Security keys have been good to Google, so now it's promoting one of its own

Google's workforce hasn't suffered a single confirmed account takeover in over a year. The impressive security stat[1] is due to small USB security keys issued to all 85,000 of the company's employees. Companies that produce these small pieces of hardware, like Yubico, have seen tremendous growth over the last two years thanks to rapidly accelerating adoption — but they will now have fresh competition.

Google will soon start widely selling its own Titan Security Key, which includes firmware developed by the omnipresent tech giant itself. The product is available now to Google Cloud customers and will eventually be available to general customers, the company announced Wednesday at its Google Cloud Next conference in San Francisco. Like similar keys from other companies, it will provide a second authentication factor for software use, network access, account management and other services. When the hardware is linked to an account, a password isn't enough — the user must plug in the key and activate it before getting access.

"We've long advocated the use of security keys as the strongest, most phishing-resistant authentication factor for high-value users, especially cloud admins, to protect against the potentially damaging consequences of credential theft," Jennifer Lin, a Google Cloud product director, said. "Titan Security Key gives you even more peace of mind that your accounts are protected, with assurance from Google of the integrity of the physical key."

Google's cloud customers typically give security keys to high-value users like administrators and root users where a compromise would be exceptionally damaging.

"It's built with a secure element including firmware we built ourselves," Google's Rob Sadowski said. "It provides a ton of security with very little interaction and effort on the part of the user." [...]

"On the backend, all you have to do on the admin console is literally check a box that says 'use Titan Security Keys for this app,'" Sadowski said. "It's that simple. If there's a man-in-the-middle attack or something of that kind, it won't have the authenticated response and will reject the connection. Very simple, very powerful."

At a time when cybersecurity experts consider multifactor authentication a necessary step — despite most Americans remaining in the dark — security keys are typically considered the strongest defense against account takeovers.

In the last two years, Yubico has seen rapidly accelerating growth, to the point where "19 of the 20 biggest internet companies on the planet," including Google,

[1] stat : statistic

now use YubiKeys, according to Stina Ehrensvärd, founder and CEO of the Swedish-American company.

For the past two years, Google has given its employees Yubikeys despite the fact that it runs and maintains its own Google Authenticator app. [...]

Phishing represents a huge threat. About 71 percent of all targeted attacks start with phishing attempts [...] — it's how hackers broke into the Democratic National Committee in 2016 and it's the top attack vector against all manner of targets.

Other common forms of two-factor authentication include text-message codes and mobile apps like Google Authenticators but they can all be phished, intercepted and hacked more easily than security keys, which typically are plug-and-play, without any special software drivers.

All of the above options, however, are exponentially more secure than having no multifactor authentication at all. Users of any online service should demand and use multifactor authentication all over the web.

Patrick Howell O'Neill, *CyberScoop*, July 25, 2018

PREMIÈRE PARTIE (10 points)

Vous rédigerez **en français** un compte rendu du texte.

Votre compte rendu devra comprendre une brève introduction qui indiquera la date, la source et le thème du document. Vous synthétiserez et reformulerez les idées essentielles du texte.

Une brève conclusion personnelle qui dégage l'intérêt du document dans une perspective professionnelle sera valorisée.

200 mots +/- 10 %. Vous indiquerez impérativement le nombre de mots de votre compte rendu.

DEUXIÈME PARTIE (10 points)

Vous êtes Edwin/Jessica Parker, consultant(e) informatique spécialisé(e) en protection des données.

Peter Kelly, chef d'entreprise irlandais qui voyage régulièrement à l'étranger, vous a contacté(e) car il souhaiterait accéder à ses documents professionnels à caractère confidentiel lors de ses déplacements.

Vous lui répondez par un courriel dans lequel vous lui indiquez les meilleures solutions pour que ses données soient bien protégées. Vous lui donnez des conseils techniques, et éventuellement juridiques, afin qu'elles soient stockées en toute sécurité.

Vous rédigerez ce courriel **en anglais**.

(Environ 150 mots)