

RAPPORT MONDIAL SUR LE SCORE DE SÉCURITÉ DE 2024

Tendances mondiales en matière de sécurité des mots de passe en 2024

Ce que le score de sécurité de Dashlane nous dit sur l'état de la cybersécurité, de l'authentification et des mots de passe dans le monde en 2024.

Introduction	03
Section 1 : L'évolution de la sécurité des mots de passe par région de 2022 à 2024	04
Section 2 : Un aperçu de la sécurité des mots de passe dans toutes les entreprises	08
Comparaisons par secteur et impact de la sécurité des mots de passe	09
Secteurs ayant les scores de sécurité les plus bas en 2024	10
Section 3 : Comment nous avons mené nos recherches	12
Section 4 : Checklist pour renforcer la robustesse de vos mots de passe	15

INTRODUCTION

Le rapport mondial sur le score de sécurité

L'évolution de la sécurité des identifiants

En 2022, Dashlane a publié le premier examen approfondi de la sécurité des mots de passe à l'échelle mondiale. Nouveauté pour le rapport de cette année, nous avons analysé l'hygiène des mots de passe spécifique aux entreprises en nous appuyant sur les données de plus de 23 000 entreprises protégées par Dashlane. Nous avons découvert que si les utilisateurs d'entreprise ont une meilleure hygiène des mots de passe que les particuliers, un grand nombre d'identifiants ne sont pas protégés par l'authentification unique (SSO). Nous avons également examiné les secteurs d'activité affichant le meilleur et le pire niveau de sécurité des mots de passe.

Depuis la publication de notre premier rapport, les utilisateurs de Dashlane du monde entier ont vu leurs scores de sécurité augmenter chaque année, soulignant que la connaissance est synonyme de pouvoir lorsqu'il s'agit de sécurité. Les avancées en matière de sécurité sont souvent progressives, et avec les clés d'identification et autres technologies sans mot de passe qui en sont encore aux premiers stades d'adoption, les identifiants compromis et non sécurisés restent un risque que les entreprises devront continuer à gérer dans les années à venir.



SECTION 1

L'évolution de la sécurité des mots de passe par région de 2022 à 2024

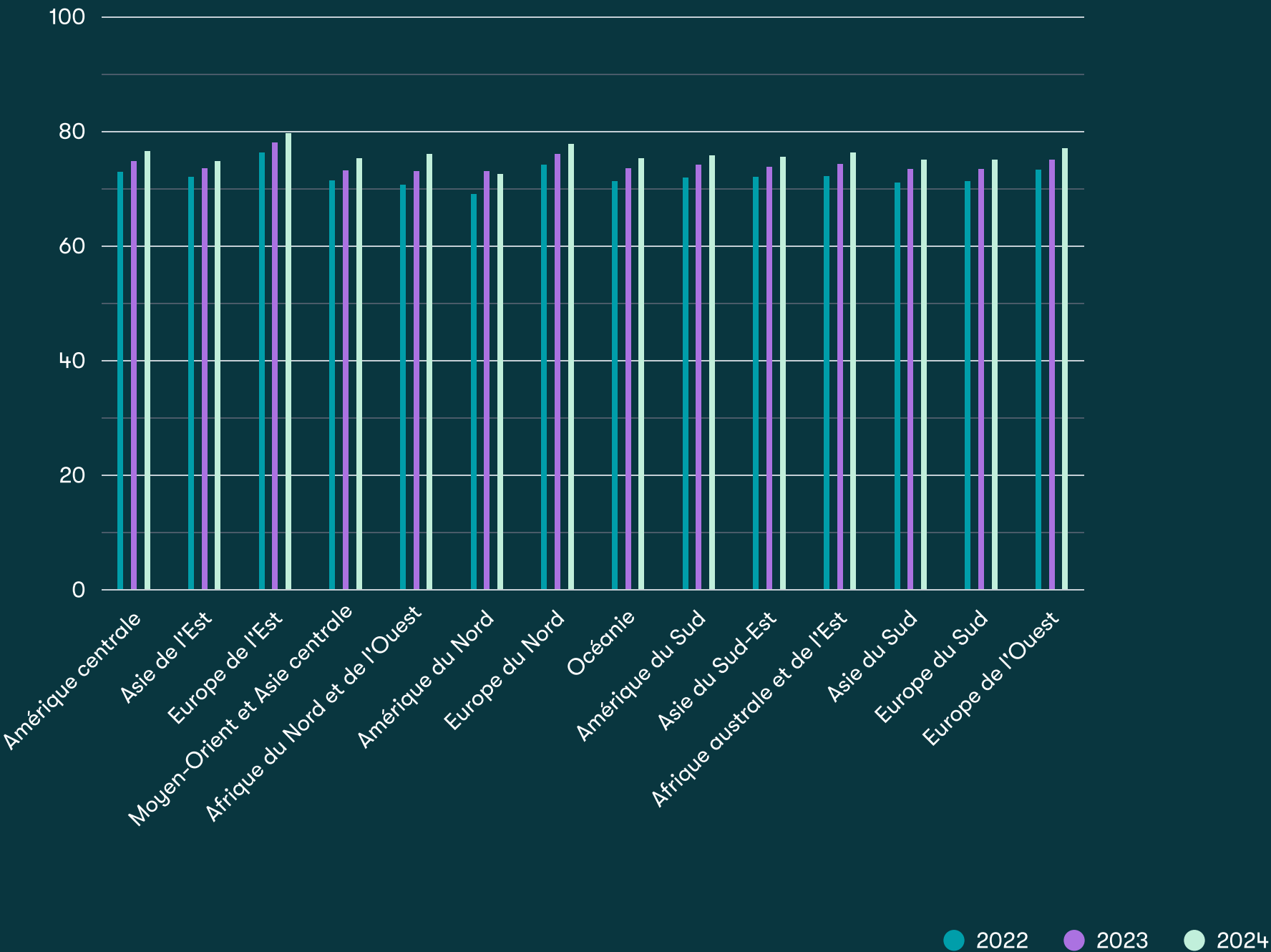
Le score de sécurité des mots de passe des utilisateurs de Dashlane à travers le monde s'est amélioré depuis l'année dernière, mais les pratiques imprudentes de gestion des identifiants persistent. Voici nos principales conclusions par région et par secteur d'activité.

La sécurité des mots de passe s'améliore à l'échelle mondiale

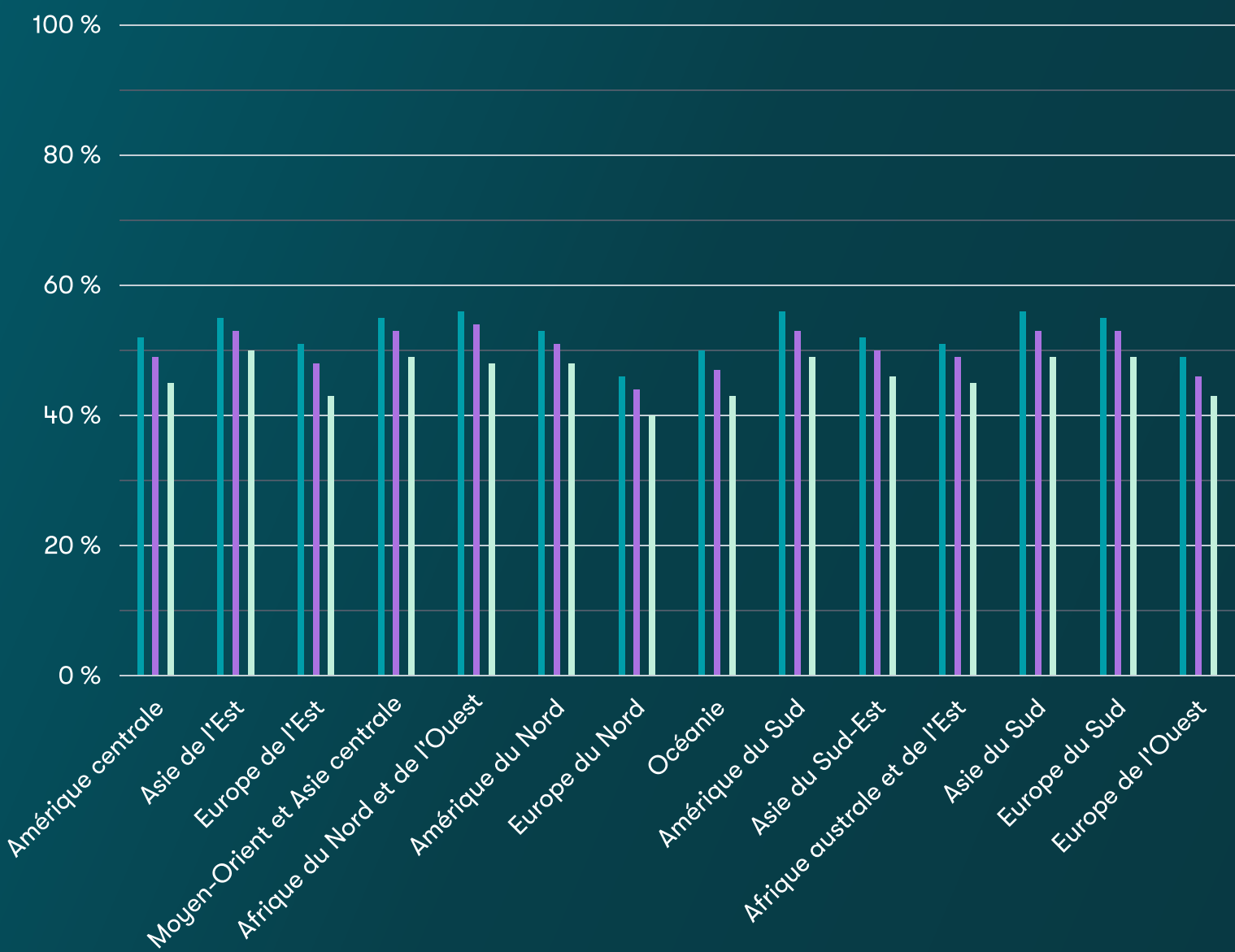
Si l'on considère l'ensemble des régions, le score de sécurité moyen en 2024 se situe entre 72,6 (Amérique du Nord) et 79,8 (Europe de l'Est). Bien que chaque région se situe dans la fourchette « Amélioration nécessaire » (un score entre 60 et 90), toutes les régions ont amélioré leur score de 2 à 4 % au cours de l'année écoulée. Cela s'explique par la diminution continue du nombre de mots de passe réutilisés et compromis au niveau mondial. Ces améliorations constantes peuvent réduire considérablement les risques pour les utilisateurs et leurs employeurs, en particulier en ce qui concerne les attaques de phishing opportunistes de grande envergure qui tirent parti d'identifiants faibles, réutilisés ou compromis.

« La cybersécurité d'une entreprise exige que ses employés soient informés et prudents », a déclaré Robin Koetje, vice-président des technologies de l'information de la marque de boutiques-hôtels Staypineapple. « Le score de sécurité permet à nos employés de trouver et de corriger facilement les mots de passe faibles et réutilisés. »

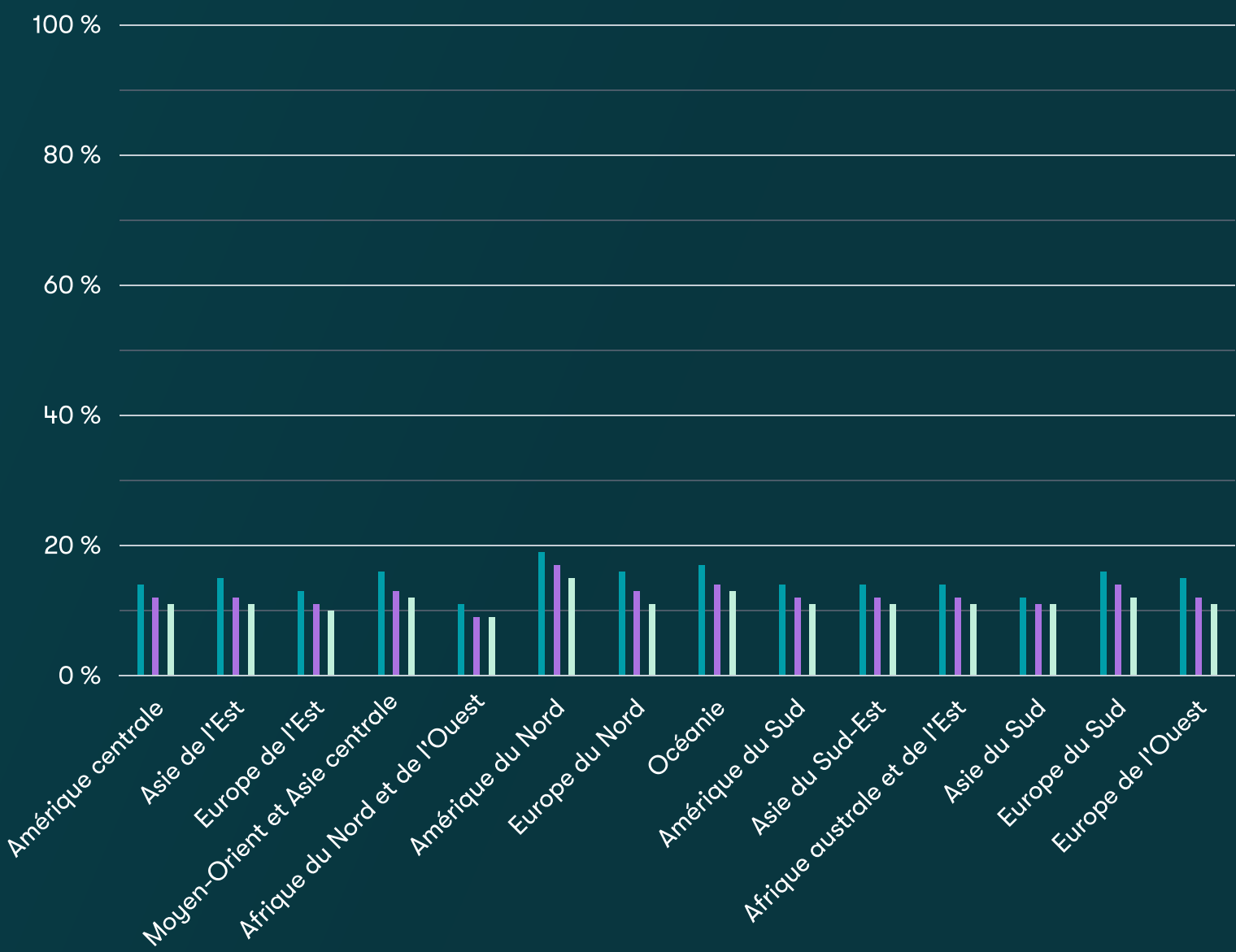
Moyenne du score de sécurité par région



Partager les mots de passe réutilisés par région



Partager les mots de passe compromis par région



2022 2023 2024

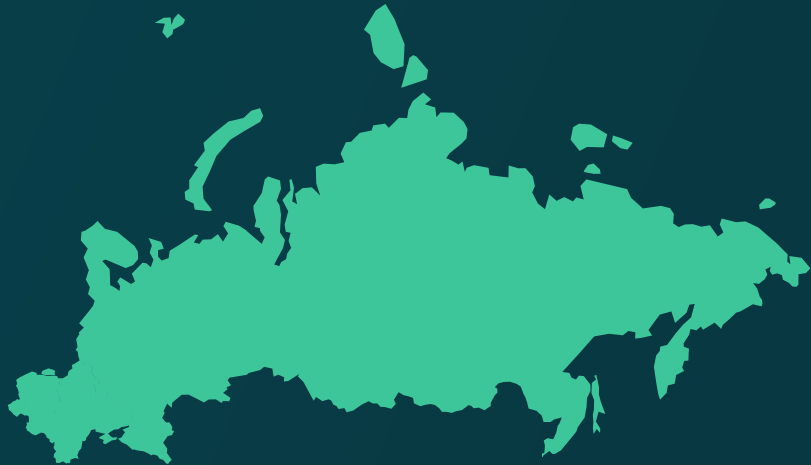
Comme le montrent les données, la part des mots de passe compromis a diminué à l'échelle mondiale, mais celle des mots de passe réutilisés reste comprise entre 40 et 50 %, ce qui témoigne de mauvaises pratiques de sécurité. La part des mots de passe faibles a eu tendance à augmenter dans toutes les régions.

Score de sécurité le plus faible :
Amérique du Nord



L'Amérique du Nord a obtenu le score de sécurité le plus bas avec 72,6, en raison du pourcentage le plus élevé de mots de passe compromis (15 %) et du pourcentage parmi les plus élevés de mots de passe réutilisés (48 %). L'Amérique du Nord est une plaque tournante pour les entreprises et est plus susceptible de générer des revenus de grande valeur, elle est donc plus souvent ciblée par les pirates.

Mots de passe les plus forts :
Europe de l'Est



L'Europe de l'Est a obtenu le score de sécurité moyen le plus élevé, soit 79,8, avec un taux de réduction des mots de passe compromis le plus rapide de 10 %.

Mots de passe compromis :
Afrique du Nord et de l'Ouest



L'Afrique du Nord et de l'Ouest présente le pourcentage le plus faible de mots de passe compromis (9 %) et le taux de réduction le plus élevé de mots de passe réutilisés (11 %).



SECTION 2

Un aperçu de la sécurité des mots de passe dans toutes les entreprises

Nouveauté du rapport en 2024 : nous avons ajouté des statistiques sur les entreprises et les industries, qui fournissent des tendances différentielles et nous permettent de d'analyser plus en détail les tendances de sécurité des mots de passe mondiales.

Comparaisons par secteur et impact de la sécurité des mots de passe

Les 5 secteurs ayant obtenu les scores de sécurité les plus élevés en 2024

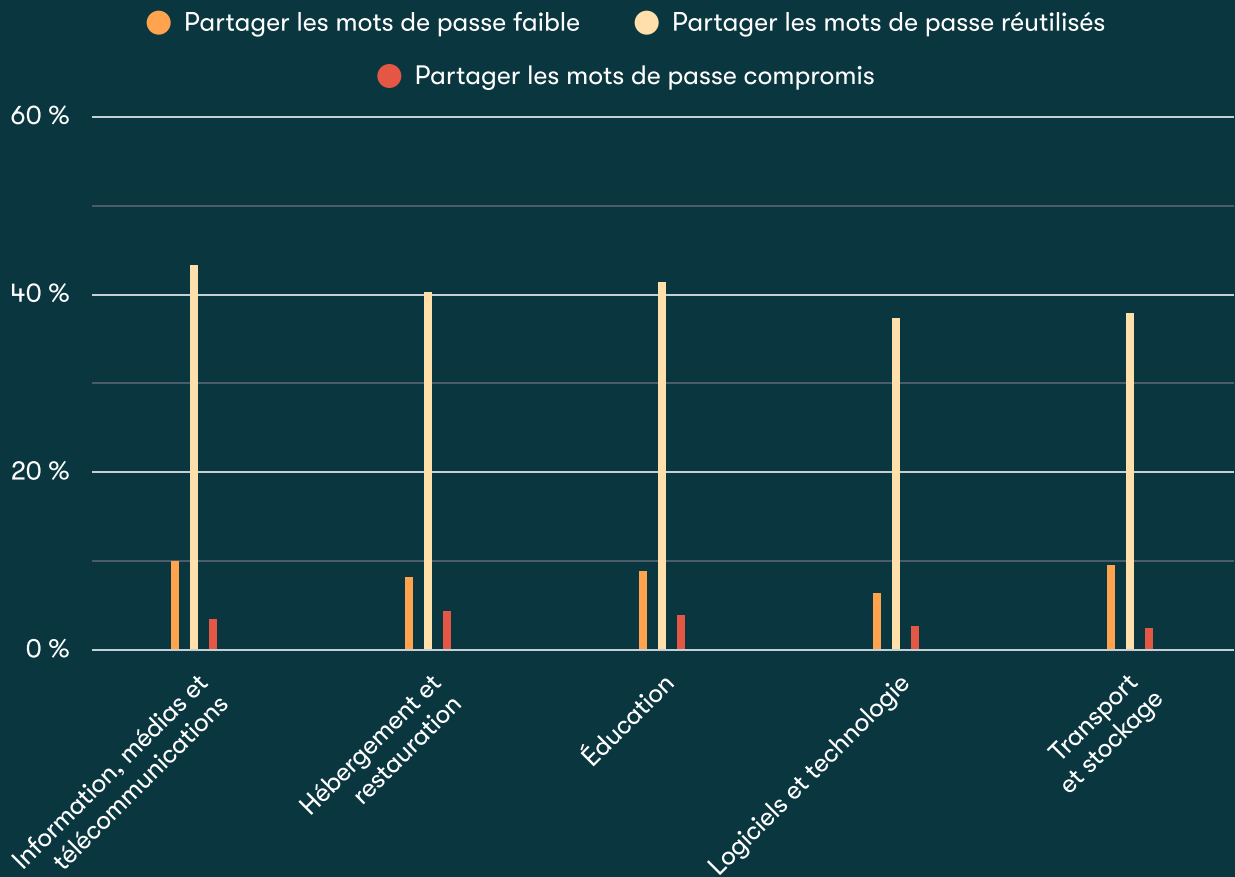
- 1. Logiciels et technologie
- 2. Information, médias et télécommunications
- 3. Éducation
- 4. Transport et stockage
- 5. Hébergement et restauration

Il n'est pas surprenant que les secteurs réputés pour leur activité en ligne et leur utilisation du SaaS (et probablement beaucoup plus conscients des risques de cybersécurité) accordent plus d'attention à leurs scores de sécurité. Ces caractéristiques sont particulièrement vraies pour les industries telles que les logiciels et la technologie, l'information, les médias et les télécommunications, ainsi que l'éducation.

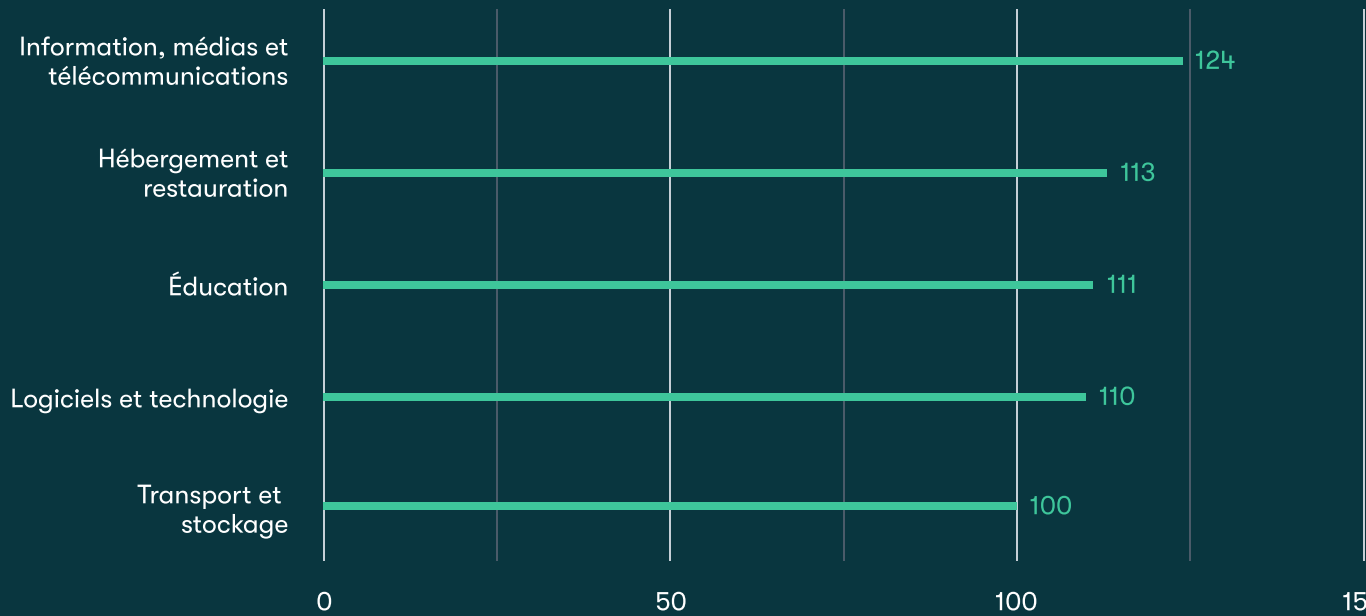
Le secteur de l'éducation se distingue par le chemin parcouru en matière de sécurité numérique. Sécuriser les données de ses enseignants et de ses étudiants tout en sensibilisant ces derniers aux bonnes pratiques informatiques n'est pas chose aisée, d'autant plus que le secteur de l'éducation est l'un des plus ciblés par les ransomwares. Si un cybercriminel parvenait à pirater un district scolaire ou le compte d'un étudiant, il pourrait exploiter des quantités considérables de données sensibles concernant des mineurs.

Les secteurs du transport et de l'entreposage ainsi que de l'hébergement et de la restauration ont souvent une perspective différente en matière de cybersécurité du fait que leur fonctionnement est fortement tributaire de la chaîne d'approvisionnement. Une cyberattaque pourrait physiquement interrompre leur production et leurs opérations.

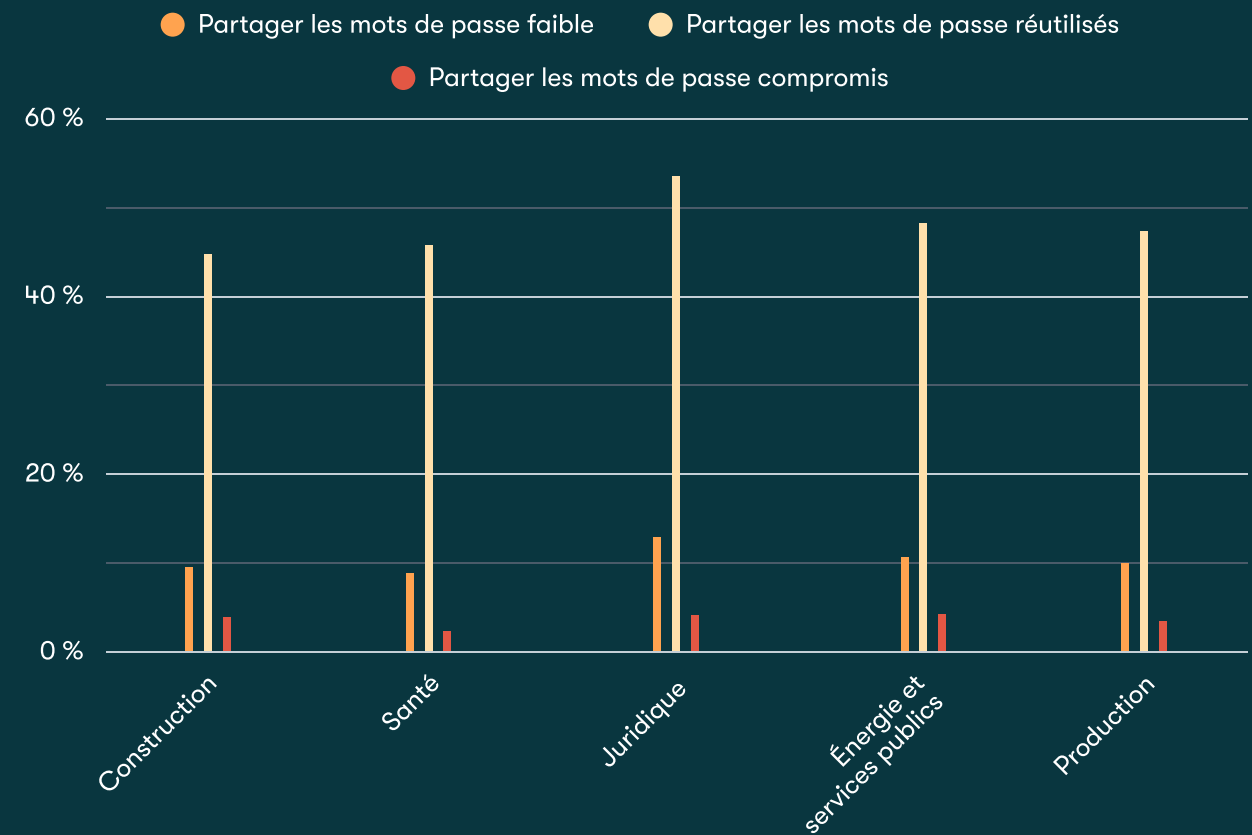
Les 5 principaux secteurs



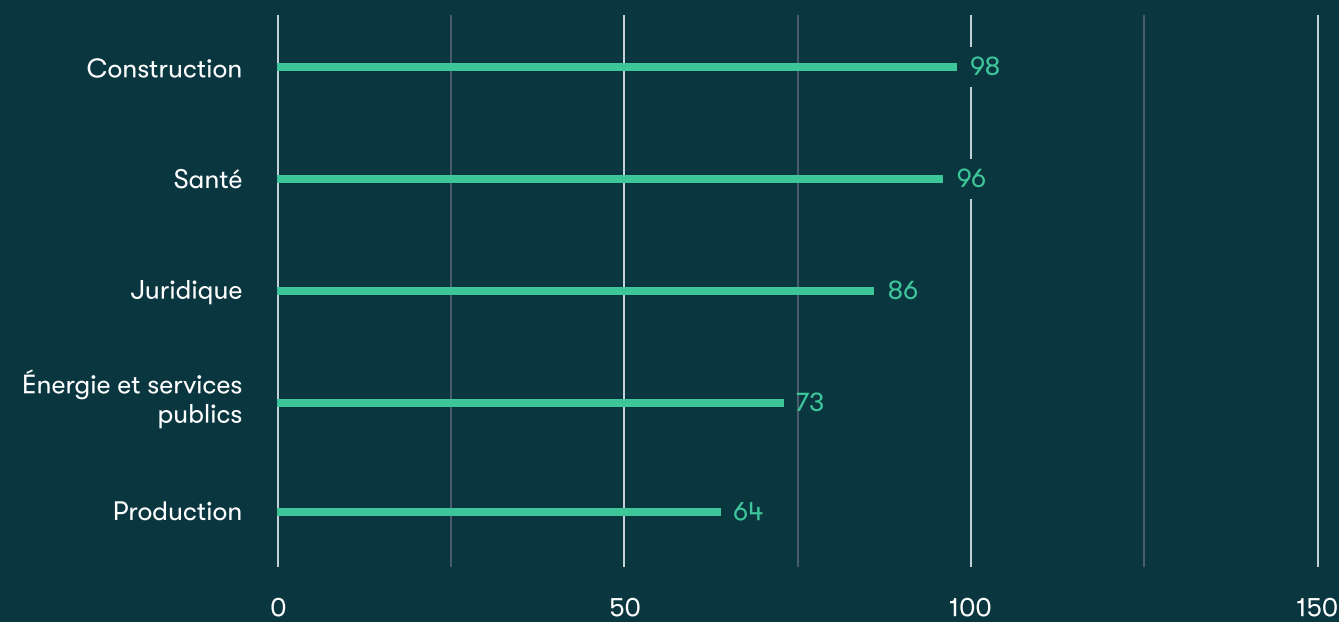
Moyenne des identifiants par utilisateur professionnel



Les 5 secteurs les plus bas



Moyenne des identifiants par utilisateur professionnel



Secteurs ayant les scores de sécurité les plus bas en 2024

- 1. Juridique
- 2. Production
- 3. Construction
- 4. Santé
- 5. Énergie et services publics

Les conclusions concernant les secteurs d'activité affichant les scores de sécurité les plus bas nous permettent de partager des informations sur chacun d'entre eux. Par exemple, le secteur juridique n'est pas traditionnellement réputé pour sa sophistication technologique ou sa rapidité d'adaptation à l'évolution du paysage en ligne. Il se retrouve souvent à la traîne.

Les secteurs de la fabrication, de la construction, de l'énergie et des services publics ont en commun le fait que leur travail se déroule dans des lieux physiques, hors ligne. Dans ces secteurs, les employés voyagent loin de leur bureau et les politiques d'entreprise exigent que les mots de passe soient modifiés tous les 90 jours, malgré les recommandations du NIST, ce qui fait que les mots de passe réutilisés sont monnaie courante, de même que les identifiants partagés.

La santé étant l'un des secteurs les plus ciblés par les cyberattaques et l'un des plus réglementés dans le cadre de la loi HIPAA, ses professionnels sont soumis à des politiques de sécurité beaucoup plus strictes que la plupart des autres secteurs. Cependant, cela peut parfois avoir l'effet inverse : les employés peuvent supposer que ces exigences réglementaires et de sécurité sont suffisantes pour assurer leur sécurité, de sorte qu'ils ne s'appuient pas autant sur des tiers pour se protéger. Si les professionnels de santé n'utilisent pas d'outils de sécurité tels que des gestionnaires de mots de passe, ils pourraient passer à côté d'une étape essentielle dans la protection des données hautement sensibles de leurs patients et de leur personnel.

Si les professionnels de santé n'utilisent pas d'outils de sécurité tels que des gestionnaires de mots de passe, ils pourraient passer à côté d'une étape essentielle dans la protection des données hautement sensibles de leurs patients et de leur personnel.

Dashlane a constaté que le nombre moyen d'identifiants par utilisateur professionnel varie considérablement lorsqu'on compare des entreprises de tailles différentes.

Les petites entreprises affichent le nombre moyen d'identifiants par utilisateur le plus élevé (122), suivi d'une chute vertigineuse pour les entreprises de taille moyenne (76) et les grandes entreprises (53). Si les moyennes et grandes entreprises disposent souvent d'une pile de sécurité des identités plus mature qui inclut le SSO, il est également courant pour elles de recourir à des applications et des services anciens qui peuvent tarder à proposer (voire ne jamais proposer) une option SSO. Même avec le SSO, le nombre d'identifiants en entreprise représente un risque important pour l'organisation s'il n'existe pas de protection adéquate.

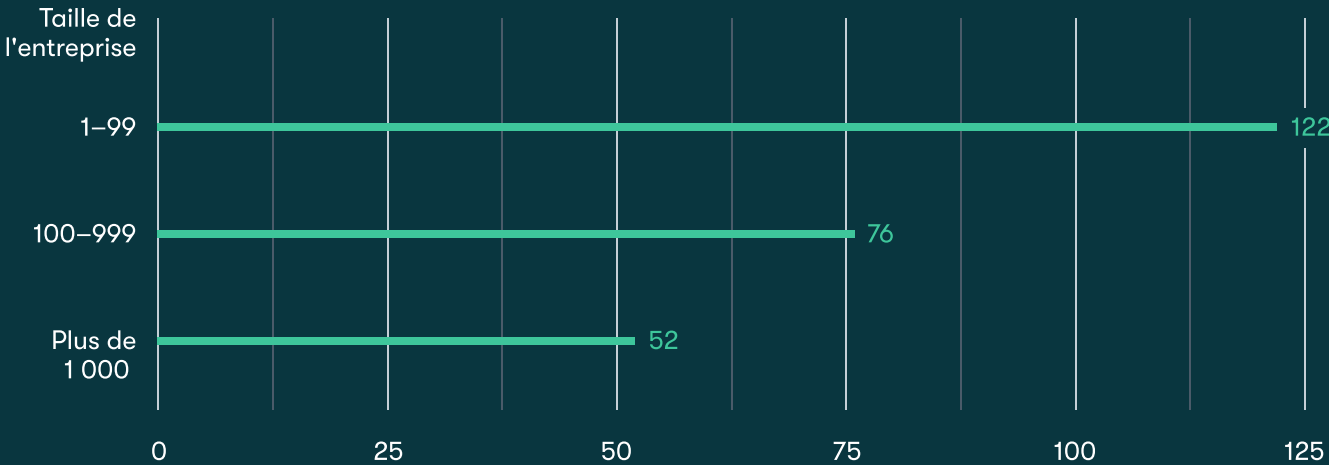
Comme le souligne un [rapport de la CISA](#), les petites et moyennes entreprises manquent souvent de connaissances techniques ou de ressources financières pour mettre en œuvre le SSO. Les fournisseurs sont connus pour facturer une « taxe SSO » pour les intégrations SSO, ce qui met souvent le contrôle hors de portée sur le plan économique.

Selon John Bennett, directeur général de Dashlane, de nombreuses petites et moyennes entreprises ne disposent pas non plus de l'infrastructure de gestion des identités sous-jacente, qu'il s'agisse d'Active Directory ou d'un autre fournisseur d'identité, pour mettre en œuvre le SSO.

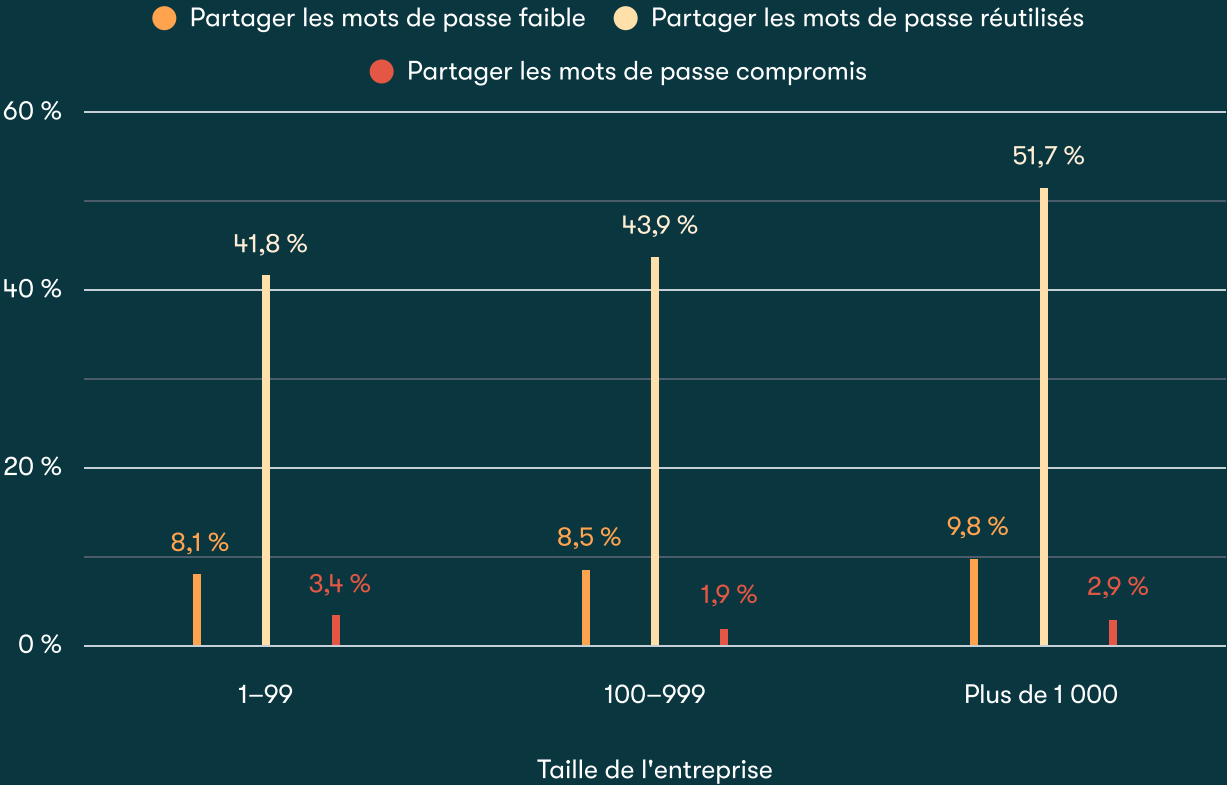
« Parier sur le SSO comme moyen de protéger les entreprises n'est pas suffisant », a déclaré J. Bennett. « Dans un contexte où de nouveaux produits et services font constamment leur apparition (même avec une recrudescence de nouvelles entreprises qui démarrent avec des LLM très accessibles), il est peu probable qu'une entreprise soit en mesure de gérer 100 % de ses services avec le SSO à un moment ou à un autre. »

Pour compléter notre regard sur les différences d'hygiène des identifiants en fonction de la taille de l'organisation, les entreprises de taille moyenne (100 à 999 employés) affichaient la part la plus faible de mots de passe compromis (1,9 %) par rapport aux petites entreprises (3,4 %) et aux grandes entreprises (2,9 %). Plus que la taille de l'entreprise, ce sont les budgets et les politiques de cybersécurité qui influent sur la sécurité des mots de passe.

Moyenne des identifiants par utilisateur professionnel



Partager les mots de passe réutilisés, faibles et compromis





SECTION 3

Comment nous avons mené nos recherches

Pour illustrer l'état de la sécurité des mots de passe en 2024, nous avons collecté des données d'utilisation anonymes à partir de comptes personnels et professionnels, en intégrant des centaines de milliards de points de données.



Quels sont les facteurs qui entrent en ligne de compte dans votre score ?

L'algorithme unique de Dashlane, le score sécurité, identifie les mots de passe faibles, réutilisés et compromis dans les coffres-forts des utilisateurs afin de dresser un état des lieux de la sécurité globale des mots de passe.



Astuce de pro

Pour améliorer votre score, assurez-vous que vos mots de passe sont difficiles à pirater en utilisant notre générateur de mots de passe doté de l'algorithme ZXCVCBN, qui mesure la robustesse des mots de passe et suggère des améliorations.



Ce que signifie votre score

Les scores de 90 et plus sont idéaux. Pour les scores compris entre 60 et 90, mettez à jour les mots de passe faibles ou compromis. Les scores inférieurs à 60 nécessitent une attention immédiate pour garantir votre sécurité en ligne.



Astuce de pro

Les mots de passe que vous ne maîtrisez pas, tels que les codes de smartphone, peuvent être stockés en toute sécurité dans un onglet séparé afin qu'ils n'aient pas d'impact sur votre score.



Données par région

Les scores de sécurité pour chaque région sont basés sur les scores moyens et médians des utilisateurs de Dashlane dans ladite région. Nous avons utilisé des données anonymes pour calculer les scores régionaux.



Réduction des biais

Tous les pays du monde ont été inclus et regroupés en régions clés. Nous avons créé des régions distinctes qui ont chacune un volume suffisamment élevé d'utilisateurs de Dashlane pour garantir une répartition cohérente des utilisateurs professionnels et individuels dans chaque région.



Pourquoi nous utilisons des scores moyens

Notre analyse a porté sur les scores médian et moyen, ainsi que sur la répartition des scores de sécurité entre les régions. Le score moyen donne l'aperçu le plus significatif de la sécurité des mots de passe à l'échelle mondiale.



Les mots de passe réutilisés et faibles sont similaires à l'échelle mondiale

Cependant, la quantité de mots de passe compromis varie considérablement d'une région à l'autre, ce qui contribue aux différences que nous avons observées dans chaque région.



« Une bonne hygiène des mots de passe est un élément essentiel pour renforcer la protection des utilisateurs contre les menaces visant les identifiants et des entreprises contre les failles. »

— John Bennett, PDG, Dashlane



SECTION 4

Checklist pour renforcer la robustesse de vos mots de passe

Prêt à renforcer la sécurité de vos mots de passe ? Voici cinq mesures à prendre pour améliorer votre sécurité en ligne.



Adopter le bon gestionnaire d'identifiants

Gartner® recommande aux entreprises d'utiliser une solution de gestion des mots de passe du personnel. Des solutions comme Dashlane aident les entreprises à comprendre et à améliorer la sécurité des mots de passe.



Mettez à jour les mots de passe réutilisés ou compromis

Dashlane vous informera des mots de passe réutilisés, faibles ou compromis dans votre coffre-fort. Mettez à jour instantanément ou créez de nouveaux mots de passe forts et uniques grâce à notre générateur de mots de passe.



Créez une culture de la sécurité

Une forte culture de la sécurité implique tous les membres d'une organisation. Faites comprendre l'importance de la protection des données sensibles et fournissez aux employés des outils pour qu'ils fassent partie de la solution.



Simplifiez la sécurité avec les bons outils

Éliminez les risques de conformité en stockant en toute sécurité les données sensibles dans un gestionnaire d'identifiants comme Dashlane, qui est conforme au RGPD et au CCPA, et offre une protection de niveau professionnel.



Activer l'authentification multifacteur

Des preuves d'identité supplémentaires, telles que la reconnaissance faciale et l'identification par empreinte digitale, renforcent la sécurité des identifiants et réduisent considérablement la probabilité de compromission des comptes.



Envisagez de passer au sans mot de passe

Les clés d'identification et les connexions sans mot de passe simplifient l'authentification et aident à se protéger contre les attaques de phishing. Dashlane a été le premier gestionnaire d'identifiants à lancer la connexion sans mot de passe.



À propos de Dashlane

Dashlane est la gestionnaire d'identifiants appréciée de tous, qui sécurise les accès et protège de manière proactive contre les failles. Plus de 23 000 marques dans le monde, dont Sephora, Air France et Forrester, font confiance à Dashlane pour ses innovations de pointe qui leur permettent de garder une longueur d'avance sur les menaces en constante évolution. Nous associons une sécurité brevetée de niveau professionnel à un design adapté au grand public au sein d'une plate-forme de premier ordre, qui permet à tout le monde de faire partie de la solution de sécurité des identifiants.

Visitez dashlane.com/blog pour plus de ressources, des conseils de sécurité numérique et des nouvelles sur les produits Dashlane.

dashlane.com

Confidentialité et sécurité

Dashlane utilise une architecture « zero-knowledge » dans notre plate-forme.

Nous ne savons pas et ne pouvons pas savoir quelles informations les utilisateurs enregistrent sur les Services (« Données sécurisées »).

Aucune « donnée personnelle » n'a été collectée pour être utilisée dans ce rapport. Comme indiqué dans notre Politique de confidentialité, Dashlane définit les « données personnelles » comme toute information qui, seule ou combinée à d'autres informations que nous détenons, identifie une personne, comme son nom, son adresse postale, son adresse e-mail, son adresse IP ou son numéro de téléphone.

Toutes les données collectées pour ce rapport sont rendues anonymes et agrégées à l'aide d'informations d'adresse IP sans les quatre derniers chiffres afin de déterminer l'emplacement des utilisateurs.

Les données anonymes sont des données qui, seules ou combinées à d'autres informations dont nous disposons ou dont dispose un tiers avec lequel les données sont partagées, ne permettent pas d'identifier un individu.

Pour obtenir le score de sécurité de votre entreprise, rendez-vous sur le site dashlane.com pour bénéficier d'une démonstration gratuite.

Clé régionale

#1 | 79,8 | Europe de l'Est :

Bulgarie, Pologne, République tchèque, Ukraine, Moldavie, Slovaquie, Fédération de Russie, Roumanie, Hongrie et Biélorussie.

#2 | 76,1 | Europe du Nord :

Estonie, Danemark, Guernsey, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Île de Man, Suède, Islande, Lettonie, Jersey, Îles Féroé, Lituanie, Irlande, Finlande, Norvège, Svalbard et Jan Mayen et Îles Åland.

#3 | 77,2 | Europe de l'Ouest :

Allemagne, France, Pays-Bas, Monaco, Suisse, Belgique, Luxembourg, Autriche et Liechtenstein.

#4 | 76,6 | Amérique centrale :

Costa Rica, République dominicaine, Porto Rico, Barbade, Martinique, Montserrat, Bonaire, Saint-Eustache et Saba, El Salvador, Belize, Sainte-Lucie, Îles Caïmans, Anguilla, Guadeloupe, Panama, Îles Vierges (États-Unis), Curaçao, Cuba, Saint-Vincent-et-les-Grenadines, Grenade, Bahamas, Honduras, Haïti, Trinité-et-Tobago, Aruba, Jamaïque, Saint-Martin, Sint Maarten (partie néerlandaise), Dominique, Mexique, Nicaragua, Guatemala, Antigua-et-Barbuda, Îles Vierges (britanniques), Saint-Barthélemy, Îles Turques et Caïques, Saint-Kitts et Nevis.

#5 | 76,4 | Afrique australe et de l'Est :

Zimbabwe, Réunion, Seychelles, Somalie, Kenya, Namibie, Mozambique, Zambie, Malawi, Érythrée, Ile Maurice, Madagascar, Comores, Soudan du Sud, Swaziland, Tanzanie, République-Unie du Botswana, Rwanda, Djibouti, Burundi, Afrique du Sud, Éthiopie, Mayotte, Lesotho et Ouganda.

#6 | 76,2 | Afrique du Nord et de l'Ouest :

Maroc, Côte d'Ivoire, Libye, Sénégal, Sierra Leone, Mali, Guinée-Bissau, Gabon, Cap-Vert, Ghana, Burkina Faso, Égypte, Congo (République démocratique du), Angola, Guinée équatoriale, Soudan, Tunisie, Togo, Algérie, Nigéria, Niger, Bénin, Guinée, Gambie, Sahara occidental, Cameroun, Mauritanie, Sainte-Hélène, Ascension et Tristan da Cunha, Libéria, République centrafricaine, Tchad, Sao Tome et Principe.

#7 | 75,9 | Amérique du Sud :

Guyane, Îles Falkland (Malouines), Argentine, Venezuela (République bolivarienne du), Colombie, Équateur, Guyane française, Suriname, Bolivie (État plurinational de), Brésil, Chili, Uruguay, Paraguay et Pérou.

#8 | 75,7 | Asie du Sud-Est :

Philippines, Vietnam, Thaïlande, Brunei Darussalam, République démocratique populaire lao, Malaisie, Cambodge, Myanmar, Singapour et Indonésie.

#9 | 75,4 | Moyen-Orient et Asie centrale :

Turquie, Oman, Ouzbékistan, Koweït, Kazakhstan, Azerbaïdjan, Yémen, Bahreïn, Turkménistan, Israël, Émirats arabes unis, Arménie, État palestinien du Tadjikistan, Chypre, Jordanie, Géorgie, Qatar, Kirghizistan, Irak, République arabe syrienne, Arabie saoudite et Liban.

#10 | 75,4 | Océanie :

Polynésie française, Fidji, Samoa, Nouvelle-Zélande, Tuvalu, Vanuatu, Îles Mariannes du Nord, Micronésie, Nauru, Pitcairn, Nouvelle-Calédonie, Wallis-et-Futuna, Îles Salomon, Tonga, Guam, Papouasie-Nouvelle-Guinée, Tokelau, Îles Cook, Îles Marshall, Australie, Samoa américaines et Palau.

#11 | 75,2 | Europe du Sud :

Portugal, Italie, Slovénie, Gibraltar, Grèce, Croatie, Macédoine, Espagne, Malte, Andorre, Bosnie-Herzégovine, Saint-Marin, Serbie, Monténégro, Saint-Siège et Albanie.

#12 | 75,1 | Asie du Sud :

Inde, Iran (République islamique d'), Népal, Maldives, Afghanistan, Sri Lanka, Pakistan, Bhoutan et Bangladesh.

#13 | 74,9 | Asie de l'Est :

Chine, Japon, Corée (République de), Macao, Corée (République populaire démocratique de), Hong Kong, Taïwan, Province de Chine et Mongolie.

#14 | 72,6 | Amérique du Nord :

Canada, Bermudes, Groenland, Saint-Pierre-et-Miquelon et États-Unis d'Amérique