VERS UN AVENIR SANS MOT DE PASSE

Un Rapport Okta

Vers un avenir sans mots de passe

Pour survivre et réussir dans l'environnement concurrentiel actuel, les entreprises doivent impérativement se tourner vers les nouvelles technologies.

Mais en dépit de leurs efforts afin d'innover et se transformer ; de trouver des solutions pour optimiser leurs interactions avec leurs clients ; et de protéger leurs employés et les données contre des menaces de plus en plus complexes, la confiance vis-à-vis de ces technologies s'effrite avec l'émergence de nouveaux défis. Les entreprises sont désormais contraintes d'évoluer toujours plus rapidement pour faire face aux problématiques de sécurité, de confidentialité et de gestion des consentements. Celles-ci affectent négativement la perception des utilisateurs de la plupart des technologies sur lesquelles nous nous appuyons aujourd'hui.

La sécurité des identités en ligne a jusqu'ici reposé sur une méthode clé : les mots de passe. Depuis plusieurs décennies, les mots de passe représentent la passerelle vers nos identités numériques et nos activités en ligne. Or nous assistons depuis bien trop longtemps à l'échec de cette méthode. Okta a donc commandité une étude pour montrer à quel point ces codes secrets affectent notre sécurité et notre qualité de vie au quotidien.

Imaginez un monde où la sécurité ne dépendrait pas de lettres et de chiffres pouvant être facilement manipulés. Un monde où l'accès aux ressources nécessaires pour vivre et travailler serait si unique que personne n'aurait les mêmes identifiants, ces derniers étant intimement liés à nos identités personnelles.

L'année 2019 marque un tournant en matière de sécurité. Les entreprises commencent en effet à se détourner des mots de passe, au profit des identités. Ces dernières jouent un rôle essentiel en permettant aux organisations d'avancer avec confiance.

Méthodologie de l'enquête

Pour le compte d'Okta, Opinium a interrogé 4 013 employés au Royaume-Uni, en France et aux Pays-Bas. Les réponses ont été collectées en mai 2019. Les références à ces travaux de recherche sont mises en évidence par l'utilisation d'expressions telles que « l'enquête d'Okta » ou « les répondants ».

PAYS

2007 1003 1003

GENRE

50% femme

49% homme

1% autre

ÂGE

21% 18-34

52% 35-54

27% 55+

EMPLOI

82% temps plein

16% temps partiel

2% temps partiel (moins de 8 heures)

TYPE DE TRAVAIL

87% bureau

13% télétravail

TAILLE DE L'ENTREPRISE

13% petite

*6% ne sait pas

30% moyenne

52% grande

1 LA SÉCURITÉ SANS MOTS DE PASSE : UNE RÉALITÉ

Confiance et identité

La confiance est le nouveau périmètre de la sécurité. Plus que jamais, les organisations doivent prouver à leurs employés et à leurs clients qu'ils peuvent se fier à elles. Ce paramètre prend une importance de plus en plus importante depuis une dizaine d'années, notamment suite à la multiplication des fuites de données et des cyberattaques, ainsi qu'aux problématiques de confidentialité de nos données personnelles liées au suivi permanent de nos identités numériques et à la monétisation de nos préférences.

L'identité est donc au cœur de la notion de confiance. Les individus y étant désormais plus attentifs, les entreprises doivent à leur tour prêter davantage d'attention à leurs approches en la matière.

Depuis plusieurs décennies, notre identité et notre sécurité sont étroitement liées, et nous utilisons des mots de passe pour les protéger. Mais cette stratégie s'est révélée inefficace pour les entreprises.

La Dr Maria Bada, chercheuse associée à l'Université de Cambridge, estime que les mots de passe représentent l'un des principaux problèmes concrets pour les ingénieurs en sécurité.

> Les employés doivent se souvenir non seulement de leurs mots de passe, mais aussi des identifiants système et utilisateur associés. Ils doivent également se rappeler s'ils ont changé de mot de passe et quand ils l'ont fait[1]. Il est surréaliste de leur demander de se souvenir de mot de passe qu'ils utilisent rarement ou changent fréquemment.
>
> Selon une enquête de Schacter, le cerveau humain est incapable de mémoriser plus de deux ou trois mots de passe forts, et il aura du mal à s'en souvenir s'il ne s'en sert pas régulièrement.[2]

[1] M. A. Sasse, S. Brostoff et D. Weirich (2001). Transforming the 'Weakest Link' -- a Human/Computer Interaction Approach to Usable and Effective Security. BT Technology Journal, 19(3), 122.

[2] D. L. Schacter, D. R. Addis, D. Hassabis, V. C. Martin, R. N. Spreng et K. K. Szpunar (2012). The future of memory: remembering, imagining, and the brain. Neuron 76, 677–694

Le défi pour l'entreprise

Les mots de passe sont à l'origine de nombreux problèmes pour les entreprises. Selon le rapport Data Breach Investigations publié par Verizon en 2018, 81 % des failles dues à des piratages étaient liées à des mots de passe faibles, dérobés ou réutilisés[3]. Et les conséquences peuvent être catastrophiques : en moyenne, le coût d'un document volé est de 148 dollars,[4] et le coût total d'une fuite de données de 3,86 millions de dollars. Pire : à la suite d'un piratage, les organisations ont 32 % de chances d'être à nouveau victimes d'une fuite de données dans les deux années suivantes. Sans oublier les dégâts souvent irréparables pour leurs réputations.

Bien que le risque d'incident soit la principale préoccupation des entreprises vis-à-vis des mots de passe, nos travaux de recherche montrent que d'autres éléments ont un impact au quotidien sur les processus métiers.

L'enquête d'Okta sur la sécurité des mots de passe révèle ainsi que lorsque ceux-ci sont oubliés :

37%
des utilisateurs **ne peuvent plus accéder** à leurs comptes

37%
ne peuvent plus accéder à des ressources dont ils ont besoin

19%
prennent du retard dans leur travail

Les mots de passe nuisant à la productivité, le risque pour les entreprises est alors de ne pas parvenir à rester compétitives, et de décevoir des clients s'attendant à des services d'exception.

[3] Verizon Enterprise. (2018). 2018 Data Breach Investigations Report.
[4] Ponemon Institute's 2018 Cost of a Data Breach Study

Le défi pour les employés

L'enquête d'Okta révèle qu'en moyenne, les personnes interrogées doivent se souvenir de 10 mots de passe au quotidien, et en oublient trois par mois. C'est bien connu : le principal risque de sécurité pour les employeurs sont leurs employés eux-mêmes : près de la moitié (49 %) des organisations de tous les secteurs doivent faire face à de graves incidents de sécurité provoqués par des erreurs commises par leurs employés.[5]

Malheureusement, les choses ne semblent pas près d'évoluer. Selon l'enquête d'Okta, les mots de passe contenant des informations sensibles ne sont pas régulièrement modifiés : seulement trois fois par an pour les identifiants professionnels. D'autres, à l'instar des mots de passe des comptes bancaires, des téléphones, des e-mails personnels et des médias sociaux ne sont mis à jour en moyenne qu'une fois par an.

10

MOTS DE PASSE

doivent être mémorisés **quotidiennement** (en moyenne)

3

MOTS DE PASSE

sont **oubliés** par **mois** (en moyenne)

18%

des personnes interrogées se sentiraient **stressées ou inquiètes** à cause du **nombre de mots de passe** à retenir

[5] Kaspersky Industrial CyberSecurity. (2018). The State of Industrial Cybersecurity 2018 | Kaspersky Industrial CyberSecurity.

Alors pourquoi les organisations continuent-elles de s'appuyer sur une méthode qui s'est révélée jusqu'ici inadaptée ?

La dépendance vis-à-vis des mots de passe a conduit les organisations et les éditeurs de logiciels à adopter une position plus stricte quant aux mots de passe autorisés. Nous avons tous été confrontés à un écran évaluant la complexité d'un mot de passe, et incitant à mélanger des chiffres, des lettres majuscules et minuscules, ou encore des caractères spéciaux. Cependant, cela ne suffit plus à renforcer la sécurité, et dans de nombreux cas, ces mesures n'ont même pas été mises en place.

DR MARIA BADA
Chercheuse associée, Université de Cambridge

> Même dans les organisations indiquant explicitement comment créer des mots de passe forts, beaucoup ne respectent pas ces principes et utilisent des mots de passe faibles.
>
> La perception qu'ont les utilisateurs de la sécurité peut influencer la conformité avec ces mécanismes. Les pratiques professionnelles non sécurisées et le manque de motivation général peuvent être dus à des mécanismes et politiques de sécurité qui ne prennent pas en compte les pratiques des utilisateurs, les stratégies des organisations, ainsi que la notion d'utilisabilité.[6]
>
> Des travaux de recherche se sont également penchés sur le lien entre les comportements vis-à-vis des mots de passe et la culture, la langue ou encore la personnalité. Cependant, aucune connexion n'a été identifiée au-delà d'un trait de caractère (l'amabilité).[7]
>
> Les mots de passe sont souvent assez révélateurs. Ils sont créés sur l'instant, poussant les utilisateurs à choisir quelque chose de facile à retenir ou ayant un véritable sens émotionnel. Ils puisent donc dans les informations se trouvant juste en dessous de notre conscience. Les cybercriminels profitent de la situation, et il leur suffit d'un peu de recherche pour deviner un mot de passe sans trop d'efforts.

[6] Adams, A., & Sasse, M. A. (1999). Users are not the enemy. Association for Computing Machinery. Communications of the ACM, 42(12), 40

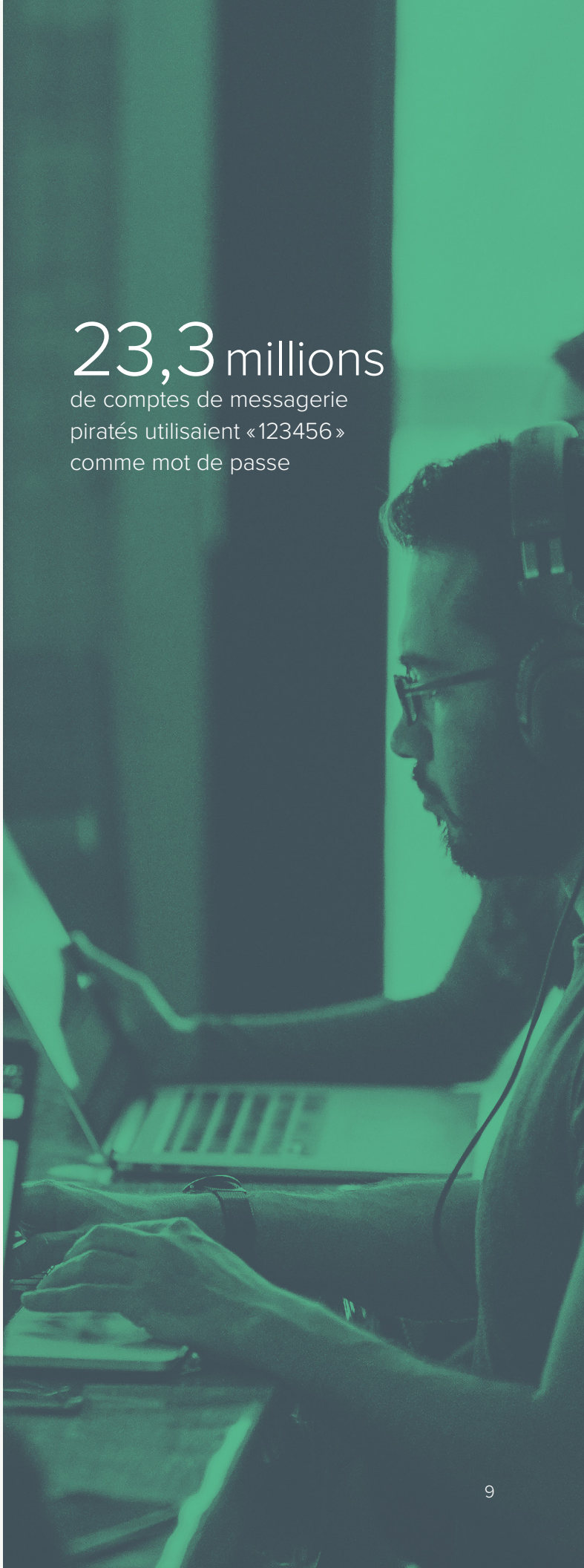
[7] Kawu, A. A, Muhammad, I, Awal A, and Abdullah, M. B 2018. Effect of mental state on password selection among mobile phone users. in Proceedings of the 2nd International Conference on Information and Communication Technology and its Application (ICTA), FUT Minna, Minna, Nigeria.

Les mots de passe : les cibles idéales des cybercriminels

Selon l'agence nationale de la cybersécurité du Royaume-Uni, 23,3 millions de comptes de messagerie piratés utilisaient «123456» comme mot de passe[8], tandis que des millions d'autres utilisaient le terme « mot de passe », le nom de leur équipe de football ou celui de leur groupe de musique préféré.

Peu importent les efforts investis par une entreprise pour sensibiliser son personnel à la nécessité de mots de passe forts, les utilisateurs continueront de choisir des identifiants faciles à mémoriser, essentiellement parce qu'ils doivent en retenir beaucoup.

Pendant de nombreuses années, les mots de passe ont été perçus comme une mesure de sécurité adéquate, avec un coût limité par rapport aux alternatives. Leur fin a d'ailleurs été annoncée par erreur à de nombreuses reprises par les spécialistes de l'industrie. La différence aujourd'hui est qu'il existe à la fois un besoin croissant de sécurité afin de renverser l'ordre établi, et surtout, de technologies et solutions finalement capables de mettre fin à leur règne.



[8] Ncsc.gov.uk. (2019). Most hacked passwords revealed as UK cyber survey exposes gaps in online security.

2 LE PROBLÈME CACHÉ DES MOTS DE PASSE

Mots de passe et bien-être sur le lieu de travail

Ces dernières années, des efforts ont été investis afin de comprendre et de répondre aux problématiques de troubles psychologiques. Cependant, la question de l'équilibre psychologique au travail, elle, commence tout juste à être évoquée. Une enquête publiée récemment[9] révèle qu'un jeune sur six souffrira d'anxiété à un stade de sa vie, et l'année dernière, **un sondage de l'Association psychiatrique américaine (APA)** a révélé que près de 40 % des citoyens étaient plus anxieux qu'en 2017. L'anxiété est un problème croissant sur le lieu de travail, et ce pour diverses raisons ; en revanche, celui de la sécurité a jusqu'ici été occulté.

DR MARIA BADA
Chercheuse associée, Université de Cambridge

> L'impact de l'oubli d'un mot de passe peut être à l'origine de niveaux de stress extrêmes et, au fil du temps, provoquer des dépressions nerveuses ou être une cause de burnout.
>
> Le fait d'être constamment focalisé sur les menaces potentielles en ligne nous rend hypersensibles au stress. À long terme, cette situation peut être une cause de problèmes psychologiques.

[9] Anxiety UK. (2019). Young People and Anxiety - Anxiety UK.

Selon l'enquête d'Okta, les mots de passe ont un lien direct avec le stress, les répondants réagissant négativement lorsqu'ils doivent se souvenir de trop de mots de passe différents :

18%

des personnes interrogées se sentiraient **stressées ou inquiètes**

47%

(Près de la moitié) des répondants seraient **nerveux** ou **contrariés**

Dans les grandes entreprises, ce pourcentage atteint les **52%**, tandis que pour les microentreprises, il se cantonne à **36%**

59 % des Français et **35 %** des Néerlandais seraient nerveux ou contrariés

63%

Deux tiers des personnes interrogées ressentiraient des **émotions négatives**

C'est en France que ce pourcentage est le plus élevé (**73%**), contre **67%** des personnes interrogées au Royaume-Uni et **52%** aux Pays-Bas.

L'oubli d'un mot de passe suscite de fortes émotions négatives chez encore plus d'individus : 62 % d'entre eux se sentiraient stressés ou nerveux. Là encore, c'est en France que ce pourcentage est le plus élevé (69 %), contre 65 % des personnes interrogées au Royaume-Uni et 53 % aux Pays-Bas.

DR MARIA BADA
Chercheuse associée, Université de Cambridge

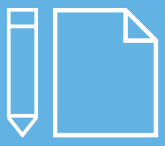
> Le stress que ressentent les utilisateurs face à la nécessité de créer, de saisir à nouveau, de se souvenir, et de changer un grand nombre de mots de passe peut atteindre des niveaux extrêmes.
>
> Différentes politiques de gestion de mots de passe peuvent provoquer cette sensation de lassitude. Le fait de demander à un utilisateur de changer son mot de passe alors qu'il est occupé peut le conduire à créer des mots de passe à la hâte, faibles, et rapidement oubliés. Des émotions similaires peuvent également être générées lorsqu'une session expire et que l'utilisateur doit se connecter à nouveau.

La pression mentale exercée par des mots de passe

Si beaucoup craignent d'oublier leurs mots de passe, cette éventualité ne constitue pas un risque de sécurité en soi. La majorité des fuites de données dues à des piratages sont liées à des mots de passe réutilisés, dérobés ou faibles ; il est donc plus risqué d'utiliser des mots de passe faibles et des moyens mnémotechniques trop simples que de les oublier et de les réinitialiser :

34%

des utilisateurs choisissent les **mêmes mots de passe** pour **plusieurs comptes**



26%

des personnes interrogées les écrivent sur du **papier**

17%

des individus les enregistrent sur leurs **smartphones** ou leurs **ordinateurs**

6%

d'entre eux admettent utiliser des mots de passe figurant parmi les **plus connus**

Au total, 78 % des répondants utilisent une méthode non sécurisée afin de se souvenir de leurs mots de passe ; ce pourcentage passe à 86 % chez les 18-34 ans. Ce phénomène démographique est surprenant étant donné que les jeunes sont considérés comme les plus à l'aise avec les nouvelles technologies, et donc a priori avec la notion de cybersécurité. Il peut néanmoins s'expliquer par le fait que les 18-34 ans utilisent généralement plus d'applications, d'appareils et de technologies nécessitant des mots de passe, et doivent donc s'appuyer sur d'autres méthodes pour s'en souvenir. C'est en France que le pourcentage d'individus se servant d'une méthode non sécurisée est le plus élevé (87 %), suivi des Pays-Bas (79 %) et du Royaume-Uni (74 %).

DR MARIA BADA
Chercheuse associée, Université de Cambridge

> Malheureusement, le stress autour de la sécurité des données ne semble pas avoir poussé la majorité des individus à améliorer leurs habitudes en matière de cybersécurité personnelle.
>
> Souvent, c'est lorsque l'on est soi-même victime d'un cybercrime que l'on se décide à changer de mot de passe. La mentalité des utilisateurs en matière de cybersécurité évoluera lorsque ceux-ci compareront le risque encouru avec la pénibilité de l'usage des mauvaises et des bonnes pratiques.

Gestionnaires des mots de passe et solutions d'authentification unique

– De plusieurs à un seul mot de passe

Il existe des solutions simples pour soulager toute cette pression : les gestionnaires de mots de passe. Ces outils représentent une alternative pratique, car il suffit d'un seul mot de passe fort pour accéder à un coffre-fort capable de générer des mots de passe fort pour chacun des services et applications utilisés. Plus besoin de créer des mots de passe uniques pour chaque service utilisé, et plus besoin de se préoccuper de les mémoriser. Cependant, selon nos enquêtes, seuls 14 % des utilisateurs auraient opté pour un gestionnaire de mots de passe. En effet, acheter, installer et gérer un logiciel supplémentaire peut être difficile. En outre, l'expérience d'utilisation sur plusieurs applications et appareils n'est pas évidente.

Pour les grandes entreprises, le déploiement d'une solution d'authentification unique (SSO) est une meilleure alternative, car elle offre l'ensemble des avantages des gestionnaires de mots de passe, et va même au-delà. Les utilisateurs n'ont ainsi qu'un code secret à retenir pour accéder à l'ensemble des applications. Mieux : puisque les solutions d'authentification unique s'appuient en coulisses sur des protocoles modernes tels que SAML 2.0 et OpenID Connect, les connexions à des applications modernes se font sans mot de passe, ce qui rend les accès bien plus sécurisés. En outre, le SSO permet d'ajouter des fonctions d'authentification multifactorielle en toute simplicité, et protège l'ensemble des accès aux applications.

3

L'ALTERNATIVE AUX MOTS DE PASSE ?

L'innovation et l'intégration

L'innovation technologique de ces dix dernières années a offert aux entreprises de nombreuses nouvelles opportunités pour adopter différentes approches en matière de sécurité. Désormais, les organisations peuvent associer des méthodes telles que la biométrie à des solutions à la fois traditionnelles et sécurisées, et supprimer dans le même temps leurs pratiques inadéquates. Après plusieurs années de fausses prédictions, la vision d'un avenir sans mot de passe pourrait enfin se concrétiser.

La recherche Okta montre une attente pour l'identification biométrique :

SIMPLIFIE LA VIE QUOTIDIENNE

24% professionnelle

28% personnelle

SÉCURISER MIEUX LES APPAREILS/ COMPTES

15% professionnels

20% personnels

RÉDUIT LES NIVEAUX DE STRESS ET D'ANXIÉTÉ

13% au travail

16% dans la vie personnelle

PERMET DE MOINS SE PRÉOCCUPER DE LA SÉCURITÉ

8% au travail

11% dans la vie personnelle

AUGMENTE LA PRODUCTIVITÉ

11% au travail

8% dans la vie personnelle

Vision du futur : la biométrie

L'authentification biométrique tirant parti des empreintes digitales, de la reconnaissance oculaire, faciale et vocale, a été essentiellement introduite pour offrir une meilleure protection contre les accès illégitimes aux comptes ou aux systèmes. Contrairement aux noms d'utilisateurs, mots de passe et autres codes PIN, les données sont uniques pour chaque employé.

L'utilisation de l'authentification biométrique se généralise pour les appareils personnels comme professionnels, et les entreprises déploient actuellement des stratégies de sécurité basées sur ces technologies.

L'enquête d'Okta révèle une appétence et une adoption croissantes pour ces solutions en guise de couche de sécurité supplémentaire, en particulier au travail, et à long terme, en lieu et place des mots de passe :

16%

des répondants s'attendent à une technologie d'authentification à l'aide **d'empreintes digitales**

6%

d'entre eux souhaitent des fonctions de **reconnaissance faciale**

4%

souhaiteraient que leurs appareils professionnels soient équipés de technologies de **reconnaissance d'iris.**

Un pourcentage impressionnant (70 %) des répondants montre qu'ils envisagent, ou utilisent actuellement la biométrie dans leurs vies personnelles. En outre, 24 % des personnes interrogées pensent que cette technologie pourrait rendre leur vie quotidienne plus simple, et 13 % estiment qu'elle pourrait réduire leurs niveaux de stress et d'anxiété au travail. En d'autres termes, l'impact négatif des mots de passe sur leur équilibre psychologique pourrait être réduit grâce à l'authentification biométrique.

Les personnes interrogées estiment également que cette technologie pourrait contribuer à rendre les comptes plus sûrs au travail (15 %) et les aider à moins se préoccuper de leur sécurité (8 %). Enfin, 11 % des répondants considèrent que la biométrie pourrait également accroître la productivité au travail.

Mettre l'accent sur la sensibilisation

Bien que la biométrie offre de nombreux avantages, les individus ne sont pas pleinement convaincus : 86 % des répondants émettent des réserves quant au partage de leurs données biométriques avec leurs employeurs.

21% 

Plus d'un cinquième (21 %) des personnes interrogées craignent que leurs **données** soient **piratées**, et de ne plus pouvoir s'en servir à l'avenir

15% 

d'entre elles pensent que ces technologies seraient **difficiles à mettre en place**, ou ont peur de ne pas pouvoir accéder aux ressources nécessaires en cas de **panne**

13% 

des répondants **ne font pas confiance** à ces **technologies**

Il y a donc du travail à accomplir pour aplanir les malentendus concernant le fonctionnement de la biométrie et instaurer un climat de confiance autour de ces technologies.

Par exemple, beaucoup d'employés pensent à tort que l'utilisation des fonctions Touch ID ou Face ID de leurs iPhone ou iPad, ou de Windows Hello For Business permettrait à leur entreprise d'accéder librement à leurs données biométriques. En réalité, ces informations sont hautement sécurisées et ne sont pas accessibles à des tiers, ni même au système d'exploitation de l'appareil. Ces données sont profondément ancrées dans les modules de sécurité des terminaux (Secure Enclave, Trusted Platform Module, etc.), ce qui signifie que même Apple ou Microsoft ne peuvent pas y accéder – et encore moins un employeur.

C'est donc aux organisations et aux ingénieurs développant ces technologies qu'il revient de montrer comment ces informations peuvent être sécurisées, et de promouvoir les avantages et la simplicité de mise en œuvre de ces outils afin de répondre aux inquiétudes émises.

DR MARIA BADA
Chercheuse associée, Université de Cambridge

> La biométrie se généralise depuis un certain temps, grâce notamment aux lecteurs d'empreintes digitales de nos smartphones et ordinateurs. Cette technologie a été pleinement adoptée sur des appareils destinés au grand public, à l'image de l'iPhone.
>
> Cependant, selon une enquête menée par Okta, les utilisateurs ont encore des réserves quant au partage de ces données avec leur employeur. Cela peut aisément s'expliquer par le manque d'expérience dans l'utilisation de la biométrie dans notre vie quotidienne.

> La solide connaissance technique obtenue ces dix dernières années et la maturité des systèmes offerts par les fournisseurs ne font que renforcer la probabilité que les mots de passe et autres dispositifs matériels seront remplacés avant que la plupart d'entre nous ne partent à la retraite.
>
> Un des avantages potentiels de la biométrie est le fait que les individus possèdent en permanence leurs caractéristiques avec eux : plus de risque d'oublier, de perdre ou de se faire voler un dispositif matériel. Les utilisateurs ont alors moins de choses à retenir, et profitent ainsi du principe d'utilisabilité lié aux accès universels.[10]

De nouveaux standards en matière de biométrie

Les technologies biométriques telles que les lecteurs d'empreintes et les solutions de reconnaissance faciale sont devenues la norme sur les principaux appareils grand public. En outre, un projet mené de la FIDO Alliance et du World Wide Web Consortium (W3C) baptisé FIDO2 a conduit à l'introduction de l'API W3C Web Authentication (WebAuthn) comme norme sur le web, et à la création du FIDO Client to Authenticator Protocol (CTAP) en mars 2019. WebAuthn permet aux applications web de simplifier et de sécuriser l'authentification des utilisateurs en se servant de clés de sécurité et de terminaux (smartphones et autres ordinateurs portables). Cette API s'appuie sur le chiffrement de clés publiques pour protéger les utilisateurs des attaques de phishing avancées, et est désormais prise en charge par tous les principaux navigateurs (Chrome, Firefox, Microsoft Edge et bientôt Safari) et systèmes d'exploitation.

Pour les consommateurs et les employés, cela signifie que la confiance peut être maintenue, WebAuthn étant une méthode plus sécurisée qui supprime les risques liés aux mots de passe. En associant cette API à des technologies biométriques hyper sécurisées capables d'authentifier les détenteurs des informations d'identification, les noms d'utilisateur et mots de passe deviennent alors superflus. Les équipes informatiques des entreprises peuvent ainsi se servir des appareils enregistrés appartenant aux utilisateurs finaux comme de facteurs d'authentification.

L'approche décrite implique un changement en profondeur qui transformera entièrement la perception des menaces. Auparavant, il suffisait de disposer des identifiants – qu'ils soient dérobés ou devinés – pour pouvoir accéder de façon illégitime à un compte. Mais aujourd'hui, avec WebAuthn, l'individu devra être en possession d'une clé de sécurité ou d'un appareil spécifique. Et avec la biométrie, il se trouvera dans une impasse.

[10] Fairhurst, M.C., Guest, R.M., Deravi, F. and George, J. (2002). Using Biometrics as an Enabling Technology in Balancing Universality and Selectivity for Management of Information Access. , in N. Carbonelle and C. Stephanidis (eds) Universal Access: Lecture Notes in Computer Science 2615, Berlin: Springer, pp. 249-59

4

CRÉER UN AVENIR SANS MOT DE PASSE DÈS AUJOURD'HUI

À l'heure où les organisations et leurs employés accordent de plus en plus d'importance à leurs identités et à la notion de confiance, nous devons nous assurer que nos informations sont protégées.

D'ores et déjà, les employeurs, développeurs, fabricants et autres responsables de la sécurité s'efforcent de renforcer la confiance que les utilisateurs ont en eux.

L'enquête d'Okta montre que les mots de passe sont actuellement la principale méthode utilisée pour protéger les applications, appareils, systèmes et comptes. Pourtant, cette solution est inadaptée, car ces codes secrets peuvent : être piratés, encourager les utilisateurs à adopter des comportements risqués, et être source de stress, d'anxiété, en plus de réduire la productivité des salariés. L'heure est venue de revoir notre utilisation des mots de passe.

Nous avons pu voir à quel point l'association de solutions SSO modernes et de facteurs d'authentification forte capables de déjouer les attaques de phishing offre une approche plus sûre et plus logique de la sécurité d'une entreprise. Cette même approche est nécessaire pour rendre possible un avenir sans mots de passe. Okta contribue à rendre cette vision facilement accessible pour les entreprises de toutes tailles et de tous les secteurs.

Okta combine ses capacités d'authentification unique (SSO) et d'authentification multifactorielle adaptative (MFA) avec des authentificateurs standard de l'industrie avec la biométrie, ce qui nous permettra de remplacer les mots de passe des organisations par une évaluation des risques entièrement contextuelle et des authentificateurs WebAuthn qui sont très résistants au phishing et ne peuvent être contournées ou dupliquées.

Les organisations peuvent tirer parti des appareils utilisés par leurs employés de façon extrêmement sécurisée, tout en respectant leur vie privée, et sans qu'aucune information sur leurs contacts ou leurs applications ne soit divulguée.

TODD MCKINNON
CEO et cofondateur d'Okta

Chez Okta, nous sommes intimement convaincus par le potentiel des nouvelles technologies, et selon nous, la confiance représente à coup sûr le nouveau périmètre pour les organisations de toutes tailles et de tous les secteurs en pleine transformation. Aujourd'hui, pour rétablir la confiance, les entreprises doivent adopter des outils leur permettant d'innover rapidement, tout en donnant la priorité à la sécurité, à la confidentialité et au contrôle des accès. Les mots de passe ayant échoué en tant que facteurs d'authentification, les entreprises ont désormais intérêt à mettre de côté cette méthode inefficace. Par conséquent, en 2019, nous devrions assister à la première vague d'entreprises abandonnant complètement les mots de passe, et les clients d'Okta seront à l'avant-garde de ce mouvement.

Visitez **www.okta.com/fr** pour en savoir plus sur notre approche