

yubico

# Enquête mondiale sur l'état de l'authentification dans les entreprises

Comment les entreprises modernes adoptent une MFA résistante à l'hameçonnage

Incluant des données exclusives de la France





## Résumé exécutif

L'authentification joue un rôle essentiel dans le paysage complexe de la cybersécurité d'aujourd'hui, car elle détermine si les cyberattaques parviennent à entrer et à faire des dégâts, ou si elles sont stoppées dans leur élan. L'utilisation d'une authentification obsolète ou inefficace crée des risques pour la sécurité et la productivité des entreprises. Yubico a donc décidé de découvrir comment les entreprises gèrent leur authentification en leur posant directement la question.

**16 000+**  
réponses

entreprises avec

**1 - 2 000+**  
employés

**8**  
pays

Notre enquête inaugurale sur le niveau d'authentification global dans les entreprises a été conçue pour dresser un instantané de l'authentification dans les entreprises du monde entier. Nous avons reçu des réponses de plus de 16 000 employés, dont 2 000 en France. Les personnes interrogées allaient des employés débutants aux chefs d'entreprises travaillant dans des organisations de 1 à 2 000 employés et plus, dans huit pays : le Royaume-Uni, les États-Unis, l'Australie, la Nouvelle-Zélande, Singapour, la France, l'Allemagne et la Suède.

Ce rapport fournit un regard approfondi sur les pratiques et les attitudes au niveau mondial qui déterminent l'authentification. Dans l'ensemble, les résultats montrent que les organisations comprennent les dangers des cyberattaques. Pourtant, trop peu d'entre elles ont pris des mesures significatives pour substituer à l'authentification traditionnelle les meilleures pratiques telles que l'authentification multi-facteurs (MFA) résistante à l'hameçonnage.

Les méthodes MFA modernes, lorsqu'elles sont utilisées correctement, offrent un moyen relativement simple, accessible et efficace pour toute organisation d'améliorer sa sécurité, mais la plupart des entreprises ne l'utilisent pas à leur avantage. Ce rapport révèle les domaines dans lesquels les pratiques d'authentification doivent encore être améliorées — et aide les organisations à comprendre comment et pourquoi.

59% des employés interrogés

\*\*\*\*\*

s'appuient toujours sur le nom d'utilisateur et le mot de passe comme méthode d'authentification primaire

## Hameçonnage



Inciter les utilisateurs à fournir des identifiants de connexion ou d'autres données sensibles

## Authentification à facteur unique

\*\*\*\*\*

Authentification basée sur un facteur unique, généralement un mot de passe personnel

## Authentification multi-facteurs



Authentification nécessitant un ou plusieurs facteurs supplémentaires tels qu'une notification push, un code à usage unique ou une clé cryptographique

## MFA résistant à l'hameçonnage



Une authentification multi-facteurs imperméable aux attaques visant à intercepter, voire à inciter les utilisateurs à révéler les informations d'accès.

# Les pratiques d'authentification des entreprises restent inchangées

## Quels sont les principaux moyens d'authentification de vos comptes

### Nom d'utilisateur et mot de passe



### Authentification mobile par SMS



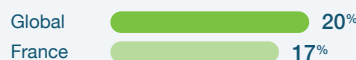
### Gestionnaire de mots de passe



### Applications mobiles TOTP/Push Authenticator



### Clés de sécurité physiques (par exemple, YubiKeys)



### Ne sait pas / Aucun / Autre



\*Multiples réponses autorisées / Tous les résultats de l'enquête dans le rapport font référence aux employés du monde entier, sauf indication contraire

Malgré les progrès considérables réalisés dans l'utilisation de l'informatique par les entreprises, la façon dont elles gèrent l'authentification n'a pas évolué assez vite. L'authentification à facteur unique (généralement un nom d'utilisateur et un mot de passe) est, de loin, le moyen d'authentification le plus courant, même s'il est largement prouvé que des acteurs malveillants peuvent acheter, voler ou forcer ces informations d'identification avec facilité. **La forme d'authentification la moins sécurisée est aussi la plus courante.**

Les autres types d'authentification — y compris les SMS, les gestionnaires de mots de passe et les applications mobiles — sont utilisés beaucoup moins fréquemment par les personnes interrogées dans le monde. Toutes ces méthodes sont plus sécurisées que l'authentification à facteur unique, mais chacune d'entre elles ont des failles. Les textos peuvent être interceptés en cours d'envoi, les applications peuvent être exploitées et les téléphones peuvent être perdus, cassés ou volés.

Les clés d'authentification physiques, telles que les YubiKeys, deviennent la référence en matière de MFA résistant à l'hameçonnage, mais elles ont été mentionnées par seulement 20 % des personnes interrogées au niveau mondial. En France, seuls 17 % des employés utilisent des clés physiques pour authentifier leurs comptes professionnels, derrière l'Allemagne (21 %) et la Suède (18 %), mais devant le Royaume-Uni (11 %).

Globalement, cette question révèle que de nombreuses entreprises sont vulnérables en raison d'une authentification à facteur unique faible. L'adoption de méthodes MFA en entreprise a encore beaucoup de chemin à parcourir.

22% des employés \*\*\*\*\*

pensent que le nom d'utilisateur et le mot de passe constituent la solution **la plus sûre**

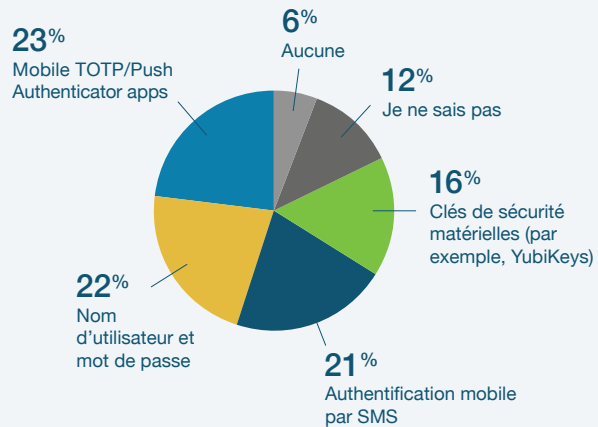
### Pourquoi les clés de sécurité sont-elles idéales pour l'authentification ?



La nécessité d'une clé spécifique et physique pour se connecter à des comptes en ligne supprime totalement le risque d'attaques à distance. Les clés de sécurité contiennent un code cryptographique unique qui ne peut être extrait et les protocoles FIDO2 signifient que les clés ne répondent qu'aux sources de confiance, ce qui les rend résistantes à l'usurpation d'identité. Les clés de sécurité se présentent sous différents formats (USB-A, USB-C, Lightning, NFC) pour s'interfacer facilement avec un plus grand nombre d'appareils. Considérées comme la forme de MFA la plus fiable pour les professionnels et les experts en sécurité, elles sont idéales pour une authentification forte.

## La perception n'est pas la réalité

### Quelle est, selon vous, la méthode d'authentification la plus sûre ?



Étonnamment, 22 % des personnes interrogées, tant au niveau mondial qu'en France, pensent que les identifiants de connexion de base (nom d'utilisateur et mot de passe) sont la forme d'authentification la plus sûre - malgré des années d'avertissements généralisés et de formations en entreprise axées sur le manque de sécurité des mots de passe. Un autre cinquième (un quart en France) fait confiance à l'authentification mobile par SMS, qui est largement considérée comme la forme la moins sûre de MFA en raison du risque élevé d'hameçonnage.

Au niveau mondial, seuls 16 % des employés ont choisi les clés de sécurité physiques comme méthode d'authentification la plus sûre. Bien qu'il s'agisse souvent d'une source d'inquiétude, le fait que, parmi tous les pays étudiés, les salariés français (18 %) soient devancés par ceux d'Allemagne (20 %) est un signe positif.

Le pourcentage d'employés au niveau mondial qui ont cité les clés de sécurité comme l'option la plus sûre est passé à 42 % au niveau des vice-présidents, ce qui pourrait indiquer que les employés de niveau supérieur sont mieux informés de la valeur d'une méthode MFA forte.



61% des employés interrogés et 79% du personnel de niveau VP



pensent que leur organisation doit passer à **une méthode MFA moderne résistant à l'hameçonnage** (comme les clés de sécurité physiques).

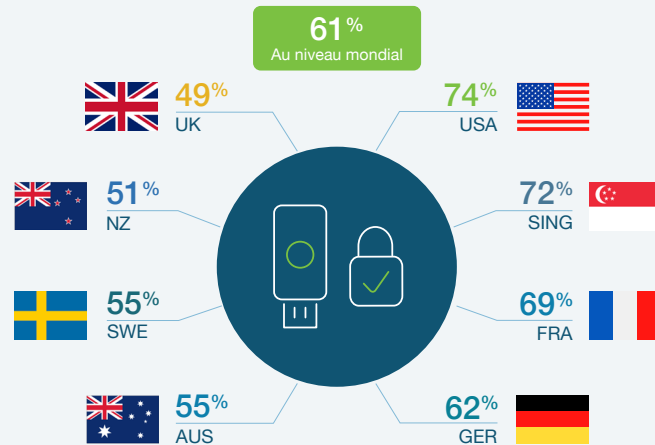
Les utilisateurs expérimentés optent pour une méthode MFA résistant à l'hameçonnage



Les données de l'enquête contenaient une information intéressante : **parmi les personnes interrogées qui se connectent quotidiennement à plus de 9 comptes ou applications, la grande majorité (76 %) souhaite que leur entreprise adopte une méthode MFA résistant à l'hameçonnage.** Ce chiffre est tombé en dessous de 40 % pour les personnes qui ne se connectent pas en moyenne quotidiennement. Il est logique que les utilisateurs les plus fréquents accordent une grande importance à la sécurité et à une authentification plus forte. Il est également logique qu'ils préfèrent une méthode MFA résistant à l'hameçonnage, qui offre une connexion beaucoup plus rapide que les applications d'authentification nécessitant de nouveaux codes à usage unique pour chaque ouverture de compte.

## Sentiments contradictoires à propos de l'authentification

Mon organisation doit passer à un MFA moderne résistant à l'hameçonnage (comme les clés de sécurité matérielles).



Plus de 60 % des personnes interrogées au niveau mondial reconnaissent que leur organisation doit passer à une méthode MFA résistant à l'hameçonnage (79 % au niveau des VP). Près d'un quart des employés ont indiqué qu'ils étaient « tout à fait » d'accord.

Ce qui est peut-être plus révélateur, c'est qu'à peine 10 % des personnes interrogées n'étaient pas d'accord, avec un fort désaccord inférieur à 5 % au niveau mondial — et seulement 4 % en France. Les résultats de l'enquête indiquent un fort soutien au niveau mondial en faveur de MFA résistant à l'hameçonnage, avec peu ou pas d'opposition significative.

Cependant, les résultats d'une autre question de l'enquête viennent compliquer ce constat : *Pour les options d'authentification que votre organisation propose, pensez-vous qu'elles offrent suffisamment de sécurité ?* Étonnamment, près de 80 % des personnes interrogées au niveau mondial sont d'accord avec cette affirmation. **Le scepticisme à l'égard de la sécurité était le plus marqué en France, 71 % seulement étant satisfaits de l'authentification offerte par leur entreprise. En fait, 23 % des salariés français étaient mécontents de l'authentification — ce qui est également le taux le plus élevé au niveau mondial.**

Dans l'ensemble, si les employés pensent que leur sécurité est adéquate, ils reconnaissent également qu'il y a place à l'amélioration — et que le MFA résistant à l'hameçonnage est une option importante.

78% des personnes interrogées



ont été exposées à une cyberattaque dans leur vie personnelle au cours des 12 derniers mois

60% des personnes interrogées



ont été exposées à une cyberattaque au travail au cours des 12 derniers mois

## Les cyberattaques sont une réalité

### À quels types de cyberattaques avez-vous été exposé au cours des 12 derniers mois ?\*

#### Les 5 réponses les plus courantes



\* Réponses multiples autorisées

Les cyberattaques n'ont jamais été aussi nombreuses, et peu de gens sont à l'abri. Ces chiffres mettent en évidence la prévalence des tactiques d'hameçonnage, tant à la maison qu'au travail. **En fait, 80 % des salariés en France disent avoir été exposés à une cyberattaque dans leur vie personnelle au cours de l'année écoulée, soit le taux le plus élevé d'Europe.**

Les attaques d'hameçonnage se présentaient sous la forme de messages textes, d'e-mails ou de notifications push demandant des informations privées, et dans certains cas, ces messages provenaient d'organisations apparemment « fiables ».

Avec une méthode MFA résistant à l'hameçonnage, peu importe que les pirates aient accès aux informations d'identification d'un utilisateur. Comme ils ne parviennent pas à compromettre la deuxième couche MFA, leurs tentatives d'attaques échouent. Sachant que la plupart des gens sont confrontés à des attaques d'hameçonnage fréquentes — et que de nombreuses entreprises utilisent encore l'authentification à facteur unique — le renforcement de l'authentification devient obligatoire.

#### Hameçonnage par harponnage



Les attaques par hameçonnage visent des personnes très précises, telles que les administrateurs système

#### La chasse à la baleine



Les attaques d'hameçonnage visant les employés de haut niveau, tels que les cadres

#### Hameçonnage vocal



Les attaques d'hameçonnage par téléphone et message vocal où l'identité de l'autre personne est difficile à confirmer

#### Hameçonnage par SMS



Les attaques d'hameçonnage qui se déroulent par texte ou par chat, où la confiance est implicite et les informations circulent librement

## Les attaques risquent d'avoir de graves conséquences

L'enquête montre que toute exposition aux cyberattaques s'accompagne de risques inquiétants et d'une forte probabilité de dommages, potentiellement dévastateurs. **Moins de 30% des personnes interrogées n'ont vu aucune conséquence aux attaques** (bien que ces données incluent également des employés subalternes qui peuvent ne pas avoir été informés des conséquences d'une attaque). 35% des personnes interrogées ont subi une atteinte à leur réputation et, de même, 35% ont subi une atteinte à leurs bénéfices. Tout aussi alarmant, 17% ont perdu des employés à cause de cyberattaques, et 20% ont vu leurs opérations suspendues. Tout est en jeu dans une cyberattaque.

## Les conséquences éclipsent les corrections

**Vous avez déclaré avoir été exposé à une cyberattaque au cours des 12 derniers mois au travail.\***

**Quelles nouvelles technologies ou politiques de sécurité, le cas échéant, votre organisation a-t-elle mises en œuvre suite à cette attaque ?**

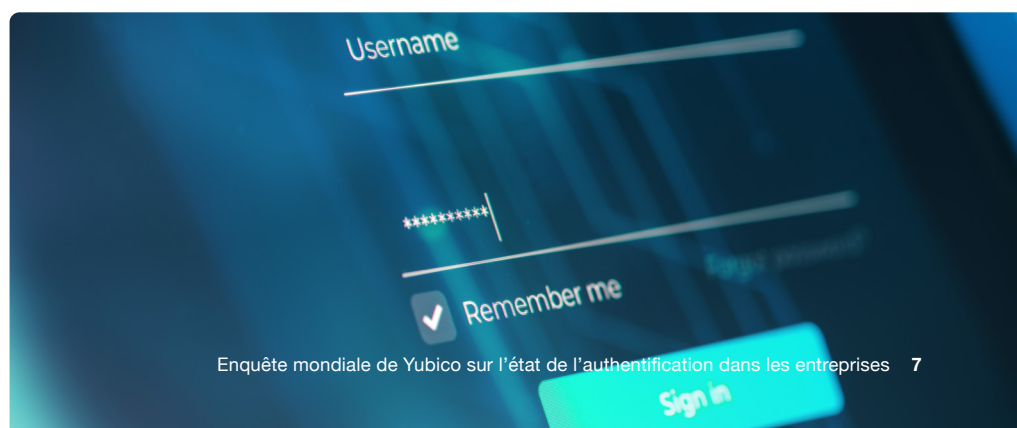


\* Réponses multiples autorisées

Compte tenu des conséquences, on pourrait s'attendre à ce que les organisations mettent en place des mises à niveau solides, mais cela ne semble pas toujours être le cas. La réponse la plus courante (réinitialisation des noms d'utilisateur et des mots de passe) n'empêche pas les pirates de voler à nouveau les informations d'identification d'une personne et de répéter la même attaque. La formation obligatoire à la sécurité, une autre réponse courante, peut sensibiliser les gens au problème, mais ne fait rien pour l'arrêter.

Seuls 17 % des employés au niveau mondial ont déclaré que leur organisation avait mis en place des clés de sécurité matérielles (par exemple, YubiKeys) en réponse à une cyberattaque. En France, ce taux est tombé à 13 %, soit moins de la moitié du taux de mise en œuvre aux États-Unis, qui arrivent en tête des huit pays avec 28 %.

Le fait qu'une méthode MFA résistante à l'hameçonnage ait été si rarement utilisée en réponse à des attaques — alors qu'il s'agit de la forme d'authentification la plus sûre — est troublant. Ce qui est encore plus inquiétant, c'est que certaines entreprises ne prennent pas de mesures supplémentaires pour renforcer la cybersécurité et améliorer l'authentification après les attaques. **Les données de l'enquête révèlent une disparité remarquable entre le risque de cyberattaques et la réponse.** L'amélioration de l'authentification s'attaque directement à cette disparité et comble rapidement les failles de sécurité qui ont permis l'attaque initiale.

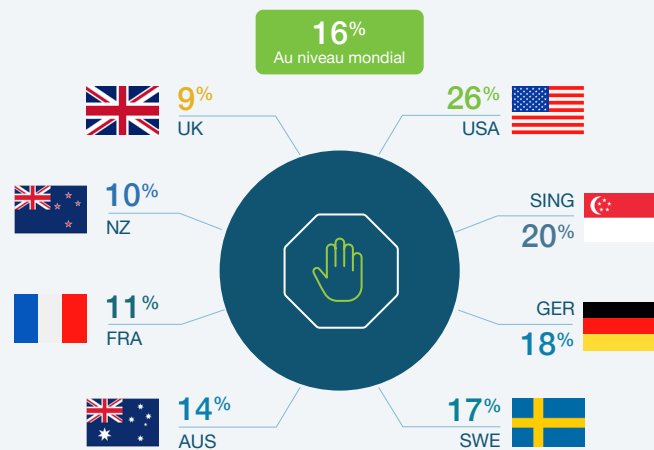


## Une adoption lente comporte des risques

Pourtant, seules 12 % des entreprises interrogées ont mis en place une méthode MFA pour toutes les applications et tous les services qu'elles utilisent. Nous avons demandé aux personnes interrogées ce qui les retient de mettre en œuvre l'authentification forte, même si elles admettent être préoccupées par les attaques. Le fait d'être lent à adopter la technologie se place au premier rang (19%), mais est suivi de près par la perception que le MFA est cher (19%), inutile (16%), chronophage (16%), compliquée à déployer (15%) ou difficile à utiliser (14%).

## L'autosatisfaction freine le progrès

Mon organisation n'a pas adopté la MFA à travers toutes les applications et les services parce qu'elle ne craint pas qu'une attaque leur arrive.

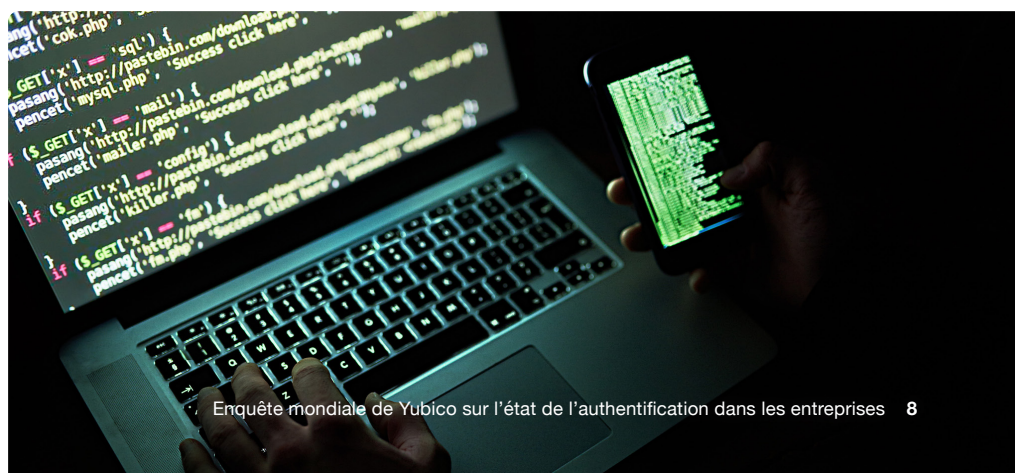


Les entreprises sont lentes à adopter la MFA, et l'enquête a révélé de multiples raisons à cela, notamment la perception que cette méthode est coûteuse, longue, compliquée ou inutile.

Le plus troublant est que de nombreuses organisations n'adoptent pas le MFA parce qu'elles ne pensent pas être exposées à un risque de cyberattaque, notamment 26 % des entreprises américaines. Bien que cela ne soit vrai que pour 11 % des entreprises en France, ce qui indique une moindre complaisance dans l'ensemble, tout faux sentiment de sécurité est source d'inquiétude. Cela signifie que ces entreprises — et les données de leurs clients — sont vulnérables aux attaques d'hameçonnage.

Une véritable protection contre la cybercriminalité exige l'utilisation de la MFA dans toutes les applications et tous les services, mais cela n'a été le cas que pour 12 % des organisations interrogées dans le monde et, fait inquiétant, pour 8 % seulement en France, soit le deuxième taux d'adoption le plus faible dans les huit pays après celui de l'Allemagne (6 %).

Le MFA universel est considéré comme une meilleure pratique d'authentification et un élément essentiel de la cybersécurité. Néanmoins, pour la plupart des entreprises, les obstacles perçus semblent l'emporter sur les avantages.

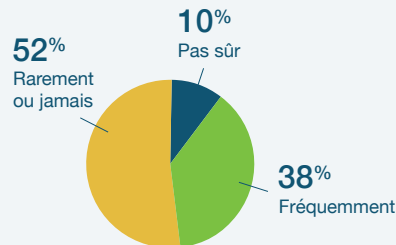


## Les cyberattaques provoquent des insomnies

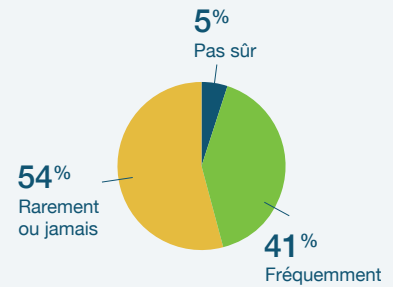
Lorsqu'on leur a demandé d'énumérer les cinq principales préoccupations en matière de cybersécurité qui les empêchent de dormir la nuit, les personnes interrogées ont répondu : se faire pirater sur un compte privé, compromettre un appareil mobile, la violation des données, la compromission des données des clients et le piratage des comptes de l'entreprise. **Moins de 30 % ont déclaré qu'aucun problème de cybersécurité ne les empêchait de dormir la nuit.** Les professionnels de tous niveaux (en particulier les cadres supérieurs) sont préoccupés par la cybersécurité et en perçoivent les conséquences pour eux-mêmes et pour leur entreprise. La réponse institutionnelle, cependant, n'a pas suivi les inquiétudes individuelles.

## La sécurité n'est pas une priorité

La cybersécurité est abordée pendant les réunions du conseil d'administration



Les employés sont tenus de suivre une formation sur la sécurité



Les cyberattaques — et la manière de les prévenir — devraient être au cœur des préoccupations de chaque organisation. Toutefois, la plupart des entreprises affirment que le sujet est rarement ou jamais abordé.

Les données de l'enquête révèlent également de grandes disparités entre les approches au niveau mondial. Les États-Unis sont en tête du peloton : la cybersécurité est fréquemment abordée lors des réunions du conseil d'administration et de la direction de 60 % des entreprises, contre une moyenne mondiale de 38 %. Bien qu'elle soit derrière les États-Unis, la France, avec 41 %, est nettement supérieure à tous les autres pays européens. De même, 62 % des employés des entreprises américaines sont tenus de suivre une formation à la cybersécurité, contre 41 % en moyenne au niveau mondial et 39 % en France.

Les employés (à tous les niveaux) sont la plus grande force ou la plus grande faiblesse de la cybersécurité, mais dans la plupart des cas, ils ne sont pas équipés pour être des cyberdéfenseurs efficaces. Le manque d'éducation et de formation des employés rend encore plus importante l'adoption par les entreprises d'une méthode MFA résistant à l'hameçonnage.

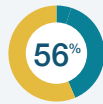


## Les entreprises cultivent la sensibilisation à la sécurité

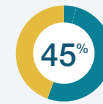
Le sérieux avec lequel une personne prend la cybersécurité dépend, dans une large mesure, de son employeur. Près de la moitié des employés dans le monde (et autant en France) ont déclaré que leur sécurité numérique personnelle s'est améliorée grâce à ce qu'ils ont appris ou fait au travail pour protéger leurs comptes. Ces résultats montrent que les entreprises peuvent (et doivent) influencer sur la façon dont les employés pratiquent la cybersécurité.

## La cyber hygiène peut encore être améliorée

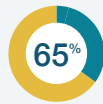
Avez-vous fait les choses suivantes au moins une fois au cours des 12 derniers mois ?



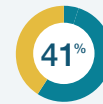
J'ai utilisé un **appareil fourni par l'entreprise** à des fins personnelles



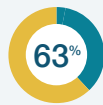
J'ai permis à quelqu'un d'autre d'utiliser mon **appareil fourni** par mon employeur



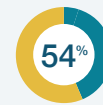
J'ai utilisé un **appareil personnel** pour le travail



Je **n'ai pas** signalé une tentative d'hameçonnage



J'ai dû faire réinitialiser mon compte en raison de la **perte** et/ou **d'un oubli de mes** informations d'identification



J'ai écrit ou **partagé** un mot de passe

L'enquête comportait une série de questions visant à déterminer la fréquence à laquelle les employés adoptent des comportements à risque qui nuisent à la cybersécurité, comme l'utilisation d'un appareil fourni par le travail à des fins personnelles ou la perte de leur ordinateur portable ou de leur téléphone professionnel.

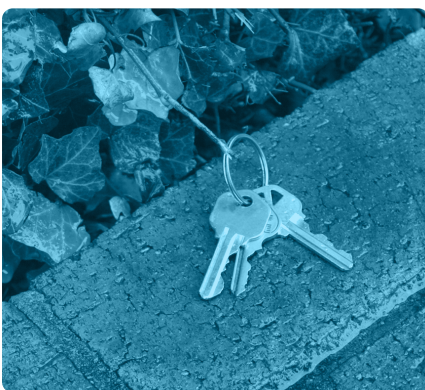
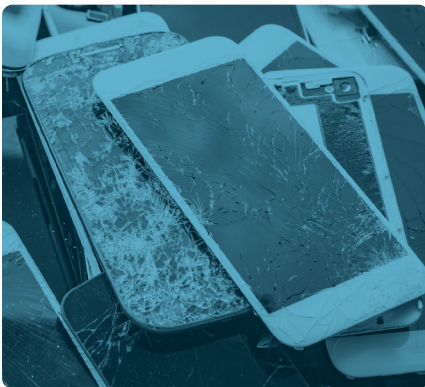
Il est rassurant de constater qu'un pourcentage élevé de personnes interrogées ne s'adonnent jamais ou rarement à des pratiques dangereuses. Cela dit, il suffit d'une erreur pour déclencher une attaque. **En effet, l'une des révélations les plus étonnantes de l'enquête est que 54 % des employés (et un pourcentage massif de 60 % en France) admettent avoir écrit ou partagé un mot de passe au cours des 12 derniers mois, ce qui révèle des problèmes répandus mais négligés en matière de sécurité des comptes.**

Le fait d'exiger une méthode MFA résistante à l'hameçonnage pour tous les comptes empêche ces vulnérabilités de permettre aux attaques de dégénérer en incidents graves.



## Quand l'authentification devient une urgence

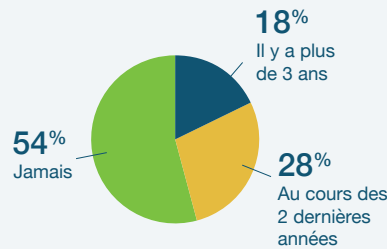
L'enquête montre que la plupart des gens se connectent quotidiennement à un à cinq comptes ou applications, et un quart à six ou plus. Ne pas pouvoir s'authentifier à cause d'un appareil perdu ou volé est plus qu'un inconvénient, c'est un obstacle insurmontable pour accomplir quoi que ce soit. L'authentification à facteur unique représente la plus grande responsabilité, *mais* la mauvaise forme de MFA comporte également des responsabilités.



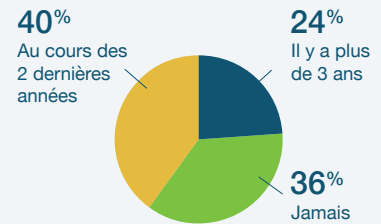
## Nous nous soucions surtout de nos clés

À quand remonte la dernière fois où vous avez perdu ou cassé votre téléphone, ou perdu vos clés de maison ou de voiture ?

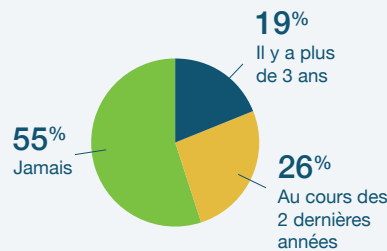
### Téléphone perdu



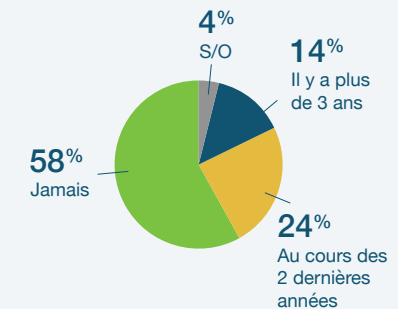
### Téléphone cassé



### Perte des clés de la maison



### Clés de voiture cassées



Lorsqu'une personne quitte la maison ou le bureau, elle emporte généralement deux objets essentiels : son téléphone et ses clés. Les employés sont beaucoup plus susceptibles de perdre ou de casser leur téléphone que leurs clés. En fait, le plus grand pourcentage de personnes n'avait jamais perdu les clés de leur voiture ou de leur maison — ni récemment, ni jamais.

Étant donné que l'authentification multifactorielle dépend souvent du fait qu'une personne ait son téléphone ou une clé de sécurité pour passer le deuxième facteur, les taux de perte sont importants. Un téléphone cassé peut rendre l'accès difficile (voire impossible), et un téléphone perdu peut tomber dans de mauvaises mains. En particulier, les directeurs et les vice-présidents (ceux qui ont accès aux informations les plus sensibles de l'entreprise) ont déclaré perdre leurs téléphones dans les proportions les plus élevées, ce qui fait courir un risque sérieux à leur organisation.

Au moment où les entreprises commencent à envisager l'ajout du MFA à l'ensemble des applications et des services, elles doivent comparer les forces et les faiblesses des différentes « secondes » étapes. Les téléphones, avec lesquels nous interagissons constamment, sont toujours vulnérables. Les clés, quant à elles, se trouvent principalement dans les poches et les sacs, ce qui explique pourquoi elles sont moins souvent perdues. En d'autres termes, le MFA basé sur des clés de sécurité plutôt que sur des téléphones correspond mieux au mode de vie réel des personnes.



La majorité des personnes interrogées s'accordent à dire que le vol d'informations d'identification est plus préoccupant que le fait de ne pas pouvoir boire son café du matin.

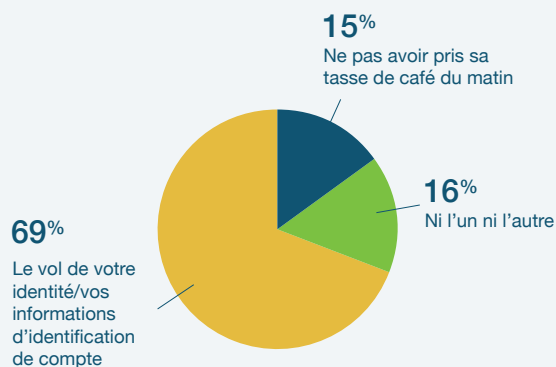
YubiKeys



Les YubiKeys, qui sont des clés de sécurité matérielles, sont une MFA résistant à l'hameçonnage qui élève l'authentification de toutes les manières. Les clés de sécurité rendent l'authentification insensible aux tentatives d'hameçonnage et les comptes inaccessibles à tous, sauf à la personne qui possède la bonne clé. La perte de la clé est moins un risque, et remplacer une clé est plus facile que de remplacer un téléphone. Plus qu'une simple clé de sécurité, Yubico offre une solution MFA d'entreprise qui convient aux petites et grandes entreprises de tous les secteurs, et en particulier aux secteurs soumis à des réglementations de sécurité étendues.

## Les personnes se soucient de leurs informations d'identification

Êtes-vous plus préoccupé par le vol de votre identité/ vos informations d'identification de compte que par l'impossibilité de prendre votre café du matin ?



Heureusement, les personnes sont beaucoup plus nombreuses à se soucier de leur identité/leurs informations d'identification de compte que de leur café du matin, ce qui traduit une vérité importante : les personnes se soucient de protéger leurs comptes. **Comme le montrent les données de l'enquête, les personnes veulent une authentification forte et multifactorielle, mais seulement si elle est simple, transparente et sécurisée.**

Alors que le cyber-risque s'aggrave à tous les égards — augmentation des attaques, aggravation des dommages, renforcement des exigences de conformité — les entreprises du monde entier doivent prendre au sérieux l'authentification multi-facteurs. C'est le premier domaine sur lequel il faut se concentrer, le plus important et celui qui a le plus d'impact. Et, comme le révèlent les données de l'enquête, c'est un domaine qui n'est pas à la hauteur dans la plupart des organisations au niveau mondial. Parmi les entreprises françaises, la prise de conscience de l'importance de la cybersécurité ne s'accompagne pas encore de l'engagement nécessaire pour mettre en œuvre une authentification plus forte.

Ciblez la MFA résistant à l'hameçonnage pour faire les plus grands progrès en matière de cybersécurité. Et choisissez les YubiKeys pour un raccourci vers une posture de sécurité forte et conforme.



## À propos de Yubico

Yubico a inventé la YubiKey, une clé qui rend les connexions sécurisées, faciles et accessibles à tous. Fondée en 2007, la société est leader dans l'établissement de nouvelles normes mondiales pour un accès sécurisé aux postes de travail, aux appareils mobiles, aux serveurs, aux navigateurs et aux applications. Yubico est le créateur et l'un des principaux contributeurs aux normes d'authentification ouvertes FIDO2, WebAuthn et FIDO Universal 2nd Factor (U2F) et pionnier reconnu dans l'authentification forte à base de clés de sécurité physique, déployables à grande échelle.

Les YubiKey sont la référence pour l'authentification multi-facteurs (MFA) anti-hameçonnage, une seule clé fonctionnant sur des centaines d'applications et de services grand public et d'entreprise. La technologie de Yubico permet une authentification, un cryptage et une signature de code sécurisés et est utilisée et appréciée par de nombreuses entreprises parmi les plus grandes au monde et des millions de clients dans plus de 160 pays.

Conformément à sa mission de rendre Internet plus sûr pour tous, Yubico fait don de ses YubiKey à des organisations qui aident les personnes à risque par le biais de l'initiative philanthropique « Secure it Forward ». Yubico est une société privée, avec une présence dans le monde entier et des bureaux à Santa Clara, San Francisco, Seattle et Stockholm. Pour plus d'informations, consultez : [www.yubico.com](http://www.yubico.com).

---

Yubico AB  
Kungsgatan 44  
2ème étage  
SE-111 35 Stockholm  
Suède

Yubico Inc.  
5201 Great America Pkwy  
Suite 122  
Santa Clara, CA 95054  
États-Unis