ONLINE SAFETY AND PRIVACY
MAR 9, 2026 | 5 MIN READ

What Is Multifactor Authentication (MFA) And How Do You Enable It?

Today, when you protect an online account with just a password, you’re relying on a single lock in a world full of sneaky digital lockpickers.

Multifactor authentication (MFA) adds a powerful extra layer of security to your accounts. This is because even if someone steals or guesses your password, MFA will stop them in their tracks their tracks.

What is multi-factor authentication?

Multifactor authentication (MFA) is a login security method that requires two or more forms of identity verification to access an account. One "factor" is usually your password, and then you can often choose the other factor.

You may also hear MFA called:

- Two-factor authentication (2FA)
- Two-step verification

They all refer to the same idea: protect yourself with more than just a password.

Why passwords alone aren’t enough

Due to sophisticated hackers, giant data breaches, and, sometimes, our own less-than-great habits, passwords can be:

- Guessed
- Reused across multiple sites
- Leaked in data breaches
- Stolen through phishing scams
- Captured by malware

Even super-strong passwords (over 16 characters long) can be compromised if a website is breached – and it had nothing to do with your amazing cyber habits.

MFA protects you by requiring a second proof of identity. So even if a criminal has your password, they still can’t get into your account. While no defense is perfect, MFA dramatically reduces your risk. Think of it this way: you're doubling up your login setup, and you essentially double your security in many ways.

How does multifactor authentication work?

When you enable MFA, your login process adds one extra step:

- Enter your username and password.
- Verify your identity a second way.

verify your identity a second way.

That second factor might be:

- A one-time code sent to your phone number or email address
- A one-time code or approval generated in an authenticator app
- A fingerprint or facial scan
- A physical security key
- An approval notification generated by your device

Some apps, like banking apps, might have MFA built into their platforms – like you approve a log-in for your bank's website through its app on your phone.

Most modern MFA systems take only a few seconds. While it slows us down slightly, that inconvenience adds enormous protection.

3 CATEGORIES OF AUTHENTICATION FACTORS

Security experts group authentication methods into three categories:

1. **Something you know**

   - Passwords
   - PINs
   - Security questions

1. **Something you have**

   - An authenticator app
   - Hardware security keys
   - Your smartphone

1. **Something you are**

   - Fingerprint

- Fingerprint
- Facial recognition
- Voice recognition

MFA combines factors from different categories. For example:

- Password (something you know) + authenticator app (something you have)
- Password (something you know) + fingerprint (something you are)

RANKING TYPES OF MFA

Not all MFA methods are equal. We have favorite factors!

1. **Passkeys**

   Passkeys are phishing-resistant and passwordless (yes, truly). They use cryptographic keys stored on your device (something you have) and typically require biometric verification (something you are).

1. **Hardware security keys**

   Physical devices (like USB or NFC keys) that must be plugged in or tapped during login. Extremely resistant to phishing. However, you must maintain (i.e., not lose) these keys.

1. **Authenticator apps**

   Apps like Google Authenticator, Microsoft Authenticator, or Duo generate time-based codes or push approvals. Strong and widely recommended.

1. **SMS text message codes**

   This form of MFA is common and better than nothing, but it is vulnerable to SIM-swapping and phishing.

1. **Email codes**

   Like text message codes, email codes are convenient, but less secure if your email account itself isn’t protected. Always turn MFA on for your email service!

Security questions

This is an old but still common form of MFA that is based on two things you know – your password and your answer to a personal question. The answers, though, are often based on information that can be guessed or found online. We don't recommend these as a second factor.

If you can, choose passkeys, hardware keys, or authenticator apps.

What is a passkey?

We say passkeys are the future of login security. A passkey is a passwordless authentication method that uses:

- A cryptographic key stored on your device
- Biometric verification (like fingerprint or Face ID)
- Or device-based approval

Unlike passwords, passkeys cannot be guessed, reused, or phished in the traditional sense. They’re built on industry standards designed to eliminate many common attack methods.

In many ways, passkeys function as a highly secure form of multifactor authentication without requiring a traditional password.

If a website offers you the option to create a passkey, take it. They are:

- Easy to use
- More secure than passwords
- Resistant to phishing
- Designed for a passwordless future
- Really simple to set up, generally

Where should you enable MFA?

Turn on MFA everywhere you can.

Start with your most sensitive accounts:

- Email

- Banking and financial apps
- Investment and retirement accounts
- Cloud storage
- Social media
- Online shopping sites
- Work and school accounts

Almost every account today contains personal data worth protecting.

If MFA is available, turn it on.

Can MFA be hacked?

MFA is extremely effective — but not invincible. There are some ways criminals try to bypass MFA.