INFORMATIQUE I-41	Protection et sécurité Mots de passe	E.GEOFFROY 2021

La cybercriminalité

Ces cybercriminels n'hésitent pas à utiliser des logiciels de piratage dans le but d'obtenir vos données et informations personnelles qui sont souvent protégées par un simple mot de passe.

Leur fonctionnement est simple : à partir d'une base de données des mots de passe les plus utilisés et de quelques-unes de vos informations : nom, prénom, adresse (souvent récupérées sur Internet ou tout simplement sur des papiers jetés dans la poubelle) un logiciel se lance et enchaîne les combinaisons jusqu'à tomber sur la bonne. La découverte peut prendre seulement 10 secondes pour les mots de passe les plus simples et jusqu'à plusieurs années pour les plus complexes.

Oubliez les mots de passe types 123456, password ou qwerty qui sont bien trop utilisés et bien trop faciles à pirater. Inutile de vous rappeler que le nom de votre chat ou chien ou de votre chanteur préféré sont à bannir également.

Les mots de passe les plus utilisés

Liste des **20 mots de passe les plus utilisés en France :**

1- 123456	2- 123456789	3- azerty	4- 1234561
5- qwerty	6- marseille	7- 0	8- 1234567891
9- doudou	10- 12345	11- loulou	12- 123
13- password	14- azertyuiop	15- 12345678	16- soleil
17- chouchou	18- 1234	19- 1234567	20- 123123

Les règles à respecter

Le gouvernement a mis en ligne les règles à respecter pour créer un bon mot de passe :

– **Règle nº1 : 12 caractères**

Un mot de passe sécurisé doit comporter **au moins 12 caractères**. Il peut être éventuellement plus court si le compte propose des sécurités complémentaires telles que le verrouillage du compte après plusieurs échecs, un test de reconnaissance de caractères ou d'images (« captcha »), la nécessité d'entrer des informations complémentaires communiquées par un autre moyen qu'Internet (exemple : un identifiant administratif envoyé par La Poste), etc.

– **Règle nº2 : des chiffres, des lettres, des caractères spéciaux**

Votre mot de passe doit se composer de **4 types de caractères différents** : majuscules, minuscules, chiffres, et signes de ponctuation ou caractères spéciaux (€, #…).

– **Règle nº3 : un mot de passe anonyme**

Votre mot de passe doit être **anonyme** : il est très risqué d'utiliser un mot de passe avec votre date de naissance, le nom de votre chien etc., car il serait facilement devinable.

– **Règle nº4 : la double authentification**

Certains sites proposent de vous informer par mail ou par téléphone si quelqu'un se connecte à votre compte depuis un terminal nouveau. Vous pouvez ainsi accepter ou refuser la connexion. N'hésitez pas à utiliser cette option.

Règle nº5 : renouveler ses mots de passe

Sur les sites où vous avez stocké des données sensibles, pensez à **changer votre mot de passe régulièrement** : tous les trois mois parait être une fréquence raisonnable.

Pour sécuriser vos comptes, les mots de passe doivent être différents sur tous les sites.

Exemples de mots de passe sécurisés :

- **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**

Mots de passe à déchiffrer :

Qdedt#2010 > ……

(solution : Qui dit étude dit travail (parole chanson Stromae) en 2010)

Rmldc!2017 > ……

(solution : Real de Madrid en ligue des champions en 2017)

p@t4t3 > ……

v@n3ss@ > ……

&hysl@!n > ……