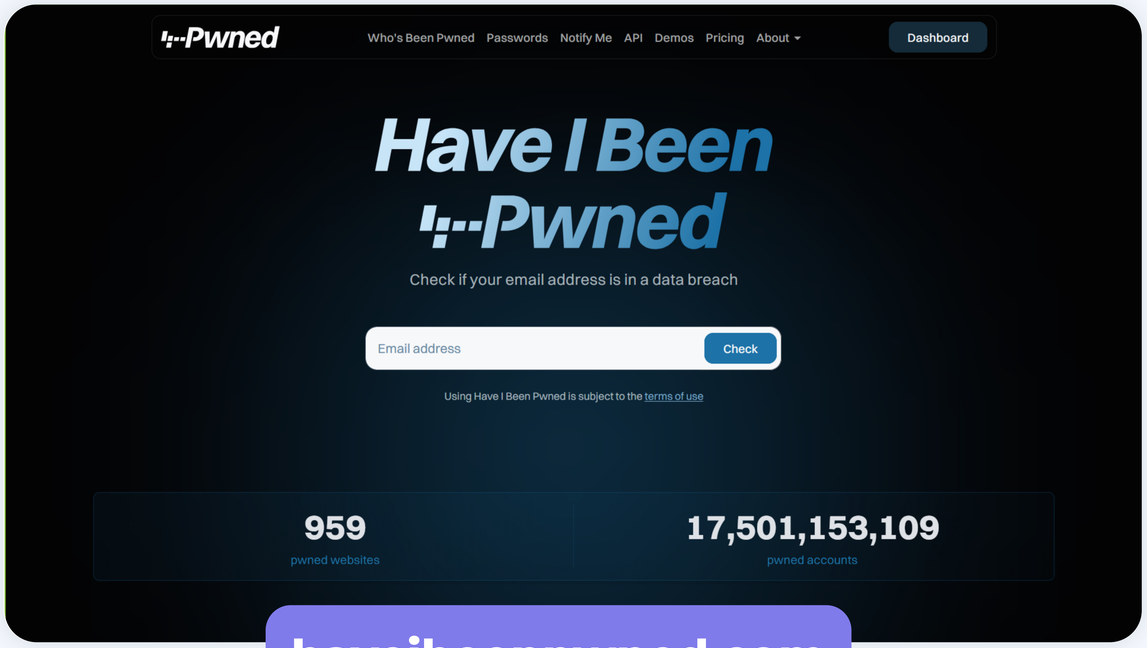
- **Documents critiques**
  (Papiers d'identité, doc. administratifs, doc. bancaires, contrats divers, etc.)
- **Fichiers de travail, projets personnels...**
- **Photos, vidéos & souvenirs irremplaçables**
- **Image système / configuration.**

Déconnexion impérative

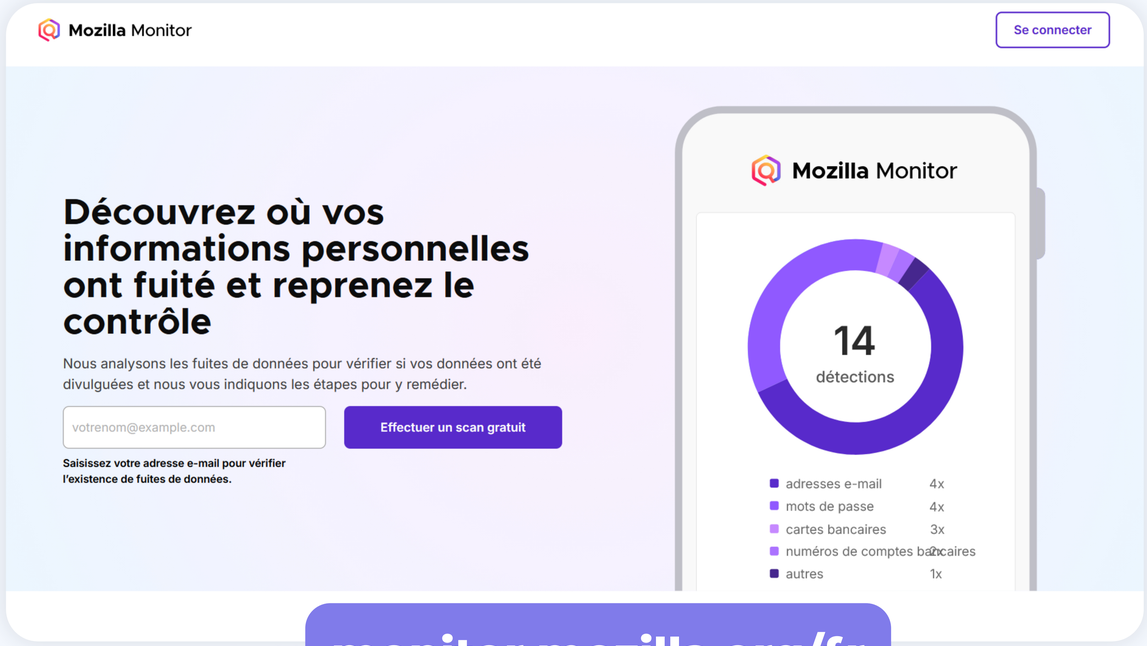
Débranchez vos disques USB après usage pour éviter qu'un ransomware ne les chiffre aussi.

Outils pour vérifier si vos identifiants* sont compromis

*Adresses mails et mots de passe



haveibeenpwned.com



monitor.mozilla.org/fr

Les fuites de données exposent vos informations personnelles (mots de passe, adresses e-mail, etc.). Elles augmentent les risques de piratage, de spam ou d'usurpation d'identité.

Vous avez des questions ?

A bientôt !

CONSEILLER NUMÉRIQUE