Twitter : une clé de sécurité physique pour une double authentification

Alors qu'auparavant, le réseau social permettait aux utilisateurs d'utiliser une clé de sécurité comme un facteur d'authentification parmi d'autres, Twitter a annoncé en mars dernier qu'il autoriserait bientôt l'utilisation de clés de sécurité physiques comme seule méthode d'authentification. Fidèle à sa promesse, Twitter vient de déployer cette fonctionnalité pour tous les utilisateurs qui souhaitent renforcer la sécurité de leur compte.

« La sécurité des personnes sur Twitter est l'une de nos principales priorités, et nous nous engageons à aider les gens à comprendre les outils de sécurité que nous proposons et à les utiliser. À partir d'aujourd'hui, les utilisateurs de Twitter ont la possibilité d'utiliser des clés de sécurité comme seule forme d'authentification à deux facteurs (2FA), qui est le moyen le plus efficace de sécuriser votre compte Twitter », a annoncé le média social.

> *Now security keys can be your one and only two-factor authentication method on mobile and web.*
>
> *Learn more about how security keys can protect your account from attacks: https://t.co/Ta7uQSFhi6 pic.twitter.com/aPDOnbRtVk*
>
> *— Twitter Support (@TwitterSupport) June 30, 2021*

L'utilisation de clés de sécurité en tant que méthode 2FA n'est pas nouvelle pour Twitter. En 2018, la plateforme a introduit l'option comme l'une des multiples méthodes 2FA, mais cela nécessitait que les utilisateurs aient également une autre forme de 2FA activée, le support étant initialement déployé uniquement sur la version web. La fonctionnalité a été étendue aux applications Android et iOS en 2020, et plus tôt cette année, l'option d'enregistrer plusieurs clés de sécurité a également été ajoutée.

Les clés de sécurité matérielles plus efficaces

Alors qu'une sagesse commune en matière de cybersécurité veut que tout type de 2FA soit préférable à aucun, les clés de sécurité matérielles offrent des garanties plus efficaces contre les prises de contrôle de comptes que le 2FA basé sur les SMS. En effet, les applications d'authentification se sont également retrouvées dans le collimateur des attaquants.

Néanmoins, on parle alors principalement des codes reçus par SMS, faciles à intercepter pour les cybercriminels déterminés. De plus, un acteur malveillant pourrait par exemple détourner des messages texte vers une autre carte SIM via une attaque par échange de carte SIM, qui consiste à se faire passer pour la cible et à contacter son opérateur télécom pour le convaincre que le téléphone de la cible a été volé et qu'elle utilise désormais une nouvelle carte SIM.

« Les clés de sécurité offrent la plus forte protection pour votre compte Twitter car elles disposent de protections intégrées pour garantir que même si une clé est utilisée sur un site de hameçonnage, les informations partagées ne peuvent pas être utilisées pour accéder à votre compte. Elles utilisent les normes de sécurité FIDO et WebAuthn pour transférer la charge de la protection contre les tentatives de hameçonnage d'un humain à un dispositif matériel. Les clés de sécurité peuvent différencier les sites légitimes des sites malveillants et bloquer les tentatives de hameçonnage, ce que ne feraient pas les SMS ou les codes de vérification », précise Twitter, en soulignant les différences entre ces méthodes de 2FA.

Si vous n'avez pas encore activé de méthode 2FA sur votre compte, vous feriez mieux de le faire immédiatement en vous basant sur les instructions figurant au guide pratique de Twitter.