Les réflexes sécurité en ligne

5 réflexes quotidiens + 3 questions avant de cliquer, pour éviter les arnaques les plus courantes.

LES 5 RÉFLEXES

1 — Lire l'adresse avant de saisir quoi que ce soit
Un seul caractère de différence = un faux site. Le cadenas ne prouve pas la légitimité : il indique seulement une connexion chiffrée.

2 — Jamais par le lien reçu
Message inattendu ? Ouvrez un nouvel onglet et tapez vous-même l'adresse officielle. SMS frauduleux : transférez-le au 33700.

3 — Un mot de passe unique par compte
Gestionnaire de mots de passe (ex. Bitwarden, gratuit). 12 caractères minimum ; une phrase longue vaut mieux qu'un mot compliqué.

4 — Mises à jour automatiques activées
Sur tous vos appareils et applications. Chaque mise à jour repoussée est une faille qui reste ouverte.

5 — Double authentification (2FA) partout où c'est possible
D'abord la messagerie, puis banque et réseaux sociaux. Préférez une application d'authentification au SMS.

En cas de doute — les 3 questions avant de cliquer

1. Est-ce que je m'attendais à ce message ?
2. Me pousse-t-on à agir vite (urgence, menace, offre limitée) ?
3. Puis-je vérifier par un autre canal sûr (application officielle, numéro au dos de la carte) ?

Une seule réponse inquiétante → on ne clique pas, on vérifie d'abord.

Victime ou tentative d'arnaque ?

Coordonnées bancaires communiquées : appelez votre banque immédiatement (opposition).
Mot de passe saisi sur un faux site : changez-le partout où il était utilisé.
Assistance officielle et gratuite : cybermalveillance.gouv.fr