Passwords vs Passkeys (Which One is Better?)

April 8, 2023 by Glen Michaelson

In today's digital age, the importance of passwords and passkeys cannot be overstated. With an increasing

SERVICES

- VoIP Services
- Computer Repair
- Network Support
- Data Recovery
- Managed Services
- Office 365
- 24/7 Monitoring

number of online accounts and sensitive information stored on our devices, keeping our data secure has become a top priority.

Passwords and passkeys are the most common methods used to protect digital information. However, the question of which one is better still remains.

In this article, we'll explore the differences between passwords and passkeys, and their respective advantages and disadvantages. By the end of this article, you'll be able to decide which one is better suited for your specific needs.

What are Passwords?

Passwords are a **series of characters, such as letters, numbers, and symbols, that are used to authenticate a user's identity.** They are typically used to secure online accounts, devices, and applications. The user sets the password, and it must be entered correctly to gain access to the protected system.

Passwords are the most commonly used method of authentication. They are easy to create and use, and users can choose a password that is easy to remember.

Managed Cybersecurity Services

FOLLOW US

However, passwords have a few drawbacks. Firstly, they are susceptible to brute force attacks, where an attacker tries to guess the password by trying different combinations of characters. Secondly, passwords can be easily forgotten, and users may have to reset their passwords, which can be time-consuming and frustrating.

What are Passkeys?

Passkeys, on the other hand, are a relatively new concept. They are a type of **passwordless authentication that uses public and private key cryptography to authenticate a user's identity.**

Passkeys work by generating a unique key pair, which is made up of a public key and a private key. The public key is stored on the server, and the private key is stored securely on the user's device.

To authenticate a user, the server sends a challenge to the user's device, which is signed with the user's private key. The signed challenge is then sent back to the server, which verifies the signature using the public key. If the signature is valid, the user is authenticated, and access is granted.

Passkeys are more secure than passwords, as they are not susceptible to brute force attacks. Additionally, they eliminate the need for users to remember passwords, which can be a significant advantage. But passkeys require the use of specialized hardware or software, and their implementation can be more complicated than passwords.

Advantages of Passwords

Passwords have been the standard method of authentication for decades, and they still have a few advantages over other methods. Here are some of the advantages of using passwords:

1. **Easy to Use:** Passwords are easy to create and use. Users can choose a password that is easy to remember and fits their preferences.
2. **Widely Accepted**: Passwords are the most commonly used method of authentication, and they are accepted by most online services and applications.
3. **No Special Hardware Required:** Passwords do not require any special hardware or software, making them accessible to all users.
4. **Flexible**: Passwords can be changed at any time, providing users with a level of flexibility that other

authentication methods may not offer.

Disadvantages of Passwords

Despite their advantages, passwords have a few significant disadvantages. Here are some things to consider before using them:

1. **Susceptible to Brute Force Attacks:** Passwords can be easily cracked through brute force attacks, where an attacker tries to guess the password by trying different combinations of characters.
2. **Easily Forgotten**: Passwords can be forgotten, which can result in users having to reset their password, which can be time-consuming and frustrating.
3. **Easily Stolen**: Passwords can be stolen through phishing attacks or by using malware to capture keystrokes.
4. **Not as Secure:** Passwords are not as secure as other authentication methods, such as passkeys or biometric authentication.

Advantages Of Passkeys

Passkeys offer a few distinct advantages over passwords, including:

1. **More Secure**: Passkeys are more secure than passwords because they use public and private key cryptography. Passkeys are not susceptible to brute force attacks, and they are resistant to phishing attacks.
2. **No Need to Remember Passwords:** Passkeys eliminate the need for users to remember passwords. This can be a significant advantage, especially for users who have a lot of online accounts.
3. **Easy to Use:** Passkeys are easy to use. Users only need to have access to the device where the private key is stored to authenticate themselves.
4. **More Convenient:** Passkeys are more convenient than passwords because they can be used on multiple devices without having to remember multiple passwords.

Disadvantages of Passkeys

Here are some of the disadvantages of using passkeys:

1. **More Complicated to Implement:** Passkeys require the use of specialized hardware or software

to generate and store the key pair. This can be more complicated to implement than passwords.

2. **Requires Specialized Hardware or Software**: Users need to have access to specialized hardware or software to use passkeys. This can be a barrier for some users.
3. **Limited Adoption:** Passkeys are a relatively new concept and have not been widely adopted yet. This may change in the future as more online services and applications start to support passkeys.

Get Password and Passkey Support

Both passwords and passkeys have their advantages and disadvantages. Passwords are easy to use and widely accepted, but they are susceptible to brute-force attacks and can be easily forgotten. Passkeys are more secure and eliminate the need for users to remember passwords, but they require specialized hardware or software and can be more complicated to implement.

Ultimately, the choice between passwords and passkeys will depend on your specific needs and circumstances. If you prioritize **convenience and accessibility**, passwords may be the best option for you. If you prioritize **security and don’t mind the additional complexity**, passkeys may be the better option.

Whichever option you choose, it’s essential to practice good password hygiene. This includes using strong passwords or passphrases, not reusing passwords, and enabling two-factor authentication when possible.

If you need help securing your online accounts or devices, don’t hesitate to **contact Connect2Geek**. Our team of experts can provide guidance on password management and security best practices for bulletproof data protection.

Filed Under: Blog Post

Share: