



## 10 règles pour gérer vos mots de passe

**1**   
Utilisez un **mot de  
passe différent** pour  
chaque accès

**2**   
Utilisez un mot de  
passe suffisamment  
**long et complexe**

**3**   
Utilisez un mot de  
passe **impossible  
à deviner**

**4**   
Utilisez un  
**gestionnaire de  
mots de passe**

**5**   
**Changez** votre  
mot de passe  
**régulièrement et  
au moindre  
soupçon**

**6**   
**Ne communiquez  
jamais** votre mot de  
passe **à personne**

**7**   
**N'utilisez pas** vos  
mots de passe sur  
un **ordinateur  
partagé**

**8**   
Activez la **double  
authentification**  
lorsque c'est  
possible

**9**   
**Changez les mots  
de passe par  
défaut** des  
services/équipeme  
nts auxquels vous  
accédez

**10**   
**N'écrivez pas** votre  
mot de passe sur un  
**papier** ou dans un  
fichier électronique  
non chiffré

## 10 Règles pour gérer vos mots de passe

### 1. Un mot de passe différent pour chaque accès

Cela permettra de limiter les dégâts en cas de vol/divulgateur.  
Choisissez pour vos comptes SG, des mots de passe différents de vos comptes à usage personnel.

### 2. Un mot de passe suffisamment long et complexe

Minimum 8 caractères + Chiffres (1, 2, 3, ...) + Lettres (a, b, c, ...) + Majuscules (A, B, C, ...) + minuscules (a, b, c, ...) + Caractères spéciaux (@, \*, #, +, \$, ...)

### 3. Un mot de passe impossible à deviner

Évitez d'utiliser des dates de naissance/mariage, nom/prénoms, nom de filiale, nom de direction, ...  
Évitez des mots de passe triviaux ou communs tels que : **Password**, **P@ssw0rd**, **Mot2p@ssE**, **Motdepasse**, **Banque12022**, **R0ot/22**, **Sankara@2022**, **SGBF12021**, ...

### 4. Un gestionnaire de mots de passe

L'outil **KeePass** homologué par le groupe vous propose des mots de passe robustes, les conserve de manière sécurisée et vous limite le nombre de mots de passe à retenir.

### 5. Un mot de passe régulièrement changé

Changez les au minimum tous les 90 jours et au moindre soupçon de compromission.

### 6. Ne jamais partager votre mot de passe

Il est strictement personnel. Il ne doit jamais être communiqué à personne.

### 7. Ne l'utilisez pas sur un ordinateur partagé

Sur un ordinateur partagé, un keylogger peut permettre d'enregistrer vos frappes de clavier. Ne saisissez vos mots de passe SG que sur votre ordinateurs SG.

### 8. Activez la double authentification si possible

Ainsi un facteur supplémentaire que vous seul êtes à même de posséder servira à vous authentifier en plus de votre mot de passe.

### 9. Changez les mots de passe par défaut

Remplacez-les systématiquement car une simple recherche sur Internet permet généralement de les retrouver.

### 10. Ne l'écrivez pas n'importe où

Ne le conservez pas sur un papier physique ou dans un document non chiffré sur votre ordinateur ou dans un répertoire partagé.