Mot de passe sûr : mode d'emploi

- La longueur d'un mot de passe importe plus que sa complexité – plus il est long, plus il est efficace. Idéalement, un **mot de passe doit se composer d'au moins douze signes** ainsi que de minuscules et majuscules, de chiffres et de caractères spéciaux.
- À chaque compte en ligne son mot de passe
- Un mot de passe consiste à utiliser les sons de chaque syllabe pour fabriquer une phrase facile à retenir. Par exemple, la phrase :
  « **le Chien de la sœur à ma Maman est vert et gris** » deviendra
  lCdlsamMev&g, puis on intercale par exemple entre mM le début du nom du site (par exemple Swisscom =swi, raiffensen= rai, coop= coo, ce qui va faire pour Swisscom : « lCdlsamswiMev&g
- Encore plus sûr : l'authentification à deux facteurs. Cette méthode est couramment utilisée par exemple dans l'e-banking. Pour vous connecter, il vous faut un élément de sécurité supplémentaire, tel qu'un code envoyé par SMS uniquement sur votre téléphone ou la lecture d'un QR-code

Avec quelle fréquence faut-il modifier le mot de passe ?
Les experts ne sont pas unanimes sur cette question. Autrefois, ils recommandaient de fréquents changements, aujourd'hui, tout dépend avant tout de la **qualité du mot de passe**. Mais changez-le en tout cas quand des tiers pourraient y avoir eu accès.

La première chose que font les pirates informatiques après avoir volé vos informations de compte, c'est essayer d'accéder à toutes sortes de services avec ces mêmes données. Si vous utilisez un seul mot de passe pour tous vos comptes, considérez-les comme étant tous piratés.

- **81%** de toutes les atteintes à la protection des données sont dues à des mots de passe volés ou faibles.
- Il faut **2 minutes** pour qu'un programme trouve un mot de passe à 5 chiffres composé de lettres minuscules.
- Il faut environ **984 ans** pour qu'un programme le fasse pour un mot de passe à 10 chiffres avec des chiffres, des lettres majuscules et minuscules et des caractères spéciaux.

Pier-Luigi Galli