TECH DRIVERS

TECH DRIVERS

Why passkeys from Apple, Google, Microsoft may soon replace your passwords

PUBLISHED SAT, FEB 11 2023•10:31 AM EST | UPDATED MON, FEB 13 2023•9:14 AM EST

Barbara Collins
@BARBARACOLL_

SHARE

KEY POINTS

- As the security of passwords continues to be threatened by hackers and phishing attempts, the use of passkeys is continuing to rise.
- Passkeys provide more security and are close to phishing resistant, according to internet security experts.
- Apple, Google and Microsoft are just some of the technology companies pushing more users towards using passkeys over passwords, which could become standard within a year.

PDFmyURL converts web pages and even full websites to PDF easily and quickly.

Naked King | Istock | Getty Images

The death of the internet password has been proclaimed many times, but this time, it may actually be coming sooner than you think. Its replacement? The passkey.

Passkeys are the way of the future in basic internet security as they're intrinsically more secure and phishing resistant, according to Kathleen Moriarty, the chief technology officer at the Center for Internet Security. As major companies including Apple ⊞, Google ⊞ and Microsoft ⊞ work with the standards developed by the FIDO Alliance and World Wide Web Consortium — two organizations that create password authentication standards — to provide support for passkeys on their platforms, the list of organizations offering passkeys as an alternative to passwords is continuing to grow.

"Passkeys are an example of what security should be: seamless and invisible to the end user," said Moriarty.

How passkeys work

PDFmyURL converts web pages and even full websites to PDF easily and quickly.

Using a passkey allows an individual to gain access to an account by approving the login on an external device, with no password required.

When someone logs into an account with a passkey, a prompt, also called a challenge, is sent to an additional device owned by the user, such as their phone, that allows them to approve their login through entering some type of PIN or using biometrics like their fingerprint or a face scan. A mathematical relationship between the public key on the system the user is logging into as well as the private key on the user’s personal device allows the system to verify that the only person logging into the account is the one with the private key.

Avoiding human error, and hackers

From a safety standpoint, passkeys are much more secure than passwords for a number of reasons.

They provide individual authentication for every user to every application — each challenge sent by the server is a new challenge, making the encryption different every time. The mutual authentication that occurs as the server authenticates the user makes them less prone to cybersecurity attacks. Gaining access to the key is much more difficult, since hackers need to access both the public key on the application as well as the private key on the user’s device to be able to get into their account.

A major issue with passwords is that humans tend to use the same or very similar phrases for their passwords across multiple platforms to make them easier to remember, and they often contain personal information. Even worse, choosing simple passwords (think “abc123” or “password”) creates the perfect

PDFmyURL converts web pages and even full websites to PDF easily and quickly.

target for hackers to easily access individuals' accounts. This means that a hacker may be able to get into multiple accounts owned by a user by just figuring out their password for a single website or platform.

Passkeys eliminate this issue since they remove the room for human errors that may become security issues. There is no reuse of passkeys, as each one is unique to each individual user as well as the application.

"You've been warned in the past, don't use passwords between different applications," Moriarty said. "Passkeys by design prevent any reuse, so that you're not going to get exposure if your key for one application is exposed for another because they're completely separate."

There have been some other efforts to have better security around passwords even when not using a passkey, such as using a password manager that securely keeps track of passwords and other sensitive information either in a browser or a separate app. But those applications aren't totally immune from security breaches, as shown in the August 2022 hack of LastPass, one of the world's largest password managers.

But regardless, users should be taking some sort of step to better secure their passwords. The volume of password attacks has soared to an estimated 921 attacks every second, a 74% rise in one year, according to the latest Microsoft Digital Defense Report.

Phishing-resistant authentication will soon be the norm

Most major operating services are now allowing passkey use. Apple's newest update, iOS 16 for iPhones as well as macOS

PDFmyURL converts web pages and even full websites to PDF easily and quickly.

Ventura for Macs, now supports passkeys. Google began rolling out passkey support for Chrome on Android, Windows and macOS in December 2022.

By the end of 2024, the federal government is expected to fully transition to phishing-resistant forms of authentication.

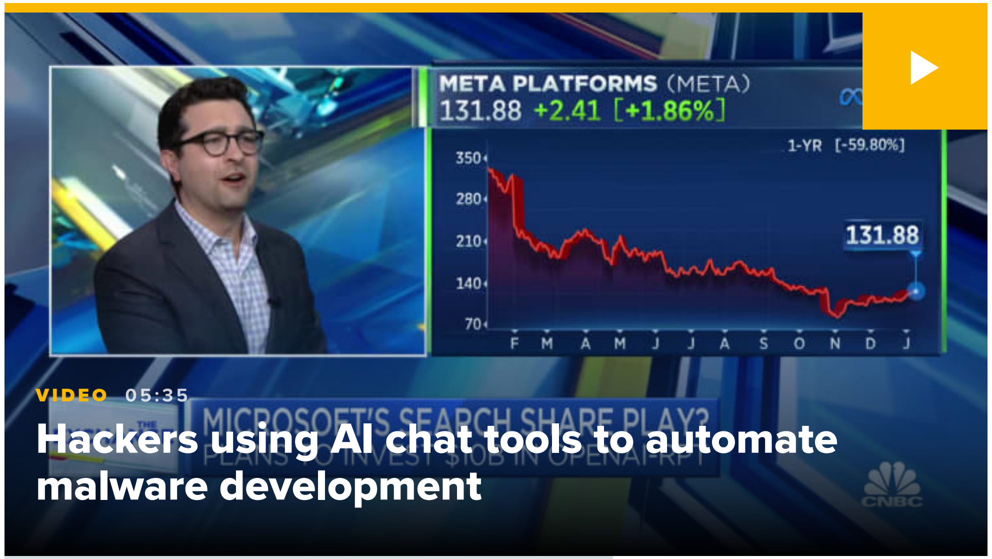
“Major operating systems now have full support where there was only partial support (previously),” Moriarty said. “So this turnaround and push for the support of passkeys is pretty fast now.”

Internet service and device risks

Since passkeys are still a relatively new form of logging into personal accounts, not all services support them yet, though they are becoming a more common feature.

The only potential disadvantage to using passkeys happens if a user loses the secondary device they use to gain access to their accounts. If this occurs, the passkey must be reset, but it is also recommended to have a backup device handy to prevent this problem from occurring.

PDFmyURL converts web pages and even full websites to PDF easily and quickly.



VIDEO 05:35

Hackers using AI chat tools to automate malware development

Meta says it will identify more AI-generated images ahead of...

Hayden Field

Here’s what Meta CEO Mark Zuckerberg has to say about the Apple Vision Pro

Ashley Capoot

Apple’s Vision Pro virtual reality headset launches in U.S.

Alex Koller

READ MORE

PDFmyURL converts web pages and even full websites to PDF easily and quickly.

CNBC

Subscribe to CNBC PRO
CNBC Councils
Join the CNBC Panel
Closed Captioning
Internships
Ad Choices
Careers

Subscribe to Investing Club
Select Personal Finance
Supply Chain Values
Digital Products
Corrections
Site Map
Help

Licensing & Reprints
CNBC on Peacock
Select Shopping
News Releases
About CNBC
Podcasts
Contact

News Tips

Got a confidential news tip? We want to hear from you.

GET IN TOUCH

CNBC Newsletters

Sign up for free newsletters and get more CNBC delivered to your inbox

SIGN UP NOW

Get this delivered to your inbox, and more info about our products and services.

Advertise With Us

PLEASE CONTACT US

Privacy Policy | ✓✕ | CA Notice | Terms of Service

© 2024 CNBC LLC. All Rights Reserved. A Division of NBCUniversal

Data is a real-time snapshot *Data is delayed at least 15 minutes. Global Business and Financial News, Stock Quotes, and Market Data and Analysis.

Market Data Terms of Use and Disclaimers

Data also provided by REFINITIV

PDFmyURL converts web pages and even full websites to PDF easily and quickly.

PDFmyURL