VIRGINIS TECHNOLOGIES

LES **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. Une telle pratique serait dangereuse, car elle augmenterait considérablement les risques de compromettre la sécurité de vos accès. **Voici 10 bonnes pratiques à adopter pour gérer efficacement vos mots de passe.**

1 UTILISEZ UN MOT DE PASSE DIFFÉRENT POUR CHAQUE SERVICE

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 pour 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 partie des listes de mots de passe les plus courants et qui sont les premières combinaisons qu'essaieront les cybercriminels pour tenter de forcer vos comptes.

4 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.

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 société chez qui vous avez un compte s'est faite 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.

Contactez-nous Email : commercial@virginis.tech - Tél : 0972 100 999 (appel non surtaxé)

COMMENT CRÉER UN MOT DE PASSE SOLIDE ?

LA MÉTHODE DES PREMIÈRES LETTRES
Un tiens 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 !

6 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 une confirmation que vous pouvez recevoir, par exemple, sous forme de code provisoire reçu par SMS ou par courrier électronique (e-mail), via une application ou une clé spécifique que vous contrôlez, ou encore par reconnaissance biométrique.

Ainsi grâce à cette confirmation, vous seul pourrez autoriser un nouvel appareil à se connecter aux comptes protégés. ***Voir encadré.***

7 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 obligé 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.

QUELQUES SERVICES PROPOSANT LA DOUBLE AUTHENTIFICATION

Outlook/Hotmail, Gmail, Yahoo Mail...
• Facebook, Instagram, LinkedIn, Snapshat, Tik Tok, Twitter...
• Skype, Teams,
• WhatsApp, Zoom...
• Amazon, eBay, Paypal...
• Apple iCloud, Dropbox, Google Drive, OneDrive...

8 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, comme 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.

*Également appelée « authentification forte », « authentification multifacteurs », « 2FA », « vérification en deux étapes », « validation en deux étapes », « authentification à deux facteurs », « identification à deux facteurs », « vérification en deux temps »...