yubico

# Pourquoi votre stratégie MFA mobile attire la cybercriminalité et comment y remédier

Nous sommes à un point critique pour la cybersécurité. Pendant la crise sanitaire due à la COVID, les cyberattaques ont grimpé de 300 %.[1] En 2020, les ransomwares faisaient une nouvelle victime toutes les 10 secondes,[2] et les incidents par hameçonnage ont doublé.[3] Le coût moyen d'une violation de données a battu un record de 17 ans en 2021, atteignant la somme colossale de 4,24 millions de dollars.[4]

Malgré la hausse et la sophistication des cyber-attaques, de nombreuses entreprises continuent d'utiliser des méthodes d'authentification multi-facteurs (MFA) héritées, telles que les noms d'utilisateur + mots de passe, ou les authentificateurs mobiles, pour sécuriser l'accès aux applications et aux données critiques et sensibles. Dans ces entreprises, les résultats sont inattendus : des attaques qui pénètrent leurs défenses et des employés frustrés.

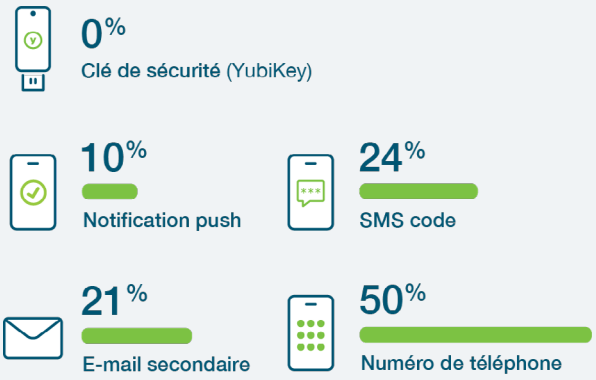
## Pourquoi l'authentification mobile met votre entreprise en danger

Bien que toute forme de MFA offre une meilleure sécurité que l'authentification basée sur un nom d'utilisateur et un mot de passe, toutes les formes de MFA ne sont pas créées égales. En effet, les MFA mobiles telles que les SMS, les OTP et les notifications push sont très sensibles aux attaques par hameçonnage, aux attaques de l'homme du milieu (MiTM), aux logiciels malveillants, aux échanges de cartes SIM et aux piratages de comptes.

La commodité et l'omniprésence des appareils mobiles sont exactement ce qui les rend si hameçonnables. Dans la MFA mobile, il n'y a aucune garantie que la clé privée se retrouve sur un élément sécurisé sur l'appareil mobile. Les appareils mobiles ont une grande surface d'attaque sur les applications, la communication, les systèmes d'exploitation et la technologie des éléments sécurisés. Les pirates d'aujourd'hui détournent de plus en plus l'OTP et envoient des notifications par interception ou hameçonnage, l'attaquant et la prise de contrôle du compte étant pratiquement invisibles pour l'utilisateur.

Des recherches menées par Google, NYU et UCSD sur la base de 350 000 tentatives de piratage dans le monde réel ont prouvé que les authentificateurs SMS et mobiles ne sont pas si efficaces pour empêcher les prises de contrôle de compte et les attaques ciblées.[5] La recherche a révélé qu'un mot de passe à usage unique (OTP) basé sur SMS n'a bloqué que 76 % des attaques ciblées et une application push n'en a bloqué que 90 %. C'est un taux de pénétration de 10 % au minimum. Avec cette approche, ce n'est pas une question de savoir si vous allez être attaqué, mais plutôt quand.

### Risque de piratage de compte




En plus d'une sécurité plus faible, les authentificateurs mobiles n'offrent pas non plus une expérience utilisateur facile. Lorsque les SMS et les notifications push sont utilisés pour une authentification à deux facteurs (2FA) ou MFA, les employés doivent attendre et saisir les codes fournis par SMS ou les applications d'authentification. Et tout cela dépend de la disponibilité de la connectivité cellulaire, du fait que le téléphone est suffisamment chargé et d'autres nuances qui peuvent affecter l'expérience de l'utilisateur. Cela augmente le temps et la complexité de l'authentification et réduit la productivité des employés, tout en laissant l'entreprise exposée.

[1] Rachel England, Le FBI voit les signalements de cybercriminalité quadrupler pendant l'épidémie de COVID-19 (20 avril 2020)

[2] Phil Muncaster, Une victime de ransomware toutes les 10 secondes en 2020, (25 février 2021)

[3] Internet Crime Complaint Center, 2020 Internet Crime Report, (17 mars 2021)

[4] IBM Security, Rapport sur le coût d'une violation de données, (28 juillet 2021)

[5] Kurt Thomas et Angelika Moscicki, Nouvelle recherche : how effective is basic account hygiene at preventing hijacking, (17 mai 2019)

## L'authentification mobile crée également des lacunes dans votre cadre MFA

Alors que les entreprises peuvent donner la priorité ou même imposer une MFA basée sur le mobile, il existe presque toujours des cas d'employés qui ne peuvent pas, n'utilisent pas ou ne veulent pas utiliser l'authentification mobile. Non seulement la couverture cellulaire peut être faible dans certaines zones géographiques, mais les employés peuvent également ne pas vouloir utiliser leurs appareils personnels pour le travail ou ne pas autoriser l'accès administrateur à leurs appareils. Il peut également y avoir des restrictions syndicales ou des exigences de conformité, et certains employés peuvent même ne pas être en mesure d'utiliser un smartphone.

Si les noms d'utilisateur et mots de passe sont utilisés comme option de secours, cela rend l'entreprise encore plus vulnérable au hameçonnage et aux prises de contrôle de compte.

Alors que les entreprises adoptent une nouvelle façon de travailler, où le travail à distance et hybride est la norme, s'appuyer sur la sécurité du périmètre n'est plus efficace. Les entreprises qui utilisent aujourd'hui des authentificateurs mobiles doivent réévaluer leur stratégie MFA à long terme et envisager de passer à des solutions MFA modernes et résistantes au hameçonnage.

Dans ces scénarios, une clé de sécurité matérielle offre aux entreprises une large couverture des scénarios d'entreprise et des groupes d'utilisateurs tout en garantissant la meilleure sécurité et la meilleure expérience utilisateur.

## Élaboration d'une stratégie MFA sécurisée à long terme

Afin de rendre votre entreprise hautement résistante au hameçonnage, les comptes d'utilisateurs doivent être sécurisés avec une 2FA ou une MFA solide qui utilise des clés de sécurité matérielles spécialement conçues pour sécuriser l'accès des utilisateurs avec les niveaux les plus élevés de défense contre le hameçonnage ainsi qu'en offrant la meilleure expérience utilisateur. Avec des clés de sécurité matérielles prenant en charge les protocoles d'authentification modernes, les utilisateurs peuvent enregistrer une clé de sécurité unique pour des centaines de services avec une paire de clés publique/privée unique générée pour chaque service. Les secrets ne sont jamais partagés entre les services, et la clé privée est stockée dans l'élément sécurisé sur la clé matérielle et ne peut pas être exfiltrée. De plus, les clés de sécurité matérielles exigent que l'utilisateur appuie ou touche un bouton pour l'authentification afin de prouver sa présence. De cette manière, les clés de sécurité matérielles arrêtent les attaques à distance, de l'homme du milieu et par hameçonnage, et contrairement à l'authentification par SMS ou à toute application mobile, seul le service enregistré est autorisé à lancer la demande d'authentification.

Les entreprises doivent également tenir compte des nouvelles réglementations et mises à jour attendues au cours des prochaines années, en particulier à la suite de la COVID-19. Alors que l'authentification mobile peut être considérée comme suffisante aujourd'hui, il se peut qu'elle ne réponde pas aux futures normes de conformité MFA. Un véritable investissement dans la sécurité à l'épreuve du temps devrait bien préparer une entreprise pour des flux de connexion sécurisés et modernes, tels que le sans mot de passe (passwordless), ainsi que pour la conformité réglementaire à long terme.

## Les YubiKeys offrent une authentification moderne et résistante au hameçonnage à grande échelle et une transition vers le sans mot de passe

La YubiKey de Yubico est une clé de sécurité matérielle spécialement conçue pour une haute sécurité ainsi que pour arrêter le hameçonnage et d'autres formes de prise de contrôle de compte dans leur élan, offrant une authentification forte à grande échelle.

Il s'agit de la seule solution éprouvée par des chercheurs indépendants pour arrêter 100 % des piratages de compte, y compris les attaques par hameçonnage et massives ciblées.[6]

Les YubiKeys offrent une solution MFA moderne et solide conçue pour répondre aux besoins des entreprises pour leurs employés de bureau à distance ou non, utilisateurs privilégiés, environnements restreints mobiles, postes de travail partagés, entités/chaînes d'approvisionnement tierces et même clients finaux. Une seule YubiKey fonctionne de manière transparente sur les systèmes et applications anciens et modernes avec une prise en charge multiprotocole pour SmartCard (PIV), OTP, OpenPGP, FIDO U2F et FIDO2/WebAuthn. Et, pour les organisations qui cherchent à commencer leur voyage vers le sans mot de passe la YubiKey offre une transition entre la situation actuelle des entreprises et un avenir moderne sans mot de passe sans rupture ni remplacement.

Configurez votre entreprise avec un investissement de sécurité à l'épreuve du temps qui offre non seulement une sécurité solide, mais peut vous aider aussi à naviguer dans le paysage de la conformité en évolution. Les entreprises les plus soucieuses de la sécurité et les plus à haut risque au monde font confiance à YubiKey pour une authentification à deux facteurs, multi-facteurs et sans mot de passe résistante au hameçonnage.

| | Authentification mobile | YubiKey |
|---|---|---|
| Résiste au hameçonnage | – | ✓ |
| Toujours sécurisée | – | ✓ |
| Rentable | – | ✓ |
| Conviviale | – | ✓ |
| Couverture à 360° | – | ✓ |
| À l'épreuve du temps | – | ✓ |

[5] Kurt Thomas et Angelika Moscicki, Nouvelle recherche : how effective is basic account hygiene at preventing hijacking, (17 mai 2019)



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

**Yubico Inc.**
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 États-Unis
844-205-6787
650-285-0088