Password Manager and MFA Quick-Start

A practical small-team rollout

Why use both?

A password manager creates and stores unique passwords. MFA adds a second sign-in check. Together they reduce dependence on reused passwords; they do not make every message or login safe.

Choose a manager

Look for business-owned administration, shared vaults, per-user access, MFA/passkeys, recovery options, export options, and a clear offboarding process. Test it with a few non-critical accounts first.

Name an owner

Assign a primary administrator and a trusted backup. Write down the recovery process. Use individual team accounts rather than one shared master login.

Start with key accounts

Secure email, finance, domain registrar, website hosting, and cloud storage first. Change reused passwords to unique ones and save each in the correct vault.

Turn on MFA

Use passkeys or security keys where supported; otherwise use an authenticator app. Use available protection rather than leaving MFA off while waiting for the ideal method.

Store recovery codes

Keep codes in a protected location with controlled access, separate from the only device or account needed to sign in. Never paste them into an ordinary team chat or this worksheet.

Teach the routine

Practice saving a login, using a shared vault, and reporting a suspicious prompt. Never approve an unexpected MFA request. Verify the site before filling a password.

Avoid common mistakes

Do not share master passwords, keep recovery only on one phone, put all team secrets in a personal vault, or assume exported passwords are encrypted. Protect exports and remove them securely when no longer needed.

Finish and maintain

Confirm each person can recover access. Remove old staff access promptly, rotate shared secrets they knew, and review vault membership regularly.

Want a hand? Explore IT Support & Team Setup at https://rosscoreit.com/