Consultation publique sur la recommandation « mots de passe »

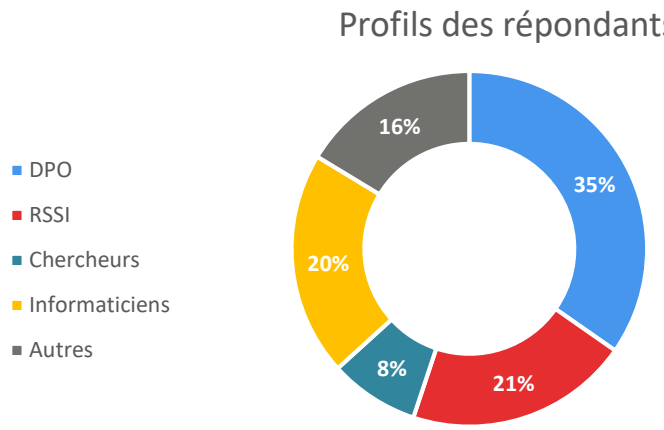
Synthèse des contributions

Le 21 octobre 2021, la CNIL a lancé une consultation publique sur son projet de recommandation « mots de passe » afin de recueillir les avis des professionnels. Les contributions ont nourri les travaux de la CNIL en vue de la publication de la version définitive de la recommandation.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

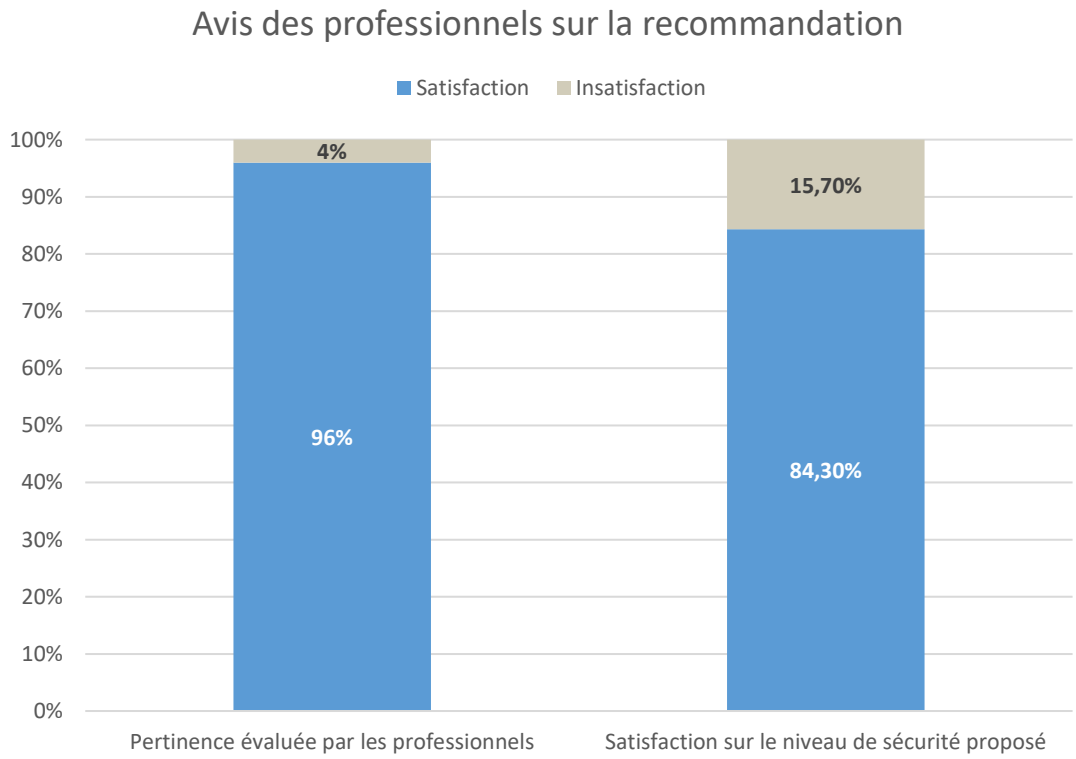
Profil des répondants

La consultation a rencontré un vif succès. Les réponses, d'une grande qualité, proviennent **de professionnels de la cybersécurité** (pour la moitié d'entre-elles) et/ou **de la protection de la vie privée** (deux-tiers des retours) mais aussi de quelques acteurs de la **société civile** (monde politique ou associatif). Ainsi, dix-sept délégués à la protection des données (DPD/DPO), dix responsables de la sécurité des systèmes d'information (RSSI), quatre chercheurs en sécurité ainsi qu'une dizaine d'informaticiens de diverses spécialités ont répondu.



Dans l'ensemble, la consultation a confirmé les grandes orientations du projet de recommandation publié en octobre 2021. Les retours, très constructifs, ont permis à la CNIL de clarifier et préciser son projet de recommandation.

En particulier, le **périmètre de la recommandation est considéré comme pertinent** par 96 % des répondants. Et, à la condition de recommander un niveau de sécurité plus élevé pour les contextes risqués, tels que l'accès aux courriels ou à des données sensibles au sens de l'article 9 du RGPD, **84,3 % des répondants considèrent le niveau choisi comme satisfaisant.**



CNIL.

Les évolutions apportées par la consultation sur la recommandation définitive

Les différents commentaires ont permis de clarifier et expliciter les recommandations sur les points principaux :

- la définition d'une règle fondée sur le degré d'imprédictibilité d'un mot de passe (l'entropie) et non sur la longueur minimale de mot de passe, pour permettre une mise en place plus libre de politiques de mots de passe robustes ;
- **l'abandon de la pratique de renouvellement régulier des mots de passe pour les comptes utilisateurs classiques** (le renouvellement reste requis pour les comptes à « privilèges », c'est-à-dire du type administrateur ou avec des droits étendus) ;
- l'introduction d'une liste de mots de passe complexes mais connus et donc à éviter compte tenu des nouveaux schémas d'attaque ;
- la précision de règles concernant la création et le renouvellement de mots de passe pour garantir une sécurité tout au long du cycle de vie du mot de passe, sous la forme de bonnes pratiques (gestionnaire de mot de passe, non recours à des informations évidentes).

Ces retours ont aussi permis à la CNIL de compléter son projet de recommandation sur plusieurs aspects :

- en mentionnant les solutions basées sur le concept de « devinabilité » qui évalue la difficulté pour un adversaire de deviner un mot de passe. Ce concept reflète parfaitement ce que la CNIL recherche dans son évolution vers l'entropie. Cependant, à sa connaissance, aucun outil francophone ne permettant actuellement d'utiliser ce critère en pratique, il est introduit uniquement de façon prospective ;
- en insistant encore davantage sur la nécessaire prise en compte du contexte particulier dans les choix techniques, que ce soit le choix du « cas » à appliquer ou des éventuelles mesures additionnelles à mettre en œuvre ;
- en rappelant la bonne pratique de cacher les caractères saisis par l'utilisateur par des points ou des étoiles ;
- en explicitant que l'utilisation de schéma dit « PAKE » (*Password-authenticated key agreement* ou « échange de clé authentifié par mot de passe » en français) ou qui permettent d'utiliser une authentification par mot de passe sans les stocker est compatible avec la recommandation ;
- en recommandant d'éviter les appels à des ressources tierces sur les pages web d'authentification afin de limiter la surface d'attaque ;
- en clarifiant le cas des mots de passes stockés dans des applications, par exemple sur smartphone ;
- en intégrant les bonnes pratiques sur les messages d'erreurs à afficher aux utilisateurs ;
- en rappelant l'application de la recommandation en matière de journalisation et les bonnes pratiques en matière journalisation de de mots de passe ;
- en ajoutant des éléments généraux sur l'application de la recommandation aux sous-traitants ;
- enfin, en recommandant aux éditeurs de logiciels de documenter leurs modalités de gestion des mots de passe, quand bien même ni le règlement général sur la protection des données (RGPD) ni la loi Informatique et Libertés ne leur sont applicables, afin de faciliter leur utilisation dans le cadre de traitements.

Enfin, les retours ont amené la CNIL **à ne plus recommander le cas d'usage où l'authentification repose sur une « information complémentaire »**. En effet, cette solution fournissait un niveau de sécurité significativement inférieur aux trois autres, ce que de nombreux contributeurs ont relevé.

La CNIL invite donc les responsables de traitement qui ont toujours recours à cette modalité d'authentification à basculer sur un des autres cas reconnus comme à l'état de l'art, ou bien à avoir recours à des mécanismes d'authentification plus sécurisés tels que des authentification multi facteurs.

Si cette modalité d'authentification ne devait plus être utilisée pour de nouveaux traitements, la CNIL prendrait en compte le délai nécessaire pour procéder aux modifications utiles pour les traitements existants.