FORMATIO | RESSOURCE INFORMATIQUE BUREAUTIQUE

LES CONSEILS POUR UN BON MOT DE PASSE

PRÉSENTÉ. PAR ALAIN WAGNER B. GEST.

Mot de passe

- *Banque, e-commerce, messagerie électronique, documents, administration : de nombreuses démarches de notre vie quotidienne passent désormais par Internet et par la création de comptes sur les différents sites. Nombre de ces espaces privatifs contiennent des informations confidentielles qui ne doivent pas être rendues disponibles à des personnes non habilitées.*

- *Pour accéder à nos comptes en ligne, nous utilisons souvent des mots de passe « faibles » ou le même mot de passe sur plusieurs comptes. Voici quelques astuces pour gérer ses mots de passe personnels en toute sécurité.*

Mot de passe – Un mot de passe en béton

Un bon mot de passe doit contenir au moins 12 caractères et 4 types différents : des minuscules, des majuscules, des chiffres et des caractères spéciaux.

MOT DE PASSE, LES MESURES DE SÉCURITÉ MINIMALES

Mot de passe	Longueur minimum	Composition	Mesures complémentaires	Exemple
Seul	12	• Majuscules, • Minuscules, • Chiffres, • Caractères spéciaux.	Conseiller l'utilisateur sur un bon mot de passe	Back office de blog, gestionnaires de mot de passe en ligne
Avec restriction d'accès	8	Au moins 3 des 4 types suivants : • Majuscules, • Minuscules, • Chiffres, • Caractères spéciaux.	Mesures de restriction d'accès au compte : • Temporisation d'accès au compte après plusieurs échecs • Verrouillage du compte après 10 échecs • Captcha	Site e-commerce
Avec information complémentaire	5	Chiffres et/ou lettres	Mesures de restriction d'accès au compte : + • Information complémentaire communiquée en propre d'une taille d'au moins 7 caractères (exemple, identifiant dédié au service) ou • Collecte de données identifiant le terminal de l'utilisateur (adresse IP, adresse mac, user agent...)	Banque en ligne
Avec matériel détenu par la personne	4	Chiffres	• Matériel détenu en propre par la personne (carte sim, carte bancaire, certificat) • Blocage au bout de 3 tentatives échouées	Carte bancaire ou téléphone

Mot de passe – Il ne dit rien sur vous

Personne ne doit deviner votre mot de passe à partir du nom de votre chien ou de votre film préféré.

Idem pour le code de votre smartphone : préférez un nombre aléatoire à une année.

- Ne jamais enregistrer de données intimes ou confidentielles.
- Activer le code PIN demandé à chaque allumage.
- Activer le code de verrouillage demandé après chaque mise en veille.
- Conserver le code IMEI en cas de perte ou de vol. (Pour connaître votre **code IMEI**, il suffit de taper *#06# sur le clavier de votre portable.)

Mot de passe – Un compte, un mot de passe

Pour éviter les piratages en cascade, chacun de vos comptes en ligne qui présente un caractère sensible (banque, messagerie, réseau social, etc.) doit être verrouillé avec un mot de passe propre et unique.

L'utilisation d'un mot de passe faible vous expose à des risques:

• Usurpation de votre boite de courriel pour piéger votre liste de contacts ;
• Ajout d'une redirection de mail (souvent indétectable après la compromission d'une boite de courriel) : vos courriels continuent de fuiter malgré tout changement de mot de passe ultérieur…
• Connexion du pirate à vos sites et applications tierces ;
• Utilisation de vos coordonnées bancaires pour payer ;
• Usurpation d'identité grâce aux données collectées dans votre boite de courriel ;
• Demande de rançon suite à des données compromettantes retrouvées dans votre boite de courriel.

Mot de passe – Ne jamais l'abandonner en pleine nature

Les post-it, les fichiers texte, votre smartphone ou votre boite de messagerie ne sont pas conçus pour sécuriser le stockage de vos mots de passe.

Pensez aussi à ne jamais les enregistrer dans le navigateur d'un ordinateur partagé.

Mot de passe – Deux cadenas valent mieux qu'un

Quand le service vous le propose, activez la double authentification. Si quelqu'un se connecte à votre compte depuis un terminal inconnu, le site vous prévient par SMS/courriel. Libre à vous d'autoriser ou de refuser l'accès !

Mot de passe - Les retenir sans les écrire … en travaillant vos neurones

Mémorisez une phrase puis utilisez la première lettre de chaque mot pour créer votre mot de passe. La phrase doit contenir des chiffres et des caractères spéciaux !
Utiliser un générateur qui permet de concevoir votre mot de passe en quelques secondes !

Mot de passe - Gestionnaires

Les retenir sans les écrire … en reposant vos méninges

Utilisez un gestionnaire de mots de passe ou un trousseau d'accès chiffré pour stocker vos mots de passe en toute sécurité. Vous n'aurez à retenir qu'un mot de passe pour accéder à l'ensemble de vos comptes !

Mot de passe - Gestionnaires

Un gestionnaire de mots de passe permet de constituer une base de données de mots de passe chiffrée par un unique mot de passe « maître » dont la sécurité a pu être vérifiée.

Cela vous permet de ne retenir qu'un seul mot de passe qui ouvre l'accès à tous les autres. Les mots de passe pourront alors être très longs, très complexes et tous différents car c'est l'ordinateur qui les retient à votre place.

Ces logiciels facilitent par ailleurs la saisie, sans erreurs, des mots de passe et permet de retenir les nombreux identifiants et comptes que l'on collectionne avec le temps.

En pratique, il existe de nombreuses solutions sur le marché. On peut citer entre autres, parmi les logiciels libres régulièrement mis à jour :

- Dashlane dont la sécurité a été évaluée par l'Agence nationale de sécurité des systèmes d'information (ANSSI) (coté 9.8/10)
- Roboform – (coté 9.3/10)
- Password Boss – (coté 9.2/10)

Mot de passe – Gestionnaires- Calculer les risques

- <Oui, mais avoir tous ses mots de passe au même endroit, ça me semble dangereux, non ?>
- C’est certain que c’est un risque à prendre. Rien n’est parfait dans le merveilleux monde de la sécurité.
- Il faut donc choisir un gestionnaire possédant une méthode de chiffrement solide.
- Un gestionnaire de mots de passe est un compromis entre une utilisation simple et une utilisation sécuritaire.
- Ils sont donc construits de manière à avoir un équilibre entre un utilisation simple et une sécurité accrues.
- Leur utilisation vous ralentira, mais c’est définitivement mieux que rien

Mot de passe – Les plus utilisés

Rank	Password	Change from 2017
1	123456	Unchanged
2	password	Unchanged
3	123456789	Up 3
4	12345678	Down 1
5	12345	Unchanged
6	111111	New
7	1234567	Up 1
8	sunshine	New
9	qwerty	Down 5
10	iloveyou	Unchanged
11	princess	New
12	admin	Down 1
13	welcome	Down 1
14	666666	New
15	abc123	Unchanged
16	football	Down 7
17	123123	Unchanged
18	monkey	Down 5
19	654321	New
20	!@#$%^&*	New
21	charlie	New
22	aa123456	New
23	donald	New
24	password1	New
25	qwerty123	New