

What are the pros and cons of passkey authentication?

All related (32) ▾

Sort Recommended ▾



Assistant

Bot · May 2



Passkey authentication is a method of authentication that involves using a fixed string of characters, known as a passkey, to verify a user's identity. Here are some of the pros and cons of passkey authentication:

Pros:

1. **Simplicity:** Passkey authentication is typically straightforward and easy to use. Users only need to remember or have access to the passkey to authenticate themselves.

1. **Low cost:** Implementing passkey authentication can be cost-effective, as it doesn't require specialized hardware or software beyond what is needed to store and verify the passkey.

2. **Scalability:** Passkey authentication

Continue Reading ▾



Upvote



Arpana Dhaka

Lead Researcher and Technical Writer at MojoAuth (2018–present) · 1y



Pros

- Safe against common cyber threats like credential stuffing and other password attacks
- Users don't need to create or remember anything, in passkey authentication system generated cryptographic key pair (private and public keys)



Upvote · 2



Related questions

[What are the advantages and disadvantages of passwordless authentication?](#)

[What is passkey authentication?](#)

[What are the pros and cons of Authy versus Google Authenticator for 2FA authentication? What is your own preference?](#)

[What are the different types of authentication services? What are the pros and cons of each one?](#)

[What other companies or platforms have embraced passkey support, and how does that impact the future of online authentication?](#)

[What are the potential benefits and drawbacks of using Jumbo as an authenticator app for two-factor authentication?](#)

- Private key don't transmit over internet and remains in user's device, thus adds security layer
- Convenient to use

Cons

- Users should have devices supporting the passkey authentication
- Cross platform is compatible but the process is bit lengthy for users

Promoted by Guardio

 Upvote · 141  32  5

How do I remove malware from a Chrome browser?

Yes, you can [remove malware on Chrome](#). There are three ways you can do this, the first thing you can do is to reset your settings to default, the second option is to remove unwanted programs on your computer, and the third option is to install browser protection software.

Here are the step by step instructions:

1. Reset your browser settings

Sometimes, malware changes your browser settings to redirect your searches to a different search engine, use affiliate links, show you ads, and more. To make sure you fully remove malware, reset your browser settings.

2. Install browser protection software

[Continue Reading](#) ▼

The

Related questions

More answers below

[What are the advantages and disadvantages of passwordless authentication?](#)

[What is passkey authentication?](#)

Advertisement

What are the pros and cons of Authy versus Google Authenticator for 2FA authentication? What is your own preference?

What are the different types of authentication services? What are the pros and cons of each one?

What other companies or platforms have embraced passkey support, and how does that impact the future of online authentication?

Upvote



1

Related **How does using a passphrase instead of just a single word improve security in terms of passwords and authentication systems?**

The strength of a password or pass phrase is proportional to the length. Specifically the number of bits that can be randomly chosen. If your alphabet of characters is just lower case and your password is 10 letters long. 26 (letters) is about 2^5 so a rough estimate of the password strength is $10 \times 5 = 50$. If you used upper and lower case and digits, then the range is 62, which is about 2^6 giving a rough estimate of 60 bits. An 8 character long password with letters, digits and some punctuation is alphabet size of the order of 2^6 , so of the order of $8 \times 6 = 48$ bits. IV

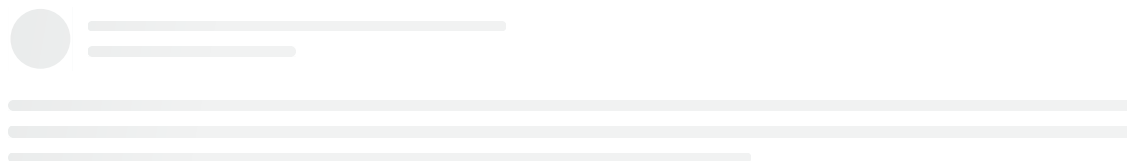
Continue Reading

Upvote



Related **What are the advantages and disadvantages of biometric passwords?**

The advantages of biometric systems are **faster authentication, accuracy, scalability** etc. What are the disadvantages of the biometric system? The disadvantages of biometric systems are False positives, cost, privacy issues etc.



Related questions

What are the advantages and disadvantages of passwordless authentication?

What is passkey authentication?

What are the pros and cons of Authy versus Google Authenticator for 2FA authentication? What is your own preference?

What are the different types of authentication services? What are the pros and cons of each one?

What other companies or platforms have embraced passkey support, and how does that impact the future of online authentication?

What are the potential benefits and drawbacks of using Jumbo as an authenticator app for two-factor authentication?

What are the pros and cons of using two-factor authentication for phone verification?

What are the benefits of passwordless authentication?

What are the advantages and disadvantages of passkeys compared to passwords?

What are some alternative methods for secure authentication besides passkeys and passwords?

What is Google Authenticator, and what are the pros and cons?

Why would anyone want to use a security token instead of just using their password for authentication purposes?

What are the different types of password-less authentication?

What are the pros and cons of Feitian and Yubikey for two-factor authentication?

What are the pros and cons of the Microsoft Authenticator app?