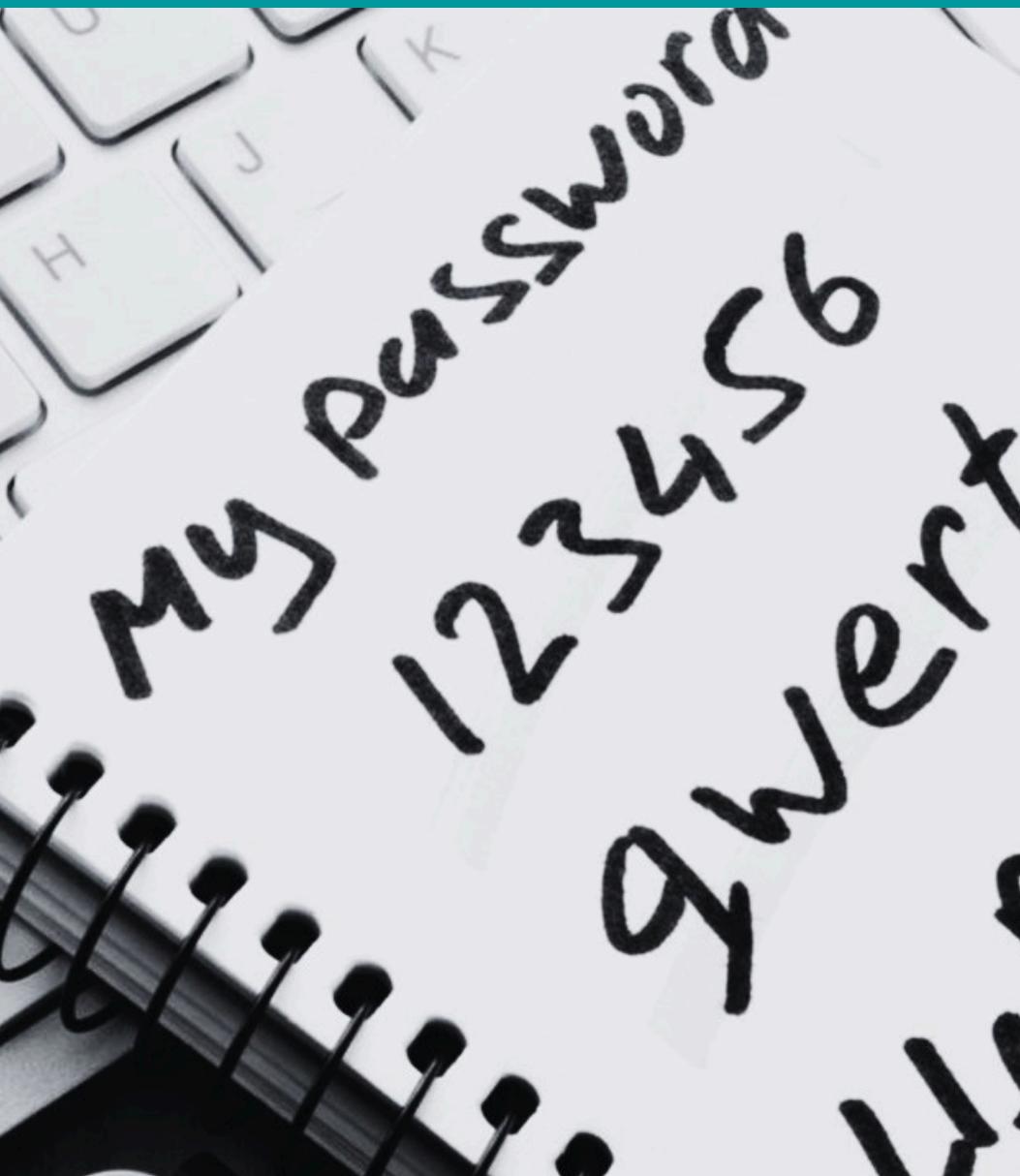


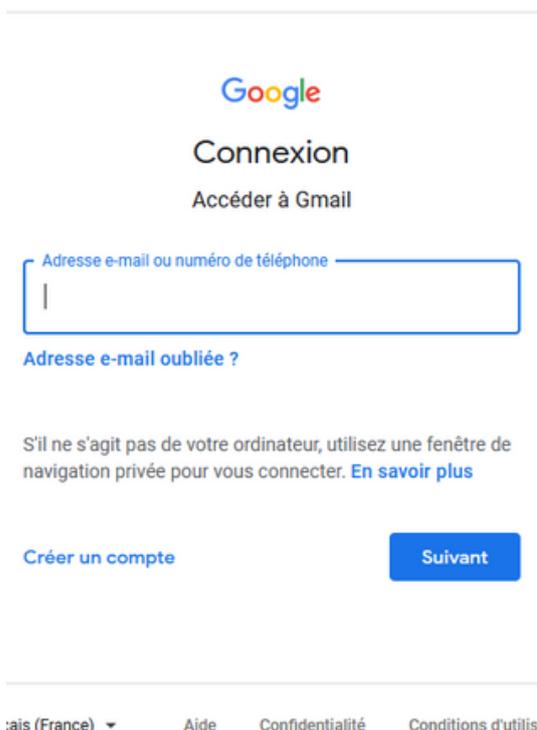
# FICHES RETEX RECOMMANDATIONS

## *Gestion des mots de passe*



*Quel est le lien entre un mot de passe et une brosse à dent ?*

Une brosse à dent se choisit avec soin, on ne la partage pas,  
on en change régulièrement et surtout on l'utilise !



The image shows a screenshot of the Google login page. At the top, the Google logo is displayed. Below it, the word "Connexion" is written in a large font, followed by "Accéder à Gmail" in a smaller font. There is a text input field with the placeholder text "Adresse e-mail ou numéro de téléphone". Below the input field, there is a link "Adresse e-mail oubliée ?". At the bottom of the page, there are two buttons: "Créer un compte" and "Suivant".



## REGLES D'USAGE

Les préconisations pour une bonne gestion d'un mot de passe sont :

- **Unique** (un seul mot de passe par site !!)
- **Secret** (un mot de passe partagé ne serait-ce qu'avec une seule personne n'est plus un secret)
- **Robuste** (il doit être résistant aux attaques et inintelligible)
- **A renouveler régulièrement** (cette mesure permet de contrer la furtivité/suspicion d'une compromission)

Il se compose idéalement de **12 à 14 caractères alphanumériques** minimum avec des **minuscules**, des **majuscules**, des caractères **spéciaux**, et il doit être impérativement **inintelligible**.

Restez vigilant si vous devez renseigner un mot de passe sur des hotspots gratuits (type Mac Do) ou des ordinateurs partagés. Utilisez une fenêtre de "navigation privée".

Évitez les pensées bêtes, les post-it ou les gestionnaires de vos smartphones et navigateurs (Firefox, Chrome, etc).

En cas de doute, changez-les immédiatement.

# UNE MÉTHODE SIMPLE ET EFFICACE

Le mot de passe se compose de différentes parties sur la base d'une **combinaison secrète** qui vous est **propre** et **intime** (une information très personnelle) : l'exemple retenu pour la démonstration est que vous adorez le film Autant en emporte le vent. Le but est de rendre le plus complexe possible la signification de cette base.

Vous définissez seul votre **propre méthodologie** (qui vous servira tout le temps) comme par exemple pour la démonstration suivante, prendre les premiers caractères des mots, ajouter des majuscules et des caractères spéciaux. On obtient donc dans un premier temps Autant en emporte le vent soit Aeelv - Vous renforcez cette **base** avec des **caractères spéciaux** et **alphanumériques** A devient @ et l devient | (obtenu avec la combinaison alt gr et touche 6) et par exemple la touche v devient 5 (en chiffre romain). On obtient @ee|5

Nous allons maintenant définir le mot de passe de votre boîte mail orange. Suivant votre méthodologie retenue et pour ce qui est de celle définie dans cet exemple, vous obtenez la combinaison Or@n (4 premiers caractères que vous avez complexifié à l'aide de votre méthodologie) - Votre mot de passe devient @ee|5Or@n

Composé de 9 caractères, nous allons renforcer ce mot de passe à l'aide d'une combinaison de touches très simples : On considère que vous êtes né en 1986 et que vous êtes originaire du 59, vous allez taper 8659 sans appuyer sur la touche MAJ de votre clavier, ce qui donne \_-(ç.

Votre mot de passe devient alors @ee|5Or@n\_-(ç pour accéder à votre boîte email orange.

Vous pouvez ainsi décliner cette méthode à vos différents espaces numériques :

Pour Facebook, votre mot de passe devient @ee|5F@ce\_-(ç

Pour Instagram, @ee|5Inst\_-(ç

.....et ainsi de suite.

Sans effort de mémoire et simplement, vous venez de définir une stratégie de mot de passe robuste et secret qui peut facilement être adaptable et modifiable.

Pour information, un attaquant met 0 seconde pour déchiffrer le mot de passe 1234567890122 contre plus de 30 ans pour @ee|5F@ce\_-(ç. Cette méthode renforcée par la double authentification vous protège grandement d'une possible atteinte.

# LA DEMONSTRATION

**LA BASE : Autant en emporte le vent = Aeelv = @ee|5**

**Né en 1986 et originaire du Nord du département 59**

**LES SITES CONCERNES :**

**Orange = Or@n**

**Facebook = F@ce**

**Gmail = Gm@i**

**MOT DE PASSE ENCORE FRAGILE : @ee|5Or@n8659**

Comme les chiffres 86 et 59 demeurent accessibles, il suffit simplement de faire la même saisie mais en retirant la touche MAJ ce qui nous donne un mot de passe robuste :

**MOT DE PASSE ROBUSTE : @ee|5Or@n\_-(ç**

1234567890122 = 4 minutes pour le « casser » contre 3 cent billions d'années pour @ee|5Or@n\_-(ç

Quelle est la sécurité de mon mot de passe?

L'outil n°1 pour renforcer les mots de passe. Approuvé et utilisé par des millions.

.....|

Cela prendrait à un ordinateur

**4 minutes**

pour trouver votre mot de passe

Quelle est la sécurité de mon mot de passe?

L'outil n°1 pour renforcer les mots de passe. Approuvé et utilisé par des millions.

.....|

Cela prendrait à un ordinateur

**6 mois**

pour trouver votre mot de passe

Quelle est la sécurité de mon mot de passe?

L'outil n°1 pour renforcer les mots de passe. Approuvé et utilisé par des millions.

.....|

Cela prendrait à un ordinateur

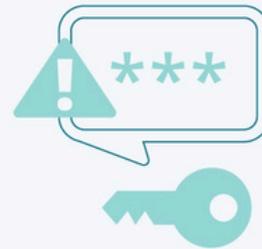
**3 hundred billion années**

pour trouver votre mot de passe

# LES PIRES MOTS DE PASSE

## Les pires mots de passe utilisés en France

Classement des mots de passe français les plus courants en 2019 \*



- |               |                |
|---------------|----------------|
| 1. 123456     | 11. loulou     |
| 2. 123456789  | 12. 123        |
| 3. azerty     | 13. password   |
| 4. 1234561    | 14. azertyuiop |
| 5. qwerty     | 15. 12345678   |
| 6. marseille  | 16. soleil     |
| 7. 000000     | 17. chouchou   |
| 8. 1234567891 | 18. 1234       |
| 9. doudou     | 19. 1234567    |
| 10. 12345     | 20. 123451     |

\* basé sur les fuites de données rendues publiques, filtrées sur les adresses e-mail en "fr".

Source : projet Richelieu



statista

## POINTS DE VIGILANCE

Certains **sites** (**bancaires** notamment) ne permettent pas de personnaliser votre mot de passe avec des caractères spéciaux. A vous d'adapter votre méthodologie.

Une autre alternative consiste à **avoir recours à un gestionnaire de mots de passe**. Je vous conseille d'utiliser LOCKPASS ou KEEPASS, tous deux certifiés par l'ANSSI.

## DOUBLE AUTHENTICATION

Pour renforcer votre sécurité liée à vos accès internet, il est vivement recommandé d'avoir recours à la double authentification (dont le but est de **fournir deux preuves d'identification distinctes** : je suis et je le prouve). Tous les services internet (Orange, Facebook, Gmail ...) permettent de renforcer la sécurité d'un compte à l'aide de cette double authentification.

Je vous conseille également le recours à une application telle que **GOOGLE AUTHENTICATOR** (sur Android et Apple).

## VÉRIFICATION DE COMPROMISSION DE DONNÉES À CARACTÈRE PERSONNEL

Une attaque informatique est par définition furtive et vous avez rarement connaissance que ces données ont été compromises. Parmi toutes les possibilités existantes de veiller sur ces dernières, la plus connue consiste à vérifier régulièrement sur le site <https://haveibeenpwned.com/>

Ce site recense toutes les données compromises et diffusées (sur le Darknet notamment) et vous permet ainsi de vérifier l'intégrité de celles-ci à travers votre adresse email et votre numéro de téléphone. En cas de retour positif, il vous renseigne sur la vulnérabilité.

Vous avez également possibilité de mettre en place une **veille permanente (alerte)** sur ce même site.

';--have i been pwned?

Check if your email or phone is in a data breach

email or phone (international format)

pwned?

# QUE FAIRE EN CAS DE COMPROMISSION?

Il est vivement préconisé de **procéder à un nettoyage** de vos différents périphériques (ordinateur et smartphone, ce dernier étant le premier vecteur d'attaque) et entreprendre une **démarche d'amélioration** quant à la gestion de vos mots de passe. Voici les préconisations les plus courantes (non exhaustives) :

- **Bannir les adresses emails qui renseignent l'attaquant sur votre véritable identité** (par ex patrick.dupont@orange.fr). Cela n'est d'aucune utilité et en cas de compromission, cela fournit un grand nombre de renseignements (profession, qualité ou prime au journal officiel, adresse, famille, etc ). Autant de renseignements qui permettent à l'auteur de vous nuire.
- **Nettoyez tous vos périphériques** (PC et téléphone) avec des **logiciels de sécurité** (antivirus, anti-malware, etc). Dans la mesure du possible faite une **sauvegarde** de toutes vos données sur un périphérique extérieur puis procédez à une **réinstallation** complète de votre système d'exploitation.

Je vous recommande de consulter le site <https://www.av-test.org/fr/> de l'institut AV-TEST GmbH, laboratoire indépendant qui soumet à des tests de qualités comparatives et individuels toutes les solutions antivirales du marché (gratuites et payantes), que ce soit pour Windows, Apple, ou téléphone Android ou Apple. Un classement est publié tous les trimestres.

Attention, un smartphone doit impérativement avoir au minimum un **antivirus**.

-**Changez tous vos mots de passe depuis un ordinateur que vous n'avez jamais utilisé auparavant** (on considère que le vôtre est compromis). Le fait de changer vos mots de passe va automatiquement déconnecter tous vos périphériques dont ceux compromis.

-**Veillez scrupuleusement à vérifier les adresses de secours ou de redirection** de vos comptes réseaux sociaux ou adresses email (les auteurs renseignent une autre adresse au travers de laquelle ils continuent de vous espionner).

-**Adoptez la double authentification.**

-Si des **emails de chantage** (bitcoin) vous sont adressés, conserver les entêtes d'email (Voir Cntech ou la cellule).

-**Restez vigilant** car vous avez été ciblé et vous restez ainsi vulnérable.

-Toutes les solutions de **remédiation** ne peuvent être ici évoquées. Pour aller plus loin, vous pouvez vous rendre sur le site <https://www.malekal.com/>



# MES MOTS DE PASSE



1) J'applique une hygiène stricte concernant mes identifiants et **je ne crée pas d'adresse email comprenant mon nom et mon prénom** :

Les préconisations pour une bonne gestion d'un mot de passe sont :

- **Unique** (un seul mot de passe par site !!)
- **Secret** (un mot de passe partagé ne serait-ce qu'avec une seule personne n'est plus un secret)
- **Robuste** (il doit être résistant aux attaques et inintelligible)
- **A renouveler régulièrement** (cette mesure permet de contrer la furtivité/suspicion d'une compromission)

Il se compose idéalement de **12 à 14 caractères alphanumériques** minimum avec des **minuscules**, des **majuscules**, des caractères **spéciaux**, et il doit être impérativement **inintelligible**

**LA BASE : Autant en emporte le vent = Aeelv = @ee|5**

**Né en 1986 et originaire du Nord du département 59**

**LES SITES CONCERNES :**

**Orange = Or@n**

**Facebook = F@ce**

**Gmail = Gm@i**

**MOT DE PASSE ENCORE FRAGILE : @ee|5Or@n8659**

Comme les chiffres 86 et 59 demeurent accessibles, il suffit simplement de faire la même saisie mais en retirant la touche MAJ ce qui nous donne un mot de passe robuste :

**MOT DE PASSE ROBUSTE : @ee|5Or@n\_-(ç)**



2) J'automatise la vérification de la vulnérabilité de mes identifiants et de mon numéro de téléphone en activant la fonction "Notify me" sur le site <https://haveibeenpwned.com/>

3) J'adopte la double authentification dès que c'est possible.