# Les navigateurs privés sont-ils vraiment privés et Conseils pour une navigation sécurisée

***NDMC: J'utilise et recommande le gestionnaire de mots de passe Dashlane***

Dashlane :

À l'heure où nos activités de recherche en ligne sont de plus en plus suivies et vendues, il n'est pas étonnant que les préoccupations relatives à la confidentialité en ligne soient dans tous les esprits.
Les internautes se tournent de plus en plus vers les options de navigation privée, mais les navigateurs privés sont-ils vraiment privés ?
Intéressons-nous de plus près au fonctionnement des navigateurs privés, ce qu'ils sont en mesure de faire ou pas pour assurer la sécurité et la confidentialité de vos sessions de navigation ainsi que les actions supplémentaires que vous pouvez entreprendre pour améliorer votre confidentialité et votre cybersécurité en ligne.

## Qu'est-ce qu'un navigateur privé ?

Les modes de protection de la vie privée offerts par les navigateurs Web populaires portent de nombreux noms différents, notamment InPrivate (Edge), Fenêtre privée (Opera) et Mode incognito (Chrome).
Tous offrent des fonctions et des fonctionnalités similaires.
En outre, de nouveaux moteurs de recherche comme Neeva offrent en permanence une expérience privée dénuée de publicités qui vous protège également des traqueurs.

La navigation privée est un excellent moyen d'empêcher votre ordinateur de stocker des données temporaires lorsque vous partagez l'accès à votre ordinateur, mais elle présente certaines limites.

### À quoi sert la navigation privée ?

- **Elle empêche le suivi de l'historique de navigation**

Le mode incognito fonctionne-t-il vraiment ?
La plupart des navigateurs enregistrent automatiquement et en permanence votre historique lorsque vous naviguez sur le Web.
Lorsque vous naviguez en mode privé ou incognito, votre historique de navigation est instantanément supprimé à la fermeture du navigateur.

Ainsi, vous n'encombrez pas votre disque dur et vous pouvez partager votre ordinateur avec d'autres personnes en toute sécurité, même s'il devient alors plus difficile de retrouver un site Web que vous avez précédemment visité.

- **Elle supprime les cookies à la fermeture du navigateur**

Les cookies enregistrés sur votre ordinateur, appelés à l'origine des cookies magiques, sont de petits morceaux de données laissés sur votre navigateur Web pour aider un site Web à se souvenir de vous (et de vos préférences) en vue de futures sessions.
Lorsque vous êtes en mode privé, les cookies que vous accumulez pendant votre session de navigation sont commodément supprimés à la fermeture de votre navigateur.
La suppression périodique des cookies enregistrés sur votre ordinateur est une bonne pratique de cybersécurité.
La suppression automatique des cookies en mode de navigation privée présente donc un avantage accessoire.

- **Elle saisit automatiquement les mots de passe des utilisateurs**

En plus des modes de navigation privée, la plupart des navigateurs populaires offrent également des gestionnaires de mots de passe intégrés qui enregistrent et saisissent automatiquement les mots de passe des utilisateurs, pour plus de commodité.
Comme la plupart de ces gestionnaires de mots de passe intégrés ne chiffrent pas (brouillent) les données afin de les protéger, il est préférable de les éviter.
Les gestionnaires de mots de passe intégrés de certains navigateurs vous permettront de saisir automatiquement les mots de passe précédemment enregistrés lorsque vous naviguez en mode privé, mais tous les nouveaux identifiants que vous enregistrez pendant la session privée seront effacés, au même titre que les cookies et l'historique de suivi.

## Les limites de la navigation privée

- **Elle n'empêche pas votre FAI de voir votre emplacement ni les sites Web que vous avez visités**

Dans quelle mesure le mode incognito est-il sécurisé ?
Une idée fausse très répandue est que la navigation incognito empêche votre fournisseur d'accès à Internet (FAI) de savoir quels sites vous avez visités ou encore où vous étiez au moment de votre connexion.
Le mot incognito vient du terme latin « inconnu ».
Or, votre historique de navigation et votre emplacement sont toujours connus de votre FAI, de votre employeur ou de votre école, en fonction du réseau sur lequel vous êtes connecté.

- **Elle ne vous protège pas des virus**

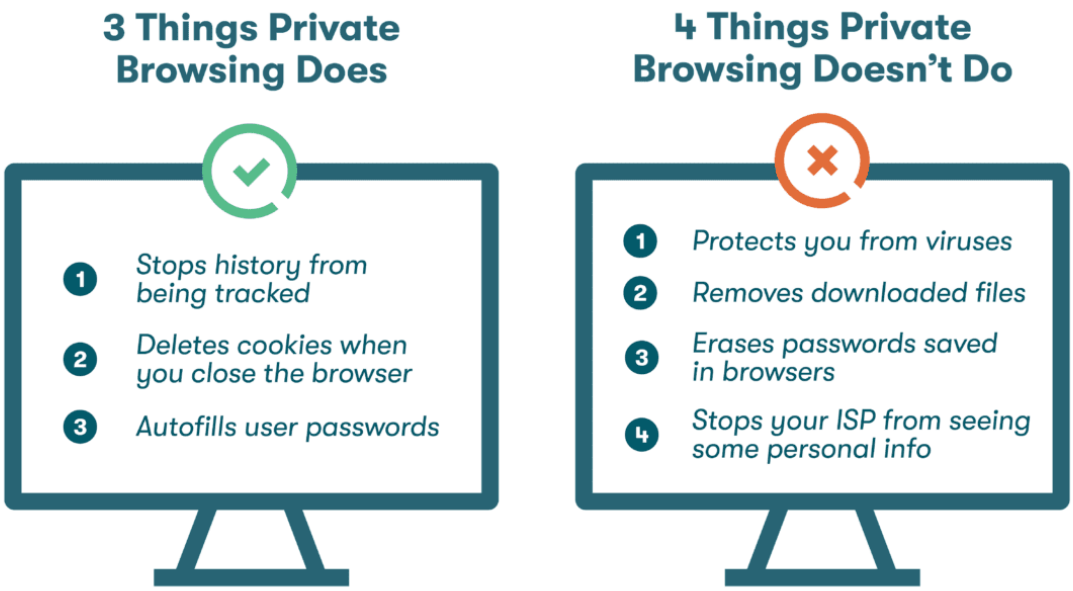
Le mode incognito est-il à l'abri des logiciels malveillants ?
Bien que les cookies et d'autres données des sites visités soient instantanément supprimés à la fermeture d'une session privée, ce n'est pas le cas des virus ou des logiciels malveillants auxquels votre système a été exposé.
Les logiciels espions installés sur votre appareil pourront toujours suivre votre activité en mode incognito.
Pour vous protéger des virus et des logiciels malveillants, assurez-vous d'activer votre logiciel antivirus en permanence et faites preuve de prudence lorsque vous cliquez sur des liens provenant de sources inconnues.

- **Elle ne supprime pas complètement les fichiers téléchargés**

Le postulat de départ des navigateurs privés implique une fenêtre « propre » à chaque nouvelle session.
Certaines personnes peuvent donc croire que les fichiers qu'elles téléchargent ou les signets qu'elles créent seront également supprimés.
Ce n'est toutefois pas le cas.
Ces fichiers seront toujours stockés sur votre disque dur lorsque vous quitterez le mode incognito : les fichiers téléchargés que vous choisissez de ne pas enregistrer doivent donc être supprimés manuellement.

- **Elle n'efface pas automatiquement les mots de passe enregistrés sur les navigateurs**

Bien que vous ne puissiez pas enregistrer de nouvelles informations en mode privé, les mots de passe que vous avez précédemment enregistrés dans votre navigateur devraient être effacés dès que vous avez trouvé une option plus sûre, comme un gestionnaire de mots de passe autonome sécurisé.
Les mots de passe, les noms d'utilisateur, les numéros de carte bancaire et les informations de compte non chiffrés enregistrés sur les navigateurs peuvent être exposés lors d'une cyberattaque.




## Les navigateurs privés sont-ils vraiment sécurisés ?

Une autre idée fausse au sujet de la navigation privée est qu'elle améliore votre cybersécurité en masquant certains aspects de votre activité.
La navigation privée n'est pas aussi privée que nous pourrions le penser : notre activité en ligne peut toujours être suivie, quels que soient les paramètres que nous choisissons ou les logiciels que nous déployons.
Voici ce que vous devriez savoir :

### Mode incognito

Qu'est-ce que le mode incognito ?
Le mode privé de Google Chrome, le mode incognito, commence chaque session de navigation privée dans une fenêtre séparée.
Toutes les fenêtres incognito supplémentaires que vous ouvrez ensuite s'intègrent à cette session.

- Votre navigateur cesse de suivre les sites Web que vous visitez dès que la session incognito commence.
- En mode incognito, vous devez vous connecter manuellement à vos comptes, même si vos identifiants ont été précédemment enregistrés dans votre navigateur.
- Les extensions de navigateur que vous avez installées ne fonctionneront pas, à moins que vous ne les ayez activées avant de passer en mode incognito.

### Surveillance de l'activité au travail

Si votre appareil est relié au réseau de votre entreprise de manière directe ou par l'intermédiaire de son réseau privé virtuel (VPN), le service informatique de votre employeur peut surveiller votre activité, même en mode privé.
En effet, la navigation privée ne supprime les détails de votre historique de navigation qu'après la session, et non pendant celle-ci.
Une meilleure option est de toujours limiter les activités non professionnelles aux appareils non professionnels.

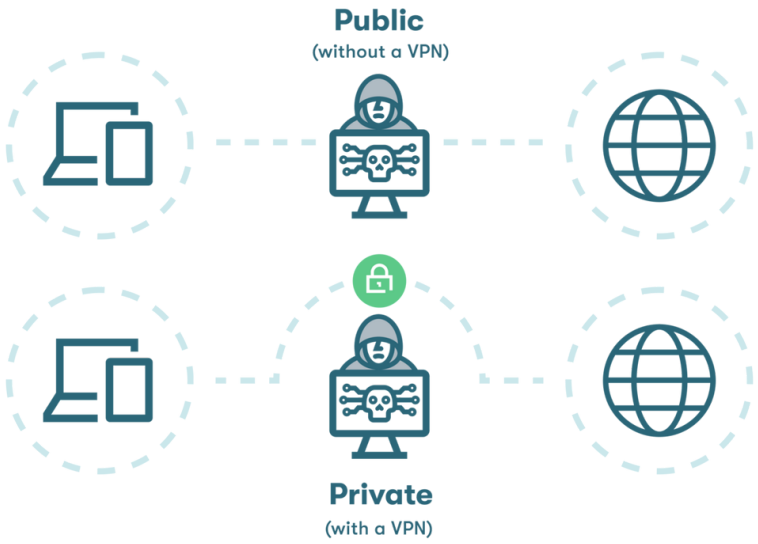
### Les navigateurs privés ne sont pas vraiment privés

Dans le fond, ce qu'il faut retenir c'est que l'activité en ligne n'est pas vraiment privée. Même en mode privé, le destinataire peut toujours voir votre adresse IP, car il a besoin de ces informations pour communiquer avec vous.
Ces empreintes numériques et le manque inhérent de confidentialité en ligne sont utiles pour les enquêteurs et les équipes informatiques lorsqu'ils cherchent la trace des pirates et d'autres cybercriminels.

## Conseils pour une navigation sécurisée avec les navigateurs Internet privés

La navigation privée ne protège pas vos données personnelles, vos mots de passe ou votre identité, mais elle peut offrir une sécurité accrue dès lors que vous comprenez comment utiliser les paramètres de votre navigateur privé avec la bonne combinaison d'outils et de pratiques cybernétiques.

1. **Utilisez un VPN :** lorsque vous utilisez un VPN, toute communication vers ou depuis votre appareil est acheminée via un portail sécurisé et chiffré sur un serveur privé.
   Le VPN agissant comme intermédiaire, votre adresse IP est masquée et votre emplacement et votre identité ne peuvent pas être suivis.
   Un VPN est surtout utile lorsque vous accédez à un service Wi-Fi public dans les aéroports, les cafés ou d'autres lieux publics.
   Le chemin sécurisé qu'il crée vous protège également des tactiques de piratage telles que les attaques de type « homme du milieu », élaborées pour intercepter des données dans ces lieux publics.




2. **Ne partagez pas vos comptes, vos mots de passe ni vos ordinateurs avec d'autres personnes :** la meilleure façon de garantir la confidentialité de vos mots de passe, de vos données personnelles et de vos appareils est de vous assurer que personne d'autre que vous n'y a accès (ou ne peut en obtenir l'accès).
   Cela se traduit par l'utilisation exclusive de votre propre ordinateur et de vos autres appareils autant que possible et le bannissement des notes autocollantes ou des bouts de papier lorsque vous devez partager vos mots de passe.
   Même les plates-formes de messagerie électronique et de communication telles que Slack ne présentent pas des options de qualité supérieure lorsqu'il s'agit de partager des mots de passe : les informations non chiffrées y sont enregistrées indéfiniment et peuvent être exposées lors d'une faille de données.
   Un portail de partage de mots de passe quant à lui offre un moyen sécurisé de partager des mots de passe pour, entre autres, les réseaux Wi-Fi, les services d'abonnement, les comptes de commerces au détail et les outils numériques avec vos amis, votre famille et vos collègues sans pour autant compromettre votre vie privée ni votre cybersécurité.
   Il vous permet également de suivre les informations que vous avez partagées et d'envoyer des mises à jour automatiquement.
3. **Utilisez une connexion Internet sécurisée :** que vous utilisiez un réseau Wi-Fi public,
   un réseau Wi-Fi à domicile ou un réseau câblé, vous devez vous assurer que votre connexion Internet est sécurisée à l'aide d'un système de chiffrement pour préserver votre confidentialité.
   Vous pouvez le vérifier en accédant au menu des paramètres de votre ordinateur ou de votre appareil, puis en sélectionnant « Wi-Fi ».
   Si votre réseau est sécurisé, un symbole de verrou se trouve à côté du symbole Wi-Fi.
   Heureusement, les navigateurs sont dotés de fonctionnalités intégrées pour déterminer si une connexion est sécurisée, et les systèmes d'exploitation les plus courants (Windows, macOS, iOS et Android) vous avertissent si des problèmes de sécurité sont détectés dans le réseau sans fil local.
4. **Utilisez une extension de navigateur de gestionnaire de mots de passe :** l'installation d'un gestionnaire de mots de passe sur votre navigateur vous permet de bénéficier plus facilement des avantages en termes de confidentialité et de sécurité lorsque vous naviguez sur Internet et que vous générez, enregistrez et saisissez automatiquement les mots de passe pour vos comptes préférés.
   Une fois l'extension du navigateur installée et votre compte de gestionnaire de mots de passe connecté, les mots de passe, les numéros de compte et toute autre information seront automatiquement enregistrés sans aucune étape supplémentaire.

De nombreuses extensions de gestionnaire de mots de passe fonctionneront même en mode privé, à condition que vous les ayez activées à l'avance.

## Navigation privée et gestion sécurisée des mots de passe

La navigation privée apporte davantage de confort d'utilisation en supprimant automatiquement les cookies et l'historique de navigation à chaque session.
Les fonctionnalités avancées du gestionnaire de mots de passe Dashlane ajoutent une couche de sécurité à la navigation incognito grâce au chiffrement AES-256 avancé, à la double authentification (2FA) et à des portails sécurisés pour le stockage et le partage de mots de passe.

L'architecture « zero-knowledge » signifie que Dashlane ne stocke vos mots de passe chiffrés que sur des serveurs cloud hébergés hautement sécurisés, où personne, pas même les employés de Dashlane, ne peut voir ni modifier vos informations.
Notre VPN masque votre adresse IP tout en fournissant sécurité et commodité dans les environnements publics et notre outil de surveillance du dark Web vérifie si vos informations ont été exposées sur le dark Web.

**L'utilisation d'un gestionnaire de mots de passe protège votre vie privée ainsi que vos données.**
**Découvrez à quel point il est facile d'améliorer vos connaissances en matière de sécurité des données en consultant** Notre guide sur la confidentialité des données**.**

## Références


1. Dashlane, « Dashlane et Neeva s'associent pour sécuriser davantage la recherche en ligne » novembre 2022.
2. Dashlane, « How Safe Is Incognito Mode/Private Browsing, Really? », février 2020.
3. TrendMicro, « Cookies Definition », 2023.
4. Dashlane, « Can You Trust Your Web Browser with Your Passwords ? », décembre 2019.
5. Dashlane, « What the Hack Is Malware? », février 2020.
6. Dashlane, « Comment supprimer les mots de passe enregistrés sur un navigateur : Guide étape par étape », novembre 2022.
7. Dashlane, « Gestionnaire de mots de passe personnel fiable », 2023.
8. Google, « How Chrome Incognito keeps your browsing private », 2023.
9. Dashlane, « Why Employees Shouldn't Let Browsers Save Their Passwords » mars 2021.
10. CNN, « Private browsing may not protect you as much as you think », juillet 2022.
11. Dashlane, « You Asked, A Hacker Answered: 7 Questions With Rachel Tobac », octobre 2021.
12. Dashlane, « Pourquoi avez-vous besoin d'un VPN ? Ses 3 grands avantages pour votre sécurité », août 2020.
13. Dashlane, « Le partage de mots de passe sur Slack : une pratique risquée », novembre 2019.
14. Dashlane, « Partager vos éléments enregistrés dans Dashlane », 2023.
15. Dashlane, « How Do I Use Dashlane in My Browser? », janvier 2020.
16. Dashlane, « A Deep Dive into Dashlane's Zero-Knowledge Security », juin 2022.
17. Dashlane Dark Web Monitoring: Your Employees Are Likely Using Compromised Passwords », juillet 2022.
18. Dashlane, « A Beginner's Guide to Two-Factor Authentication », août 2022.
19. Dashlane, « Notre guide sur la confidentialité des données », 2023.
20. Dashlane, « La sécurité avant tout : comment Dashlane protège vos données », janvier 2023.



*Recherche et mise en page:*
*Michel Cloutier*
*CIVBDL*

*20230731*
*"C'est ensemble qu'on avance"*