Commandement n°1 -Tu changeras régulièrement tes mots de passe et ils seront de qualité. Ta session utilisateur se verrouillera automatiquement

A quoi sert un mot de passe

Le mot de passe est un des moyens d'authentification qui permet de vérifier que la personne qui s'identifie est bien celle qu'elle prétend être. Il convient donc que ce mot de passe reste confidentiel et qu'il soit de qualité pour éviter qu'une personne malveillante ne le retrouve facilement.

Choix d'un mot de passe de qualité

Criticité des données protégées par le mot de passe

Il existe de nombreux moyens pour définir un mot de passe de qualité (complexité, longueur...). Plus les données protégées par un mot de passe sont critiques, plus celui-ci devra être de qualité. Par exemple, le mot de passe d'accès à votre compte bancaire devra être de très bonne qualité par rapport à celui qui vous permet d'accéder à un site d'information.

Longueur du mot de passe

Plus votre mot de passe est long, plus il sera difficile à une personne malveillante (pirate, concurrent...) de le trouver. Si vos données sont cruciales, il est recommandé de choisir un mot de passe d'au moins 12 caractères.

Pas d'information personnelle dans le mot de passe

Le mot de passe ne doit pas comporter d'informations personnelles. Lors du choix d'un mot de passe, ne pas utiliser votre nom, votre prénom, votre date de naissance, votre numéro de téléphone, le nom de vos enfants, votre plaque d'immatriculation... Ces informations sont faciles à trouver.

Changement régulier de vos mots de passe

Pour les accès à des données sensibles, il est fortement conseillé de changer régulièrement vos mots de passe.

Variété des caractères utilisés dans les mots de passe

Utiliser à la fois des minuscules, des majuscules, des chiffres et des caractères spéciaux ($!&%*/*-+µ …).

Mot de passe de votre messagerie

De nombreux sites web vous permettent de régénérer votre mot de passe en cas d'oubli, en vous envoyant un courriel. Il convient donc de protéger fortement l'accès à votre messagerie en utilisant un mot de passe de qualité.

Mots de passe différents

Si vous possédez plusieurs comptes d'authentification (internet, professionnel, à domicile...), il est vivement conseillé d'avoir un mot de passe différent pour chacun de ces comptes d'accès.

Confidentialité d'un mot de passe

Il convient de ne pas divulguer ses mots de passe ; dans la plupart des cas, vous devez être la seule personne à les connaître. Si vous devez partager un mot de passe, évitez de le communiquer par courriel ou par écrit.
Lorsque vous saisissez votre mot de passe dans une application web, vérifiez que le cadenas est fermé (ne manquez pas de lire prochainement le commandement "Lors de l'envoi de données confidentielles sur internet, tu vérifieras que le cadenas est verrouillé ").

Comment mémoriser son mot de passe

Pour mémoriser plus facilement vos mots de passe et pour éviter par exemple de les écrire sur un papier ou dans un fichier non sécurisé, nous vous proposons les techniques suivantes :

- prendre les premières lettres d'une phrase ou expression. Par exemple : "Il est plus facile de désintégrer un atome qu'un préjugé" (A. Einstein) donnera le mot de passe "i&+f2d1aq'1p", ou "Na te 'auvaha o te Clusir e huri i tera parau i roto i te reo Tahiti" générera le mot de passe "Nt'aotCehitpiritrT"
- utiliser la méthode phonétique. Par exemple : "Elle a deux fois plus de Bandes Dessinées et de CD" donnera le mot de passe "la2x+2BD&2CD"

Outils

Des programmes ont été créés pour faciliter la gestion des mots de passe.
Certains génèrent des mots de passe totalement aléatoires avec des critères prédéfinis (longueur, nombre de caractères spéciaux, …) : par exemple PWGen (http://pwgen-win.sourceforge.net/).
D'autres permettent de stocker de manière sûre les mots de passe, par exemple KeePass (http://keepass.info/).

Verrouillez votre session, déconnectez vous

Quand vous n'utilisez plus votre poste de travail, votre ordinateur, votre smartphone, pensez à verrouiller votre session utilisateur pour éviter qu'une personne malveillante n'accède à vos données. La plupart des systèmes d'exploitation (Windows, Mac OS, Linux, Android...) permettent de configurer un verrouillage automatique de votre appareil après une période donnée d'inactivité de votre part.
De même, lorsque vous vous connectez à des applications sur internet, pensez à vous déconnecter quand vous n'en avez plus besoin, et vérifiez que le navigateur ne mémorise pas vos mots de passe les plus importants.