

Turn on multi-factor authentication



Protect your personal information and accounts with multi-factor authentication (MFA), also known as two-step verification. MFA is a secure way to verify your identity with more than a username and password when you sign in to online accounts.

WHAT YOU CAN DO

Turn on MFA whenever possible for each of your online work, school, and personal accounts or apps – bank, credit card, email, healthcare, online retailers, and social media.

Set up MFA on your accounts

- Go to Settings. It may be called Account Settings, Settings & Privacy, or something similar.
- Look for and turn on MFA. It might be called two-step verification or two-factor authentication.
- Confirm your MFA option. Select how you want to provide extra login security, such as by entering a code sent via text or email, or by using facial recognition.
- After setting up MFA, logging in might require you to complete the MFA security step each time. While it's an extra step, it only takes a few moments, and it makes your account significantly safer from cyber criminals.

MFA FACTORS

MFA is a security measure that requires users to provide two or more forms of proof or verification to access an app or online account:



Something you know

A password, passphrase, or personal identification number (PIN).



Something you have

A code from a key fob, authenticator application, text, or email.



Something you are

A user ID, your fingerprint, or facial recognition.

