J3 Systems Group Quick Resource

Password and MFA Best Practices

A quick handout for improving password and MFA habits across a small business.

Practical guidance for small businesses and nonprofit organizations

Prepared by J3 Systems Group LLC

Overview

Passwords and MFA are two of the most important protections for business accounts. This guide explains the basics in plain English so employees and leaders can make safer choices.

Who This Is For

- Small businesses that want stronger account protection.
- Office managers who need simple security guidance for staff.
- Teams that use Microsoft 365, Google Workspace, payroll, banking, or cloud applications.

Best Practices

What makes a strong password

- Use a long password or passphrase that is hard to guess.
- Use a different password for every business account.
- Avoid personal details, company names, seasons, sports teams, and common patterns.

Why password reuse is risky

- If one reused password is exposed, other accounts may be tested by attackers.
- Reused passwords can turn a small website breach into a business email compromise.
- Every important account should have its own password.

Why a password manager helps

- A password manager stores unique passwords so employees do not need to memorize every one.
- It reduces the chance that passwords are kept in notes, spreadsheets, or messages.
- It makes access transfer and recovery easier when handled correctly.

What MFA is

- MFA means a second proof is needed after the password.
- Common methods include authenticator apps, push approvals, text messages, phone calls, and security keys.
- MFA helps protect the account even if the password is stolen.

Recommended MFA methods

- Use authenticator apps or security keys when possible.
- Protect administrator accounts with the strongest available MFA method.
- Keep backup codes in a safe business controlled location.

Shared account risks

- Shared accounts make it hard to know who took an action.
- Shared accounts are harder to offboard safely.
- Individual accounts with role based access are easier to manage and audit.

What not to do

- Do not reuse business passwords on personal websites.
- Do not share passwords in email, chat, spreadsheets, or sticky notes.
- Do not approve an MFA prompt that was not personally started.

When Outside Help Makes Sense

Ask for help when admin roles are unclear, business data is spread across personal accounts, access removal depends on memory, security alerts are not being reviewed, or the organization is not sure which settings are currently protecting users and files.

Quick Review

☐ Each account has a unique password.
☐ MFA is turned on for important systems.
☐ Backup codes are stored safely.
☐ Shared accounts are reviewed.
☐ Employees know how to report suspicious prompts.

Conclusion

Good password and MFA habits reduce the chance that one stolen password becomes a larger business security incident.

Need help reviewing your Microsoft 365, Google Workspace, offboarding, or small business IT security setup?

J3 Systems Group LLC provides practical IT support, documentation, cloud administration, and security focused reviews for small businesses and nonprofit organizations.

Contact J3 Systems Group LLC to request a practical review and clear next steps.