FICHE PRATIQUE A

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

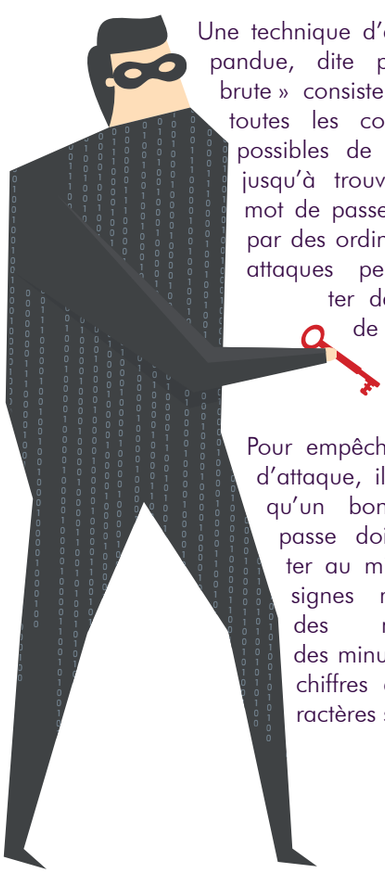
GÉRER SES MOTS DE PASSE

Messageries, réseaux sociaux, banques, administrations et commerces en ligne, réseaux et applications d'entreprise… la sécurité de l'accès à tous ces services du quotidien repose aujourd'hui essentiellement sur les mots de passe. Face à la profusion des mots de passe, la tentation est forte d'en avoir une gestion trop simple. Mais une telle pratique serait dangereuse, car elle augmenterait considérablement les risques de compromettre la sécurité de vos accès. Cette fiche pratique présente les **10 principales règles à adopter pour gérer efficacement ses mots de passe et assurer ainsi au mieux sa sécurité numérique.**

1 Utiliser un mot de passe différent pour chaque accès

Ainsi en cas de perte ou de vol d'un de vos mots de passe seul le service concerné sera vulnérable. Dans le cas contraire, tous les services sur lesquels vous utilisez le même mot de passe compromis seraient piratables.

2 Utilisez un mot de passe suffisamment long et complexe



Une technique d'attaque répandue, dite par « force brute » consiste à essayer toutes les combinaisons possibles de caractères, jusqu'à trouver le bon mot de passe. Réalisées par des ordinateurs, ces attaques peuvent tester des dizaines de milliers de combinaisons par seconde. Pour empêcher ce type d'attaque, il est admis qu'un bon mot de passe doit comporter au minimum 12 signes mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux.

3 Utilisez un mot de passe impossible à deviner

Une autre technique d'attaque utilisée par les pirates est d'essayer de « deviner » votre mot de passe. Évitez donc d'employer dans vos mots de passe des informations personnelles qui pourraient être faciles à retrouver (sur les réseaux sociaux par exemple), comme le prénom de votre enfant, une date anniversaire, ou votre groupe de musique préféré. Évitez également les suites logiques simples comme 123456, azerty, abcdef… qui font parties des listes de mots de passe les plus courants et qui sont les premières combinaisons qu'essaieront les cybercriminels pour essayer de forcer vos comptes.

4 Utilisez un gestionnaire de mots de passe

Il est humainement impossible de retenir les dizaines de mots de passe longs et complexes que chacun est amené à utiliser quotidiennement. Ne commettez pas pour autant l'erreur de les noter sur un pense-bête que vous laisseriez à proximité de votre équipement, ni de les inscrire dans votre messagerie, ou dans un fichier non protégé de votre ordinateur ou encore dans votre téléphone mobile auquel un cybercriminel pourrait avoir accès. Apprenez à utiliser un gestionnaire de mot de passe sécurisé qui s'en chargera à votre place, pour ne plus avoir à retenir que le seul mot de passe qui permet d'en ouvrir l'accès. *Voir notre encadré sur Keepass.*

5 Changez votre mot de passe au moindre soupçon

Vous avez un doute sur la sécurité d'un de vos comptes ou vous entendez qu'une organisation ou une société chez qui vous avez un compte s'est fait pirater. N'attendez pas de savoir si c'est vrai ou pas. Changez immédiatement le mot de passe concerné avant qu'il ne tombe dans de mauvaises mains.

EXEMPLES DE MÉTHODES POUR CRÉER UN MOT DE PASSE SOLIDE

LA MÉTHODE DES PREMIÈRES LETTRES
Un tien vaut mieux que deux tu l'auras
1tvmQ2tl'A

LA MÉTHODE PHONÉTIQUE
J'ai acheté huit CD pour cent euros cet après-midi
ght8CD%E7am

Inventez votre propre méthode connue de vous seul !

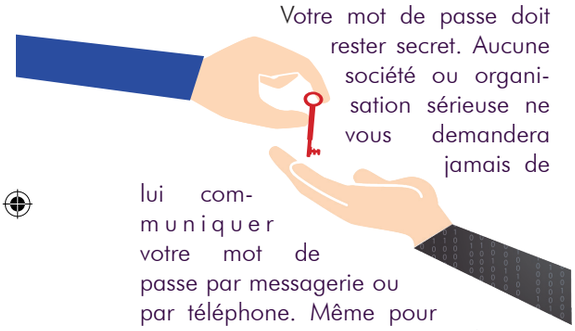
KEEPASS

UN GESTIONNAIRE DE MOTS DE PASSE SÉCURISÉ ET GRATUIT

Ce petit logiciel libre et en français, certifié par l'ANSSI, permet de stocker en sécurité vos mots de passe pour les utiliser dans vos applications. Il dispose aussi d'une fonction permettant de générer des mots de passe complexes aléatoires.

https://keepass.info

6 Ne communiquez jamais votre mot de passe à un tiers



Votre mot de passe doit rester secret. Aucune société ou organisation sérieuse ne vous demandera jamais de lui communiquer votre mot de passe par messagerie ou par téléphone. Même pour une « maintenance » ou un « dépannage informatique ». Si l'on vous demande votre mot de passe, considérez que vous êtes face à une tentative de piratage ou d'escroquerie.

7 N'utilisez pas vos mots de passe sur un ordinateur partagé

Les ordinateurs en libre accès que vous pouvez utiliser dans des hôtels, cybercafés et autres lieux publics peuvent être piégés et vos mots de passe peuvent être récupérés par un criminel. Si vous êtes obligé d'utiliser un ordinateur partagé ou qui n'est pas le vôtre : utilisez le mode de « navigation privée » du navigateur qui permet d'éviter de laisser trop de traces informatiques ; veillez à bien fermer vos sessions après utilisation ; 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.

8 Activez la « double authentification » lorsque c'est possible

Pour renforcer la sécurité de vos accès, de plus en plus de services proposent cette option. 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 exemple, 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. *Voir encadré.*

9 Changez les mots de passe par défaut des différents services auxquels vous accédez

De nombreux services proposent des mots de passe par défaut que vous n'êtes parfois pas obligés de changer. Ces mots de passe par défaut sont souvent connus des cybercriminels. Aussi, il est important de les remplacer au plus vite par vos propres mots de passe que vous contrôlez.

EXEMPLES (NON EXHAUSTIFS) DE SERVICES RÉPANDUS PROPOSANT LA DOUBLE AUTHENTIFICATION

- Outlook, Gmail, Yahoo Mail...
- Facebook, Google +, Instragram, LinkedIn, Twitter...
- Skype, WhatsApp...
- Amazon, eBay, Paypal...
- Apple iCloud, Dropbox, Google Drive, OneDrive...

10 Choisissez un mot de passe particulièrement robuste pour votre messagerie

Votre adresse de messagerie est généralement associée à beaucoup de vos comptes en ligne. Cela 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. Votre mot de passe de messagerie est donc un des mots de passe les plus importants à protéger.

POUR ALLER PLUS LOIN :

- Le site de la CNIL : www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe
- Le site de l'ANSSI : www.ssi.gouv.fr/guide/mot-de-passe

DOCUMENT RÉALISÉ AVEC NOS MEMBRES :

Fédération Française de l'Assurance · KASPERSKY lab · LE GROUPE LA POSTE · signal spam

En partenariat avec l'Agence nationale de la sécurité des systèmes d'information

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Version 1.0