Enquête mondiale 2025 sur l'état de l'authentification

Perceptions vs réalité :
Les lacunes de manière d’authentification

Perspectives de Yubico

yubico

Table des matières

Introduction

Les menaces liées à la cybersécurité représentent un danger en constante évolution pour les entreprises de toutes tailles, mais de nombreuses organisations tardent à réagir aux risques nouveaux et émergents. En effet, de nombreux employés et entreprises pensent aujourd'hui que les protocoles de sécurité traditionnels sont aussi efficaces qu'il y a quelques mois, voire quelques années. Malheureusement, cette perception ne correspond pas à la réalité.

Les menaces croissantes liées aux attaques basées sur l'intelligence artificielle (IA), combinées à des directives de cybersécurité obsolètes et à des habitudes à haut risque de la part des employés, ont rendu d'innombrables organisations vulnérables aux failles de sécurité. Notre enquête explore les habitudes des individus en matière de cybersécurité, tant sur leur lieu de travail que dans leur vie personnelle. Elle examine également les dangers liés à des pratiques de sécurité insuffisantes et évalue les préoccupations croissantes concernant les technologies émergentes telles que l'IA et leurs implications pour la sécurité des organisations et des individus.

Résumé

Yubico a commandé une enquête mondiale auprès de 18 000 adultes actifs en Australie, en Inde, au Japon, en France, en Allemagne, à Singapour, en Suède, au Royaume-Uni et aux États-Unis, qui a révélé des lacunes fondamentales dans la sécurité des organisations, dues à un décalage entre ce que les employés et leurs entreprises considèrent comme sûr et la réalité de leur vulnérabilité aux cybermenaces modernes.

L’enquête a notamment démontré que près de la moitié des personnes interrogées n'ont jamais reçu de formation en matière de cybersécurité et utilisent encore des méthodes d'authentification qui, bien qu'elles aient été autrefois considérées comme sûres, sont désormais facilement contournées par des attaques sophistiquées telles que le phishing. Les mots de passe, la vérification par SMS et même l'authentification multi-facteurs (MFA) de base sont de plus en plus vulnérables et constituent des points faibles que les cybercriminels peuvent exploiter.

Plus révélateur encore, les habitudes de sécurité personnelles compromettent également les protocoles de protection des entreprises, avec 50 % des employés utilisant leurs comptes personnels sur leurs appareils professionnels, et vice versa. En outre, près d'un tiers des personnes interrogées n'utilisent aucune forme d'authentification multi-facteurs en dehors du travail, ce qui permet aux cybercriminels d'exploiter les informations personnelles pour cibler les entreprises.

Aussi, la croissance rapide et l'adoption de l'IA par les hackers ont considérablement accéléré le rythme d'apparition de nouvelles menaces. Nos conclusions indiquent que les personnes interrogées sont conscientes de cette nouvelle réalité. 76 % d'entre elles s'inquiétent du fait que leurs comptes sont désormais exposés à un risque d'attaque beaucoup plus élevé, ce qui représente une forte augmentation par rapport aux 58 % qui partageaient ce sentiment dans un rapport similaire publié en 2024.

Plus De

18 000+

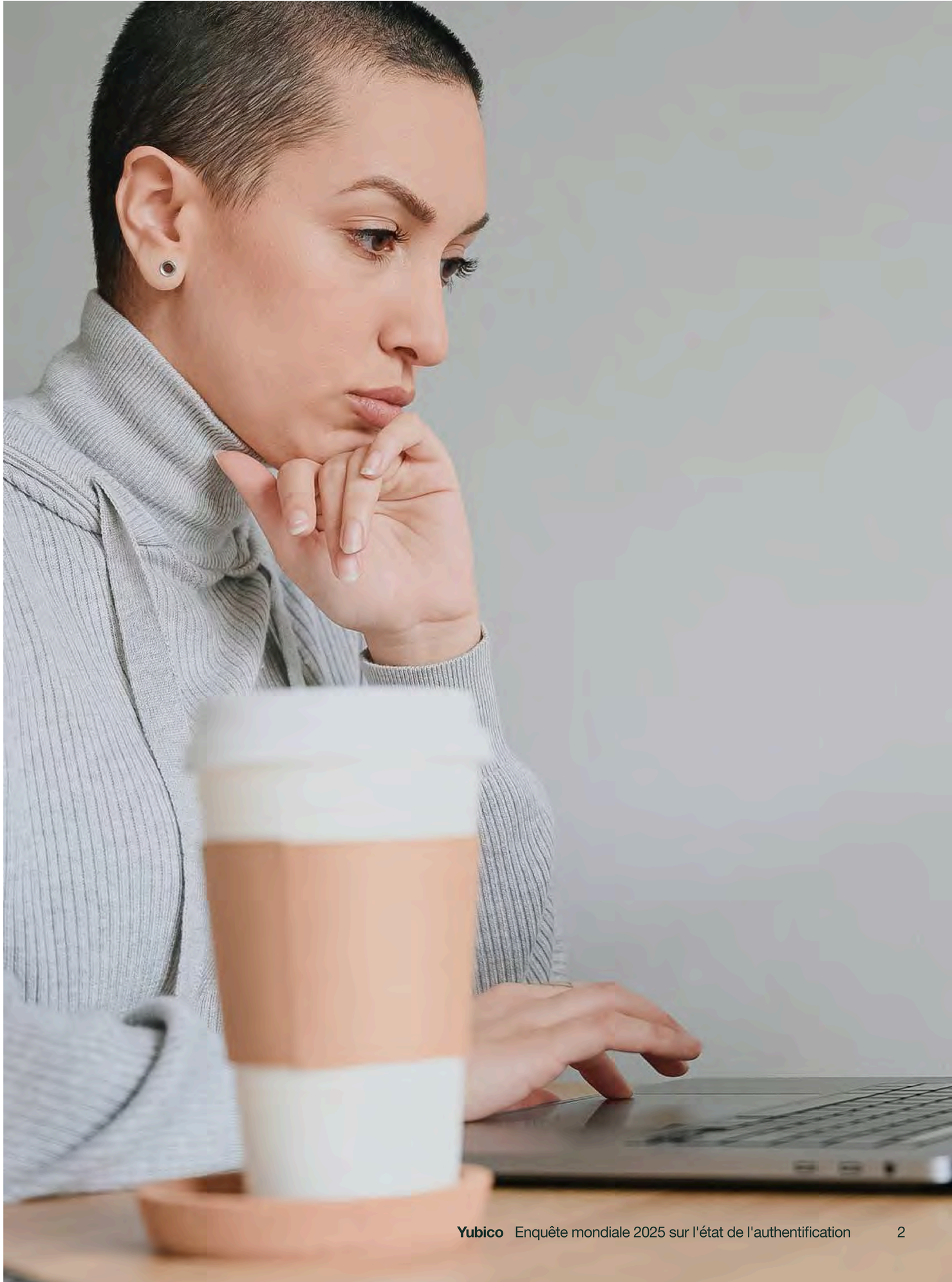
Réponses

9

Pays

I.

Le nouveau paysage cybernétique



Un signal d'alarme mondial en matière de cybersécurité

Notre étude révèle que 4 employés sur 10 (40 %) n'ont jamais reçu de formation sur la cybersécurité, sous quelque forme que ce soit. De plus, 44 % des entreprises attendent plus de 3 à 5 mois avant de mettre à jour leurs politiques de cybersécurité.

Ces deux statistiques suggèrent que près de la moitié des employés n'ont jamais été informés des directives de sécurité de leur entreprise et qu'environ la moitié de ceux qui ont suivi une formation en cybersécurité travaillent avec des informations obsolètes.

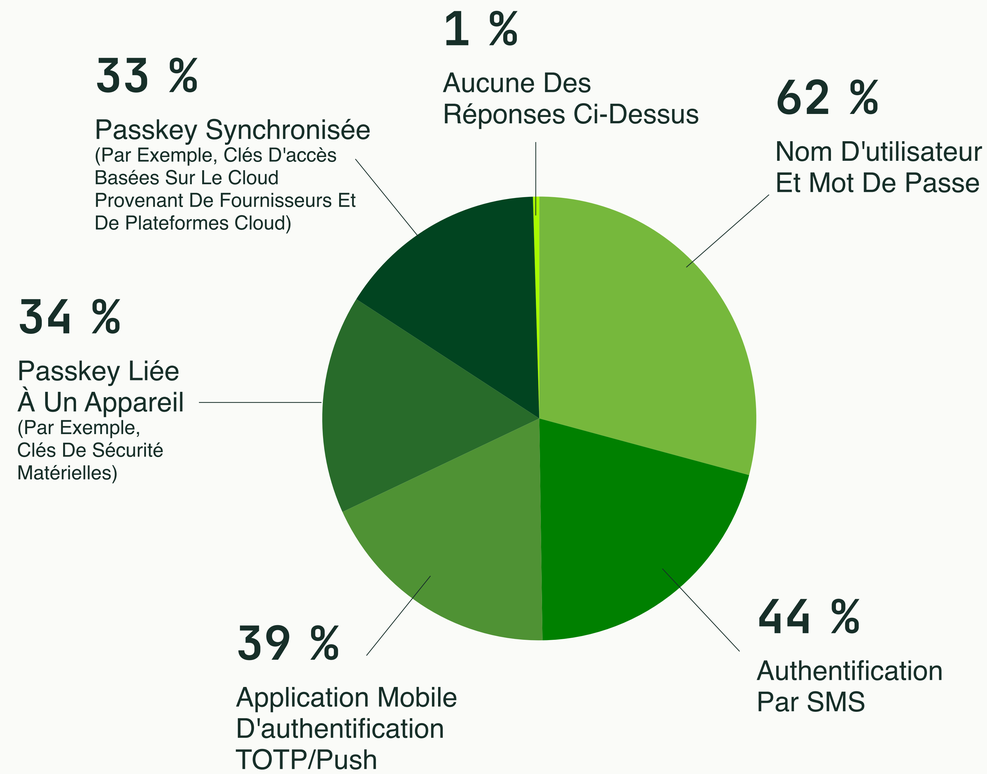
Avec l'émergence quasi constante de nouveaux vecteurs d'attaque et la montée en puissance des menaces basées sur l'IA, le manque de cohérence dans les pratiques de formation à la cybersécurité expose de nombreuses organisations et leurs employés à une vulnérabilité permanente.

Authentification Inconsistante

L'utilisation inconsistante de l'authentification augmente encore davantage les risques pour les systèmes d'entreprise modernes. Les entreprises qui fournissent à leurs employés plusieurs méthodes d'authentification pour les applications et les services créent une défense plus faible contre les vulnérabilités potentielles.

Plus surprenant encore, 62 % des organisations continuent de s'appuyer principalement sur des identifiants de type nom d'utilisateur/mot de passe, malgré les nombreuses preuves démontrant que cette technologie obsolète est de plus en plus vulnérable. 44 % des entreprises utilisent des mots de passe à usage unique (OTP) envoyés par SMS, qui sont insuffisants face aux attaques de SIM-swapping et à l'ingénierie sociale qui, grâce à l'IA, est désormais plus sophistiquée.

Quelles formes d'authentification votre entreprise utilise-t-elle pour les différentes applications/programmes qu'elle utilise ?



Perceptions vs réalité

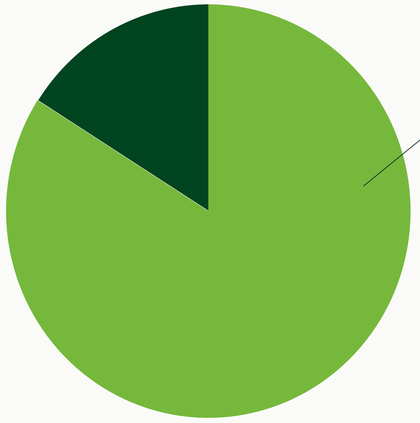
Nos conclusions montrent que les employés **sous-estiment** systématiquement les risques liés à la sécurité de leurs informations de connexion et **surestiment** les capacités des systèmes destinés à les protéger.

Dans notre étude, 41 % des répondants considèrent que l'authentification par SMS est la méthode la plus sûre, tandis que 33 % estiment que les mots de passe à usage unique (OTP), à durée limitée et fournis par des applications mobiles dédiées, sont les plus sûrs. Bien que ces méthodes soient préférables à l'absence totale de protection, elles sont très vulnérables à diverses menaces, allant de l'ingénierie sociale au SIM-swapping, voire au vol de téléphones mobiles. Étonnamment, plus d'un quart (26 %) des personnes interrogées continuent de croire que les mots de passe, qui sont très vulnérables aux attaques de phishing, sont les plus sûrs.

Les passkeys liées à un appareil, comme celles des clés de sécurité matérielles, n'étaient considérées comme les plus sûres que par 30 % des répondants, bien qu'elles soient très efficaces contre divers types de cyberattaques. Ces idées préconçues et fausses influencent à la fois les choix individuels en matière de sécurité et les politiques générales des entreprises, ce qui accroît leur vulnérabilité face aux cybermenaces.

Malgré ces vulnérabilités, 84 % des personnes interrogées, et dont les entreprises appliquent des mesures de sécurité différentes selon les postes, estiment que leur cybersécurité est au niveau requis. Cette confiance mal placée ignore le fait que, pour être réellement efficaces, les outils de cybersécurité doivent protéger de manière uniforme tous les niveaux de l’organisation.

Bien que les vulnérabilités persistent, 84 % des personnes interrogées, dont les entreprises adaptent les mesures de sécurité selon les rôles et les besoins, continuent de considérer la cybersécurité de leur organisation comme suffisante, signe d'un excès de confiance.



84 %

croient toujours que la cybersécurité de leur entreprise est aussi sûre qu'elle devrait l'être.

Quelle est la méthode d'authentification la plus sûre ?

Les clés de sécurité matérielles sont largement considérées comme la forme d'authentification la plus sûre. Ces petits dispositifs physiques doivent être en votre possession pour vérifier votre identité, ce qui les rend très efficaces pour prévenir les attaques de phishing et l'usurpation d'identité. Les passkeys liées à un dispositif, un type de clé stocké sur une clé de sécurité matérielle, sont considérées comme la « norme d'excellence ».

Les habitudes personnelles compromettent la sécurité de l'entreprise

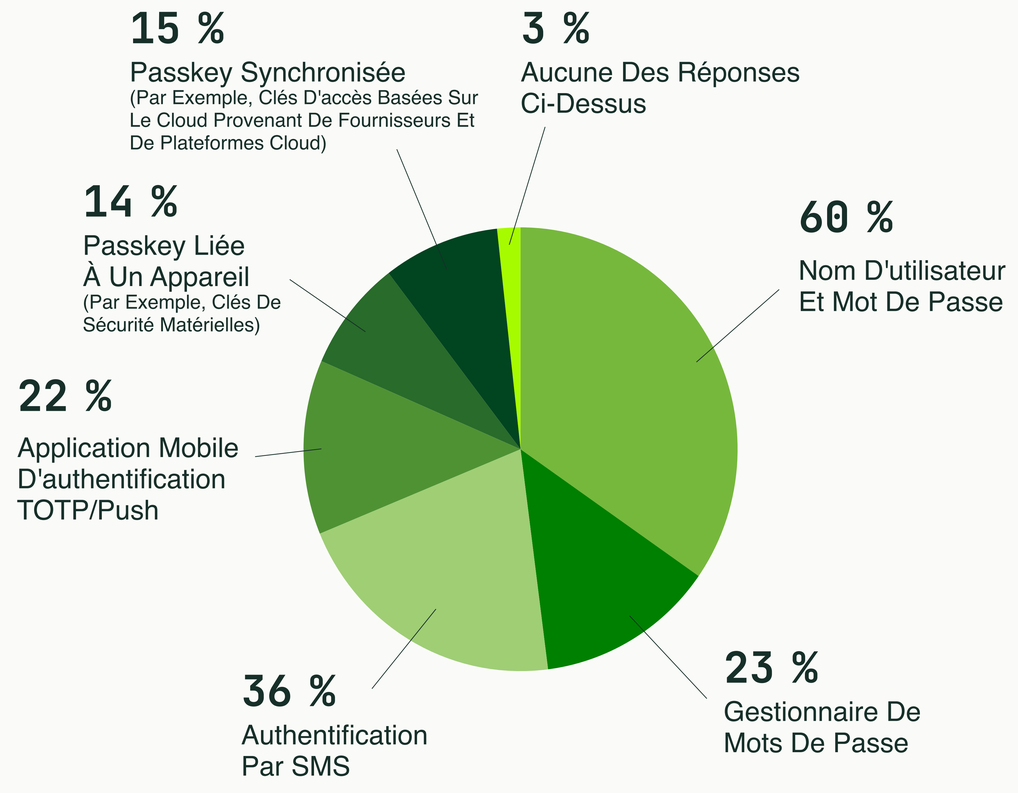
La frontière entre vie privée et vie professionnelle s’estompe, et les pratiques de cybersécurité adoptées en télétravail à domicile peuvent rapidement créer des risques pour l’employeur. Nos conclusions révèlent un fort chevauchement entre l'utilisation des appareils personnels et professionnels, 40 % des employés utilisant leurs appareils professionnels pour consulter leurs e-mails personnels et 40 % d'entre eux, ce qui est tout aussi préoccupant, accédant à leurs e-mails professionnels à partir de leurs appareils personnels. Ces habitudes créent de multiples voies d'accès pour les hackers qui souhaitent pirater des comptes professionnels sans attaquer directement une cible d'entreprise.

Etant donné que 29 % des personnes interrogées n’activent pas l’authentification multi-facteurs (MFA) sur leurs e-mails personnels, cela crée des points d’entrée exploitables par des cybercriminels pour accéder aux systèmes professionnels, lancer des attaques de phishing ciblées contre des collègues ou encore collecter des données personnelles pour des opérations d’ingénierie sociale.

Sans surprise, les habitudes d'authentification personnelles ressemblent étroitement aux tendances observées dans les environnements d'entreprise : les méthodes les plus courantes de sécurité des comptes personnels sont les mots de passe (60 %) et les SMS (36 %). Seules 14 % des personnes utilisent des passkeys liées à un appareil pour leurs comptes personnels.

> « Les employés utilisent leurs appareils personnels pour travailler et leurs appareils professionnels à des fins privées, transformant une erreur individuelle en une faille potentielle pour l’entreprise. La cybersécurité personnelle et professionnelle doivent aller de pair et être mutuellement bénéfiques. »
>
> **Ronnie Manning, Chief Brand Advocate, Yubico**

Comment vous authentifiez-vous/vous connectez-vous à vos comptes personnels ?



L'IA a dopé les cyberattaques

L'IA permet à un individu d'en faire plus en moins de temps. Si elle présente des avantages au travail, tels que la productivité et la croissance, elle a également transformé le paysage des cybermenaces. Les barrières techniques à la mise en œuvre d'attaques sophistiquées ont considérablement diminué : grâce à l'IA, même des hackers inexpérimentés peuvent désormais causer des dommages majeurs.

La capacité de l'IA à renforcer la cybercriminalité va au-delà des outils automatisés ou des bots. Elle permet aux cybercriminels de rédiger des e-mails de phishing très convaincants, de les personnaliser en fonction de cibles individuelles et d'augmenter considérablement leurs chances de succès. Désormais, même sans compétences en programmation, des hackers peuvent créer de faux sites quasi identiques aux originaux, produire des vidéos et audios deepfake pour tromper leurs collègues, et ce, rapidement et à grande échelle.

La bonne nouvelle, c'est que de nombreuses personnes sont effectivement conscientes de l'augmentation des escroqueries en ligne et du phishing dopé à l'IA. Ainsi, 78 % des personnes interrogées déclarent être conscientes des nouveaux dangers et 70 % estiment que ce type d'attaques est plus efficace. Ces chiffres confirment les tendances observées à l'échelle mondiale, la plupart reconnaissent la rapidité d'évolution du paysage des menaces, mais beaucoup d'organisations restent inactives.

Il est encourageant de constater que 76 % des répondants se disent préoccupés par l'impact de l'IA sur la sécurité de leurs comptes personnels ou professionnels. C'est une hausse de 18 points par rapport à l'enquête 2024 de Talker et Yubico, où seuls 58 % partageaient cette inquiétude. Cela traduit une prise de conscience croissante face aux risques liés à l'IA.

« L'IA est en train de réécrire les règles de la cybercriminalité, permettant aux cybercriminels de lancer plus facilement des attaques sophistiquées et très ciblées. Les organisations qui utilisent des méthodes d'authentification basiques telles que les mots de passe et les SMS vont se retrouver à la traîne. Il est clair que le moment est venu pour les entreprises de se moderniser et d'adopter des méthodes de sécurité qui ont fait leurs preuves contre les menaces actuelles. »

Ronnie Manning, Chief Brand Advocate, Yubico

Frontières floues entre la communication humaine et la communication IA

L'une des principales menaces que représente l'IA dans le domaine de la cybersécurité est sa capacité étonnante à imiter les schémas de communication humains. Cette capacité déconcertante annule l'un des moyens les plus efficaces de filtrer les attaques de phishing : l'identification des dialogues suspects ou inhabituels.

Nous avons constaté que parmi les victimes de phishing, 34 % expliquent avoir été trompées parce que le message semblait provenir d'une source fiable. Avec sa capacité à personnaliser les attaques et à exploiter de vastes ensembles de données, l'IA renforce l'efficacité de ces menaces.

Nos données montrent aussi que beaucoup ont du mal à distinguer un contenu généré par un humain d'un contenu produit par l'IA. Confrontés à des exemples de messages, seuls 30 % des répondants ont correctement identifié un texte rédigé par un humain, tandis que 70 % l'ont attribué à tort à l'IA ou sont restés incertains. À l'inverse, 54 % ont échoué à reconnaître un texte généré par l'IA, contre 46 % qui l'ont identifié correctement.

Les résultats varient cependant selon l'âge : les jeunes générations distinguent mieux les écrits humains, signe que leur familiarité avec ces technologies leur donne un certain avantage intuitif.

E-mail humain

Bonjour [NOM],

Afin de garantir la sécurité de notre réseau, nous demandons à tous les utilisateurs de réinitialiser leurs identifiants de connexion au système de gestion de projet tous les 90 jours. Votre connexion va bientôt expirer, veuillez donc utiliser le lien ci-dessous pour réinitialiser vos identifiants. N'hésitez pas à nous contacter si vous rencontrez des difficultés.

https://link/example.com

Merci,
[NOM]
Administrateur de l'entreprise

Email IA

Bonjour [NOM],

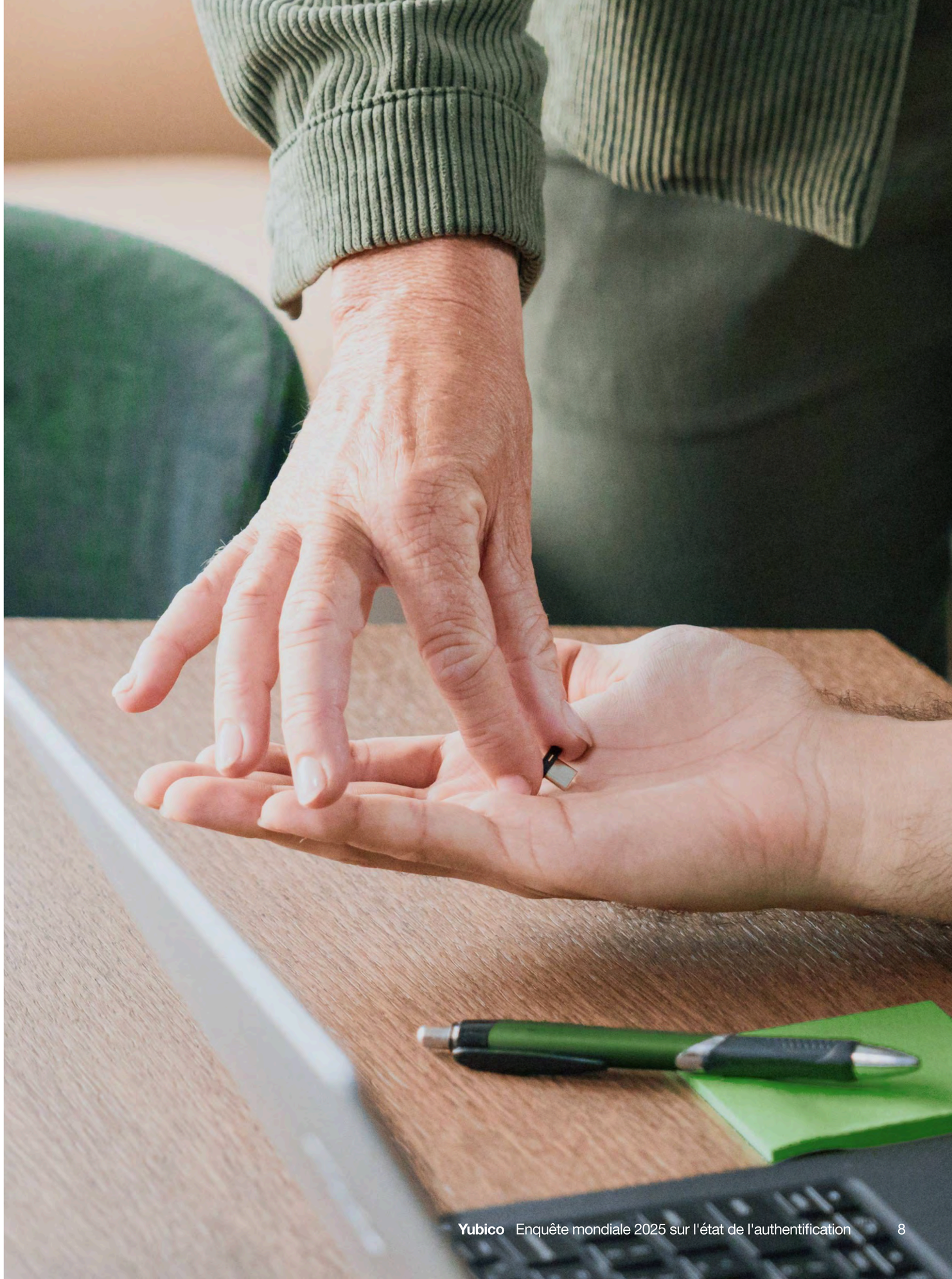
Petit rappel : votre identifiant pour le système de gestion de projet de l'entreprise a expiré (les réinitialisations sont effectuées tous les 90 jours). Pour des raisons de sécurité, nous vous demandons de créer un nouveau mot de passe. Pour ce faire, cliquez sur le lien ci-dessous : https://link/example.com

N'hésitez pas à nous contacter si vous rencontrez des difficultés.

Cordialement,
[NOM]
Administrateur de l'entreprise

II.

Solutions : la voie vers la cyber-résilience



La connaissance est la première ligne de défense

Une cybersécurité efficace nécessite une approche multidimensionnelle. La technologie seule ne suffit pas, les employés doivent acquérir les connaissances nécessaires pour se protéger eux-mêmes et protéger leur organisation. Nos conclusions suggèrent qu'il existe des lacunes importantes dans la formation générale à la cybersécurité, auxquelles il convient de remédier afin de résister aux cybermenaces modernes.

Le manque d'adoption de l'authentification multi-facteurs (MFA) illustre parfaitement comment les idées préconçues et fausses peuvent compromettre les efforts de sécurité. Les personnes interrogées qui évitent d'utiliser la MFA sur leurs comptes personnels expliquent qu'elles le font par manque de familiarité (40 %), par crainte de la complexité (24 %), par manque de temps (22 %) et par crainte du coût (9 %).

De même, le faible taux d'adoption des passkeys semble provenir de lacunes dans les connaissances plutôt que d'obstacles techniques. Parmi les personnes interrogées qui n'utilisent pas de passkeys, 45 % ont déclaré n'en avoir jamais entendu parler. 12 % supplémentaires ont déclaré qu'elles ne sont pas disponibles pour les sites et services qu’elles utilisent, et 11 % craignaient qu'elles soient trop compliquées. Cela suggère un besoin de formation et d'engagement organisationnel pour renforcer la sécurité de l'authentification.

Stratégies de sensibilisation efficaces

Renforcer la résilience des entreprises en matière de cybersécurité nécessite une approche pratique qui inclut des programmes éducatifs, des formations techniques et un examen régulier des habitudes de sécurité. Il est important de corriger les idées reçues sur la complexité perçue de la cybersécurité et de présenter les outils disponibles en termes simples. Les solutions de sécurité modernes sont conçues pour les utilisateurs lambda et offrent une approche simplifiée par rapport aux mots de passe obsolètes.

Les programmes éducatifs doivent souligner l'importance de la cybersécurité tant professionnelle que personnelle, en donnant aux employés une compréhension approfondie de l'impact que leurs habitudes personnelles peuvent avoir sur la sécurité au travail. Des sessions de formation régulières sont essentielles dans le contexte actuel de menaces en constante évolution, et les entreprises doivent fournir une formation continue sur les risques émergents, y compris des évaluations pour garantir la rétention des connaissances.

> « Les entreprises doivent sensibiliser leurs employés et dissiper le mythe selon lequel la cybersécurité est réservée aux experts en technologie. Avec les connaissances et les outils appropriés, chaque membre de l'entreprise peut et doit contribuer à un écosystème de cybersécurité sûr. »
>
> **Ronnie Manning, Chief Brand Advocate, Yubico**

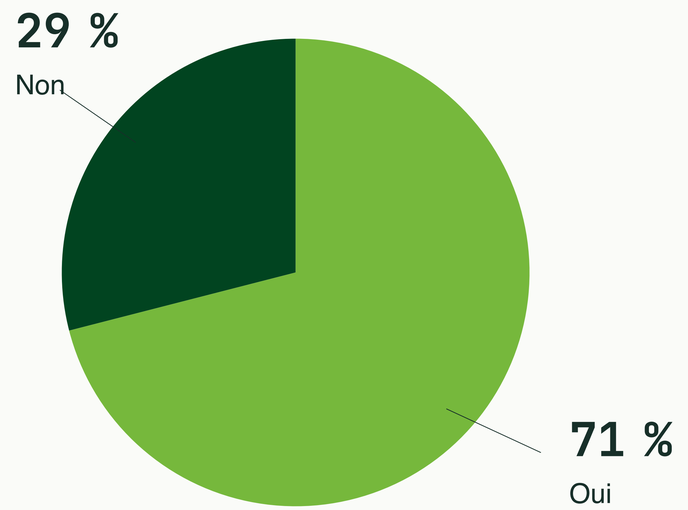
Combler le fossé en matière d'adoption de l'authentification multi-facteurs

Nos données révèlent une dynamique positive autour de la MFA : individus comme organisations souhaitent en savoir davantage, ce qui devrait favoriser son adoption à grande échelle. Les jeunes générations affichent déjà des taux élevés — 71 % pour la Gen Z et 68 % pour la Gen Y —, laissant penser que l'adoption progressera naturellement. Mais les entreprises ne doivent pas attendre et devraient dès maintenant encourager une mise en place généralisée.

Les écarts régionaux d'adoption fournissent par ailleurs des enseignements précieux sur les stratégies efficaces. Dans l'ensemble, 82 % des personnes interrogées déclarent connaître les passkeys MFA, les États-Unis arrivant en deuxième position (33 %) derrière l'Inde (39 %) en termes d'utilisation de passkeys liées à un appareil. L'Australie et Singapour figurent en tête du classement mondial avec 78 % d'adoption de la MFA sur les comptes personnels, démontrant ce qu'il est possible d'atteindre grâce à une formation et un accompagnement adaptés.

Il est essentiel que les organisations s'efforcent d'éliminer les obstacles à l'adoption de l'authentification multi-facteurs (MFA) dans un premier temps. Pour ce faire, elles doivent notamment fournir des outils conviviaux, des conseils faciles à comprendre, ainsi qu'une assistance et un dépannage continus. L'objectif doit être de rendre les options MFA pratiques et simplifiées, et non pas simplement d'en rendre l'utilisation obligatoire.

Avez-vous activé l'authentification multi-facteurs (MFA) pour votre e-mail personnel ?



Ce qui empêche les utilisateurs d'adopter la MFA

Parmi ceux qui n'utilisent pas la MFA (authentification multi-facteurs), les principales raisons invoquées sont le manque de familiarité (40 %), le sentiment de ne pas avoir les connaissances techniques nécessaires (24 %), le fait de penser que cela prend trop de temps (22 %) et la conviction que c'est trop coûteux (9 %).

Les arguments en faveur des clés de sécurité matérielles

Dans le contexte actuel, où les tentatives de phishing sont optimisées par l'IA et que les techniques d'ingénierie sociale deviennent de plus en plus puissantes, les clés de sécurité matérielles avec codes d'accès offrent une défense robuste. Elles permettent une authentification résistante au phishing qui nécessite la possession physique d’une clé ainsi qu’une l'interaction de l'utilisateur.

En exigeant à la fois la possession d’un appareil et la présence humaine, les clés de sécurité matérielles offrent une protection robuste contre les attaques de phishing les plus sophistiquées, y compris celles dopées par l’IA. Alors que les mots de passe peuvent être piratés et utilisés à distance, et que les SMS peuvent être interceptés, les clés de sécurité matérielles ne sont pas vulnérables à ces vecteurs d'attaque.

Les passkeys liées à un appareil, telles que les clés de sécurité matérielles, constituent aujourd'hui la norme de référence. Si les passkeys synchronisées dans le cloud offrent un niveau de sécurité supérieur à celui des simples mots de passe, elles restent potentiellement vulnérables à une compromission si un cybercriminel parvient à s'introduire dans le service cloud ou dans le compte individuel de l'utilisateur. Les passkeys liées à un appareil, qui stockent des clés cryptographiques localement, ne présentent pas ces mêmes risques.

Bien qu'il s'agisse de l'outil le plus efficace et le plus résistant au phishing disponible à l'heure actuelle, seules 17 % des entreprises utilisent des passkeys liées à un appareil pour leur personnel, ce qui suggère qu'il existe une marge d'amélioration significative parmi les entreprises. Les données générationnelles offrent une lueur d’espoir : 20 % des millennials et 19 % de la génération Z affichent les taux d’utilisation professionnelle les plus élevés.

Comme pour l'adoption de toute nouvelle technologie, la mise en œuvre de clés de sécurité matérielles nécessite une planification et une assistance aux utilisateurs, mais les avantages l'emportent largement sur l'investissement initial et la formation éventuellement nécessaire. Le déploiement réussi de clés de sécurité matérielles se traduit généralement par un retour sur investissement significatif, une baisse spectaculaire des incidents liés aux comptes compromis, une réduction de l'assistance technique et une amélioration de la confiance et de la tranquillité d'esprit des utilisateurs dans leur ensemble.

Tendances Générationnelles

Les tendances générationnelles sont porteuses d'optimisme pour une adoption accrue, les Millennials (20 %) et la Gen Z (19 %) étant en tête de l'utilisation de la MFA dans les environnements d'entreprise.

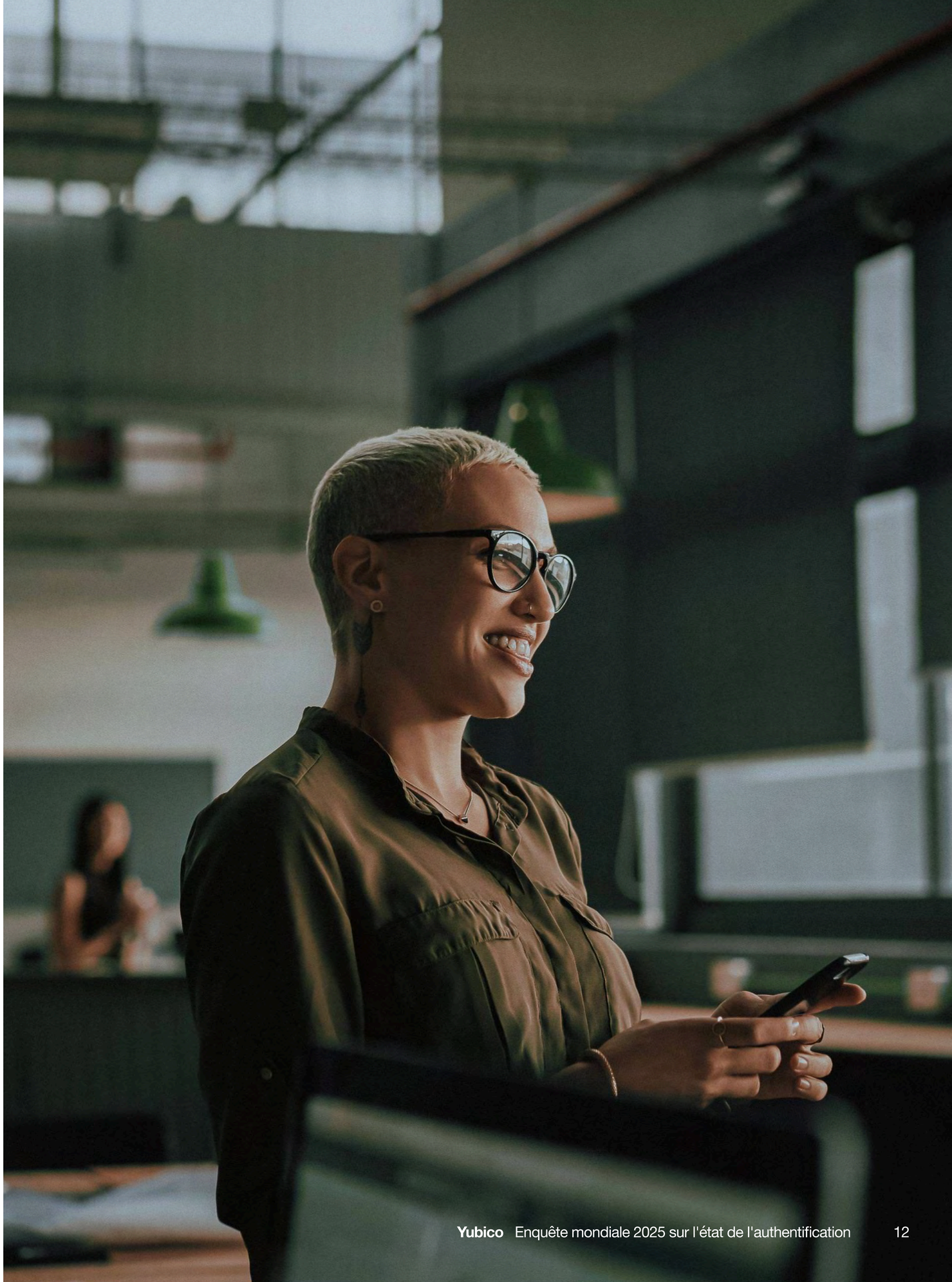
Conclusion

Le paysage de la cybersécurité évolue aujourd’hui plus vite que jamais et se révèle de plus en plus exposé. On pourrait s'attendre à ce que les approches traditionnelles soient suffisantes, mais la réalité est que les cyberattaques améliorées par l'IA et les pratiques MFA de base peuvent exposer de nombreuses organisations à des risques dangereux. Le recours à des méthodes d’authentification faibles, à une formation incohérente des employés et à des politiques de sécurité fragmentées a creusé un fossé entre ce que les entreprises pensent être protégées et la réalité de leur niveau de défense.

Il existe déjà des solutions éprouvées. Les passkeys liées à un appareil, telles que les clés de sécurité matérielles, sont largement disponibles, efficaces et prêtes à être déployées à grande échelle. Les obstacles à leur adoption sont moins liés à la technologie qu'à la maturité digitale des entreprises, ce qui signifie que le changement est à la fois possible et à portée de main.

Les tendances générationnelles nous donnent des raisons d'être optimistes quant à l'avenir, les jeunes employés adoptant plus rapidement les options de sécurité avancées et faisant preuve d'un plus grand scepticisme à l'égard des contenus générés par l'IA. Ces natifs du numérique se positionnant pour occuper des postes de direction, nous anticipons que ces évolutions favoriseront l’adoption généralisée de protocoles de sécurité avancés dans les organisations.

La voie à suivre pour les organisations est claire : adopter des approches intégrées avec des technologies éprouvées qui offrent une véritable protection contre les cyberattaques. En prenant des mesures décisives dès aujourd'hui, les entreprises peuvent combler le fossé entre les attentes et la réalité et créer un avenir où la sécurité est une force commune plutôt qu'une vulnérabilité persistante.



À propos de Yubico

Yubico (Nasdaq Stockholm : YUBICO), l'inventrice de la YubiKey, offre la norme d'excellence en matière d'authentification multifactorielle (MFA) résistante au phishing, stoppant net les prises de contrôle de comptes et rendant la connexion sécurisée facile et accessible à tous. Depuis sa création en 2007, l'entreprise a joué un rôle de premier plan dans l'établissement de normes mondiales pour l'accès sécurisé aux ordinateurs, aux appareils mobiles, aux serveurs, aux navigateurs et aux comptes Internet. Yubico est le créateur et le principal contributeur des normes d'authentification ouvertes FIDO2, WebAuthn et FIDO Universal 2nd Factor (U2F), et en même temps un pionnier dans la fourniture à des clients de plus de 160 pays d'une authentification sans mot de passe basée sur le matériel et utilisant les clés de sécurité les plus sûres.

Les solutions de Yubico permettent de se connecter sans mot de passe en utilisant la forme la plus sûre de la technologie des clés d'accès. Les YubiKeys fonctionnent dès le départ dans des centaines d'applications et de services grand public et d'entreprise, offrant une sécurité forte avec une expérience rapide et facile.

Dans le cadre de sa mission visant à rendre Internet plus sûr pour tous, Yubico fait don de YubiKeys à des organisations qui aident les personnes à risque grâce à l'initiative philanthropique Secure it Forward. La société a son siège social à Stockholm et Santa Clara, en Californie. Pour plus d'informations sur Yubico, rendez-vous sur www.yubico.com.

Méthodologie

Talker Research a interrogé 18 000 actifs, dont 2 000 dans chacun des pays suivants : États-Unis, Royaume-Uni, Australie, Inde, Japon, Singapour, France, Allemagne et Suède. L'enquête a été commandée par Yubico et réalisée en ligne entre le 15 et le 27 août 2025.