

Gratuit · 7 réflexes · 5 minutes de lecture

# 7 réflexes pour une vie numérique **blindée**

Pas besoin d'être expert. Ces gestes simples bloquent l'immense majorité des piratages et des arnaques. À appliquer une fois, tranquille pour longtemps.



# Les 7 réflexes essentiels

Du plus rentable au plus avancé. Si vous n'en faites que trois, faites les trois premiers.

## 1 Un mot de passe unique par compte priorité

Réutiliser le même mot de passe, c'est donner un passe-partout. La longueur compte plus que les symboles : visez une phrase de 4 mots (« cheval-bleu-orage-citron »).

## 2 Un gestionnaire de mots de passe

Il crée et retient des mots de passe uniques à votre place. Vous n'en mémorisez qu'un seul, long et solide. Bitwarden (gratuit) est une excellente porte d'entrée.

## 3 La double authentification priorité

Un second code en plus du mot de passe. Même si celui-ci fuit, le pirate reste bloqué. À activer d'abord sur votre boîte mail, puis la banque. Préférez une application au SMS.

## 4 Repérer le phishing avant de cliquer priorité

Urgence (« compte bloqué »), expéditeur bizarre, lien qui ne mène pas au vrai site : autant de signaux. Dans le doute, ne cliquez pas, allez sur le site officiel vous-même.

## 5 Mettre à jour ses appareils

Les mises à jour bouchent les failles que les pirates exploitent. Activez les mises à jour automatiques du téléphone, de l'ordinateur et des applications.

## 6 Sauvegarder ses données (règle 3-2-1)

3 copies, sur 2 supports, dont 1 hors site. C'est votre assurance contre la panne, le vol et les rançongiciels. Un cloud automatique plus un disque externe débranché suffisent.

## 7 Se méfier du Wi-Fi public

Évitez la banque sur un Wi-Fi ouvert, ou passez par un VPN qui chiffre votre connexion. En déplacement, le partage de connexion 4G de votre téléphone est plus sûr.

## Votre check-list express

Cochez au fur et à mesure. Objectif : tout cocher.

- Mot de passe unique sur l'email et la banque
- Gestionnaire de mots de passe installé
- Double authentification activée sur l'email
- Double authentification sur la banque et les réseaux sociaux
- Mises à jour automatiques activées (tél. et ordinateur)
- Une sauvegarde automatique en place
- Une copie déconnectée (disque externe rangé)
- Je sais reconnaître un faux SMS ou email

## Aller plus loin, gratuitement

Testez vos mots de passe, vérifiez si votre email a fuité, faites le quiz sécurité.

[cybercarapace.fr](https://cybercarapace.fr)

---

Cybercarapace est un guide indépendant de cybersécurité pour les particuliers. Nous ne vendons rien et ne donnons aucun conseil personnalisé : nous informons, comparons et vous orientons.