Les règles de sécurité informatique des mots de passe

Une des règles essentielles de bonne gestion de la sécurité informatique est que chaque utilisateur doit avoir son login et son mot de passe et que les règles de renouvellement des logins et des mots de passe soient définies.

Cette fiche technique vous détaille les notions à connaître au sujet des mots de passe.

Objet du mot de passe

Dans le monde informatique, le mot de passe est l'équivalent d'une clef donnant accès à des informations, des logiciels, des matériels ou des réseaux.
Il peut permettre :

- de restreindre les accès à une base de données,
- de verrouiller l'accès à un document,
- d'interdire l'usage à un logiciel applicatif,
- de limiter l'accès à un système d'exploitation et aux fichiers le constituant,
- de masquer les fichiers ou informations confidentielles,
- de contingenter les droits d'utilisation d'un système, de contrôler les utilisateurs accédant à un disque partagé via le réseau,
- d'authentifier la personne qui accède à une boite de courrier électronique,
- etc.

En résumé, le mot de passe permet de contrôler l'accès ou l'utilisation d'une ressource ayant de la valeur.
En revanche, il est inutile de protéger quelque chose qui n'a pas de valeur.

Que peut faire un tiers avec votre mot de passe ?

Au niveau professionnel

Accéder à des dossiers médicaux confidentiels (CR, clinique médicale, résultats d'examen, …).
Modifier vos saisies et vos données professionnelles.

Les activités personnelles

Un tiers malveillant peut se substituer à vous pour (liste non exhaustive) :

- Envoyer des mails de votre part.
- Répondre à votre place à des mails.
- Prendre des rendez-vous pour vous.
- Ouvrir de nouveaux comptes et effectuer de nombreux achats.
- Discuter en ligne en votre nom.
- Mener des enchères à votre place.
- Annuler des enchères qui gênent sans votre avis.
- Effectuer des virements auprès de votre banque.
- Acheter ou vendre des actions.
- Souscrire des emprunts, y compris des hypothèques.
- Accéder aux informations qui se trouvent sur votre ordinateur, telles que vos enregistrements financiers, vos messages électroniques, vos listes de mots de passe stockés et vos informations privées.

Il faut savoir que votre responsabilité juridique est engagée si votre mot de passe est piraté et utilisé à des fins répréhensibles, voire criminelles :
- envoi de propos racistes dans les forums,
- envoi massif de courriers non désirés (spams),
- visite de sites pédophiles,
- arnaque à la carte bancaire,
- piratage informatique,
- terrorisme,
- etc.

Règles d'utilisation des mots de passe

Un mot de passe est strictement personnel et confidentiel et ne doit être ni partagé, ni confié à autrui.

Il faut changer impérativement les mots de passe attribués d'office lors de la première connexion.

Si pour une raison quelconque, vous devez confier un mot de passe, cela doit être temporaire et il devra être changé aussi vite que possible.

Un mot de passe ne doit être utilisé qu'une seule fois. On ne doit pas se servir d'un mot de passe utilisé 6 mois auparavant par manque d'imagination.

Pour chaque système qui nécessite un mot de passe, il est conseillé d'utiliser un mot de passe différent.

Un mot de passe doit avoir une durée limitée. Il doit donc être modifié régulièrement. Cette modification ne doit pas être une simple variante, mais une réécriture complète.

Comment doit être formulé un mot de passe ?

Le mot de passe doit être :
- un mot signifiant,
- facile à mémoriser,
- choisi avec une fréquence de modification prédéfinie,
- éventuellement un trait d'humour,
- difficile à trouver, mais facile à retenir,
- absent du dictionnaire.

Les pièges à éviter pour choisir un mot de passe

Il convient d'éviter les mots de passe faciles à découvrir :
- Les mots de passe classiques : 123, bonjour, mois en cours, …
- Un mot de passe utilisé sur un autre système.
- Le nom d'utilisateur.
- Le prénom.
- Le nom ou prénom d'un membre de la famille.
- Le surnom.
- Le numéro de sécurité sociale.
- Les combinaisons de syllabes extraites de nom ou de prénom.
- Le nom de la ville de résidence.
- Le nom de l'animal de compagnie, du bateau, de la maison de vacances, …
- Les numéros de plaque de voiture ou de téléphone.
- La date de naissance personnelle ou des proches.
- Le mot de passe identique au login.

- Le nom du service.
- Les combinaisons de lettres contiguës sur le clavier « azerty ».

Le mot de passe ne doit pas être écrit sur un post-it, le clavier, la souris ou sur l'écran.

Comment se protéger correctement ?

Utiliser la longueur maximum autorisée par votre système, même si cela vous semble un peu long : 6 à 8 caractères minimum.

Choisir un mot de passe avec au moins 2 lettres majuscules, des minuscules, des chiffres, des caractères de ponctuation et des signes spéciaux. Un mot de passe constitué de cette façon sera beaucoup plus difficile à trouver qu'un mot de passe constitué uniquement de lettres.

Bannir les noms communs du dictionnaire assortis d'un chiffre. Exemple : « château 1 » remplacé par « château 2 » le mois suivant. Le mot de passe ne doit être ni évident, ni être un vrai mot.

Proscrire votre vie : nom, prénom personnel ou de la famille, lieu de voyage, dates, passions, …

Caractères spéciaux : si votre système l'autorise, utiliser les caractères spéciaux tels que les signes de ponctuation. Eviter la majuscule en tête qui est tellement évidente qu'elle ne protège plus.

Utiliser une méthode mnémotechnique pour vous souvenir de votre mot de passe.

Il est conseillé de choisir un mot de passe avec la méthode phonétique :

Ex : « J'ai acheté 8 CD pour 100 euros cet après-midi » deviendra « ght8CD%E7am » ; ou « un tiens vaut mieux que deux tu l'auras » deviendra « 1tvmQ2tl'A ».