

SÉGUR DU NUMÉRIQUE EN SANTÉ en Normandie

Accompagnement Cybersécurité

SÉGUR
NUMÉRIQUE

► GUIDE : "les mots de passe"





Table des matières

1. Pourquoi changer son mot de passe régulièrement ?	2
2. Comment changer son mot de passe Windows ?.....	2
3. Un mot de passe « fort » qu'est-ce que c'est ?.....	2
4. Définir et retenir facilement un mot de passe : quelques méthodes.....	2
4.1. La méthode PHONETIQUE	2
4.2. La méthode des PREMIERES LETTRES	3
4.3. La méthode de la PHRASE DE PASSE.....	3
4.4. L'ELEMENT CULTUREL	3
5. En synthèse pour un mot de passe fort	3
6. Comment me rappeler de tous les mots de passe ?.....	3
8. Les règles pour un bon code de téléphone.....	4

1. Pourquoi changer son mot de passe régulièrement ?



Si vous utilisez le même mot de passe sur plusieurs sites ou applications pour une utilisation professionnelle et/ou personnelle, **vous n'êtes pas à l'abri d'une fuite de votre mot de passe**. En effet, des compromissions de sites internet ont lieu chaque semaine.

Plus votre mot de passe est vieux, plus le risque augmente !

Si votre adresse électronique et votre mot de passe fuient, un pirate ne rencontrera aucune difficulté à accéder à l'ensemble de vos applications. Il pourra notamment voler votre identité et s'infiltrer sur le réseau informatique de votre entreprise.

C'est pour cela qu'il faut renouveler votre mot de passe régulièrement et privilégier le modèle :



Un mot de passe = Une application

2. Comment changer son mot de passe Windows ?



- Rendez-vous sur votre site de travail
- Ouvrez une session utilisateur
- Tapez « **CTRL + ALT + SUPPR** » sur votre clavier
- Sélectionnez « **Modifier un mot de passe** »

3. Un mot de passe « fort » qu'est-ce que c'est ?

Vous devez utiliser des mots de passe robustes contenant au **moins 12 caractères et incluant ces 4 éléments** :



- Majuscules
- Minuscules
- Chiffres
- Caractères spéciaux

4. Définir et retenir facilement un mot de passe : quelques méthodes

4.1. LA METHODE PHONETIQUE

On part d'une phrase que l'on transforme en mot de passe.

- « J'ai acheté huit cd pour cent euros cet après-midi » ► « **ght8CD%€7am** »
- « Jamais deux sans trois » ► « **J@mais2-100-3!** »

4.2. LA METHODE DES PREMIERES LETTRES

On part d'une phrase et on construit son mot de passe avec les premières lettres :

- « Un tien vaut mieux que deux tu l'auras » ► « 1tvmQ2tl'0r@ »

4.3. LA METHODE DE LA PHRASE DE PASSE

(Recommandée actuellement) :

On construit une phrase de 4 mots minimum dont l'enchaînement n'a de sens que pour vous ou qui répond à une logique qui vous est propre. Vous pouvez ensuite modifier quelques éléments pour complexifier (argot, majuscule, chiffre...).

- « Planche sable vent vague » ► « PI@nche-\$@ble-VenV@g »
- « Semaine Dodo enfants 8h00 ! » ► « \$em@ineD0D0_€nfant:8h00! »

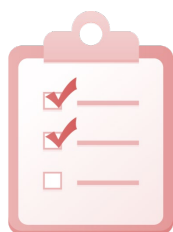
4.4. L'ELEMENT CULTUREL

(Révisez vos classiques en faisant de la sécurité) :

On prend une information historique, géographique ou autre comme base.

- « Le Mont-Blanc mesure 4807 mètres » ► « M0ntBl@nc=4807m! »
- « La Révolution française en 1789 » ► « Rév0lut°FR=1789 »
- « La seconde Guerre mondiale de 1939 à 1945 » ► « 2ndWW=1939-45 »

5. En synthèse pour un mot de passe fort



Un mot de passe doit être :

- ✓ Unique pour chacun de vos comptes
- ✓ Renouvelé tous les 3 mois
- ✓ Suffisamment long et complexe

Et ne doit pas :

- ✗ Contenir de mots de dictionnaire
- ✗ Être écrit (sur papier, post-it)
- ✗ Être partagé avec d'autres personnes

6. Comment me rappeler de tous les mots de passe ?

Avoir **plusieurs mots de passe** est une **très bonne chose**, ça permet de segmenter l'accès à vos informations personnelles (messagerie, banque...) **mais** il peut être **difficile de tous se les rappeler**.



Il existe des **coffres forts numériques** pour stocker vos mots de passe en sécurité.

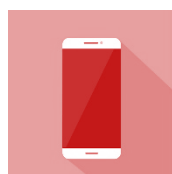
L'application « **KEEPASS** » (certifiée par l'**ANSSI**) est l'une des solutions recommandées.

Plus d'information sur :



- Keepass : <https://keepass.info/>
- Plus d'information sur les solutions certifiées ANSSI : <https://www.ssi.gouv.fr/administration/produits-certifies/cspn/produits-certifies-cspn/>

7. Et la sécurité de mon téléphone ?



Rappeler-vous une chose importante : **Les smartphones sont des ordinateurs !** Et soyons honnêtes, **ils contiennent beaucoup d'informations personnelles** (mails, photos, notes, comptes...) **Il faut donc les protéger !!**

Deux protections possibles :

- **Code PIN**
- **Code de déverrouillage**

Il est **recommandé d'activer les deux** (et pas le même code)

8. Les règles pour un bon code de téléphone



Votre code PIN doit être :

- ✓ Unique à votre téléphone
- ✓ Composé de chiffres différents

Et ne doit pas être :

- × 0000, 1234, 1111... 9999, 2022
- × Une date qui vous est familière
- × Écrit (sur papier/dos du téléphone)
- × Partagé avec d'autres personnes

SÉCURITÉ
NUMÉRIQUE

