SE PROTÉGER AVEC UN BON MOT DE PASSE

Hacke-moi si tu peux !

🔍 Comment les pirates trouvent vos mots de passe

- **La devinette.** Le pirate cherche vos informations personnelles sur internet et les essaie comme mot de passe.
- **La force brute.** Un logiciel essaie automatiquement toutes les combinaisons possibles, des milliers par seconde. Un mot de passe court tombe en un instant ; un mot de passe long peut demander des siècles.
- **Le dictionnaire.** Le pirate commence par une liste toute prête des mots de passe les plus courants.
- **La réutilisation.** Si vous utilisez le même mot de passe partout et qu'un seul site est piraté, tous vos comptes tombent en même temps.
- **L'hameçonnage (phishing)**. Le pirate se fait passer pour votre banque, les impôts ou un livreur, par mail, SMS ou téléphone, pour vous pousser à donner vous-même vos informations.

🔐 Créer un mot de passe solide : la phrase de passe

Le meilleur mot de passe est long et complexe. La méthode la plus simple, c'est la phrase de passe : choisissez quatre mots sans rapport entre eux, par exemple girafe, bougie, rivière, casquette. Collez-les ensemble et ajoutez une majuscule, un chiffre et un caractère spécial : GirafeBougieRivièreCasquette7!. C'est très long, donc très difficile à casser. Pour vous aider, vous pouvez aussi utiliser le générateur de mots de passe de la CNIL.

🗂️ Retenir tous ses mots de passe

Chaque compte devrait avoir son propre mot de passe. Trois solutions, de la plus simple à la plus complète :

- Le carnet papier, rangé chez vous en lieu sûr. Simple, et hors de portée des pirates puisqu'il n'est pas sur internet.
- Le navigateur (Chrome, Firefox…) peut retenir vos mots de passe. C'est pratique et déjà mieux que d'utiliser le même partout. Sa limite : tout est accessible dès que quelqu'un utilise votre ordinateur.
- Le gestionnaire de mots de passe, une application qui range tous vos mots de passe derrière un seul mot de passe principal. La solution la plus complète, à envisager une fois qu'on est à l'aise.

🎣 Reconnaître un hameçonnage

Une entreprise sérieuse ne demande jamais votre mot de passe, ni par mail, ni par SMS, ni par téléphone. Les signaux qui doivent alerter :

- Un message qui fait peur ou qui presse (« votre compte va être fermé », « votre colis est bloqué »).
- Une adresse d'expéditeur bizarre, différente de l'adresse habituelle.
- Un « Cher client » impersonnel alors que votre banque connaît votre nom.
- Un bouton ou un lien qui vous emmène vers un site à saisir vos identifiants.

Le bon réflexe : ne cliquez jamais sur le lien d'un message. Allez sur le site vous-même, par votre favori ou en tapant l'adresse habituelle.

🛡️ La double authentification : votre deuxième verrou

Même le meilleur mot de passe peut être volé. La double authentification ajoute une deuxième vérification, le plus souvent un code envoyé par SMS ou par mail. Résultat : même si un pirate a votre mot de passe, il ne peut rien faire sans votre téléphone. À activer dans les réglages de sécurité de vos comptes.

✅ Les 5 réflexes à retenir

1. Jamais d'information personnelle dans un mot de passe.
2. Un mot de passe long plutôt que compliqué : pensez à la phrase de passe.
3. Un mot de passe différent pour chaque compte important.
4. On ne donne jamais son mot de passe. En cas de doute, allez sur le site vous-même.
5. Activez la double authentification.

📌 Où trouver de l'aide

Vérifier si mon adresse mail a fuité : Have I Been Pwned (haveibeenpwned.com, site en anglais).

En cas d'arnaque ou de piratage : Cybermalveillance.gouv.fr.