SECURITY GUIDE

Two-Factor Authentication

Add a second layer of protection to your accounts. Even if your password is stolen, 2FA keeps attackers out.

THE BASICS

What Is Two-Factor Authentication?

2FA requires you to verify your identity in two distinct ways before accessing an account. Even if someone steals your password, they still can't get in without the second factor. The three factor types are:

🔑

FACTOR 1

Something You Know

A password, PIN, or security answer — the classic first layer.

📱

FACTOR 2

Something You Have

A phone, authenticator app, or hardware key that only you possess.

👁

FACTOR 3

Something You Are

A fingerprint, face scan, or other biometric tied to your body.

SETUP PROCESS

How to Enable 2FA

The exact interface varies by service, but the general process is the same across almost every platform.

1. **Open Account Settings**
   Log in and navigate to Settings — sometimes labeled Account, Security, or Privacy.

2. **Find the Security Section**
   Look for Security, Sign-In, or Two-Factor Authentication and click into it.

3. **Enable 2FA**
   Select "Enable Two-Factor Authentication" or a similarly worded option.

4. **Choose Your Method**
   Pick an authenticator app, SMS, hardware key, or email code (see methods below).

5. **Link Your Device**
   Follow the on-screen prompts — typically scan a QR code or enter your phone number.

6. **Verify Setup**
   Enter the test code when prompted to confirm everything is working correctly.

7. **Save Backup Codes**
   Store your recovery codes securely — a password manager or printed copy kept somewhere safe.

AUTHENTICATION METHODS

Which Method Should You Use?

Not all 2FA methods are equally secure. Here's what to know before you choose.

★ RECOMMENDED

Authenticator App

An app like Google Authenticator, Microsoft Authenticator, or Authy generates a time-based 6-digit code that refreshes every 30 seconds. Scan a QR code during setup to link it.

- Works offline — no cell signal needed
- Most secure option widely available to consumers
- Apps: Google Authenticator, Authy, Microsoft Authenticator

GOOD

💬 SMS Text Message

A one-time code is sent to your phone number when you log in. Easy to set up, but vulnerable to SIM-swapping attacks.

- Very easy to set up
- Still far better than no 2FA
- Susceptible to SIM-swap fraud

STRONGEST

🔑 Hardware Key

A physical USB or NFC device (like a YubiKey) you plug in or tap. Phishing-resistant and the gold standard for high-value accounts.

- Immune to phishing attacks
- Best for business or power users
- Requires carrying a physical device

PRIORITY ACCOUNTS

Where to Enable 2FA First

Start with accounts tied to money, identity, or that control access to other accounts. If a service offers 2FA, turn it on.

CATEGORY	ACCOUNT EXAMPLES	WHY IT MATTERS
Email	Gmail, Outlook, Yahoo, iCloud Mail, Work Email	Email resets every other account — it's the master key
Financial	Banks, Brokerages, Crypto Wallets, PayPal, Venmo	Direct access to money; fraud can be immediate and hard to reverse
Password Manager	1Password, Bitwarden, LastPass, Dashlane	Securing this protects every password you own
Work & Productivity	Microsoft 365, Google Workspace, Slack, Zoom, VPN	Protects employer data and prevents unauthorized system access
Healthcare	Patient portals, Insurance, Pharmacy, Telehealth	Contains highly sensitive medical and insurance data
Government	IRS, Social Security, State DMV, Benefits portals	Identity theft via these accounts is serious and difficult to resolve
Cloud Storage	Google Drive, Dropbox, OneDrive, iCloud	Often contains sensitive personal or business files
Social Media	Facebook, Instagram, LinkedIn, X, TikTok	Hijacking damages reputation and enables scams targeting your contacts
Shopping	Amazon, eBay, Etsy, Target, Walmart	Stores saved payment info and shipping addresses
Developer Tools	GitHub, GitLab, AWS, Cloudflare, npm, Docker Hub	Code repos and servers may contain API keys or infrastructure access

PRO TIP

Start with your email accounts and password manager first — securing those protects everything else, since they're the keys to resetting or accessing every other login you have.