Mots de passe et authentification

> **Référentiel BTS — BC3 / C3.5** « Concevoir et maintenir sécurisé son environnement numérique de travail ».

> **L'essentiel :** un mot de passe protège un dossier patient exactement comme une serrure protège un local. La **longueur** compte plus que la complexité, la **réutilisation** est le vrai danger, et l'**authentification à plusieurs facteurs** rend le vol de mot de passe presque sans effet.

Objectif

À la fin de cette page, vous savez :

- construire un mot de passe robuste et mémorisable ;
- expliquer pourquoi réutiliser un mot de passe est le risque principal ;
- utiliser un gestionnaire de mots de passe et l'authentification à plusieurs facteurs.

Comment un mot de passe est réellement cassé

Trois méthodes, par ordre de fréquence :

1. **La réutilisation.** Un site de commerce se fait pirater, votre adresse et votre mot de passe se retrouvent dans une liste publique. L'attaquant les essaie **partout ailleurs**. Si le mot de passe du logiciel métier est le même que celui d'un forum, la protection est nulle, quelle que soit sa complexité.

2. **L'hameçonnage.** On vous le demande, et vous le donnez. Aucune longueur ne protège de cela (voir la page *Reconnaître les menaces*).
3. **La force brute / le dictionnaire.** L'essai automatique de milliards de combinaisons et de mots courants. C'est **la longueur** qui y résiste, pas les caractères exotiques.

Construire un bon mot de passe

La règle courte : long, unique, et jamais deviné à partir de vous.

- **Longueur d'abord** : visez **au moins 12 à 15 caractères**. Une phrase de passe fonctionne très bien — *« MonChatDort3FoisParJour! »* est à la fois plus long, plus mémorisable et plus solide que *« Xk7$p2 »*.
- **Unique par service** : c'est le point non négociable.
- **Rien de personnel** : prénom des enfants, date de naissance, nom du cabinet, plaque d'immatriculation. Ces éléments se trouvent en quelques minutes.
- **Pas de variation évidente** : `Cabinet2024!` puis `Cabinet2025!` n'est pas un changement de mot de passe.

Ce qui a changé depuis les vieilles consignes : on ne recommande plus le **changement périodique obligatoire** sans raison. Il pousse aux variantes prévisibles et notées sur un papier. On change un mot de passe **quand il y a une raison** : soupçon de compromission, départ d'un collègue qui le connaissait, service piraté.

Le gestionnaire de mots de passe

Retenir 30 mots de passe uniques est impossible. C'est exactement ce que résout un **gestionnaire de mots de passe** : un coffre chiffré qui les stocke tous, protégé par **un seul** mot de passe très solide (celui-là, on le retient) et idéalement une seconde vérification.

Il génère aussi des mots de passe aléatoires, les remplit automatiquement — ce qui, au passage, **protège de l'hameçonnage** : le gestionnaire ne remplit rien sur un faux site, parce que l'adresse ne correspond pas.

Ce qu'il ne faut pas faire à la place : le fichier `mots de passe.xlsx` sur le bureau, le carnet dans le tiroir de l'accueil, le post-it sous le clavier, l'enregistrement dans un navigateur partagé par plusieurs personnes.

L'authentification à plusieurs facteurs (MFA / 2FA)

Principe : pour se connecter, il faut **deux preuves de nature différente** —

- quelque chose que **je sais** (mot de passe),
- quelque chose que **je possède** (téléphone, carte CPS, clé de sécurité),
- quelque chose que **je suis** (empreinte, visage).

Un mot de passe volé ne suffit alors plus. C'est la mesure qui offre le meilleur rapport effort/protection.

En santé, vous l'utilisez déjà : la **carte CPS** et son équivalent mobile l'**e-CPS** sont des authentifications à deux facteurs — quelque chose que l'on **possède** (la carte, ou le téléphone) et quelque chose que l'on **sait** (le code), parfois complété par la biométrie. C'est pour cela qu'une carte CPS volée sans son code ne permet rien.

À activer partout où c'est proposé : messagerie professionnelle, banque, portail de l'éditeur, outils d'administration.

> ⚠ Un code reçu par SMS est **mieux que rien**, mais moins sûr qu'une application d'authentification ou une clé physique. Et un code de validation **ne se communique jamais** à quelqu'un qui vous appelle, quel que soit le motif invoqué.

Cas particuliers du cabinet

- **Le compte d'administration** du logiciel ou du système ne sert **qu'à administrer** : on ne travaille pas au quotidien avec.
- **Les comptes de service** (sauvegarde, interface comptable) doivent avoir des mots de passe propres, longs, stockés dans le coffre — pas le mot de passe du gérant.
- **La continuité** : les accès critiques doivent être récupérables si le gérant est absent ou empêché. Un coffre partagé avec accès d'urgence, ou une procédure écrite déposée en lieu sûr, évite la paralysie.

À retenir

- **Long, unique, impersonnel** : dans cet ordre.
- La **réutilisation** est le risque n°1, devant la complexité.
- **Gestionnaire de mots de passe** : la seule méthode réaliste pour tenir l'unicité.
- **Authentification à deux facteurs** partout où c'est possible — la CPS en est une.
- On **ne change plus pour changer** : on change quand il y a une raison.

Revision #5
Created 2026-09-15 17:24:22 UTC by Antoine
Updated 2026-09-16 07:03:13 UTC by Antoine