The downsides to using passkeys

By **Martin Brinkmann** | Published 1 year ago

No Comments

Got News? Contact Us

Recent Headlines

Microsoft brings Xbox cloud gaming to Amazon Fire TV: No console required

TP-Link Archer GE800 BE19000 Tri-Band Wi-Fi 7 Gaming Router now available

STM Goods unveils new range of cases for Apple iPad and Microsoft Surface

New nation-state campaigns target government, banking and healthcare

0patch will keep Windows 10 secure for at least five more years after Microsoft abandons it

CISOs believe AI will outpace security teams

Belkin unveils BoostCharge Pro Magnetic Power Bank with MagSafe and Qi2

Most Commented Stories

Say goodbye to Microsoft Windows 11: Nitrux Linux 3.5.0 is the operating system you need!
87 Comments

Say goodbye to Microsoft Windows 11: openSUSE Leap 15.6 is the Linux-based operating system you need!
59 Comments

Say goodbye to Microsoft Windows 11 and hello to Ubuntu-based Linux Lite 7.0
42 Comments

Passkeys is an a relatively new authentication standard by an alliance of companies that reads like the Who's Who of Tech.

Passkeys are created on user devices and remain there, and all it takes to sign-in is to select the right one to login to services and websites. Passwords are no longer required and that is one of the main advantages of the feature.

Passwords are traditionally stored as hashes on servers. When a user enters a password, the hash is generated and compared to the data on the server. This leads to disadvantages, including that a successful server breach may give criminals access to the hashes, which may be cracked to reveal the passwords. Also, passwords may be brute forced and phishing attacks are common to steal passwords from users.

All of these forms of attacks do not work against passkeys. The server does not store the required data anymore and users do not enter passwords. Brute forcing is also not possible.

While passkeys improve security, users need to be aware of some downsides associated with them. Some of these are temporary in nature, others may pose a permanent problem.

1. Passkeys are device specific. Syncing functionality is not widely available yet, but many password managers and also operating systems may support syncing eventually.
2. Most websites and apps do not support passkeys. This too will change in the future as support is spreading. For now, only some sites and services support the security feature.
3. Losing access to a device. If a user loses access to all their devices, they may have troubles recovering account access. Most sites and services support account recovery options if a password has been forgotten. Similar functionality may be provided for passkeys, and this may involve providing IDs or other forms of legitimation. Passkeys to support recovery keys, but these need to be saved by the user actively.

Photo Credit: Dr. Cloud/Shutterstock

'The downsides to using passkeys' first appeared in Weekly Tech Insights, a free weekly newsletter that you can sign up to here.

No Comments Share

Lucky for some -- Windows 13 is everything Windows 11 should be
28 Comments

SDesk ISO 19 released: Say goodbye to Microsoft Windows 11 and hello to Linux
21 Comments

CachyOS June 2024 release makes it easy to say goodbye to Microsoft Windows 11 and hello to Linux
17 Comments

Joe Biden implements Kaspersky ban ahead of debate with Donald Trump, citing national security concerns
17 Comments

Deepin Linux V23 RC2 delivers a kung fu kick from China to knock out Windows 11
16 Comments

Comments are closed.