IDENTITY MANAGEMENT & ACCESS CONTROL ENDPOINT SECURITY

Is Passkey Authentication More Secure Than Traditional Passwords?

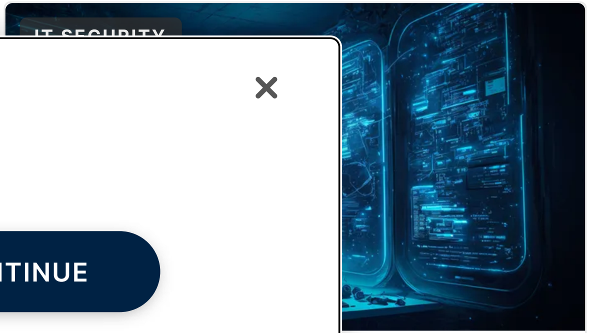
Many organizations are interested in using passkeys instead of conventional passwords, but how much better are they?

Alyse Burnside, Contributor

February 29, 2024

3 Min Read

Editor's Choice



y: Protect and

by **Brien Posey**

About Cookies On This Site

We and our partners use cookies to enhance your website experience, learn how our site is used, offer personalised features, measure the effectiveness of our services, and tailor content and ads to your interests while you navigate on the web or interact with us across devices. By clicking "Continue" or continuing to browse our site you are agreeing to our and our partners use of cookies. For more information see Privacy Policy

CONTINUE

ALAMY

Despite rising concerns about password security and a growing trend towards passkeys and other multifactor authentication tools, passwords remain the primary mode of authentication.

That’s according to the recent Specops Breach Password Report, which surveyed 151 cybersecurity professionals. The survey found that 88% of organizations continue to rely on passwords for authentication.

The prevalence of poor password hygiene and password fatigue contribute to security breaches, prompting some organizations to consider passkeys as an

MAY 21, 2024 5 MIN READ

IT OPERATIONS

How to Get Executive Buy-In for IT Projects

by **Christopher Tozzi**

MAY 28, 2024 6 MIN READ

POWERSHELL

Using ChatGPT as a PowerShell Debugging Tool

by **Brien Posey**

JUN 4, 2024 4 MIN READ

alternative. However, while passkeys offer users a higher degree of security, they do not eliminate all risks.

In a discussion with ITPro Today, cybersecurity experts shared insights on passwords, passkeys, and measures for IT professionals to protect their organizations.

How Much Safer Are Passkeys Really?

Passkeys differ from other forms of authentication by leveraging devices, like an iPhone, to authenticate users via biometric sensors (e.g., a fingerprint or face ID). Based on FIDO Alliance's Web Authn standard, passkeys are tied to the website where they are created and remain localized on the user's device. An advantage of passkeys is that they can prevent breaches resulting from weak password practices, such as using recycled, easily guessed, or compromised passwords. Additionally, passkeys provide convenient access across various devices, minimizing password fatigue.

Passkeys are not entirely foolproof, however. Cybercriminals have evolved their strategies, with session hijacking emerging as a common method for account takeover. "Instead of trying to access a user's login credentials, cybercriminals now use malware-exfiltrated session cookies to launch session hijacking attacks – bypassing passkeys entirely," said Trevor Hilligoss, vice president of SpyCloud Labs.

"Criminals can insert these active cookies into anti-detect browsers, tricking the website into thinking they are the already authenticated user and entirely [bypass] the login process," Hilligoss explained.

This poses a significant risk, especially if session cookies are stolen from corporate devices, potentially granting criminals access to confidential information and bank accounts.

How Can IT Professionals Protect Their Organizations, Passwords, and Passkeys?

IT professionals can take proactive measures, such as early detection, post-remediation efforts, and user education on strong password practices. Additionally, implementing multifactor authentication (MFA) strategies, addressing session hijacking, and adopting centralized authentication through Single Sign-On enhance security.

Organizations are advised to use MFA on every website and application. For added security, users should use MFA methods with a physical token or software-based authenticators rather than less secure methods like text or email-based authentication.

Wolf Goerlich, a faculty member at IANS Research, suggested that IT professionals expand their focus beyond the initial authentication factor. “This should include device identity and posture, and the context and conditions of the request,” Goerlich said. “This risk-based authentication provides a defense against account takeovers by session hijacking, along with other common attack techniques.”

Goerlich also recommended that development teams pay attention to session handling, giving careful consideration to the detection and prevention of session hijacking.

For passkey security, IT professionals can enhance measures by regularly rotating API passkeys and enforcing least privilege policies, noted Eric Schwake, the director of cybersecurity strategy at Salt Security. Additionally, Schwake suggested using a secure storage mechanism like a dedicated passkey vault.

Other steps for enhancing the security of passkeys include vigilance against suspicious behavior that could indicate passkey misuse. This calls for staying informed about passkey security best practices, detection and reporting, and the constantly changing landscape threat. Above all, it is important to recognize that security measures must continually evolve to keep pace with the increasing sophistication of threats.

About the Author(s)

Alyse Burnside

Contributor, ITPro Today

Alyse Burnside is a writer and editor living in Brooklyn. She is working on a collection of personal essays about queerness, visibility, and the hyperreal. She's especially interested in writing...

You May Also Like