Compte compromis : le protocole

Les 5 étapes de reprise de contrôle, dans le bon ordre — à imprimer avant d'en avoir besoin.

LES 5 ÉTAPES, DANS L'ORDRE

1 — La messagerie d'abord, toujours
C'est la clé maîtresse : qui la contrôle réinitialise tout le reste. Commencez par elle, même si un autre compte semble touché.

2 — Mot de passe changé ET sessions déconnectées
Changer le mot de passe ne suffit pas : utilisez « Se déconnecter de tous les appareils » dans les paramètres de sécurité.

3 — Récupération et règles inspectées
Adresse de secours, téléphone : les vôtres ? Règles de transfert et filtres : liste vide ou connue — c'est là que l'attaquant s'installe.

4 — 2FA activée, comptes liés traités
Double authentification sur le compte repris, puis mot de passe changé partout où le même servait.

5 — Prévenir qui doit l'être
Banque (opposition), contacts si messages envoyés en votre nom, signalement selon votre situation.

Ai-je fuité ? — 5 minutes

1. haveibeenpwned.com : entrez votre adresse e-mail, lisez les fuites listées.
2. Tout mot de passe fuité encore utilisé quelque part : changez-le partout, maintenant.
3. Activez les alertes de fuite de votre gestionnaire (Bitwarden : Rapports) — automatique ensuite.

On ne réagit pas à ce qu'on ignore.

La sauvegarde 3-2-1 — la dernière ligne de défense

Deux copies en plus de l'original : cloud de confiance + disque externe débranché hors sauvegarde.
Testez une restauration une fois par an — une sauvegarde jamais testée est un espoir.
Assistance officielle et gratuite : cybermalveillance.gouv.fr