

# Recommandations de la CNIL sur les mot de passe (Délibération n° 2017-012 du 19 janvier 2017)

*Le mot de passe reste le moyen d'authentification le plus répandu. Alors que les compromissions de bases entières de mots de passe se multiplient, la CNIL a adopté une nouvelle recommandation sur les mots de passe. Elle fixe les mesures minimales à mettre en œuvre.*

x	<b>Recommandations de la CNIL sur les mot de passe (Délibération n° 2017-012 du 19 janvier 2017)</b>
---	--

---

Le mot de passe reste le moyen d'authentification le plus répandu. Alors que les compromissions de bases entières de mots de passe se multiplient, la CNIL a adopté une nouvelle recommandation sur les mots de passe. Elle fixe les mesures minimales à mettre en œuvre.

Basée sur la notion d'un secret, l'authentification par identifiant et mot de passe est un moyen simple et peu coûteux à déployer pour contrôler un accès. Toutefois, cette méthode d'authentification présente un niveau de sécurité faible. Les données sensibles, de nombreuses attaques informatiques ont entraîné la compromission de bases de données entières de comptes et des mots de passe associés. Ces failles de données ont notamment contribué à élargir les connaissances des pirates et des hackers sur les mots de passe. Les risques de compromission des comptes associés à cette méthode d'authentification se sont fortement accrues et nécessitent une vigilance particulière. Les risques liés à la gestion des mots de passe sont multiples et passent notamment par :

1. La complexité du mot de passe ;
2. L'absence sur le réseau afin de collecter les mots de passe transmis ;
3. La compromission de mot de passe ;
4. La faiblesse des modalités de renouvellement du mot de passe en cas d'usurpation (cas des questions « secrètes »).

Les préférences résumées identifiées au cours du cycle de vie d'un mot de passe :

- 1) l'absence de définition sécurisée d'un bon mot de passe, mais sa complexité et la longueur permettent de dissuader le risque de réussite d'une attaque informatique qui consistent à tester successivement de nombreux mots de passe (attaque dite en force brute). On considère que la longueur du mot de passe suffit pour résister aux attaques courantes à partir de 12 caractères. Lorsque la taille du mot de passe dépasse, des mesures complémentaires doivent être prévues.
- 2) l'absence de définition d'un bon mot de passe, mais sa complexité et la longueur permettent de dissuader le risque de réussite d'une attaque informatique qui consistent à tester successivement de nombreux mots de passe (attaque dite en force brute). On considère que la longueur du mot de passe suffit pour résister aux attaques courantes à partir de 12 caractères. Lorsque la taille du mot de passe dépasse, des mesures complémentaires doivent être prévues.

**PHRASEPASSE : UN OUTIL POUR ACCOMPAGNER LES UTILISATEURS**

Pour rendre les utilisateurs à choisir un mot de passe sécurisé et à mieux mémoriser, la CNIL a développé un outil pour générer un mot de passe à partir d'une phrase. Le code de cet outil est disponible sous la forme d'une extension logicielle en JavaScript, afin que vous puissiez l'intégrer dans vos applications.

**Les exigences de la CNIL**

L'authentification par mot de passe : longueur, complexité, mesures complémentaires

Le processus d'authentification par mot de passe, par sa complexité et la longueur permettent de dissuader le risque de réussite d'une attaque informatique qui consistent à tester successivement de nombreux mots de passe (attaque dite en force brute). On considère que la longueur du mot de passe suffit pour résister aux attaques courantes à partir de 12 caractères. Lorsque la taille du mot de passe dépasse, des mesures complémentaires doivent être prévues.

Le processus d'authentification par mot de passe, par sa complexité et la longueur permettent de dissuader le risque de réussite d'une attaque informatique qui consistent à tester successivement de nombreux mots de passe (attaque dite en force brute). On considère que la longueur du mot de passe suffit pour résister aux attaques courantes à partir de 12 caractères. Lorsque la taille du mot de passe dépasse, des mesures complémentaires doivent être prévues.

La table ci-dessous fait état des 4 cas d'authentification par mot de passe identifiés par la CNIL, des mesures complémentaires				
Mot de passe simple	Exemple d'utilisation	Longueur minimale	Complexité du mot de passe	Mesures complémentaires
	FORUM, BLOG	12	- minuscules - majuscules - chiffres - caractères spéciaux	Connecter l'utilisateur sur un bon mot de passe
Avec restriction d'accès (cas plus répandu)	SIÈGE DE E-COMMERCE, COMPTE D'ENTREPRISE, MESSAGERIE	8	Au moins 3 des 4 types suivants : - minuscules - majuscules - chiffres - caractères spéciaux	Éloignement des tentatives multiples : - temporisation d'accès au compte après plusieurs échecs - verrouillage de compte après 10 échecs
Avec information complémentaire	BANQUE EN LIGNE	5	Chiffres et/ou lettres	Éloignement des tentatives multiples - information complémentaire complémentaire en propre d'une taille d'au moins 7 caractères (ex : identifiant dédié au service) de
Avec matériel dédié par la personne	CARTE BANCAIRE DE TELEPHONE	4	Chiffres	Matériel dédié en propre par la personne (ex : carte SIM, carte bancaire, certificat) - Éloignement de tentatives multiples

Dans tous les cas, le mot de passe ne doit pas être communiqué à l'utilisateur en clair par courrier électronique. Ces exigences sont des règles minimales. Le contrôle d'accès peut devoir répondre sur des règles plus robustes selon les risques auxquels le système est exposé.

**Sécurisation de l'authentification**

Quelle que soit la mesure mise en place, la fonction d'authentification doit être sûre :

- être basée sur un algorithme cryptographique sûr ;
- ne pas être basée sur un algorithme cryptographique obsolète ;
- être basée sur un algorithme cryptographique sûr ;
- être basée sur un algorithme cryptographique sûr ;
- être basée sur un algorithme cryptographique sûr ;

**La conservation des mots de passe**

Le mot de passe ne doit jamais être stocké en clair. Il doit être transformé au moyen d'une fonction cryptographique non-réversible et sûre, intégrant l'utilisation d'un sel ou d'une clé. Le sel ou la clé doit être généré au hasard et être stocké de manière sécurisée cryptologiquement sûr (il utilise un algorithme public réputé fort et sa base en source logicielle est exemptée de vulnérabilité connue). Il ne doit pas être stocké dans la même espace de stockage que l'élément de vérification du mot de passe.

**Le renouvellement du mot de passe**

Le renouvellement périodique

La responsabilité de traitement veille à proposer un renouvellement du mot de passe selon une périodicité pertinente et raisonnable, qui dépend notamment de la complexité imposée du mot de passe, des données traitées et des risques auxquels il est exposé.

**Renouvellement des données**

La responsabilité de traitement veille à proposer un renouvellement du mot de passe selon une périodicité pertinente et raisonnable, qui dépend notamment de la complexité imposée du mot de passe, des données traitées et des risques auxquels il est exposé.

**Que faire en cas de risque de compromission du mot de passe ?**

En cas de compromission des données, la responsabilité de traitement doit :

- être basée sur un algorithme cryptographique sûr ;
- être basée sur un algorithme cryptographique sûr ;
- être basée sur un algorithme cryptographique sûr ;
- être basée sur un algorithme cryptographique sûr ;
- être basée sur un algorithme cryptographique sûr ;

**Recommandations par de vos entreprises**

Les professionnels sont invités à consulter la CNIL. Les difficultés de mise en œuvre que pourrait poser l'application de cette recommandation. Cette recommandation pourra faire l'objet de révisions et de mises à jour.

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)

**Notes finales**

1) Délégation n° 2017-022 du 18 janvier 2017 portant adoption d'une recommandation relative aux mots de passe (lire la suite)