

Le navigateur, votre outil le plus exposé : le sécuriser

Tout passe par lui — recherches, banque, outils métier. Extensions, profils, réglages : le durcir en une heure.

7 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/navigateur-securise

Le navigateur est devenu LE poste de travail : messagerie, banque, CRM, cloud — tout y transite. C'est donc la cible idéale : pages piégées, fausses extensions, vols de sessions. Bonne nouvelle : les navigateurs modernes sont robustes, et l'essentiel des risques vient de leur configuration et de ce qu'on y greffe. Une heure de ménage suffit à changer la donne.

1. Les fondamentaux

- Un navigateur moderne et À JOUR (Chrome, Edge, Firefox) — la mise à jour automatique ne se désactive jamais
- La navigation protégée activée (Safe Browsing / protection renforcée) : elle bloque une grande partie des sites malveillants connus
- Le remplissage des mots de passe confié au gestionnaire d'entreprise, pas au navigateur en mode « libre » — et jamais de carte bancaire enregistrée sur les postes partagés
- HTTPS partout : un avertissement de certificat sur un site connu ne se contourne pas, il se signale

2. Les extensions : le vrai maillon faible

Chaque extension a potentiellement accès à tout ce que vous faites dans le navigateur — lecture des pages, saisies, cookies. Des extensions populaires ont déjà été rachetées puis transformées en logiciels espions via une simple mise à jour.

- L'inventaire d'abord : passez en revue les extensions installées sur chaque poste — il y a toujours des surprises
- La règle du strict nécessaire : chaque extension doit se justifier ; le reste se supprime
- Sources et permissions : uniquement les stores officiels, et méfiance devant une extension qui demande « l'accès à toutes les données sur tous les sites » pour un service anodin
- En entreprise : les navigateurs se gèrent centralement (liste d'extensions autorisées) via les outils Microsoft/Google — pertinent dès quelques postes

ATTENTION

Le faux convertisseur PDF, le « super bloqueur de pub » inconnu, l'extension coupon miracle : les extensions malveillantes se déguisent en utilitaires banals. Une fois installées, elles lisent tout — y compris vos sessions bancaires. Dans le doute, on n'installe pas : le besoin réel trouve presque toujours une réponse dans un outil établi.

3. Séparer les usages avec les profils

Les navigateurs gèrent des profils distincts — chacun avec ses comptes, extensions, cookies et historique. Utilisés correctement, ils cloisonnent : un profil « travail » (comptes pro, extensions validées) séparé du profil « perso » évite qu'un site douteux visité en pause déjeuner côtoie la session de la banque de l'entreprise. Sur un poste partagé, chaque personne a son profil, et l'invité une session... d'invité.

4. Les pièges de navigation courants

- Les fausses alertes « votre PC est infecté, appelez ce numéro » : fermez l'onglet (Ctrl+W ou gestionnaire de tâches), n'appellez jamais — c'est le point d'entrée de l'arnaque au faux support
- Les notifications de sites : n'acceptez pas les demandes de notifications par réflexe — des sites malveillants en abusent pour pousser de fausses alertes système
- Les résultats sponsorisés trompeurs : les fraudeurs achètent des publicités imitant des sites connus — vérifiez l'adresse ou passez par vos favoris pour les sites sensibles
- Le téléchargement de logiciels : uniquement depuis l'éditeur officiel — les sites « de téléchargement » regroupent l'utile et l'infecté

L'essentiel à retenir

- 01 Mettre à jour le navigateur automatiquement, partout
- 02 Faire l'inventaire des extensions et supprimer le superflu
- 03 Confier les mots de passe au gestionnaire d'entreprise
- 04 Créer des profils séparés travail / personnel
- 05 Mettre les sites sensibles (banque...) en favoris et n'y accéder que par là
- 06 Former aux fausses alertes et aux résultats sponsorisés trompeurs

Questions fréquentes

Quel navigateur est le plus sûr ?

Les trois grands (Chrome, Edge, Firefox) offrent un excellent niveau à jour et bien configurés — l'écart entre eux est marginal comparé à l'écart entre un navigateur à jour et un navigateur obsolète. Choisissez selon votre écosystème, standardisez sur un ou deux navigateurs dans l'entreprise, et concentrez l'énergie sur extensions et mises à jour.

Le mode navigation privée protège-t-il ?

Il efface l'historique local en fermant la fenêtre — c'est tout. Il ne rend pas anonyme, ne protège pas des sites malveillants et n'empêche pas l'interception sur un réseau douteux. Utile pour un poste partagé ponctuellement, il ne remplace ni les profils ni les vraies protections.

Un bloqueur de publicité est-il recommandé en entreprise ?

Un bloqueur réputé (uBlock Origin) réduit réellement la surface d'attaque : moins de publicités, c'est moins de « malvertising » (publicités piégées) et de faux résultats sponsorisés. Comme toute extension, il se choisit une fois, officiellement, pour tout le monde — plutôt que dix bloqueurs exotiques installés au hasard.

Pour aller plus loin

Cybermalveillance.gouv.fr — naviguer sur Internet en sécurité — www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/usages-web

ANSSI — Guide d'hygiène informatique — cyber.gouv.fr/publications/guide-dhygiene-informatique

Besoin d'aide pour le mettre en place ?

Audit, durcissement, accompagnement : Cyberionis sécurise les TPE, PME et collectivités, à Nancy, Lure et à distance.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr