Rapport de recherche exclusif

Sponsorisé par Keeper Security

Pollfish

 | keeper.io/malpracticereport

Introduction

La mauvaise gestion des mots de passe professionnels n'a pas attendu le COVID-19 pour venir menacer la cybersécurité des entreprises. Et lorsque la situation sanitaire a contraint les organisations du monde entier à déployer et mettre en œuvre le télétravail, les équipes ont commencé à se connecter aux ressources de l'organisation à distance, dans des environnements hors du champ de contrôle de leurs employeurs, et utilisant souvent leurs propres appareils.

Les personnes interrogées dans le cadre de l'étude **La cybersécurité à l'ère du télétravail : rapport sur les risques dans le monde**, commandée par Keeper Security en 2020, ont exprimé de fortes inquiétudes concernant la sécurité des mots de passe au sein de leurs organisations :

- 60 % des personnes interrogées ont affirmé que leur entreprise avait subi une cyberattaque au cours des 12 mois précédents.
- Plus de 50 % de ces attaques impliquaient une usurpation d'identifiants.
- Le vol d'actifs informatiques a causé 5 millions de dollars ou plus en dommages pour 25 % des entreprises.

La pandémie a forcé les organisations à déployer rapidement une myriade de nouvelles technologies pour que le personnel reste connecté et puisse continuer à travailler. De Zoom à Google Workspace en passant par Slack, les collaboratrices et collaborateurs ont dû s'inscrire à des comptes en ligne supplémentaires – et se souvenir de tout autant de mots de passe.

Keeper s'est demandé à quel point la sécurité des mots de passe avait évolué depuis l'adoption massive du télétravail. Les employés en télétravail suivaient-ils de bonnes pratiques simples pour sécuriser leurs mots de passe, ou bien ont-ils été victimes de la « fatigue des mots de passe », adoptant de mauvaises habitudes ayant entraîné des risques de cybersécurité conséquents ? Pour le découvrir, nous avons mené, en partenariat avec Pollfish, une étude sur les mauvaises pratiques professionnelles en matière de mot de passe.

Si Ponemon interrogeait des dirigeants d'entreprise, nous avons décidé cette fois de poser directement des questions aux collaboratrices et collaborateurs. Nous avons donc sondé un millier d'employés à plein temps aux États-Unis pour connaître leurs habitudes en matière de mot de passe. Achevée en février 2021, notre enquête portait exclusivement sur les personnes ayant utilisé des mots de passe pour se connecter à leurs comptes en ligne à usage professionnel.

Les principales conclusions de l'enquête sont présentées dans les pages qui suivent. L'intégralité des données peut être consultée en page 6.

Conclusion n° 1 : les collaborateurs américains ne gèrent pas leurs identifiants de manière sécurisée

Notre enquête a révélé qu'aux États-Unis, les collaboratrices et collaborateurs ne suivaient pas les meilleures pratiques de stockage et de suivi de leurs mots de passe professionnels, ce qui engendre des risques majeurs de cybersécurité pour leurs employeurs.

- Plus de la moitié des personnes interrogées (57 %) admettent écrire leurs mots de passe professionnels sur des notes adhésives, et deux tiers (67 %) reconnaissent avoir égaré ces notes. Outre le fait de laisser des informations sensibles de l'entreprise à la vue de quiconque vit ou est en visite chez elles, cela impacte l'efficacité de l'organisation : perdre ses notes autocollantes, c'est perdre ses mots de passe, ce qui engendre des tickets de support pour réinitialiser les mots de passe en question.

- 62 % des personnes interrogées enregistrent leurs identifiants dans un carnet ou un journal, et la vaste majorité (82 %) affirme conserver ce carnet à proximité de leur appareil de travail, où toute personne vivant chez eux ou leur rendant visite peut potentiellement y accéder.

La gestion des mots de passe sur papier est devenue encore plus problématique à l'ère du télétravail. La plupart des personnes interrogées (66 %) affirment être plus susceptibles de noter sur papier les mots de passe professionnels en télétravail qu'au bureau.

Même lorsqu'ils utilisent des méthodes numériques pour gérer leurs mots de passe, les collaboratrices et collaborateurs américains appliquent de mauvaises pratiques de sécurité en matière de mots de passe.

- Près de la moitié des personnes interrogées (49 %) enregistrent leurs mots de passe professionnels dans le cloud.

- Un peu plus de la moitié (51 %) affirment sauvegarder actuellement leurs mots de passe dans un document enregistré sur leur PC.

- 55 % des personnes interrogées enregistrent les mots de passe professionnels sur leur téléphone.

Enregistrer des mots de passe dans des fichiers non chiffrés est une pratique extrêmement risquée. Il suffit en effet à un cybercriminel de pirater le stockage sur le cloud, le PC ou l'appareil portable pour accéder à tous les mots de passe de l'employé.

Conclusion n° 2 : les collaborateurs américains choisissent des mots de passe faibles, faciles à deviner

Un mot de passe fort se compose d'une série aléatoire de caractères en majuscule et en minuscule, de chiffres et de caractères spéciaux. Cependant, de nombreuses personnes interrogées ont reconnu utiliser des mots de passe contenant des informations personnelles, que les cybercriminels peuvent facilement trouver sur les réseaux sociaux.

- Plus d'un tiers (37 %) des personnes interrogées ont utilisé le nom de leur entreprise dans un mot de passe professionnel.

- Plus d'un tiers (34 %) ont utilisé le nom ou la date d'anniversaire de leur conjoint.

- Près d'un tiers (31 %) ont utilisé le nom ou la date d'anniversaire de leur enfant.

La réutilisation des mots de passe entre les comptes personnels et professionnels représente désormais un risque important en matière de cybersécurité pour les entreprises, 44 % des personnes interrogées admettant qu'elles réutilisaient les mots de passe de leurs comptes personnels pour leurs comptes professionnels sur leurs appareils professionnels.

Conclusion n° 3 : les collaborateurs américains partagent leurs mots de passe professionnels avec des tiers non autorisés

Un grand nombre d'employés américains ne font pas preuve de discernement quant aux personnes avec lesquelles ils partagent leurs mots de passe professionnels. Cela entraîne un risque de violation des données pour les organisations si ces mots de passe devaient se retrouver entre les mains d'une personne négligente ou mal intentionnée.

- Durant l'année passée, 14 % des personnes interrogées ont partagé leurs mots de passe professionnels avec leur partenaire ou leur conjoint.
- 11 % des personnes interrogées ont partagé leurs mots de passe professionnels avec un membre de leur famille.

Même en l'absence d'une violation de données, un employeur peut être déclaré comme non conforme et se voir imposer des pénalités très importantes si l'on découvre que des tiers non autorisés ont consulté des données protégées par la conformité.

Conclusion n° 4 : les collaborateurs américains ne prennent pas les mesures nécessaires pour garantir un partage des mots de passe sécurisé et/ou uniquement avec des tiers autorisés

Il ressort de notre enquête que les mots de passe sont souvent partagés au travail.

- Près de la moitié des personnes interrogées (46 %) affirment que leur entreprise partage des mots de passe liés à des comptes utilisés par différentes personnes.
- Plus d'un tiers (34 %) ont partagé des mots de passe professionnels avec des collègues de la même équipe.
- Près d'un tiers (32 %) ont partagé des mots de passe professionnels avec leurs managers.
- 19 % ont partagé leurs mots de passe avec leur équipe exécutive.

La meilleure chose à faire est de donner à chaque utilisateur un mot de passe unique pour chaque application ou compte professionnel, ce qui est aisément mis en œuvre avec un gestionnaire de mots de passe d'entreprise (EPM). Le partage des mots de passe au sein du lieu de travail ne présente pas de danger si les mots de passe sont partagés de manière sécurisée et uniquement transmis aux personnes autorisées. Les résultats de notre enquête montrent que de nombreux employeurs américains n'appliquent aucune stratégie de réduction des risques permettant d'instaurer un partage sécurisé des mots de passe.

- La majorité des personnes interrogées (62 %) indiquent avoir partagé un mot de passe professionnel par SMS ou e-mail. Or, un mot de passe en transit peut être intercepté par des cybercriminels.
- Près d'un tiers des personnes interrogées (32 %) reconnaissent avoir accédé à un compte en ligne appartenant à un ancien employeur, ce qui indique que de nombreux employeurs ne désactivent pas les comptes lorsque les collaboratrices et collaborateurs quittent l'entreprise.

Bilan

L'adoption et la mise en œuvre d'une plateforme de gestion des mots de passe telle que Keeper Enterprise permettent de remédier aux mauvaises pratiques identifiées par cette enquête. Le chiffrement zero-knowledge des mots de passe et le framework zero-trust de Keeper fournit une gestion des mots de passe avancée, un partage sécurisé et des fonctionnalités de sécurité additionnelles. Les administrateurs informatiques et les dirigeants obtiennent une visibilité et un contrôle complet des pratiques de leur personnel en matière de mots de passe, qui reposent sur les éléments suivants :

- Modèle de sécurité exclusif zero-knowledge et système de framework zero-trust ; toutes les données en transit et au repos sont chiffrées ; elles ne peuvent pas être visualisées par le personnel de Keeper Security ni aucune tierce partie.
- Déploiement rapide sur tous les appareils, sans frais d'équipement ou d'installation.
- Introduction personnalisée, assistance 24h/24 et 7j/7 et formation dispensées par un spécialiste dédié.
- Prise en charge du contrôle RBAC, du 2FA, des audits, des rapports, et de différentes normes de conformité, y compris HIPAA, DPA, FINRA et RGPD.
- Fourniture de dossiers partagés, sous-dossiers et mots de passe sécurisés pour les équipes.
- Authentification Single Sign-On (SAML 2.0)
- Déblocage d'un accès hors ligne au coffre-fort lorsque l'authentification SSO n'est pas disponible.
- Approvisionnement dynamique de coffres-forts via SCIM.
- Configuration haute disponibilité (HA).
- Authentification à deux facteurs/multi-facteurs avancée
- Synchronisation avec Active Directory et LDP
- Approvisionnement SCIM et Azure AD
- API développeurs pour la rotation des mots de passe et l'intégration back-end

Résultats de l'enquête

UNE SEULE RÉPONSE

SQ1. Occupez-vous actuellement un poste à plein temps ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	100,00 %	1000
A2	Non	0,00 %	0

UNE SEULE RÉPONSE

SQ2. Utilisez-vous actuellement des mots de passe pour vous connecter à des comptes professionnels ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	100,00 %	1000
A2	Non	0,00 %	0

UNE SEULE RÉPONSE

Q1. Avez-vous actuellement des mots de passe professionnels en ligne écrits sur une note adhésive ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	57,30 %	573
A2	Non	42,70 %	427

UNE SEULE RÉPONSE

Q2. Si oui, avez-vous déjà perdu cette note adhésive ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	66,55 %	382
A2	Non	33,45 %	192

UNE SEULE RÉPONSE

Q3. Êtes-vous davantage susceptible de noter sur papier des mots de passe professionnels en ligne lorsque vous travaillez à domicile ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	66,00 %	660
A2	Non	34,00 %	340

UNE SEULE RÉPONSE

Q4. Disposez-vous actuellement d'un carnet ou d'un cahier sur lequel vous notez vos identifiants et vos mots de passe ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	62,10 %	621
A2	Non	37,90 %	379

UNE SEULE RÉPONSE

Q5. Si oui, ce carnet se trouve-t-il près de l'appareil que vous utilisez pour le travail ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	81,79 %	512
A2	Non	18,21 %	114

UNE SEULE RÉPONSE

Q6. Enregistrez-vous vos mots de passe professionnels dans un document enregistré dans le cloud ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	48,90 %	489
A2	Non	51,10 %	511

UNE SEULE RÉPONSE

Q7. Enregistrez-vous vos mots de passe professionnels dans un document enregistré sur votre PC ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	50,60 %	506
A2	Non	49,40 %	494

UNE SEULE RÉPONSE

Q8. Enregistrez-vous actuellement vos mots de passe professionnels sur votre téléphone ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	54,70 %	547
A2	Non	45,30 %	453

UNE SEULE RÉPONSE

Q9. Avez-vous déjà partagé un mot de passe professionnel par SMS ou e-mail ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	38,10 %	381
A2	Non	61,90 %	619

PLUSIEURS RÉPONSES POSSIBLES

Q10. Avec qui avez-vous partagé vos mots de passe professionnels au cours de l'année passée (sélectionnez toutes les réponses qui conviennent) ?

Le pourcentage (personnes interrogées) est calculé en divisant chaque nombre de réponses par le total de personnes interrogées uniques.

Le pourcentage (réponses) est calculé en divisant chaque nombre de réponses par le nombre total de réponses recueillies.

#	Réponses	Personnes interrogées (%)	Réponses (%)	Nombre
A1	Collègues de la même équipe	34,40 %	18,86 %	344
A2	Collègues d'autres départements	13,10 %	7,18 %	131
A3	Managers	31,70 %	17,38 %	317
A4	Équipe dirigeante	18,50 %	10,14 %	185
A5	Anciens collègues	6,90 %	3,78 %	69
A6	Conjoint·e ou époux·se	14,40 %	7,89 %	144
A7	Enfant	7,90 %	4,33 %	79
A8	Autre membre de la famille	10,60 %	5,81 %	106
A9	Ami·e avec qui je ne travaille pas	4,70 %	2,58 %	47
A10	Aucune des réponses ci-dessus	37,60 %	20,61 %	376
A11	Autre	2,60 %	1,43 %	26

UNE SEULE RÉPONSE

Q11. Vous êtes-vous déjà connecté·e à un compte en ligne appartenant à votre ancien employeur après votre départ ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	32,40 %	324
A2	Non	67,60 %	676

UNE SEULE RÉPONSE

Q12. Au moment de créer le nouveau mot de passe d'un compte professionnel, avez-vous utilisé le nom de votre entreprise ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	36,70 %	367
A2	Non	63,30 %	633

UNE SEULE RÉPONSE

Q13. Votre entreprise partage-t-elle des mots de passe pour des comptes utilisés par plusieurs personnes ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	46,10 %	461
A2	Non	53,90 %	539

UNE SEULE RÉPONSE

Q14. Vos mots de passe professionnels partagés entre collègues comportent-ils le nom de l'entreprise ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	33,80 %	338
A2	Non	47,20 %	472
A3	Non applicable	19,00 %	190

UNE SEULE RÉPONSE

Q15. Utilisez-vous actuellement le même mot de passe pour vos comptes personnels et professionnels ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	43,70 %	437
A2	Non	56,30 %	563

UNE SEULE RÉPONSE

Q16. Parmi vos mots de passe professionnels, certains comportent-ils le nom ou la date d'anniversaire de votre conjoint·e ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	34,20 %	342
A2	Non	65,80 %	658

UNE SEULE RÉPONSE

Q17. Parmi vos mots de passe professionnels, certains comportent-ils le nom ou la date d'anniversaire de votre enfant ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	31,40 %	314
A2	Non	52,00 %	520
A3	Je n'ai pas d'enfant	16,60 %	166

UNE SEULE RÉPONSE

Q18. Vos enfants se sont-ils déjà connectés ou ont-ils déjà accédé à vos applications ou comptes professionnels ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	20,60 %	206
A2	Non	59,40 %	594
A3	Je n'ai pas d'enfant	20,00 %	200

UNE SEULE RÉPONSE

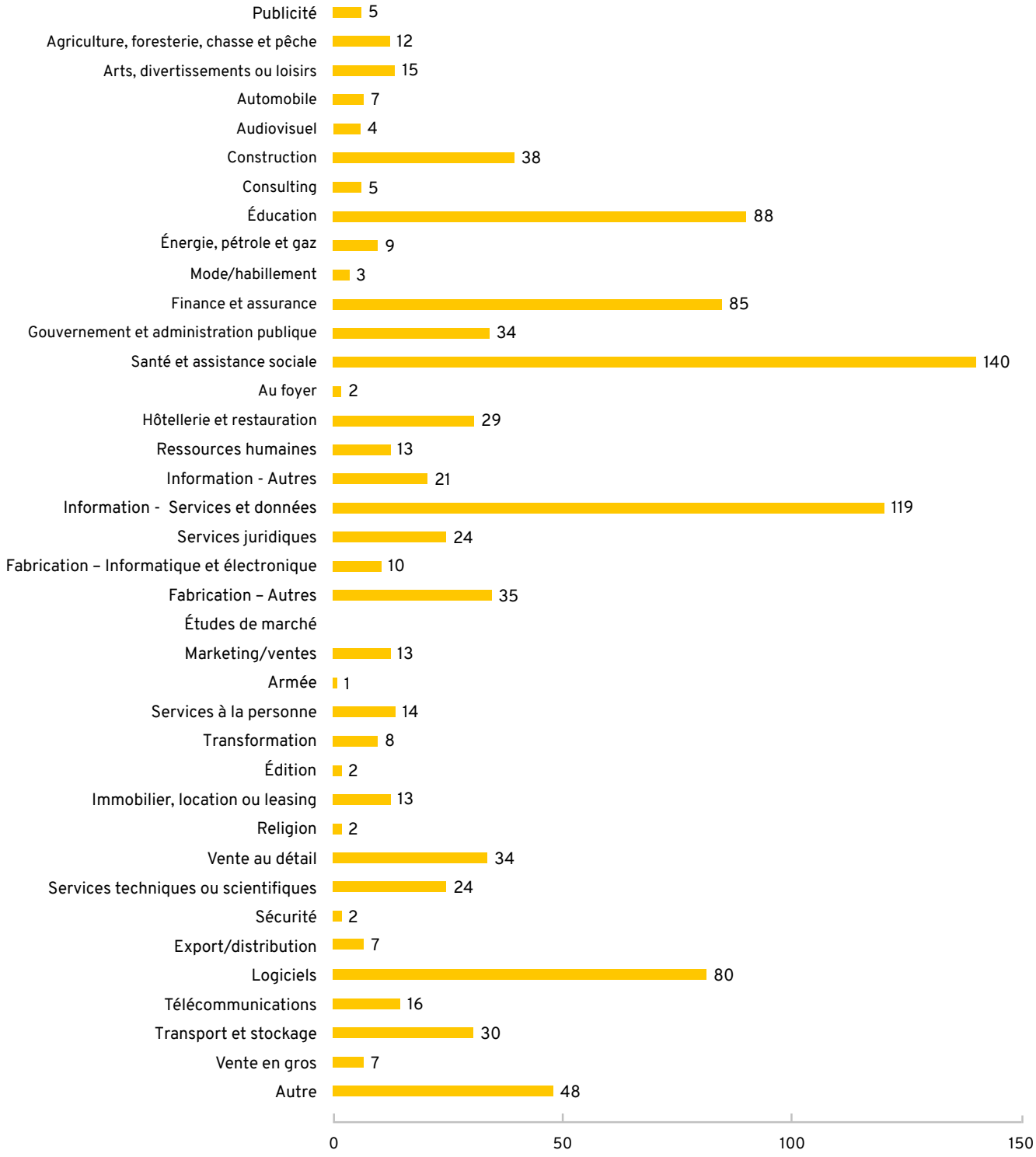
Q19. Avez-vous des comptes personnels protégés par mots de passe sur vos appareils professionnels ?

#	Réponses	Réponses (%)	Nombre
A1	Oui	53,35 %	534
A2	Non	46,65 %	467

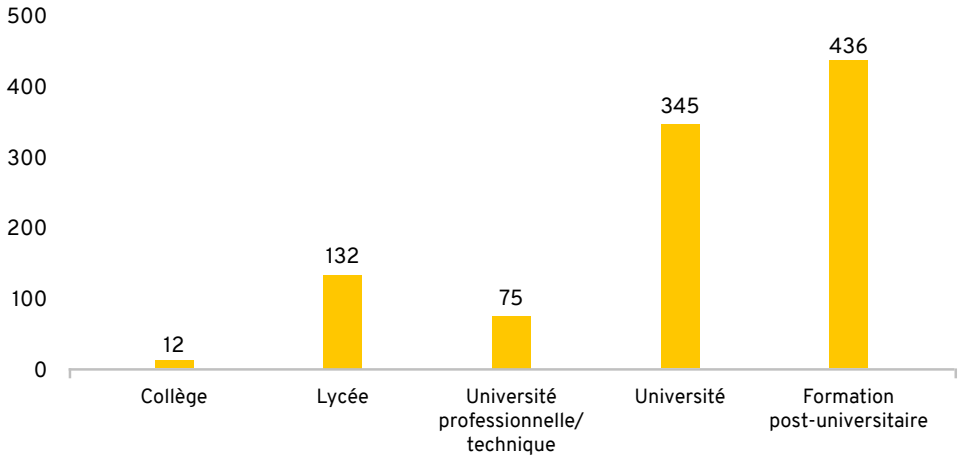
Données démographiques des personnes interrogées

Taille de l'échantillon 1 000

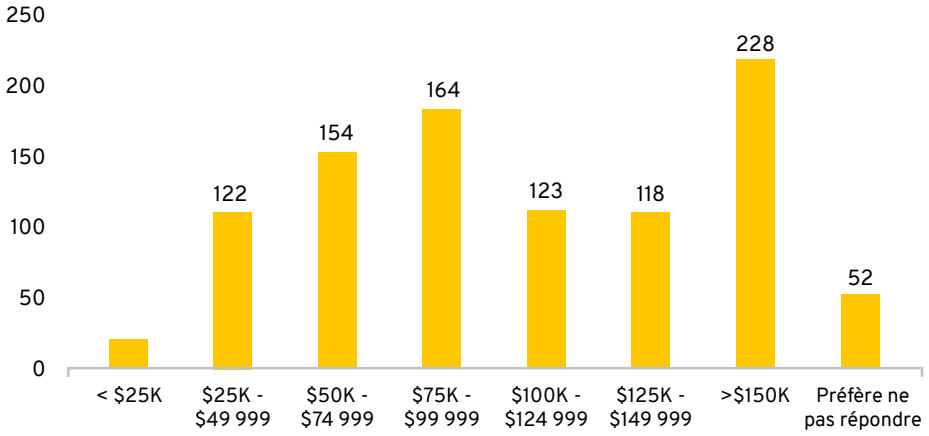
Profession



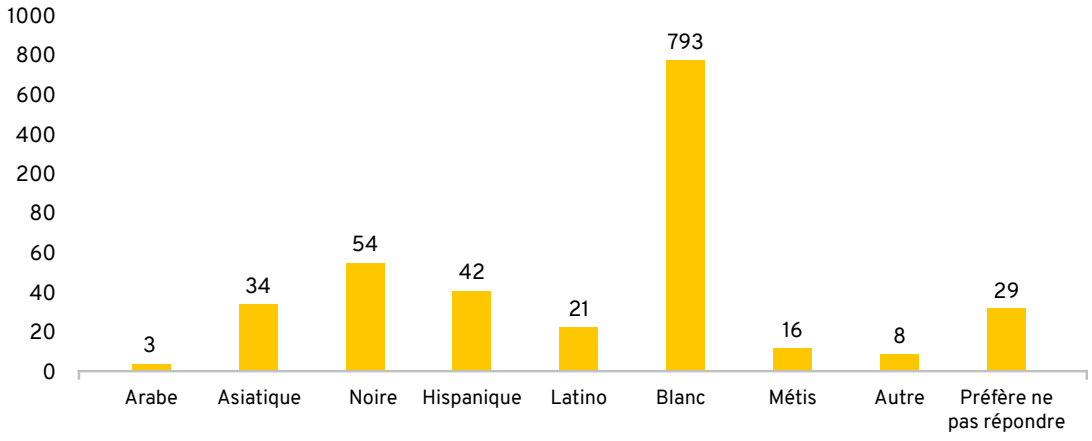
Éducation



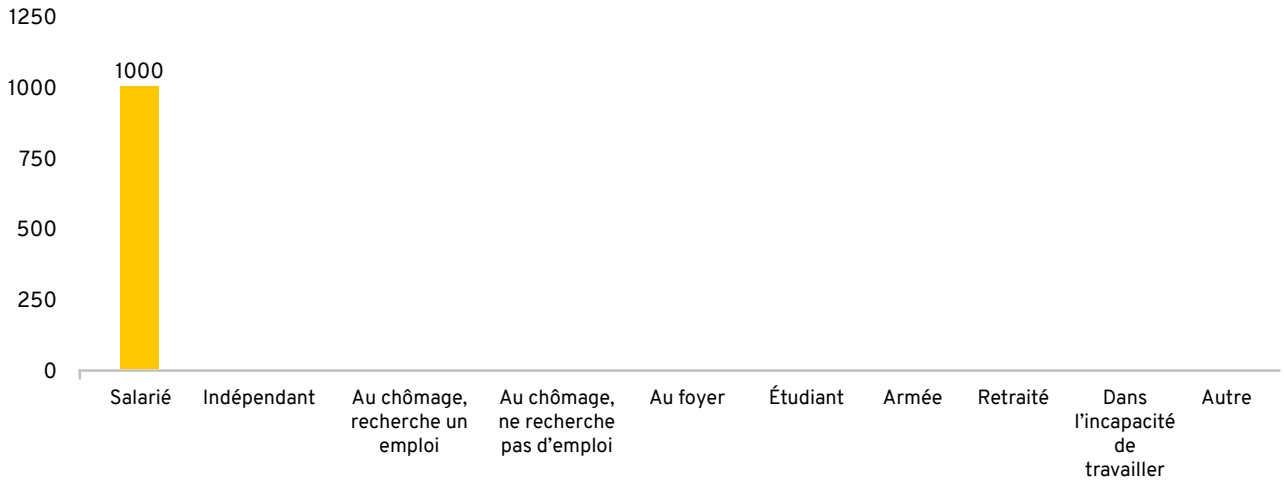
Revenus



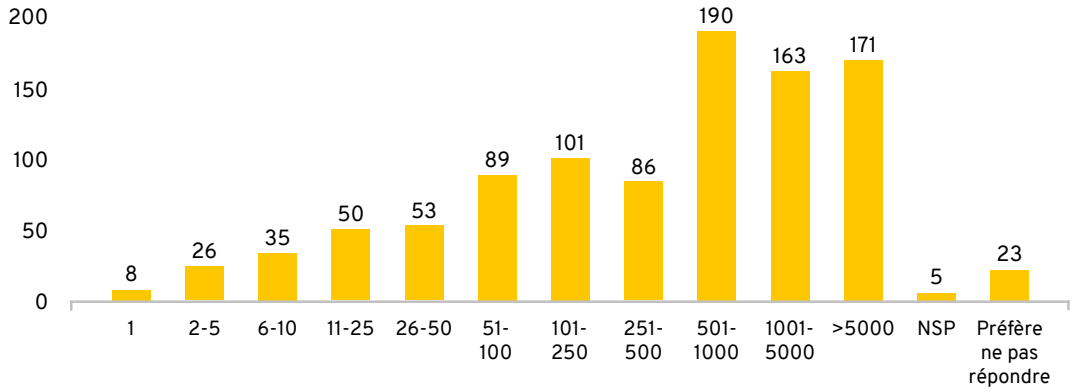
Origine ethnique



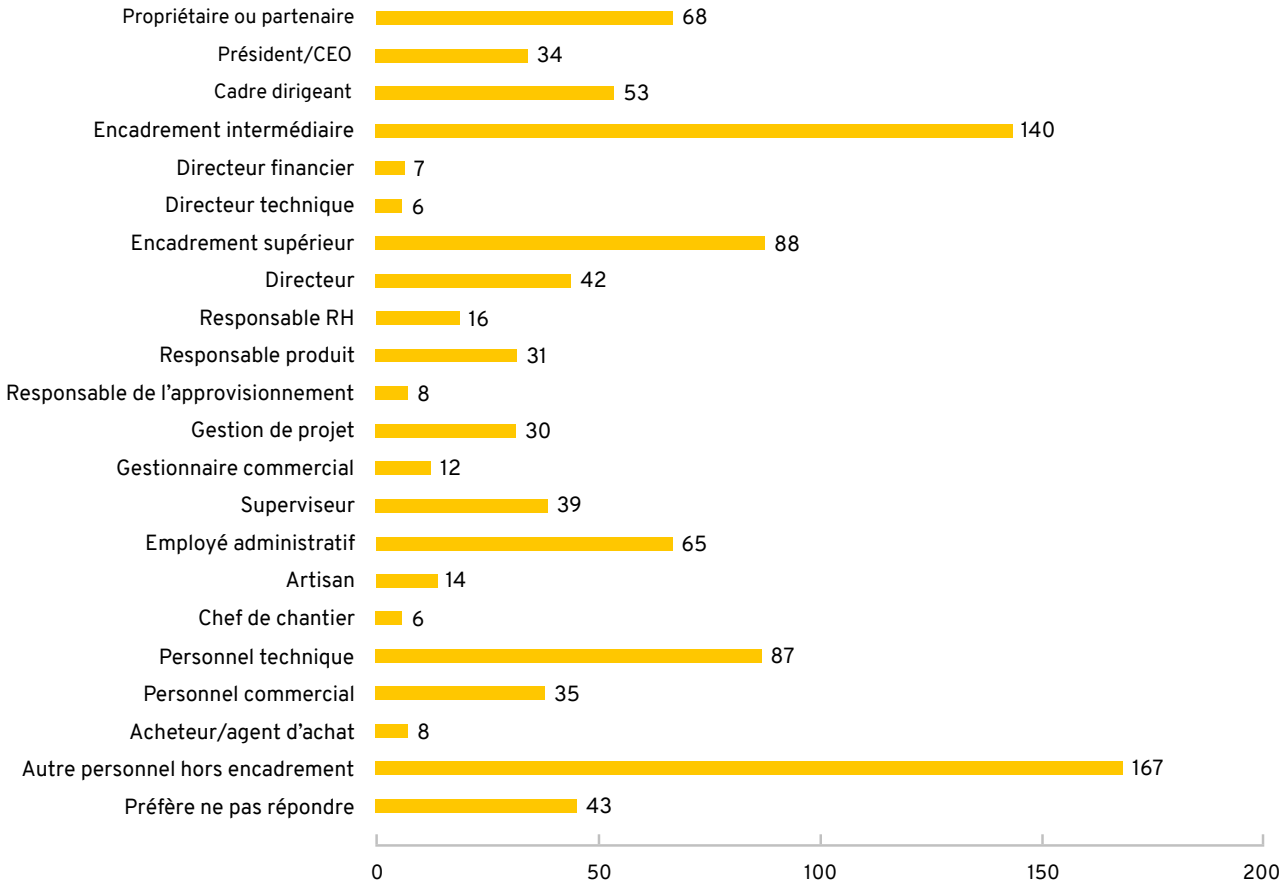
Statut d'emploi



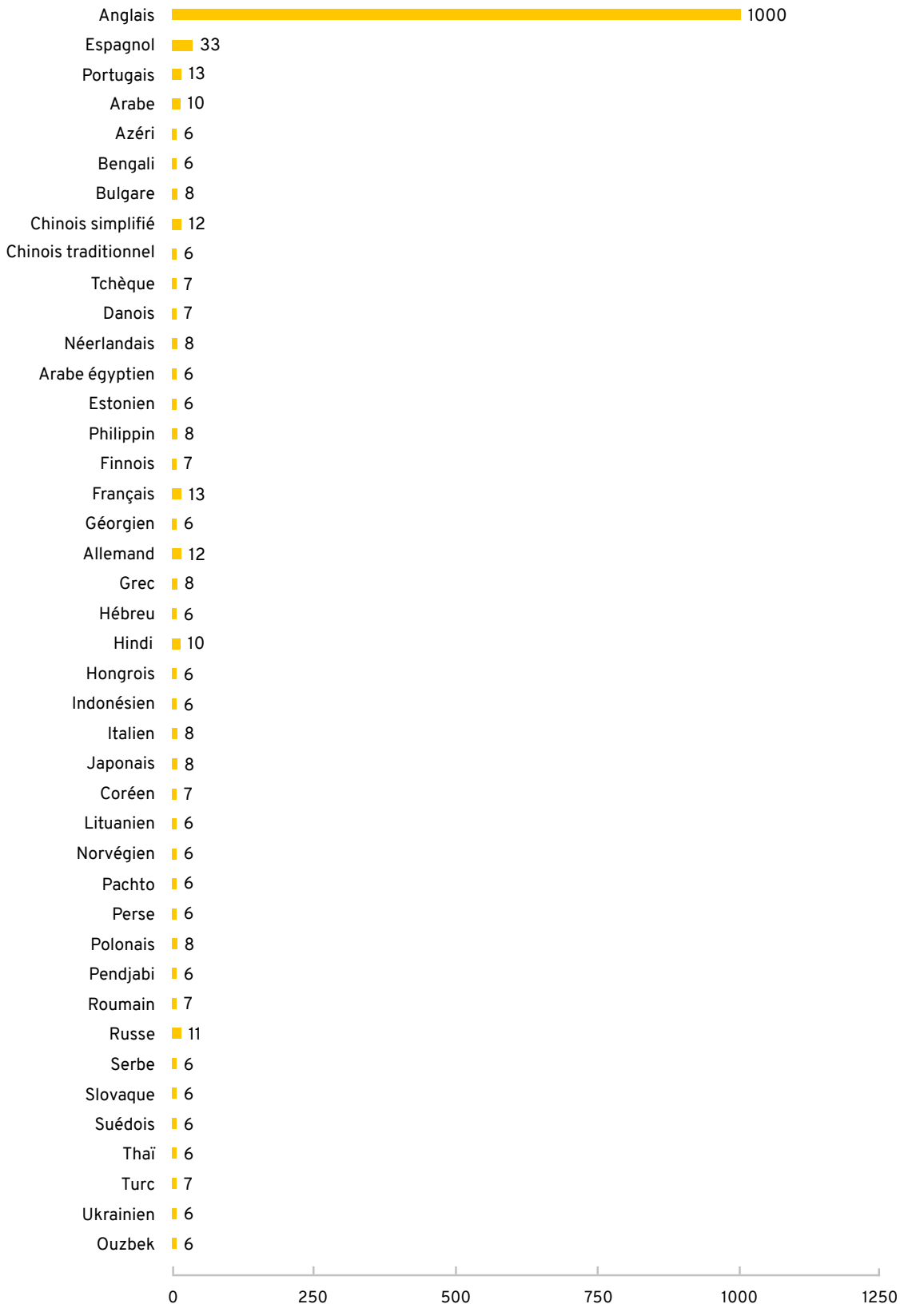
Nombre d'employés



Rôle au sein de l'organisation



Langues parlées



Prix et récompenses

Keeper a été élu Meilleur gestionnaire de mots de passe et Choix de la rédaction par PC Magazine, Choix de la rédaction par PCWorld pendant deux années consécutives et a remporté quatre G2 Best Software Awards et quatre InfoSec Awards du Meilleur outil de gestion de mots de passe pour les PME et Meilleur outil pour la cybersécurité des PME. Keeper est certifié SOC-2 et ISO 27001 et figure sur la liste autorisée du gouvernement fédéral américain via le System for Award Management (SAM).

Gartner Peer Insights
4,9 étoiles sur 5

Spiceworks
5 étoiles sur 5

Choix de la rédaction
4,5 étoiles sur 5

2020 Enterprise Leader
4,7 étoiles sur 5

- **Choix de la rédaction Cybersécurité Gestion des mots de passe**
- **Directeur général innovant de l'année**

- **Meilleur outil de gestion de mots de passe**
- **Meilleur outil pour la cybersécurité des PME**
- **Choix de la rédaction pour le Directeur général de l'année**
- **CTO le plus innovant de l'année**

Meilleur gestionnaire de mots de passe de l'année & Choix de la rédaction 2019 & 2020

Choix de la rédaction 2018 & 2019

Pour télécharger un exemplaire du Rapport sur les mauvaises pratiques professionnelles en matière de mot de passe, des graphiques et plus encore, rendez-vous sur notre **plateforme de ressources**. Pour obtenir de plus amples informations sur Keeper Security ou découvrir comment protéger votre organisation contre les violations de données par mot de passe, veuillez visiter **keepersecurity.com**.

Méthodologie

Keeper Security a confié à Pollfish la conduite de cette étude portant sur 1 000 collaboratrices et collaborateurs aux États-Unis. Seules les personnes ayant utilisé des mots de passe pour se connecter à leurs comptes en ligne à usage professionnel ont été incluses. L'enquête a été achevée en juin 2021.

À propos de Keeper Security, Inc.

Keeper Security, Inc. (Keeper) est une plateforme de cybersécurité brevetée et primée qui permet de prévenir les atteintes aux données et les cybermenaces liées aux mots de passe. Des millions de particuliers et des milliers d'entreprises à travers le monde font confiance à l'environnement de sécurité zero-knowledge et au logiciel de chiffrement de Keeper. Celui-ci réduit les risques de cybervol, augmente la productivité des employés et respecte les normes de conformité. En 2020, Keeper a été élu pour la troisième fois Meilleur gestionnaire de mots de passe de l'année et Choix de la rédaction par PC Mag. Keeper a également été élu Choix de la rédaction par PCWorld et a remporté quatre G2 Best Software Awards et l'InfoSec Award du Meilleur outil de gestion de mots de passe pour la cybersécurité des PME. Keeper est certifié SOC-2 et ISO 27001 et figure également sur la liste autorisée du gouvernement fédéral américain via le System for Award Management (SAM).