

# 3E RAPPORT ANNUEL MONDIAL SUR LA SÉCURITÉ DES MOTS DE PASSE

Nous avons analysé les comportements de sécurité de plus de 47 000 entreprises de différentes tailles, industries et régions. Voici les tendances en matière d'accès et d'authentification que nous avons observées dans les entreprises du monde entier.



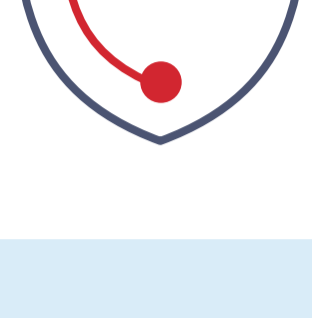
Le Danemark est en tête pour l'utilisation de l'authentification multifacteur.



**57%** 57% des entreprises du monde entier ont des employés qui utilisent l'authentification multifacteur, une hausse de 12 points par rapport à l'an dernier.



**46%** des employés au Danemark utilisent l'authentification multifacteur.

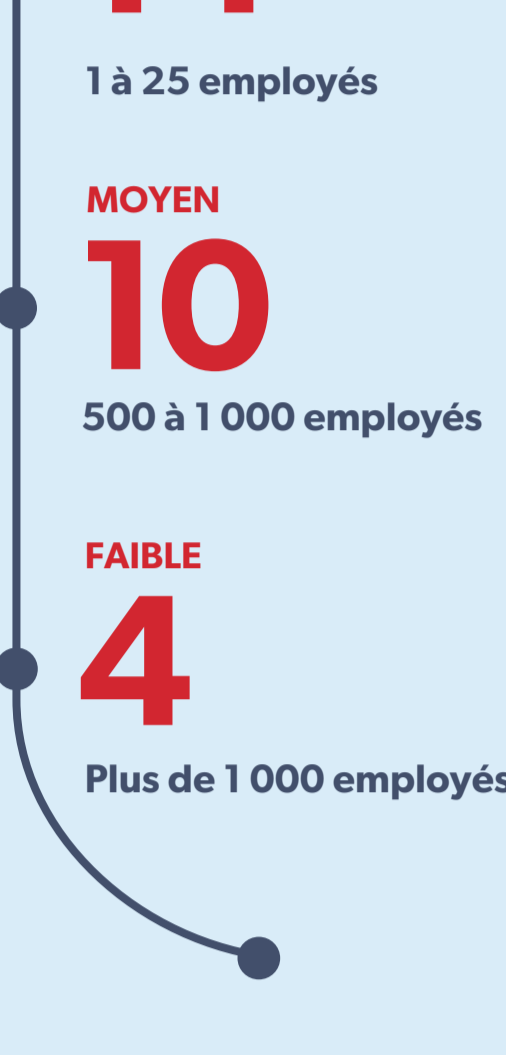


**La réutilisation des mots de passe reste courante, et affaiblit les scores de sécurité.**

## NOMBRE MOYEN DE MOTS DE PASSE RÉUTILISÉS

### PAR NOMBRE D'EMPLOYÉS

Les entreprises avec moins de 1 000 employés sont les plus confrontées à la réutilisation des mots de passe.



### PAR SECTEUR D'ACTIVITÉ

Les entreprises de certains secteurs réutilisent les mots de passe près de deux fois plus souvent que d'autres.



Les Pays-Bas sont en tête en matière de sécurité.



**L'accès universel par mot de passe est préférable pour les employés.**

La possibilité d'accéder aux comptes sur appareils mobiles améliore considérablement l'expérience, et donc l'adoption par les employés des solutions de sécurité.



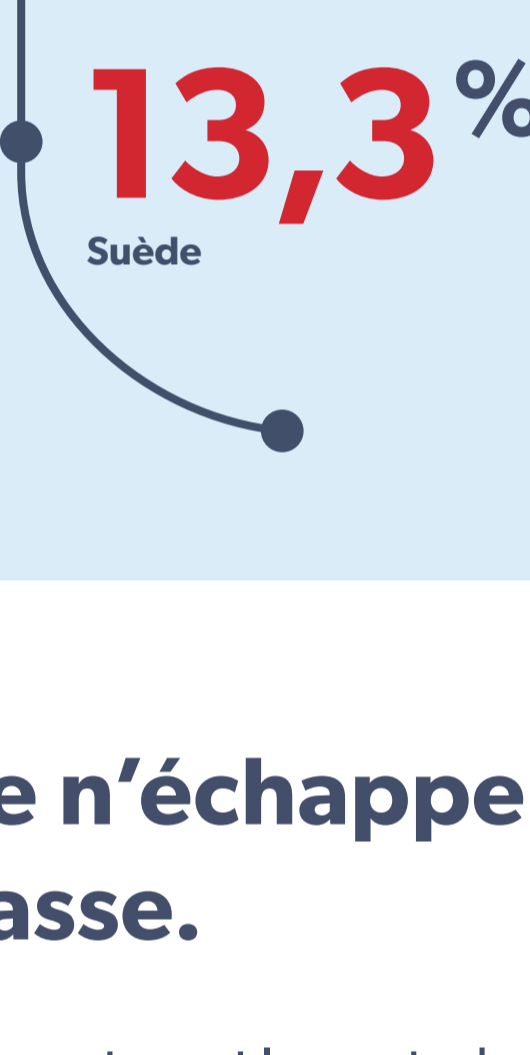
**23%** des employés dans le monde ont accès à leurs coffres-forts de mots de passe sur leur smartphone, dont 14% qui utilisent l'app LastPass pour iOS et 9% qui utilisent l'app pour Android.

## UTILISATION PAR LES EMPLOYÉS DE L'APP LASTPASS

### TOP 3 PAYS : ANDROID



### TOP 3 PAYS : iOS



**Info : aucune entreprise n'échappe au partage des mots de passe.**

La question n'est pas de savoir si les employés partagent les mots de passe, mais comment ils peuvent le faire en toute sécurité.



En moyenne, une entreprise utilise 185 dossiers partagés.

**Les employés dans les médias et la publicité sont submergés de mots de passe.**

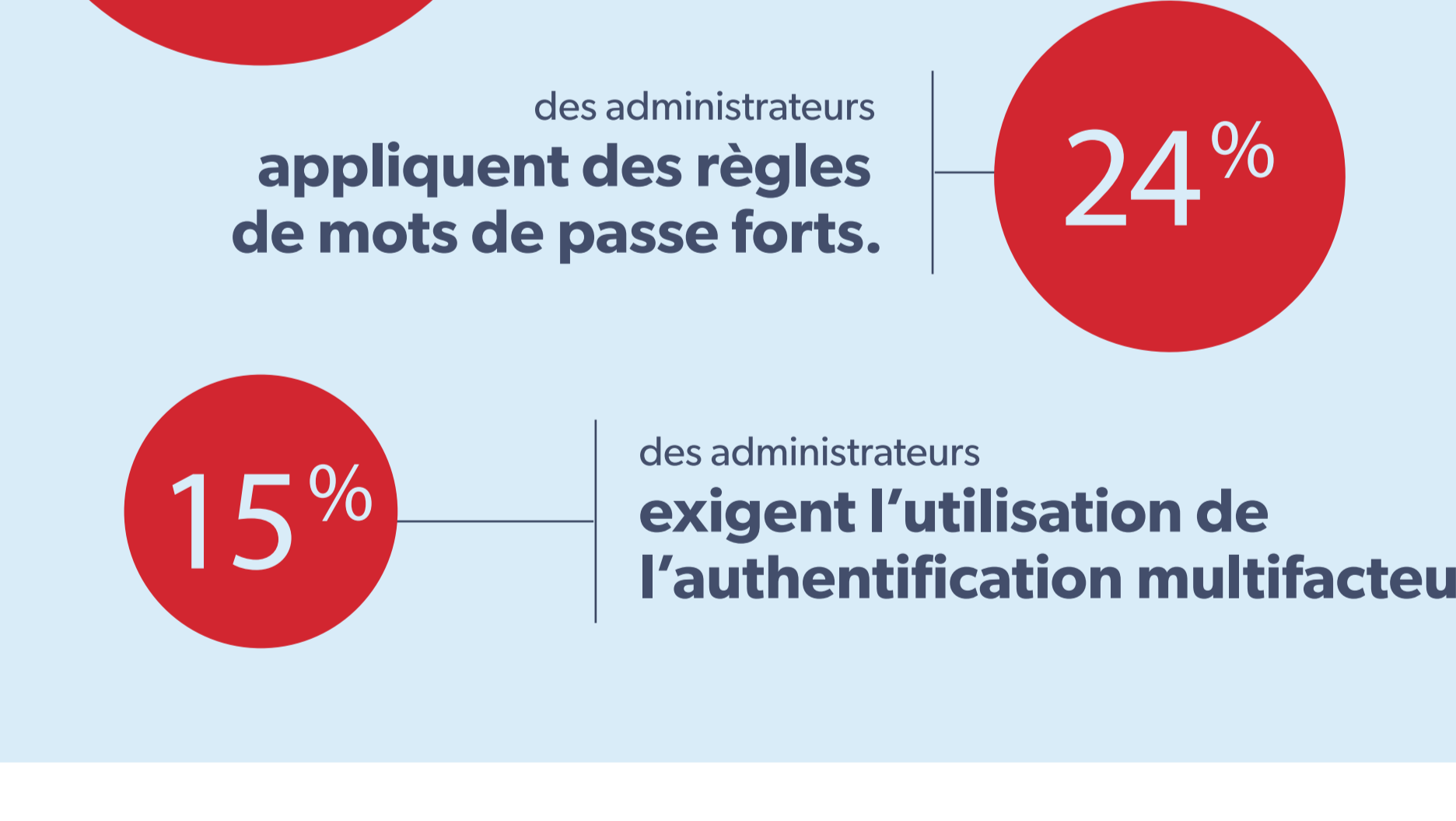
Votre métier peut affecter le nombre de mots de passe que vous devez utiliser et mémoriser.



Gérer les comptes des clients sur les réseaux sociaux, travailler avec des consultants...ça va vite !

**Les règles de sécurité sont essentielles, mais elles sont sous-exploitées.**

Les administrateurs informatiques exploitent les règles et intégrations pour renforcer la sécurité et rationaliser la gestion, même s'ils pourraient être plus nombreux à exiger l'authentification multifacteur.



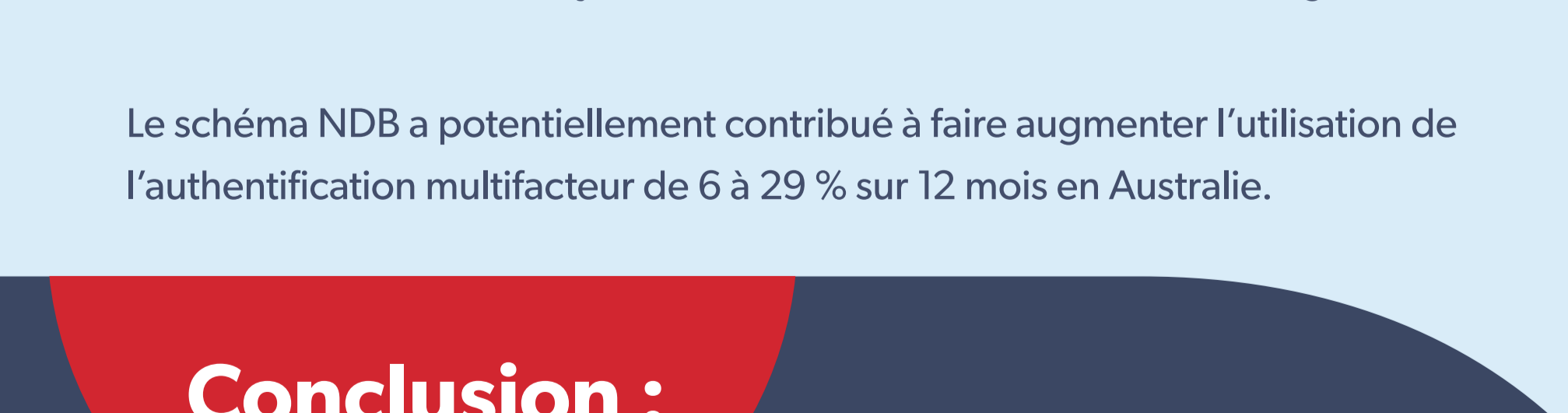
**25%** des entreprises ont intégré un gestionnaire de mots de passe avec leur annuaire pour automatiser les inscriptions, radiations et autres tâches de gestion quotidiennes.

## FOURNISSEURS D'IDENTITÉ POPULAIRES DANS LES ENTREPRISES QUI UTILISENT L'INTÉGRATION AUX ANNUAIRES AVEC LASTPASS



**Les nouvelles réglementations incitent à l'action dans les régions EMEA et APAC**

Le RGPD a potentiellement contribué à une hausse importante de l'adoption de l'AMF dans des pays comme le Danemark, les Pays-Bas, la Suisse et l'Allemagne.



Le schéma NDB a potentiellement contribué à faire augmenter l'utilisation de l'authentification multifacteur de 6 à 29% sur 12 mois en Australie.

## Conclusion :

**la situation s'est améliorée en 2019, mais les administrateurs informatiques ont encore du pain sur la planche.**

Le SI doit être moteur dans la formation continue, et prendre des mesures proactives pour éliminer les comportements à risque liés aux mots de passe. Il en va de la sécurité générale de l'entreprise.

Investir dans une solution d'identité comme LastPass contribue à la diminution des risques liés aux mots de passe, simplifie les accès des employés et renforce la sécurité avec l'authentification multifacteur, afin d'améliorer le score de sécurité de votre entreprise et mieux la protéger.

**Lire le rapport mondial 2019 sur la sécurité des mots de passe**

En savoir plus sur les tendances en matière d'accès et d'authentification, afin de les exploiter pour renforcer la sécurité de votre organisation.

[Lire le rapport](#)