



Stay **safer** with **MULTIFACTOR AUTHENTICATION** (MFA)

How to turn on MFA

MFA provides extra security for our online accounts and apps. This security could be a code sent via text or email or generated by an app, or biometrics like fingerprints and facial recognition. Using MFA confirms our identities when logging into our accounts.

Follow these easy
steps on each
account



Go to Settings. It may be called Account Settings, Settings & Privacy or similar.

Look for and turn on MFA. It may be called two-factor authentication, two-step verification or similar.

Multifactor Authentication



Confirm. Select how to provide extra login security, such as by entering a code sent via text or email or using facial recognition.

Congratulations!

After setting up MFA, logging in may require completing the MFA security step to prove our identities. It only takes a moment but makes us **significantly safer from malicious hackers!**

Turn on MFA for every online account or app that offers it. Doing so will protect our:



Email



Banking



Social Media



Online Purchases



Identities

Using MFA is one way to
Secure Our World.



We can all help one another stay safer online, so share these tips with a family member or friend!

cisa.gov/SecureOurWorld

 cisa.gov  [@CISACyber](https://twitter.com/CISACyber)  [@CISA.gov](https://www.facebook.com/CISA.gov)    [@cisa.gov](https://www.instagram.com/cisa.gov)

 central@cisa.dhs.gov

As of August 14, 2023