What Are the Pros & Cons of SWITCHING FROM PASSWORDS TO PASSKEYS?

B-COMPSERVICES
IT SOLUTIONS AND SUPPORT

Strong, unique passwords are an important part of any online security strategy. This is because they keep our accounts safe as long as they are strong enough. However, in recent times, passwords have

Search...

come to be the not-so-best option for online security. While they do provide some form of security, they have distinct disadvantages, and those disadvantages are frequently exploited by hackers.

According to Finance Online, 81% of company data breaches are caused by poor passwords. This is why many security experts now recommend that business owners, employees, and individuals move away from passwords and toward passkeys.

Although passkeys provide similar benefits to passwords, they are more secure. They are the new passwordless authentication method that may eventually replace traditional passwords, due to their high safety features.

Developed by companies such as Apple, Google, and Microsoft to improve security and make logging in more convenient, passkeys are the way of the future in basic internet security. This is why the call to switch from passwords to passkeys is being made. However, switching to passkeys from passwords has its pros and cons.

Read on to understand the pros and cons of switching from passwords to passkeys.

Pros of Switching from Passwords to Passkeys

Passkeys are a password-replacement authentication technology, and there are numerous benefits to using passkeys instead of passwords. Here are some of the pros of switching to passkeys:

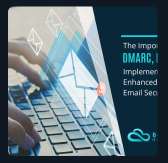
It's a bit more tricky to attack than a password

Passkeys have the advantage of being much more difficult to crack than passwords. Each passkey is distinct and linked to the user's device via a public/private cryptographic pair, making it much more difficult for an attacker to gain unauthorized access without physical possession of the device.

Improves cybersecurity strategy

Passwordless authentication improves business cybersecurity by effectively reducing data and identity theft caused by unauthorized access when compared to password authentication. Password security risks are heavily reliant on user password authentication, which passwordless authentication

Latest Post

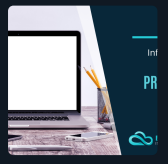

Importance of Implementing Enhanced Email Security
May 29, 2024

Navigating the IPv6 Landscape: Trends, Challenges, and Strategies
May 3, 2024


The Role of Computer Support Services in Enhancing Business Efficiency Through Automation
April 19, 2024


Navigating the Cybersecurity Threat Landscape: Strategies for Prevention and Mitigation
April 5, 2024


Effective Remote Work Solutions: Maximizing Productivity with Computer Support Services
March 22, 2024


Optimizing IT Infrastructure for Enhanced Productivity
March 8, 2024

successfully reduces. Also, the absence of passwords eradicates the need for organizations to manage password storage and meet password regulation requirements.

Smooth user experience

Passkeys enable users to sign in without a password in a convenient and secure way. Nowadays, users have multiple accounts with different businesses based on their needs, and remembering all of these passwords has become challenging for them. As a result, they frequently forget and reset passwords, resulting in an unpleasant user experience.

However, with passkeys, users no longer need to create or remember complex passwords. Instead, they can authenticate using their mobile, email, or biometrics, making logins more seamless, thereby improving the overall experience.

Every passkey is strong by default

You don’t have to manually generate anything or worry about whether your private key is long enough or random enough. All you have to do is to generate an account and request that your authenticator generate a secure public and private key pair on your behalf.

Future-proof

Passkeys are expected to become more common in the coming years as more businesses will use them as a more secure alternative to passwords. Passkeys allow users to future-proof their online security by avoiding the need to constantly update and change their passwords as security threats evolve.

Convenient to use

Another advantage of switching to passkeys is that they are more suitable to use than passwords. Users don’t need to remember long complex passwords, they can log in to their accounts more speedily and easily. This saves time and reduces frustration, especially for users who manage dozens of online accounts. Passkeys can be used for more than just logging into accounts, such as encrypting emails or signing digital documents, making them a versatile online security tool.

Lower long-term costs

Passwordless authentication saves businesses money on unnecessary password costs. The amount of money and effort spent by businesses on password storage and administration is referred to as password-related costs. This includes the time IT spends dealing with the constantly changing legal requirements for password storage and password resets.

Cons of Switching From password to Passkeys

While there are numerous advantages to using passwordless logins, they are by no means perfect. There are still some things you need to keep in mind. Here are some of the potential downsides to passkeys:

The Learning Curve

Passkeys are a new and unfamiliar technology for many users, making it difficult for them to adopt and integrate this method into their daily routines. Users may need to learn how to use their passkey device and adjust to the new authentication process, which can be time-consuming and frustrating.

Biometrics Issue

Because passkeys can only be created using biometrics, there may be a problem verifying your account. To use it, you have to make sure your fingers are clean. The same is applicable to the user's face. Another concern is that passkeys may be more difficult to use for users with disabilities or older devices. As users with limited mobility may struggle with biometric authentication, and older devices may not support the most recent passkey technologies.

Passkey is not supported by all websites or applications

Not all websites and apps support passkey authentication, therefore, this method may be ineffective for some users. Depending on the websites and apps that users use, they may need to use multiple authentication methods (such as passwords and passkeys), which can be confusing and inconvenient.

Cost

Passkeys are more expensive than passwords because the user is needed to buy a separate device to store their passkey. While some passkey devices are reasonably priced, others can cost hundreds of dollars, which may be prohibitively expensive for some users. Passkeys are also more overwhelming to set up and use than passwords because they necessitate the use of specialized software and hardware.

Go Passwordless to Secure Your Account

B-Comp Services can help you switch from passwords to passkeys to protect your business and employees against various forms of cyber-attack. Contact us to learn more.

B-COMPSERVICES
IT SOLUTIONS AND SUPPORT
uce@b-compservices.com

B-COMPSERVICES
IT SOLUTIONS AND SUPPORT

B-Comp provides Managed IT Services & Support, Cloud Migration & Management, Cybersecurity and Virtual CIO (vCIO) services to businesses throughout the United States.

Services

- Managed IT Services
- Cloud Services
- Cybersecurity
- Virtual CIO (vCIO)
- Web Design

Support

- Get Connected
- Ticket Support
- FAQ
- Contact us

Company

- About Us
- Leadership
- Careers
- Articles & News

Site by B-Web Services

Accessibility Statement Privacy Policy