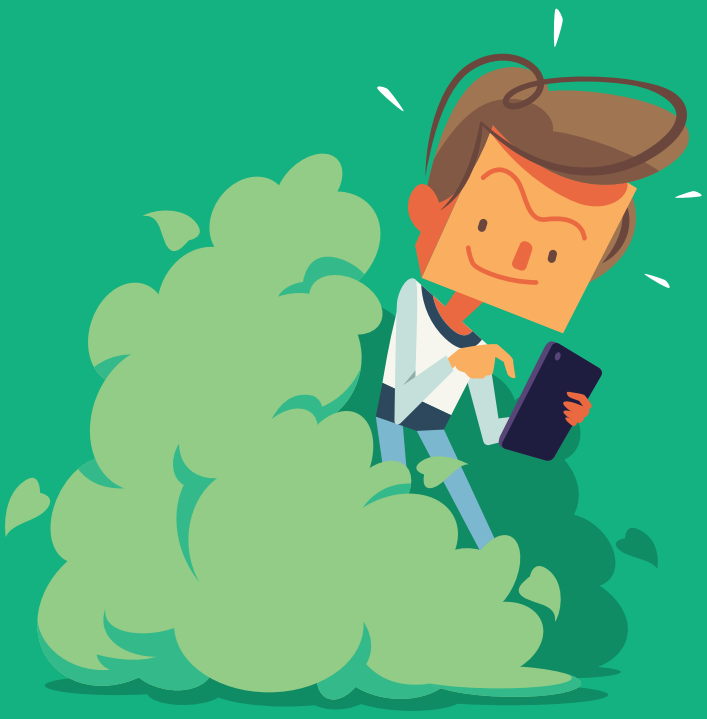
COMMENT FERMER L'ACCÈS À MON COMPTE À D'AUTRES PERSONNES ?

Pour sécuriser vos comptes, vos mots de passe doivent non seulement être suffisamment sûrs, mais aussi rester confidentiels. Evitez donc de communiquer vos mots de passe à d'autres, soyez discret quand vous introduisez vos mots de passe et, surtout, ne les laissez pas traîner sur un bout de papier.



06. NE COMMUNIQUEZ JAMAIS VOS MOTS DE PASSE À QUI QUE CE SOIT

Le mot de passe est strictement personnel. On ne sait jamais à qui on peut se fier entièrement. Ne laissez donc jamais personne regarder au moment où vous introduisez votre mot de passe ou votre code PIN. Et ne le partagez jamais avec d'autres, encore moins par e-mail : les messages peuvent être interceptés ou détournés à votre insu. Si vous devez communiquer un mot de passe pour une urgence, faites-le par Signal ou WhatsApp et veillez à le modifier par la suite.

07. UTILISEZ UN MOT DE PASSE DIFFÉRENT POUR CHAQUE COMPTE

Utilisez un mot de passe différent pour chacun de vos comptes. Si des pirates devaient en obtenir un, ils ne pourraient accéder qu'à un seul de vos comptes et non aux autres.

08. NE CONSERVEZ PAS VOS MOTS DE PASSE À UN ENDROIT ÉVIDENT

Ne conservez jamais vos mots de passe à un endroit évident pour une personne animée de mauvaises intentions, comme dans votre portefeuille, dans votre agenda ou à proximité de votre PC. Ne les conservez pas non plus sur un appareil, sauf dans un fichier verrouillé ou, mieux encore, utilisez un gestionnaire de mots de passe.

09. CHANGEZ TOUS VOS MOTS DE PASSE QUAND UN SITE QUE VOUS UTILISEZ A ÉTÉ PIRATÉ

Si vous apprenez que l'un des sites où vous avez un compte a été piraté, modifiez aussitôt vos mots de passe. Vous éviterez ainsi toute intrusion dans votre compte sur le site concerné et d'autres sites éventuels. Si vous aviez également utilisé ce mot de passe pour vous connecter à d'autres sites, modifiez-le sur-le-champ. Et utilisez ensuite un mot de passe différent pour chacun de vos comptes !

10. ACTIVEZ LA VALIDATION EN DEUX ÉTAPES

La validation en deux étapes (également appelée authentification à deux facteurs) double la protection de vos comptes. Chaque fois que vous utilisez vos mots de passe, vous recevez sur votre téléphone mobile un code qui vous permet d'accéder réellement à votre compte ou à l'appareil concerné.

Si quelqu'un devait s'emparer de votre mot de passe, cette seconde couche de protection empêcherait toute intrusion. Voici comment faire pour vos différents comptes :

- Apple : Vous pouvez l'activer sur votre iPhone via **Réglages** > Cliquez sur votre nom > **Mot de passe et sécurité**; sur votre Mac, allez à **Menu Pomme > Préférences Système >Identifiant Apple > Mot de passe et sécurité**.
- Facebook : Cliquez en haut à droite sur > **Paramètres et confidentialité > Sécurité et connexion > Utiliser l'authentification à deux facteurs**.
- Google : Connectez-vous à myaccount.google.com et allez dans Sécurité. Là, cliquez dans "Connexion à Google" sur **Validation en deux étapes**.
- Microsoft : Connectez-vous à account.microsoft.com/security et choisissez **Options de sécurité avancées**. Dans "Sécurité supplémentaire", cliquez sur **Vérification en deux étapes**.
- Twitter : Cliquez à gauche sur **Plus** (sur mobile, votre photo de profil) **> Paramètres et confidentialité > Sécurité et accès au compte > Sécurité > Authentification à deux facteurs**.

SAVIEZ-VOUS QUE ...

le mot de passe classique pourrait être appelé à disparaître à l'avenir ? Selon le World Wide Web Consortium (W3C), les mots de passe sont "l'un des maillons les plus faibles de la sécurisation d'internet". C'est pourquoi ils ont élaboré en 2019 une nouvelle norme internet (WebAuthn) largement basée sur le principe de la vérification en deux étapes : on prouve son identité par un code reçu sur son smartphone par exemple, ou avec une clé USB spéciale.