

GUIDE DE SOUVERAINETÉ NUMÉRIQUE

Fiches pratiques pour reprendre le contrôle
de votre vie numérique

Débutants & utilisateurs avancés



Méthode d'émancipation numérique
en 4 vagues



Gabriel Ananda



gabriel.ananda@mailo.com

Version 4.1

5 octobre 2026

Petite histoire de notre liberté numérique et pourquoi ces fiches sont une nécessité

Il fut un temps, pas si lointain, où Internet ressemblait à une immense bibliothèque et à une place publique à la fois. Un endroit où l'on partageait des connaissances, des fichiers, des idées, sans avoir à se demander qui écoutait, qui regardait, qui analysait. C'était l'époque des débuts du web : des forums, des blogs personnels, des pages web montées à la main, des logiciels libres échangés par passion. L'internaute était un acteur, un contributeur, parfois même un anonyme parmi d'autres anonymes.

À cette époque, l'utopie du réseau était simple : tout le monde pouvait parler à tout le monde, sans intermédiaire, sans surveillance, sans marchand.

L'âge d'or (naïf) de la liberté numérique

Le protocole TCP/IP, le World Wide Web de Tim Berners-Lee, les premiers navigateurs... tout avait été pensé pour l'ouverture et la décentralisation. On croyait (on voulait croire) que la technique, par nature, protégeait les individus. Les moteurs de recherche eux-mêmes se voulaient de simples index, pas des profilers.

C'est dans ce contexte qu'est née une génération d'internautes qui pensait que le réseau serait un rempart contre l'autorité et le commerce de masse.

La marchandisation : vous n'êtes plus un internaute, vous êtes un produit

Cette époque idyllique n'a pas duré. Très vite, quelques entreprises ont compris une chose fondamentale : l'attention et les données des utilisateurs valent de l'or.

Google, Facebook (Meta), Amazon, Microsoft, Apple n'ont pas gagné parce qu'ils avaient les meilleurs services, mais parce qu'ils ont transformé l'internaute en client potentiel permanent.

Chaque clic, chaque recherche, chaque vidéo regardée, chaque email lu est devenu une matière première pour construire un profil ultra-précis : vos opinions, vos faiblesses, vos désirs, vos habitudes, vos fréquentations. On ne se contente plus de vous proposer un service ; on vous invente des besoins, on vous pousse à la consommation, on vous enferme dans une bulle algorithmique.

Vous n'êtes plus libre. Vous êtes prédictible.

Les big tech ont capturé la quasi-totalité des usages quotidiens : la recherche web, la messagerie, le stockage de fichiers, la cartographie, les réseaux sociaux, la vidéo, la bureautique... Parfois gratuitement, parfois en échange de vos données, parfois en payant un abonnement... mais en restant toujours sous leur regard.

La surveillance de masse : quand les États s'en mêlent

Dans le même temps, les gouvernements – y compris ceux qui se disent démocratiques – ont compris l'intérêt stratégique de ce gigantesque mouchard. Le Cloud Act américain permet à Washington de réquisitionner des données stockées... même en Europe, si la maison mère est américaine. En France, en Allemagne, ailleurs, les lois sur le renseignement se sont élargies. Les fournisseurs d'accès sont mis à contribution. Les box, les routeurs, les OS propriétaires (Windows, macOS, Android, iOS) sont devenus des portes dérobées potentielles.

Nous sommes passés d'un Internet libertaire à un Internet sous double tutelle :

- celle des entreprises qui vous traquent pour mieux vous vendre ;
- celle des États qui vous surveillent (parfois pour de bonnes raisons, souvent sans contrôle).

Face à cela, l'individu seul se sent impuissant. « De toute façon, ils ont déjà toutes mes données. » « Je ne peux rien y changer. » C'est ce qu'on appelle l'éloge de l'apathie – et c'est l'arme la plus efficace des Big Tech et des gouvernements autoritaires.

Sauf que... c'est faux. On peut résister. On peut reprendre le contrôle, un outil à la fois, un service à la fois.

Pas besoin de changer du jour au lendemain. Pas besoin de tout auto-héberger ou de disparaître du réseau. L'objectif n'est pas la perfection ; c'est la progression.

Chaque fois que vous remplacez Gmail par Proton Mail, WhatsApp par SimpleX ou Element, Google Maps par Organic Maps, Google Drive par Cryptpad ou Syncthing, vous retirez une petite brique à l'édifice de la surveillance et de la marchandisation. Vous devenez un peu plus propriétaire de votre vie numérique.

Comment utiliser ce guide : la méthode des vagues successives

Vous venez de lire l'histoire de notre liberté numérique : comment nous sommes passés d'un Internet ouvert et décentralisé à un univers de surveillance et de marchandisation. Et vous vous dites peut-être : "C'est bien beau, mais par où commencer ?"

La réponse est simple : **pas à pas, vague après vague.**

Ce guide contient 58 fiches pratiques. Si vous les lisez toutes d'un seul coup, vous risquez la **surcharge cognitive** : trop d'informations, trop d'actions à mener, trop de décisions à prendre. Le risque ? Vous décourager et ne rien faire.

Pour éviter cela, nous vous proposons une **approche par vagues successives**. L'idée est simple : vous ne devez pas tout faire en même temps. Vous allez avancer **par étapes**, en consolidant chaque nouvelle habitude avant de passer à la suivante.

Les 4 vagues pour une transition progressive.

La Vague 0 est un pré-requis, spécialement pour les débutants.

Vague	Objectif	Fiches concernées
Vague 0	Comprendre le vocabulaire (1 semaine)	Petit guide pour comprendre l'informatique sans se prendre la tête
Vague 1	Les bases de la sécurité (2 semaines)	N°16 (mots de passe), N°18 (2FA), N°2 (navigateur), N°17 (moteur de recherche)
Vague 2	Protéger ses communications (3 semaines)	N°10 (email éthique), N°15 (messagerie instantanée), N°6 (DNS)
Vague 3	Libérer ses données (1 mois)	N°7 (cloud), N°3 (YouTube), N°21 (RSS), N°24 (cartographie)
Vague 4	Aller plus loin (selon vos besoins)	N°13 (Linux), N°20 (auto-hébergement), N°38 (Pi-hole), N°27 (Tor), N°45 (Warren VPN)

Comment lire ce guide

1. **Ne sautez pas les vagues** : Chaque vague prépare la suivante. Par exemple, sans gestionnaire de mots de passe (Vague 1), activer la 2FA (Vague 1) ou changer de messagerie (Vague 2) est plus complexe.
2. **Prenez votre temps** : Une vague peut durer plusieurs semaines. L'objectif est d'intégrer durablement les nouvelles habitudes, pas de cocher des cases.
3. **Une fiche à la fois** : Ne lisez pas toutes les fiches d'une vague en même temps. Prenez une fiche, appliquez-la, testez-la, puis passez à la suivante.
4. **Adaptez à votre rythme** : Si une fiche vous semble trop technique, passez à la suivante et revenez-y plus tard. L'important est de progresser, pas d'être parfait.

Pourquoi cette méthode fonctionne

- **Diminue l'anxiété** : Vous ne vous sentez pas submergé par une montagne de choses à faire.
- **Renforce la confiance** : Chaque petite victoire (changer de navigateur, sécuriser ses mots de passe) vous motive à continuer.

•**Évite les erreurs** : En allant trop vite, on fait des impasses (ex: oublier la 2FA après avoir changé de gestionnaire de mots de passe). Les vagues vous protègent de ces oublis.

Votre plan d'action personnel

1.**Commencez par la Vague 1**. Ouvrez la fiche N°16, installez un gestionnaire de mots de passe, changez vos mots de passe importants. Prenez une semaine pour vous habituer.

2.**Passez à la Vague 2**. Une fois que vous maîtrisez vos mots de passe, changez de navigateur, puis de moteur de recherche.

3.**Continuez à votre rythme**. Les vagues 3 et 4 vous attendent quand vous serez prêt.

Lorsque vous aurez terminé les 3 premières vagues, vous aurez déjà atteint 80 % de votre objectif de Souveraineté Numérique.

Pour les autres fiches, prenez votre temps et voyez ce qui vous parle en fonction de vos besoins propres.

Rappel : L'objectif n'est pas la perfection, c'est la progression. Chaque petit pas vous rapproche de votre souveraineté numérique.

Table des matières

Introduction

⇒ [Petit guide pour comprendre l'informatique sans se prendre la tête](#) :

Glossaire de 26 notions de base, avec analogies simples (maison, voiture, océan, restaurant). **À lire en premier si vous débutez**.

•**Partie 1** : Les bases (ordinateur, OS, logiciel, Internet/Web, navigateur, moteur de recherche, logiciel propriétaire/libre, pièges des « gratuits »)

•**Partie 2** : Notions complémentaires (cloud, chiffrement, donnée, IP, pare-feu, cookie, VPN, serveur, client, protocole, permissions, base de données, mot de passe, DNS, sauvegarde, antivirus)

•**Partie 3** : Récapitulatif général (tableau des 26 notions, phrase à retenir, trois conseils pour commencer)



Bureautique et logiciels (remplacer Microsoft Office, Google Docs, Adobe)

[Fiche N°1 – Libérez-vous des suites bureautiques propriétaires](#)

[Fiche N°23 – Outils libres de retouche photo \(GIMP, Darktable, RawTherapee\)](#)



Navigateurs et vie privée (remplacer Chrome, Edge, Safari)

[Fiche N° 2 – Naviguez sans être pisté \(protection de base\)](#)

[Fiche N°11 – Naviguez sans être pisté \(protection avancée\)](#)

[Fiche N°14a – Nettoyez vos liens partagés](#)

[Fiche N°14b – Cas particuliers du nettoyage de liens partagés](#)

[Fiche N°41 – Raccourcissez vos URLs en souveraineté numérique](#)



Moteurs de recherche (remplacer Google Search, Bing)

[Fiche N°17 – Utilisez un moteur de recherche qui ne vous traque pas](#)



Messagerie éthique (remplacer Gmail, Outlook, Yahoo, iCloud)

[Fiche N°10 – Messagerie email éthique](#)

[Fiche N°36 - Auto-hébergement mail pur](#)



Messageries instantanées (remplacer WhatsApp, Messenger, Telegram, Signal)

[Fiche N°15 – Messageries instantanées cryptées sans numéro de téléphone](#)

[Fiche N°33 - Element / Matrix – Guide détaillé](#)



Cloud, stockage et synchronisation (remplacer Google Drive, iCloud, OneDrive, Dropbox)

[Fiche N° 7 – Alternatives libres à Google Drive et Google Doc](#)

[Fiche N°29 – Synchronisez vos appareils sans Cloud avec Syncthing](#)

[Fiche N°31 – Utilisation d'un NAS pour centraliser et sauvegarder vos données](#)

[Fiche N°34 - Nextcloud – Auto-hébergement pas à pas \(votre propre cloud privé\)](#)

Téléphones et alternatives mobiles (remplacer Play Store, services Google)

[Fiche N°42 – Aurora Store – Google Play Store sans compte Google](#)

Sécurité, mots de passe et chiffrement

[Fiche N°16 – Gestionnaires libres de mots de passe](#)

[Fiche N°18 – Authentification à deux facteurs \(2FA\) pour plus de sécurité](#)

[Fiche N°26 – Chiffrez vos fichiers sensibles](#)

[Fiche N°35 - Vaultwarden – Auto-hébergement Bitwarden \(gestion de mots de passe\)](#)

[Fiche N°37 - Vérifier l'intégrité des fichiers avec GPG \(signatures, checksums\)](#)

[Fiche N°40 - Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur](#)

Cartographie (remplacer Google Maps, Waze, Apple Plans)

[Fiche N°24 – Outils de cartographie sans pistage](#)

Vidéo et streaming (remplacer YouTube)

[Fiche N°3 – Utilisez YouTube sans publicités](#)

[Fiche N°25 – Publiez des vidéos sans YouTube avec Peertube](#)

VPN, DNS et protection réseau

[Fiche N° 4 – Installez et utilisez Proton VPN \(version gratuite possible\)](#)

[Fiche N° 5 – Installez et utilisez Mullvad VPN \(version payante uniquement\)](#)

[Fiche N°45 - Installez et utilisez Warren VPN \(bêta gratuite, version payante à venir\)](#)

[Fiche N° 6 – Changez votre serveur DNS pour plus de confidentialité et de sécurité](#)

[Fiche N°30 – Sécurisez la porte d'entrée de votre réseau \(mise à jour de votre box\)](#)

[Fiche N°38 - Installez Pi-hole sur Raspberry Pi ou vieux PC – Bloquez les publicités au niveau de votre réseau](#)

[Fiche N°44 - Les limites du VPN, l'anonymat réel et le brouillage d'empreinte](#)

Désintoxication numérique (quitter les big tech)

[Fiche N° 9 – Désactivez les fonctions Cloud des Big Tech](#)

[Fiche N°12 – Renoncer progressivement aux outils Big Tech](#)

[Fiche N°13 – Libérez vous de Windows ou MacOS et passez à Linux](#)

[Fiche N°39 - Nettoyer son empreinte numérique](#)

Sondages et formulaires (remplacer Google Forms, Doodle)

[Fiche N° 8 – Alternatives libres à Doodle](#)

Auto-hébergement et serveurs personnels

[Fiche N°20 – Auto-hébergez vos services avec Yunohost](#)

[Fiche N°20a : Installer WireGuard sur YunoHost pour un accès VPN sécurisé](#)

[Fiche N°20b : Installer SearXNG sur un sous-domaine local avec YunoHost](#)

[Fiche N°20c : Installer AdGuard Home sur un serveur local avec YunoHost](#)

[Fiche N°20d : Installer Jitsi Meet sur un VPS avec YunoHost](#)

[Fiche N°20e : Installer PeerTube sur un VPS avec YunoHost](#)

[Fiche N°28 – Choisissez un hébergeur web européen et éthique](#)



Anonymat et sécurité extrême

[Fiche N°27 – Apprenez à surfer anonymement avec Tor Browser](#)

[Fiche N°32 - Installation et utilisation de Tails - Naviguez sans laisser de traces](#)



Sauvegardes (remplacer iCloud Backup, Google Backup)

[Fiche N°19a – Sauvegardez vos données sous Linux Mint](#)

[Fiche N°19b – Sauvegardez vos données sous Windows](#)

[Fiche N°19c – Sauvegardez vos données sous macOS](#)

[Fiche N°19d – Sauvegardez vos données sous Android](#)

[Fiche N°19e – Sauvegardez vos données sous IOS-IPhone](#)



Agrégateur RSS (remplacer les réseaux sociaux et newsletters)

[Fiche N°21 – Reprenez le contrôle de votre fil d'actualités avec un agrégateur RSS](#)



Réseaux sociaux (remplacer Twitter, Facebook, Instagram)

[Fiche N°22 – Rejoignez le Fédiverse sans algorithme ni pub \(Mastodon / Bluesky\)](#)

Conseils pratiques à mettre en œuvre sans aucune installation supplémentaire

[Fiche N°46 : Les 20 gestes de base sans outil](#)

[Fiche N°47 : Reconnaître et déjouer les arnaques en ligne](#)

[Fiche N°48 : 14 outils de cybersécurité dans votre navigateur](#)

Dans le même répertoire vous trouverez aussi un fichier de suivi de votre progression :

[Suivez votre progression sans compte](#)

Classement par niveau de difficulté

Niveau	N° des fiches
★★★★☆ (Très facile)	N°2, N°3, N°8, N°14a, N°17, N°29, N°30, N°46, N°47, N°48
★★★☆☆ (Facile)	N°1, N°4, N°6, N°7, N°9, N°10, N°11, N°12, N°13, N°14b, N°15, N°16, N°18, N°19a-e, N°21, N°22, N°24, N°26, N°27, N°31, N°32, N°39, N°42, N°45
★★★★☆ (Moyen)	N°5, N°20, N°23, N°25, N°28, N°33, N°34, N°35, N°37, N°38, N°40
★★★★☆ (Avancé)	N°36



Suggestions de lecture par profil

Vous êtes...	Commencez par les fiches...
Débutant	Petit Guide → N°1 (bureautique) → N°2 (navigateur) → N°3 (YouTube) → N°10 (email) → N°16 (mots de passe) → N°40 (frly.eu) → N°42 (Aurora Store) → N°46 (gestes de base) → N°47 (anti-arnaque) → N°48 (outils cybersécurité)
Famille / particulier	Petit Guide → N°10 (email) → N°15 (messaging) → N°24 (cartographie) → N°31 (NAS) → N°40 (frly.eu) → N°42 (Aurora Store) → N°46 (gestes de base) → N°47 (anti-arnaque) → N°48 (outils cybersécurité)
Entreprise / association	Petit Guide → N°20 (Yunohost) → N°28 (hébergeur) → N°25 (Peertube) → N°33 (Matrix) → N°40 (BIOS/UEFI) → N°42 (Aurora Store) → N°46 (gestes de base) → N°47 (anti-arnaque) → N°48 (outils cybersécurité)
Militant / journaliste	Petit Guide → N°27 (Tor) → N°32 (Tails) → N°15 (SimpleX) → N°18 (2FA) → N°39 (empreinte numérique) → N°40 (BIOS/UEFI)
Exigeant / paranoïaque	Petit Guide → N°5 (Mullvad) → N°36 (mail pur) → N°37 (GPG) → N°38 (Pi-hole) → N°35 (Vaultwarden) → N°40 (BIOS/UEFI) → N°46 (gestes de base) → N°47 (anti-arnaque) → N°48 (outils cybersécurité)
Curieux de Linux	N°13 (Linux) → N°20 (Yunohost) → N°34 (Nextcloud) → N°40 (BIOS/UEFI) → N°46 (gestes de base) → N°47 (anti-arnaque) → N°48 (outils cybersécurité)
Adepte de l'anonymat total	Petit Guide → N°45 (Warren VPN) → N°5 (Mullvad) → N°27 (Tor) → N°32 (Tails) → N°36 (mail pur) → N°40 (BIOS/UEFI) → N°46 (gestes de base) → N°47 (anti-arnaque) → N°48 (outils cybersécurité)

Ce que vous allez trouver dans ce guide

- Un glossaire (**petit guide pour comprendre l'informatique sans se prendre la tête**) à destination des débutants.
- Des solutions concrètes pour chaque besoin (mail, cloud, cartographie, réseau social, mots de passe, 2FA, sauvegardes...).
- Des comparaisons claires entre les grandes options (Bitwarden / KeePass / Proton Pass, Organic Maps / Magic Earth, etc.).
- Des mises en garde sur les pièges courants (Google Authenticator, Cloud Act, UPnP, WPS, liens trackés...).
- Des challenges pour tester et adopter durablement de nouveaux réflexes.
- Une philosophie : pas de culte de la pureté, pas de paranoïa, mais une stratégie de reprise de contrôle progressive et réaliste.

Ce que vous ne trouverez pas (et pourquoi)

Ce guide n'est pas un manifeste contre le progrès ou une incitation à la clandestinité numérique. Il ne vous demande pas de devenir un hacker ou de vivre hors réseau. Il vous donne simplement les moyens de choisir : choisir qui voit vos données, choisir de ne pas être le produit, choisir de ne pas être surveillé sans raison.

Dernier conseil avant de commencer

N'ouvrez pas toutes ces fiches en même temps. Prenez une fiche, une seule, celle qui correspond à votre besoin le plus immédiat. Installez l'alternative. Laissez-vous le temps de vous habituer. Puis passez à la suivante.

C'est ainsi que l'on reprend le contrôle : pas à pas, victoire après victoire.

L'apathie dit : « C'est trop tard, trop compliqué, trop tard. »

Ces fiches disent : « Commence aujourd'hui. Même petit. Ici et maintenant. »

Bonne lecture, et bienvenue dans votre souveraineté numérique.

Annexe : Liens croisés entre les 26 notions du glossaire et les fiches du Guide de Souveraineté Numérique

Partie 1 : Les bases de l'informatique

Notion du glossaire	Fiche(s) associée(s) du guide	Pourquoi ce lien
§1 – Ordinateur / PC	N°13 – Libérez-vous de Windows ou MacOS et passez à Linux N°40 – Sécurisez votre BIOS/UEFI	La fiche N°13 aide à choisir un système d'exploitation ; la N°40 protège la première porte d'entrée matérielle de l'ordinateur
§2 – Système d'exploitation (OS)	N°13 – Libérez-vous de Windows ou MacOS et passez à Linux N°19a – Sauvegardez vos données sous Linux Mint N°19b – Sauvegardez vos données sous Windows N°19c – Sauvegardez vos données sous macOS	Chaque fiche de sauvegarde est spécifique à un OS
§3 – Logiciel / Application	Toutes les fiches	Chaque fiche recommande des logiciels alternatifs
§4 – Internet vs Web	N°2 – Naviguez sans être pisté (protection de base) N°17 – Utilisez un moteur de recherche qui ne vous traque pas	Distinction fondamentale pour comprendre le navigateur et le moteur de recherche
§5 – Navigateur web	N°2 – Naviguez sans être pisté (protection de base)	Toutes les fiches liées à la navigation web

	N°11 – Naviguez sans être pisté (protection avancée) N°14a – Nettoyez vos liens partagés N°14b – Cas particuliers du nettoyage de liens partagés N°41 – Raccourcissez vos URLs en souveraineté numérique	
§6 – Moteur de recherche	N°17 – Utilisez un moteur de recherche qui ne vous traque pas N°20b – Installer SearXNG sur un sous-domaine local avec YunoHost	SearXNG est un métamoteur auto-hébergé
§7 – Logiciel propriétaire	N°1 – Libérez-vous des suites bureautiques propriétaires N°23 – Outils libres de retouche photo (GIMP, Darktable, RawTherapee) N°13 – Libérez-vous de Windows ou MacOS et passez à Linux	Alternatives aux logiciels propriétaires
§8 – Logiciel libre / Open Source	N°1 – Libérez-vous des suites bureautiques propriétaires N°23 – Outils libres de retouche photo N°20 – Auto-hébergez vos services avec Yunohost	Toutes les alternatives libres recommandées
§9 – Les pièges des « gratuits » en ligne	N°10 – Messagerie email éthique N°12 – Renoncer progressivement aux outils Big Tech N°22 – Rejoignez le Fédiverse	Comprendre pourquoi Gmail, Facebook, etc. sont problématiques

	sans algorithme ni pub	
§10 – Récap des bases	—	Synthèse, pas de fiche associée

Partie 2 : Notions complémentaires

Notion du glossaire	Fiche(s) associée(s) du guide	Pourquoi ce lien
§11 – Cloud	N°7 – Alternatives libres à Google Drive et Google Doc N°29 – Synchronisez vos appareils sans Cloud avec Syncthing N°31 – Utilisation d'un NAS pour centraliser et sauvegarder vos données N°34 – Nextcloud – Auto-hébergement pas à pas	Toutes les alternatives au cloud propriétaire
§12 – Chiffrement	N°26 – Chiffrez vos fichiers sensibles N°37 – Vérifier l'intégrité des fichiers avec GPG N°18 – Authentification à deux facteurs (2FA) N°10 – Messagerie email éthique N°15 – Messageries instantanées cryptées	Chiffrement des fichiers, des emails, des messageries
§13 – Donnée	N°39 – Nettoyer son empreinte numérique N°9 – Désactivez les fonctions Cloud des Big Tech	Comprendre ce que les Big Tech collectent
§14 – Adresse IP	N°4 – Installez et utilisez Proton VPN N°5 – Installez et utilisez Mullvad VPN N°45 – Installez et utilisez Warren VPN	Les VPN masquent l'adresse IP

	N°44 – Les limites du VPN, l'anonymat réel et le brouillage d'empreinte	
§15 – Pare-feu	N°30 – Sécurisez la porte d'entrée de votre réseau (mise à jour de votre box) N°38 – Installez Pi-hole sur Raspberry Pi ou vieux PC	Protection réseau et blocage des publicités
§16 – Cookie	N°2 – Naviguez sans être pisté (protection de base) N°11 – Naviguez sans être pisté (protection avancée)	Gestion des cookies et des traqueurs
§17 – VPN	N°4 – Installez et utilisez Proton VPN N°5 – Installez et utilisez Mullvad VPN N°45 – Installez et utilisez Warren VPN N°44 – Les limites du VPN, l'anonymat réel et le brouillage d'empreinte N°20a – Installer WireGuard sur YunoHost	Toutes les fiches VPN
§18 – Serveur	N°20 – Auto-hébergez vos services avec Yunohost N°28 – Choisissez un hébergeur web européen et éthique N°31 – Utilisation d'un NAS pour centraliser et sauvegarder vos données N°34 – Nextcloud – Auto- hébergement pas à pas	Auto-hébergement et serveurs personnels
§19 – Client	N°4 – Installez et utilisez Proton VPN N°5 – Installez et utilisez Mullvad VPN N°45 – Installez et utilisez Warren VPN	Les applications VPN sont des clients
§20 – Protocole	N°6 – Changez votre serveur DNS	DNS et WireGuard sont des

	pour plus de confidentialité et de sécurité N°20a – Installer WireGuard sur YunoHost pour un accès VPN sécurisé	protocoles
§21 – Permissions	N°40 – Sécurisez votre BIOS/UEFI	Gestion des droits d'accès au matériel
§22 – Base de données	N°34 – Nextcloud – Auto-hébergement pas à pas	Nextcloud utilise une base de données
§23 – Mot de passe / authentification	N°16 – Gestionnaires libres de mots de passe N°18 – Authentification à deux facteurs (2FA) N°35 – Vaultwarden – Auto-hébergement Bitwarden	Gestion des mots de passe et 2FA
§24 – DNS	N°6 – Changez votre serveur DNS pour plus de confidentialité et de sécurité N°20b – Installer SearXNG sur un sous-domaine local avec YunoHost N°20c – Installer AdGuard Home sur un serveur local avec YunoHost	DNS et services associés
§25 – Sauvegarde	N°19a – Sauvegardez vos données sous Linux Mint N°19b – Sauvegardez vos données sous Windows N°19c – Sauvegardez vos données sous macOS N°19d – Sauvegardez vos données sous Android N°31 – Utilisation d'un NAS pour centraliser et sauvegarder vos données	Toutes les fiches de sauvegarde
§26 – Antivirus / malware	N°38 – Installez Pi-hole sur Raspberry Pi ou vieux PC N°26 – Chiffrez vos fichiers sensibles	Blocage des malwares et protection des données

Tableau récapitulatif synthétique

#	Notion	Fiches principales
1	Ordinateur / PC	N°13, N°40
2	Système d'exploitation	N°13, N°19a-d
3	Logiciel / Application	Toutes
4	Internet vs Web	N°2, N°17
5	Navigateur web	N°2, N°11, N°14a, N°14b, N°41
6	Moteur de recherche	N°17, N°20b
7	Logiciel propriétaire	N°1, N°23, N°13
8	Logiciel libre / Open Source	N°1, N°23, N°20
9	Pièges des « gratuits »	N°10, N°12, N°22
10	Récap des bases	—
11	Cloud	N°7, N°29, N°31, N°34
12	Chiffrement	N°26, N°37, N°18, N°10, N°15
13	Donnée	N°39, N°9
14	Adresse IP	N°4, N°5, N°45, N°44
15	Pare-feu	N°30, N°38
16	Cookie	N°2, N°11
17	VPN	N°4, N°5, N°45, N°44, N°20a
18	Serveur	N°20, N°28, N°31, N°34
19	Client	N°4, N°5, N°45
20	Protocole	N°6, N°20a
21	Permissions	N°40
22	Base de données	N°34
23	Mot de passe / authentification	N°16, N°18, N°35

24	DNS	N°6, N°20b, N°20c
25	Sauvegarde	N°19a-d, N°31
26	Antivirus / malware	N°38, N°26

Comment utiliser ces liens croisés

1. Pour les débutants : Lisez d'abord le glossaire (§1 à §26), puis ouvrez les fiches associées une par une.

2. Pour les utilisateurs avancés : Utilisez les fiches comme point d'entrée, et consultez le glossaire pour les notions que vous ne maîtrisez pas.

3. Pour les formateurs : Ces liens permettent de construire des parcours pédagogiques cohérents (ex. : « Comprendre le VPN » = §17 + N°4 + N°5 + N°45 + N°44).