RESOURCE CENTER

What is an OTP?

Get the full interactive view at
https://bitwarden.com/resources/what-is-an-otp/

bitwarden

What does OTP mean in security and passwords?

You may have seen the term OTP, or one-time password, when logging into a bank account, email, or social media platform. In the world of digital security, OTPs help protect your accounts by providing an extra layer of verification during login or transactions.

Understanding how OTPs work and how to manage them securely can help keep your personal information safe online. Tools like Bitwarden make it easier to use and store OTPs alongside your passwords, so you don't have to choose between security and convenience.

What is an OTP, and why does it matter?

A one-time password is exactly what it sounds like: a temporary code that can only be used once. There are two types. The one most people are familiar with is timed one-time passwords, TOTPs. They are usually sent to your email, phone, or generated by an app. TOTPs expire after a short period and are part of a security method called multi-factor authentication (MFA).

Multi-factor authentication combines something you know, like your password, with something you have, like a one-time code. This makes it much harder for someone else to access your account, even if they know your password.

Common types of one-time passwords

There are two main kinds of OTPs you might come across:

- Time-based one-time passwords (TOTP): These refresh every 30 to 60 seconds and are typically generated by authenticator apps like Bitwarden Authenticator. They're often used for banking, email, and other services where timing is key.
- HMAC-based one-time passwords (HOTP): These hash-based message authentication codes only change when requested — usually when you log in — and stay valid until used. These are often used as emergency recovery codes for logging in.

Both types offer strong protection because they are temporary and can't be reused. That means even if someone gets access to an old code, it won't work again.

Why OTPs are safer than static passwords alone

Unlike a regular password that stays the same until you change it, OTPs are designed to be short-lived. Their single-use nature reduces the risk of someone reusing a stolen password or guessing their way into your account. OTPs are a key part of making sure your accounts are protected — even if your account password is compromised.

Where you might use an OTP

One-time passwords are often used during logins that involve sensitive information. For example:

- Using government services online
- Logging into financial accounts
- Accessing health records
- Changing account settings
- Logging into social accounts
- Signing into email from a new device
- Making online purchases

In each case, the OTP adds an extra checkpoint to verify your identity.

How OTPs are delivered

You might receive an OTP in different ways:

- **Hardware security keys (most secure)**: Physical devices that generate codes and must be in your possession.
- **Authenticator apps (very secure)**: These work offline and generate codes directly within the software. Bitwarden offers two options:
  - The standalone Bitwarden Authenticator app for iOS and Android
  - Integrated TOTP generation within Bitwarden Password Manager for Premium, Families, Teams, or Enterprise users
- **Email (secure)**: A code sent to the email associated with the account. Make sure this email account is protected by a strong and unique password and two-factor authentication!
- **SMS text messages (less secure)**: A text sent to the phone number associated with the account.

Users often prefer authenticator apps because they work offline and are more secure than SMS-based codes, which can be vulnerable to SIM swapping and interception.

Common OTP challenges and solutions

Users might encounter practical challenges even when they understand OTP and its benefits. Fortunately, the right tools can address these issues.

Too many apps to manage?

Bitwarden Premium integrates TOTP generation with password management, allowing autofill of both passwords and OTP codes.

Need for quick access?

TOTP codes are easily accessible at the top of the Bitwarden mobile app, and premium Bitwarden users with Apple Watches can view TOTP codes directly on their watch.

Concerns about losing access?

Users can easily export TOTP seeds from Bitwarden for backup purposes.

Switching between devices?

Bitwarden automatically syncs TOTP secrets across all devices.

Best practices for using OTPs

Users should consider the following recommended practices to maximize what OTP means for security while minimizing potential hassles.

- Set up TOTPs by scanning QR codes in the Bitwarden mobile app or manually entering the TOTP seed.
  - The Bitwarden browser extension also has a camera icon that can scan on-screen QR codes.
- Use the Bitwarden autofill capability to streamline the login process.
- Consider the standalone Bitwarden Authenticator for those who prefer a dedicated app.
- Regularly export TOTP seeds as a backup precaution.
  - When using the integrated Bitwarden solution, TOTP are included in password manager backups.

Make sure to save a backup of TOTP seeds to ensure continuous access to accounts. Following these guidelines helps maintain strong password practices while keeping the authentication process smooth and trouble-free.

How OTPs fit into your security strategy

OTPs are just one piece of a strong security setup. Combine them with a password manager, strong and unique passwords, regular software updates, and secure sharing practices. This layered approach gives you better protection against account takeovers and phishing attacks.

How Bitwarden helps you use OTPs

Bitwarden makes implementing OTP for enhanced security easy with two approaches that simplify your workflow, especially if you're juggling multiple accounts, and help you stay consistent with your security habits.

Standalone Bitwarden Authenticator

The standalone Bitwarden Authenticator is an open source mobile app for iOS and Android that generates 6-digit TOTPs. It works independently of the password manager, enabling easy QR code scanning to set up 2FA.

Bitwarden Password Manager built-in authenticator

For an all-in-one solution, the Bitwarden Password Manager includes integrated TOTP functionality for Premium, Families, Teams, or Enterprise users. This integration automatically generates and fills TOTPs during login, streamlining the authentication process.

The autofill feature works seamlessly with the Bitwarden browser extensions and mobile apps. Examples include integrating TOTP generation directly into Bitwarden Password Manager and automatically filling both the password and current TOTP code.

Take the next step with OTP security

Adding OTPs to your login process doesn't have to be complicated. With Bitwarden, you can keep all your login information, including your one-time passwords, in one secure place.

Discover the integrated authenticator solution. For those who prefer a separate authenticator app, the open source Bitwarden Authenticator provides a robust solution for managing 2FA needs.

Get started with Bitwarden today to better protect what matters most with OTP security. Feel the peace of mind that comes with knowing your accounts are secure.