

# VPN – Réseau privé virtuel

Internet nous rend de plus en plus transparents. Les informations que nous révélons à travers notre comportement sur Internet, comme par exemple les recherches que nous effectuons, sont utilisées par les entreprises et par les cybercriminels pour nous profiler à des fins commerciales (analyses de marché, etc.) ou criminelles (arnaques). Un VPN permet d'empêcher que vos données soient interceptées ou surveillées.

## Conseils pour l'utilisation des services VPN

- Choisissez un fournisseur de VPN fiable et sérieux, comme p. ex. [ProtonVPN \(https://protonvpn.com/fr/\)](https://protonvpn.com/fr/), [NordVPN \(https://nordvpn.com/fr/\)](https://nordvpn.com/fr/) ou [ExpressVPN \(https://www.expressvpn.com/fr/\)](https://www.expressvpn.com/fr/)
- Sachez qu'un VPN ne permet pas d'assurer une sécurité à 100%
- Tenez compte du fait que le service ne permet de sécuriser que la connexion entre votre appareil et le serveur VPN.

## VPN: un tunnel d'échange de données «sécurisé» pour naviguer sur Internet

Lorsqu'un internaute se rend sur un site web ou une boutique en ligne, le navigateur établit une connexion directe avec le serveur correspondant. Un certain nombre de données, telles que la position géographique de l'utilisateur, sont ainsi directement transmises au serveur du site en question. Par contre, si le même site web est consulté via un service de VPN, celui-ci vient s'interposer dans la communication. Le navigateur contacte d'abord, via une connexion chiffrée, le fournisseur de VPN qui va, à son tour, se connecter avec le site web choisi. Mais attention : il faut prendre conscience du fait que la connexion entre le serveur VPN et le site web consulté ne sera pas forcément protégée.

Par ailleurs, il ne faut pas confondre un VPN avec une connexion sécurisée par «https». Le protocole «https» signifie uniquement que la communication entre votre navigateur et le site web consulté est chiffrée. Un VPN en revanche chiffre tout le trafic entre votre appareil et le serveur VPN, ce qui comprend également vos communications via email par exemple.

Un VPN peut être intégré dans les paramètres de votre appareil.

### Windows

Windows 11 dispose d'une fonctionnalité VPN intégrée qui permet de se connecter directement à un VPN («Paramètres VPN»), mais il est également possible d'utiliser le programme mis à disposition par le fournisseur de VPN. Dans tous les cas, vous devez choisir un fournisseur de VPN, tel que par exemple:

- [ProtonVPN \(notamment la version gratuite\) \(https://protonvpn.com/fr/\)](https://protonvpn.com/fr/)
- [NordVPN \(https://nordvpn.com/fr/\)](https://nordvpn.com/fr/)
- [ExpressVPN \(https://www.expressvpn.com/fr/\)](https://www.expressvpn.com/fr/)

## 🍏 macOS

Une fois l'application de VPN téléchargée et installée, MacOS offre également la possibilité d'utiliser et de gérer une connexion VPN intégré dans les Réglages réseau. Il est également possible d'utiliser le programme proposé par le fournisseur de VPN. Dans les deux cas, il faudra choisir un fournisseur de VPN, comme par exemple:

- [ProtonVPN \(notamment la version gratuite\) \(https://protonvpn.com/fr\)](https://protonvpn.com/fr)
- [NordVPN \(https://nordvpn.com/fr/\)](https://nordvpn.com/fr/)
- [ExpressVPN \(https://www.expressvpn.com/fr\)](https://www.expressvpn.com/fr)

## 📱 Smartphones et tablettes

Sur les dispositifs mobiles tels que smartphones et tablettes, il convient d'installer et d'utiliser l'application proposée par le fournisseur de VPN, comme par exemple:

- [ProtonVPN \(notamment la version gratuite\) \(https://protonvpn.com/fr\)](https://protonvpn.com/fr)
- [NordVPN \(https://nordvpn.com/fr/\)](https://nordvpn.com/fr/)
- [ExpressVPN \(https://www.expressvpn.com/fr\)](https://www.expressvpn.com/fr)

## Un VPN peut s'avérer particulièrement utile dans différentes situations:

- **Home office et télétravail:** lorsque vous travaillez depuis votre domicile ou depuis un autre endroit que votre bureau, un VPN vous permet de disposer d'un accès sécurisé au réseau de votre entreprise.
- **Protection de la vie privée:** les VPNs servent également à protéger votre activité en ligne des regards indiscrets. Vous pouvez empêcher les criminels ou les entreprises d'analyser votre comportement d'internaute en vue de vous proposer de la publicité ciblée ou d'accéder à vos données.
- **Navigation sur un wifi public:** les réseaux wifi publics ne sont généralement pas bien sécurisés. Un VPN vous permettra de mieux protéger vos données dans ce type de réseau.
- **À l'étranger:** utiliser un VPN vous permet de conserver votre anonymat en ligne. Lorsque vous vous connecterez depuis l'étranger, pendant vos vacances par exemple, vous pourrez ainsi regarder vos programmes télévisés sans aucune limitation. Dans les pays qui imposent de fortes restrictions d'accès à Internet, un VPN vous permettra de consulter des sites censurés. Il faut savoir aussi que les VPNs sont interdits dans certains pays. Il est donc essentiel d'en avoir conscience avant votre départ pour ne pas risquer d'enfreindre la loi locale. L'utilisation des VPNs est généralement prohibée dans les pays qui pratiquent la censure sur Internet.
- **Shopping en ligne:** un VPN peut également vous servir à faire des économies lorsque vous effectuez des achats sur Internet. Le simple fait de changer votre position géographique vous permet parfois de profiter d'offres disponibles uniquement dans tel ou tel autre pays.

N'oubliez pas qu'un VPN ne garantit pas une protection à 100 %, dans la mesure où il ne fait que déplacer la surface d'exposition aux attaques. S'il est vrai que vos données sont protégées entre votre appareil et le serveur VPN, celles-ci peuvent toujours être interceptées entre le serveur VPN et le site Web. Le fournisseur de VPN lui-même pourrait théoriquement accéder à vos données.

## Comment trouver le bon fournisseur de VPN?

Les réseaux virtuels privés connaissent une popularité croissante qui va de pair avec la multiplication du nombre de fournisseurs VPN. Avec l'arrivée constante de nouvelles firmes, choisir son VPN n'est pas une mince affaire. Un bon service de VPN doit disposer d'un système de chiffrement robuste, ne conserve pas de registre d'activités des utilisateurs et ne partage aucune donnée avec des parties tierces.

### Voici donc les critères à prendre en compte lors du choix d'un fournisseur de VPN:

- **Localisation du fournisseur de service:** vérifiez où se trouve le siège de la société. La loi concernant la protection des données peut être plus stricte dans certains pays. En règle générale, vos données seront mieux protégées dans des pays comme la Suisse ou l'Allemagne.
- **Réputation:** comparez les avis des utilisateurs en considérant non seulement les opinions positives, mais aussi négatives.
- **Chiffrement et protocoles de sécurité:** vérifiez la fiabilité du système de cryptage et du protocole de sécurité utilisés par le fournisseur. Il est donc recommandé de s'orienter vers un cryptage AES-256 par exemple et des protocoles de sécurité de type OpenVPN ou IKEv2.
- **VPN sans log:** choisissez un service VPN qui ne conserve pas les logs (journaux d'activité) de ses utilisateurs.

*Un VPN (Virtual Private Network) est une technologie qui crée un « tunnel » chiffré par lequel passe tout le trafic Internet entre votre dispositif et le serveur du fournisseur du service.*

*Un VPN est généralement utilisé pour connecter de manière sécurisée un dispositif via un réseau existant (non protégé), par exemple Internet, à un autre réseau (sécurisé), comme par exemple le réseau de l'entreprise. Les données échangées seront ainsi protégées par cryptage pendant leur transport (chiffrement de bout en bout).*