

Lock Your 10 Most Important Accounts Tonight

A plain-English guide to turning on MFA: the 2-minute setting that blocks more than 99.2% of account-compromise attacks.

Start with these 10, in this order

#	Account	Where to find the setting	Done
01	Main email (Gmail)	myaccount.google.com → Security → 2-Step Verification. Add a passkey while you're there.	☐
02	Main email (Outlook / Microsoft)	account.microsoft.com → Security → sign-in options → Two-step verification	☐
03	Apple Account	iPhone: Settings → [your name] → Sign-In & Security → Two-Factor Authentication	☐
04	Banking apps	In your bank's app, under Security. Turn on login and payment notifications too.	☐
05	Password manager	Settings → Security → Two-step login. It protects everything else, so protect it first.	☐
06	WhatsApp	Settings → Account → Two-step verification → Turn on (choose a 6-digit PIN)	☐
07	Instagram & Facebook	Accounts Center → Password and security → Two-factor authentication	☐
08	LinkedIn	Settings & Privacy → Sign in & security → Two-step verification	☐
09	TikTok / X	TikTok: Settings and privacy → Security → 2-step verification. X: Settings → Security and account access → Security → Two-factor authentication	☐
10	Online shopping (e.g. Amazon)	Your Account → Login & security → 2-Step Verification	☐

Apps rename their menus often. If a name is slightly different, search the app's settings for "two-step", "2-step" or "two-factor".

99.2%

of account-compromise attacks blocked by MFA (Microsoft)

881,387

infected systems seen by Sphere TI in 60 days

89%

of those systems were running antivirus

• UNVERIFIED



```
> trust = 0; verify --all
```

What MFA is

A second check when you log in, usually a code or a tap on your phone. Even if someone steals your password, **they can't get in without it.**

Best option

A **passkey** or an **authenticator app**. SMS codes are better than nothing, but easier to intercept.

Don't get locked out

- Save the **backup codes** somewhere safe and offline.
- Add a second method where you can.
- New phone? Move your authenticator app **before** you wipe the old one.

The golden rules

- **Never share a code.** Nobody legitimate needs it.
- **Never approve a login you didn't start.** Tap Deny, then change your password.

Why Alphatechs

24/7 security operations with a 30-minute response, penetration testing, and Sphere TI, our own threat intelligence platform.

Take the Next Step

Is your work email in a data breach or stealer log? Free Exposure Report at sphereti.com