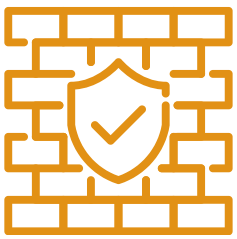
DO THE TWO-STEP

Use an Authenticator App

It's better to use a special app like Google Authenticator or Microsoft Authenticator instead of using texts. These apps create the codes on your phone, so they're harder for hackers to steal.

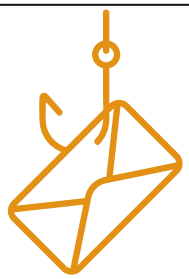
Enable MFA

Apply MFA to your most sensitive accounts first: email, banking and financial services, cloud storage, and password managers. Attackers often pivot from one compromised account to others, so protect the core first.



Backups

Ensure you've set up secure backup codes or recovery methods (like a trusted device or email). Without these, losing access to your primary authentication method (like a lost phone) can lock you out of your accounts.



Beware of Phishing

MFA is strong, but it's not bulletproof. Some phishing attacks can trick you into giving up codes. Always check URLs carefully, don't approve login requests you didn't initiate, and use phishing-resistant MFA methods when possible

Stay Informed

You don't need to be an expert to stay informed. Subscribe to an easy-to-read tech newsletter or follow trusted sources like CISA or the FBI website.

Resources:

- cisa.gov/MFA
- cyberhouserock.info
- cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication