

ACCOUNT SECURITY

Passwords, Passphrases, MFA & Encryption Quick Guide

Simple, current guidance based on the National Institute of Standards and Technology (NIST) Digital Identity Guidelines (SP 800-63B) and the Cybersecurity and Infrastructure Security Agency (CISA). In short: length beats complexity, a password manager beats memory, and multi-factor authentication (MFA), a second proof of identity such as a phone app or security key, stops most account takeovers.

Passwords and passphrases

- [] Use long passphrases: four or more random words, 15+ characters for important accounts
- [] Prefer length over forced complexity rules; avoid predictable substitutions (P@ssw0rd)
- [] Never reuse passwords; check exposure at [Have I Been Pwned](#)
- [] Change passwords when there is evidence of compromise, not on an arbitrary schedule

Password managers

- [] Use a reputable password manager (business edition for teams) with a strong master passphrase
- [] Turn on MFA for the password manager itself
- [] Use shared vaults instead of spreadsheets or sticky notes
- [] Generate unique random passwords for every account

Multi-factor authentication (MFA)

- [] Turn on MFA everywhere, starting with email, banking, admin, and remote access
- [] Best: phishing-resistant MFA such as passkeys or FIDO2 security keys
- [] Good: authenticator app with number matching; avoid SMS codes where possible
- [] Never approve an MFA prompt you did not start

Encryption

- [] Data at rest: turn on full-disk encryption (BitLocker, FileVault) on laptops and phones
- [] Data in transit: make sure websites and apps use encrypted connections (HTTPS, the padlock in your browser, using Transport Layer Security (TLS) 1.2 or newer)
- [] Backups: encrypt backups and keep at least one copy offline or immutable

-
- [] Email and files: use built-in encryption or sensitivity labels for confidential data
-
- [] Protect encryption keys and recovery keys in a secure, separate location
-

General guidance for training and planning, not legal advice. Adapt to your environment, contracts, and regulators.