Passwords vs Passkeys

Last Updated : 08 May, 2024

Passwords are generated by the individual user, whereas passkeys are generated automatically by public key cryptography. It’s strongly suggested that a password is secret, usually paired with a username to provide authentication. Passkeys are not only phishing-resistant but also error-proof. Users cannot make mistakes while generating a passkey, as they may when creating passwords.

What is a Password?

A password is a string of characters used to access online accounts in conjunction with a username. They are collectively known as your login credentials. Strong passwords differ in length and include a mix of upper and lowercase characters, digits, and symbols. A longer and more complicated password will better protect an account.

How Does a Password Work?

- Passwords are used for authentication to the apps or websites, therefore they are extensively supported across several systems and platforms.
- Passwords are often saved on servers, either unencrypted or hashed.
- The user enters a password during authentication, which is then

Benefits of Passwords

- **Ease of implementation:** Password-based authentication is simple for service providers to deploy and does not require specific infrastructure.
- **Accessibility:** Passwords are simple to share or convey, allowing numerous individuals to access accounts or in emergency scenarios.
- **Incremental security measures:** Two-factor authentication (2FA) can be easily combined with passwords to provide additional safety.
- **Familiarity and compatibility:** Passwords have been the main factor of authentication technique for decades, therefore they are extensively supported across a variety of systems and platforms.

What is Passkey?

A passkey is an innovative way to enter into online accounts without using a password. To understand what a passkey is, you must first understand how they function. A passkey consists of both a private and a public cryptographic key. The firm with which you created your account stores the public key, while the private key is kept locally on the device used to generate the passkey.

Benefits of Passkeys

- **Fast signing:** Passwords are four times easier to use since they do not need memory or typing. Simply use your fingerprint, face scan, or screen lock to sign in across all of your devices and platforms.
- **Convenience and usability:** Passkey provides a smooth and user-friendly authentication experience, reducing the user's need to memorize complicated passwords.

- **Enhanced security:** Passwords are not susceptible to common attacks such as phishing or reusing, resulting in improved security. There are no weak or reused passkeys.
- **Reduced reliance on servers**: Since passkeys are not saved on servers, they are less vulnerable to massive data breaches.

How Does a Passkey Work?

- Passkeys employ Bluetooth technology. Bluetooth requires proximity to validate the user.
- After logging in and connecting accounts, the device receives a push notice over Bluetooth. The user must then unlock their device using their private key, which may be either biometric authentication or a PIN, to generate a unique public key associated with their login.
- At the next login, the user will just need to provide the selected credential when requested, which is their private identifier no password to remember. The passkey option will show in the username box.

Difference Between Passwords and Passkeys

Passwords	Passkeys
A password is a string of characters widely used to access online accounts in conjunction with a username.	A passkey is an innovative way to enter into online accounts without using a password.

Passwords can be words, phrases, characters, digits, or a combination.	Passkeys are set using biometrics or PINs.
Encrypted or hashed passwords are stored on the application server.	In passkey, The public key is stored on the application server and the private key is saved in a secure wallet.
It is not secure against password-based attacks.	It is secure against password-based attacks.

Are Passkeys More Secure Than Passwords?

Passkeys are more secure than passwords. Passkeys are not only phishing-resistant but also error-proof. Users cannot make mistakes while generating a passkey, as they may when creating passwords. Passkeys, in addition to being phishing-resistant and error-proof, have been created to facilitate Two-Factor Authentication (2FA). It is a secondary authentication method that should be activated on all online accounts whenever available.

However, because passkeys are associated with the devices on which they are produced, maintaining them across several operating systems and device types is complex.

Conclusion

In this article, we have learned about passwords and passkey. Passwords can be words, phrases, characters, digits, or a combination and Passkeys are set using biometrics or PINs.

Frequently Asked Questions on Passwords and Passkeys – FAQs

Do passkeys work without the Internet?

No, you do not need an internet because it is stored on your local device. You can unlock your computer using a passkey from your phone.

Can passkeys be used on multiple devices?

Once activated, a Passkey is saved to your cloud service account. You can use Passkey on all devices linked to that account.

Do passkeys require Bluetooth?

A Bluetooth connection is not required you are logging in to an account using the same device to generate your passkey.

Can passkeys be hacked?

Yes, Someone can utilize your passkey and get access to your device.

How safe is Passkey?

Passkeys are more secure than passwords. Passkeys are not only phishing-resistant but also error-proof.

D dido...

Next Article

OTP vs Passwords

Similar Reads

What are Different Types of Passwords used in Securing Cisco...

Passwords are an essential part of the cisco router access control methods. These are used to restrict access to a CISCO router; As there...

4 min read

How to encrypt passwords in a Spring Boot project using Jasypt

In this article, we will learn how to encrypt data in Spring Boot application config files like application.properties or application.yml....

🕓 4 min read

Passwords and Cryptographic hash function

We have introduced and discussed importance of hashed passwords. To create strong hashed passwords, we must understand some...

🕓 3 min read

3D passwords-Advanced Authentication Systems

The increase in the usage of computer systems has given rise to many security concerns. One of the major security concern is authentication,...

🕓 2 min read

Advantages and Disadvantages of Long Passwords

Long Passwords are generally preferred by many people in the field of digital security. Long passwords remain effective in protecting comput...

🕓 6 min read

View More Articles

Article Tags : cryptography Computer Networks

GeeksforGeeks
Sanchhaya Education Private Limited

A-143, 9th Floor, Sovereign Corporate Tower, Sector-136, Noida, Uttar Pradesh - 201305

Company

- About Us
- Legal
- In Media
- Contact Us
- Advertise with us
- GFG Corporate Solution
- Placement Training Program

Explore

- Hack-A-Thons
- GfG Weekly Contest
- DSA in JAVA/C++
- Master System Design
- Master CP
- GeeksforGeeks Videos
- Geeks Community

Languages

- Python
- Java
- C++
- PHP
- GoLang
- SQL
- R Language
- Android Tutorial
- Tutorials Archive

DSA

- Data Structures
- Algorithms
- DSA for Beginners
- Basic DSA Problems
- DSA Roadmap
- Top 100 DSA Interview Problems
- DSA Roadmap by Sandeep Jain
- All Cheat Sheets

Data Science & ML

- Data Science With Python
- Data Science For Beginner
- Machine Learning Tutorial
- ML Maths
- Data Visualisation Tutorial
- Pandas Tutorial
- NumPy Tutorial
- NLP Tutorial
- Deep Learning Tutorial

HTML & CSS

- HTML
- CSS
- Web Templates
- CSS Frameworks
- Bootstrap
- Tailwind CSS
- SASS
- LESS
- Web Design

Python Tutorial

- Python Programming Examples
- Python Projects
- Python Tkinter

Computer Science

- Operating Systems
- Computer Network

DevOps

- Git
- AWS
- Docker
- Kubernetes
- Azure

Competitive Programming

- Top DS or Algo for CP
- Top 50 Tree
- Top 50 Graph

System Design

- High Level Design
- Low Level Design
- UML Diagrams
- Interview Guide
- Design Patterns

JavaScript

- JavaScript Examples
- TypeScript
- ReactJS
- NextJS

- Web Scraping
- OpenCV Tutorial
- Python Interview Question
- Django

- Database Management System
- Software Engineering
- Digital Logic Design
- Engineering Maths

- GCP
- DevOps Roadmap

- Top 50 Array
- Top 50 String
- Top 50 DP
- Top 15 Websites for CP

- OOAD
- System Design Bootcamp
- Interview Questions

- AngularJS
- NodeJS
- Lodash
- Web Browser

Preparation Corner

- Company-Wise Recruitment Process
- Resume Templates
- Aptitude Preparation
- Puzzles
- Company-Wise Preparation

School Subjects

- Mathematics
- Physics
- Chemistry
- Biology
- Social Science
- English Grammar
- World GK

Management & Finance

- Management
- HR Management
- Finance
- Organisational Behaviour
- Marketing

Free Online Tools

- Typing Test
- Image Editor
- Code Formatters
- Code Converters
- Currency Converter
- Random Number Generator
- Random Password Generator

More Tutorials

- Software Development
- Software Testing
- Product Management
- SEO - Search Engine Optimization
- Linux
- Excel
- All Cheatsheets

GeeksforGeeks Videos

- DSA
- Python
- Java
- C++
- Web Development
- Data Science
- CS Subjects