

SOUVERAINETÉ NUMÉRIQUE : 5 GESTES PRATIQUES

Cinq gestes concrets pour reprendre le contrôle de tes données, avec les outils nommés, le temps que ça prend et ce que chacun ne protège pas.

INTRODUCTION

La souveraineté numérique n'est pas un état qu'on atteint, c'est une série de décisions concrètes. Le problème habituel n'est pas le manque de volonté : c'est qu'on ne sait pas par où commencer, et qu'on finit par tout faire à moitié. Les cinq gestes ci-dessous ont été retenus sur un seul critère — le rapport entre l'effort réel et la protection obtenue. Chacun indique l'outil, le temps, et surtout ce contre quoi il **ne** protège **pas**. C'est cette dernière ligne qui compte le plus : croire qu'on est protégé quand on ne l'est pas est pire que de ne rien faire.

Ce qui n'est pas dans la liste, volontairement : l'auto-hébergement. Un serveur mal maintenu chez toi est moins sûr qu'un service géré, et le temps investi ne rapporte presque rien en protection. Si tu veux quitter les GAFAM sur le stockage, le geste rentable est de basculer vers un fournisseur européen chiffré (Proton Drive, kDrive d'Infomaniak, Tresorit) ou de chiffrer côté client avec **Cryptomator** (gratuit) avant l'envoi vers le cloud que tu utilises déjà.

LES CONCEPTS ESSENTIELS

Geste 1 — Un gestionnaire de mots de passe. 45 minutes, puis 10 secondes par compte.

Installe **Bitwarden** (gratuit, multi-appareils) ou **KeePassXC** (gratuit, local). Un seul mot de passe à retenir : une **phrase de passe** de quatre à cinq mots rares sans lien logique entre eux, bien plus solide et bien plus mémorisable qu'un Tr0ub4dor!. Migre d'abord les cinq comptes critiques : messagerie principale, banque, opérateur, gestionnaire lui-même, réseau social professionnel. Le reste au fil de l'eau.

Ce que ça ne protège pas : si un logiciel espion tourne déjà sur ta machine, il voit ce que tu tapes. Et si un service se fait pirater côté serveur, ton mot de passe unique limite les dégâts à ce service — il ne les annule pas.

Geste 2 — La double authentification par application, pas par SMS. 20 minutes.

Utilise **Aegis** (Android) ou **Ente Auth** (iOS et Android, gratuits, open source) plutôt que les codes par SMS. Le SMS est vulnérable au **SIM swapping** : quelqu'un convainc l'opérateur de porter ton numéro sur sa carte, et reçoit tes codes. Pour tes deux ou trois comptes les plus sensibles, une clé matérielle (YubiKey, Nitrokey, 25 à 60 €) ou une **passkey** est nettement supérieure.

Ce que ça ne protège pas : un hameçonnage en temps réel où un faux site te demande ton code et le rejoue immédiatement chez le vrai service. Le code TOTP est reproductible pendant 30 secondes. Seules les clés FIDO2 et les passkeys bloquent cette attaque, parce qu'elles sont liées au nom de domaine et refusent de répondre à un site imposteur.

Geste 3 — Chiffrer le disque et sauvegarder en 3-2-1. 1 heure, puis automatique.

Active **BitLocker** (Windows Pro), **FileVault** (macOS) ou **LUKS** (Linux) — c'est une case à cocher. Puis applique le 3-2-1 : 3 copies de tes données, sur 2 supports différents, dont 1 hors du domicile. En pratique : ton disque,

un disque externe avec **restic** ou Time Machine, et une copie chiffrée en ligne.

Ce que ça ne protège pas : le chiffrement du disque protège contre le vol ou la perte du matériel, point. Machine allumée et session ouverte, tout est lisible. Et une sauvegarde branchée en permanence sera chiffrée par un rançongiciel en même temps que le reste : garde une copie débranchée.

Geste 4 — Une messagerie chiffrée de bout en bout. 15 minutes.

Signal (gratuit, à but non lucratif) chiffre le contenu et minimise les métadonnées conservées. Le geste utile n'est pas de l'installer, c'est d'y déplacer deux ou trois conversations réelles — sinon l'application reste vide.

Ce que ça ne protège pas : rien de ce qui se passe sur le téléphone de ton correspondant, y compris ses captures d'écran et ses sauvegardes. Ça ne masque pas non plus le fait que vous vous parlez, ni à qui. Et une conversation chiffrée sur un appareil compromis est lue en clair, avant chiffrement.

Geste 5 — Reprendre le navigateur et le DNS. 30 minutes.

Firefox avec **uBlock Origin** coupe l'essentiel du pistage publicitaire. Côté résolution de noms, active le DNS chiffré vers **Quad9**, **dns0.eu** ou **NextDNS** : ton fournisseur d'accès cesse de voir la liste des sites que tu consultes, et les domaines malveillants connus sont bloqués en amont.

Ce que ça ne protège pas : ce n'est pas un VPN, ton adresse IP reste visible des sites que tu visites. Le résolveur DNS que tu choisis voit désormais tes requêtes — tu déplaces une confiance, tu ne la supprimes pas. Et l'empreinte de navigateur reste partiellement exploitable.

MINI-LEXIQUE

- **Phrase de passe** — plusieurs mots sans lien entre eux ; sa longueur fait sa force, pas ses caractères bizarres.
- **Chiffrement de bout en bout** — seuls l'expéditeur et le destinataire peuvent lire ; le serveur qui transporte ne le peut pas.
- **TOTP** — code à six chiffres généré localement toutes les 30 secondes par ton application d'authentification.
- **SIM swapping** — détournement de ton numéro de téléphone auprès de l'opérateur, pour intercepter tes codes SMS.
- **FIDO2 / passkey** — authentification liée au nom de domaine, la seule qui résiste à un faux site.
- **DNS chiffré (DoH / DoT)** — tes requêtes de noms de domaine circulent chiffrées au lieu d'être lisibles par ton FAI.
- **3-2-1** — 3 copies, 2 supports, 1 hors site.
- **Chiffrement côté client** — tes fichiers sont chiffrés sur ta machine avant d'atteindre le cloud.

EXEMPLE PRATIQUE

Camille, graphiste indépendante, y consacre un samedi matin. 9h : Bitwarden installé, phrase de passe choisie, cinq comptes critiques migrés avec des mots de passe régénérés. 10h : Ente Auth configuré sur ces mêmes cinq comptes, SMS désactivé partout où c'est possible, codes de secours imprimés et rangés ailleurs qu'à l'écran. 10h45 : FileVault activé, disque externe branché, première sauvegarde lancée en tâche de fond. 11h15 : Firefox, uBlock Origin, DNS basculé sur dns0.eu. 11h45 : Signal installé, deux clients sensibles invités.

Trois heures. Le résultat n'est pas l'anonymat — ce n'était pas l'objectif. C'est qu'une fuite de base de données chez un prestataire ne donne plus accès à sa boîte mail, et qu'un ordinateur portable volé dans un train ne donne plus accès aux fichiers de ses clients.

CE QU'IL FAUT RETENIR

- Ces cinq gestes couvrent les scénarios réellement fréquents : réutilisation de mots de passe, vol de compte, perte de matériel, interception, pistage. Pas les attaques ciblées par un adversaire déterminé.
- Chaque outil a une frontière nette. Connaître ce qu'il ne fait pas est aussi utile que l'installer.
- Fait à moitié vaut mieux que pas fait — mais commence par le gestionnaire de mots de passe, il conditionne les autres.

ENVIE D'APPROFONDIR ?

Le niveau suivant traite du modèle de menace : définir contre qui tu te protèges, parce que la réponse change complètement les outils à choisir.

Ce mini-cours a été généré avec MCPMN, la méthode d'Unchain Academy, en accès libre. Pour recevoir le guide et la méthodologie et générer les tiens avec un compte Claude gratuit, écris à info@unchainacademy.com. Pour aller plus loin avec un humain — accompagnement individuel, ponctuel ou régulier — c'est la même adresse.

Licence CC BY-NC-SA 4.0. Tu peux copier, modifier et adapter ce cours, à condition de citer Victor Lardé / Unchain Academy et de partager tes versions sous la même licence. Toute vente ou usage commercial demande un accord écrit : licences commerciales sur demande à info@unchainacademy.com.