

NOT ALL TWO-FACTOR IS EQUAL.

Know the difference before you pick one.

2FA adds another proof of identity after your password.



SMS / TEXT CODE

BEST FIT

Easy setup. Use only when stronger options are not offered.

TRADE-OFF

A SIM swap can send your text codes to someone else.

WEAK

PHISHING

Vulnerable

SIM SWAP

Direct risk



EMAIL ONE-TIME CODE

BEST FIT

No extra app. A fallback when nothing stronger is available.

TRADE-OFF

If your inbox is compromised, your code is exposed too.

WEAK

PHISHING

Vulnerable

SIM SWAP

Recovery-dependent



AUTHENTICATOR APP

BEST FIT

A practical default for email, banking and social media.

TRADE-OFF

Works offline. Save backup codes in case you lose the phone.

GOOD

PHISHING

Vulnerable

SIM SWAP

No direct risk



PUSH NOTIFICATION

BEST FIT

Common at work. Review the device and location shown.

TRADE-OFF

Prompt spam can trick you. Prefer matching the login-screen number over one-tap approval.

VARIES

PHISHING

Vulnerable

SIM SWAP

No direct risk



HARDWARE SECURITY KEY

BEST FIT

For high-value email, banking, password-manager and crypto accounts.

TRADE-OFF

Paid device; prices vary. Keep a spare key or recovery option.

STRONGEST

PHISHING

Resistant*

SIM SWAP

No direct risk

START WITH EMAIL AND BANKING.

Move off SMS to an authenticator app. For stronger phishing protection, use a FIDO security key where supported.

KEEP A SPARE KEY OR RECOVERY OPTION.

* FIDO/WebAuthn keys. Recovery settings can still expose an account.

"No direct risk" excludes phone-based account recovery.