› VIE PRATIQUE

Sécurité numérique : un bon mot de passe, c'est comment ?

Nous disposons de plusieurs mots de passe pour nos démarches en ligne : messagerie, achats, banque, etc. Quelqu'un m'a dit qu'ils se ressemblent trop et qu'ils ne sont pas assez sécurisés ! Quels sont les conseils pour utiliser des mots de passe suffisamment protecteurs ?

La réponse de Service-public.fr : ***« Il existe des règles simples à adopter pour protéger votre sécurité numérique et éviter d'être la proie de cybercriminels. Le site cybermalveillance.gouv.fr vous conseille ».***

› EN VOICI QUELQUES-UNS :

- Utilisez un mot de passe différent pour chaque accès : si l'un est piraté, seul le service concerné sera vulnérable.

- Créez des mots de passe suffisamment longs et complexes : un bon mot de passe doit comporter au minimum 12 signes mélangeant majuscules, minuscules, chiffres et caractères spéciaux, afin de freiner les attaques réalisées par des ordinateurs qui testent des dizaines de milliers de combinaisons par seconde.

- Créez des mots de passe impossibles à deviner : évitez d'employer des informations personnelles faciles à retrouver, comme le prénom de votre enfant, une date d'anniversaire, votre groupe de musique préféré. Évitez également les suites logiques simples comme 123 456, AZERTY, abcdef... qui font partie des mots de passe les plus courants et qui sont les premières combinaisons qu'essaieront les cybercriminels pour tenter de forcer vos comptes. Par exemple, choisissez la première lettre des mots d'une citation.

- Utilisez un gestionnaire de mots de passe sécurisé : il se chargera d'enregistrer vos mots de passe à votre place et vous évitera ainsi de les noter dans un endroit non sécurisé. Vous n'aurez plus à retenir que celui qui permet d'en ouvrir l'accès.

- Changez votre mot de passe au moindre soupçon : en cas de doute sur la sécurité d'un de vos comptes ou si une société chez qui vous avez un compte s'est fait pirater, changez-le sans attendre. Quelles que soient les circonstances, pensez à changer vos mots de passe régulièrement.

- Ne communiquez jamais votre mot de passe à un tiers : aucun organisme sérieux ne demande de le lui communiquer par messagerie ou par téléphone, même pour une maintenance ou un dépannage informatique.

- N'utilisez jamais vos mots de passe sur un ordinateur partagé (hôtels, cybercafés...), ils pourraient être récupérés par un cybercriminel

Si vous êtes obligé d'utiliser un ordinateur qui n'est pas le vôtre, utilisez le mode de navigation privée du navigateur, veillez à bien fermer vos sessions après utilisation et n'enregistrez jamais vos mots de passe dans le navigateur. Enfin, dès que vous avez, à nouveau, accès à un ordinateur de confiance, changez au plus vite tous les mots de passe que vous avez utilisés sur l'ordinateur partagé.

- Activez la double authentification lorsque c'est possible : en plus de votre nom de compte et de votre mot de passe, ces services vous demandent un code provisoire que vous pouvez recevoir par SMS sur votre téléphone mobile ou qui peut être généré par une application ou une clé spécifique que vous contrôlez. Ainsi, grâce à ce code, vous seul pourrez, par exemple, autoriser un nouvel appareil à se connecter aux comptes protégés ou autoriser une transaction bancaire.

- Changez les mots de passe par défaut des différents services auxquels vous accédez : ils sont souvent connus des cybercriminels. Il est important de les remplacer au plus vite par vos propres mots de passe.

- Choisissez un mot de passe particulièrement robuste pour votre messagerie : c'est un des mots de passe les plus importants à protéger. En effet, votre adresse de messagerie est généralement associée à beaucoup de vos comptes en ligne. Elle permet notamment de recevoir les liens de réinitialisation des mots de passe de vos autres comptes. Un cybercriminel qui réussirait à pirater votre messagerie pourrait facilement utiliser la fonction « mot de passe oublié » des différents services auxquels vous pouvez accéder tel que votre compte bancaire, pour en prendre le contrôle.

Daniel Bertrand

› À SAVOIR :
cybermalveillance.gouv.fr propose des supports et des conseils par thème pour comprendre et lutter contre la cybermalveillance : vidéos, fiches réflexes, fiches pratiques, infographies...