



Google MFA Security Guide

A Complete Multi-Factor Authentication Playbook for Small Businesses &
Nonprofits

Beacon Cyber Defense
www.beaconcyberdefense.com

© 2025 Beacon Cyber Defense — Confidential

Table of Contents

1. Why MFA Is Critical in 2025
2. Understanding Google MFA
3. Step-by-Step Setup Instructions
4. Choosing the Right MFA Method
5. Admin Enforcement for Google Workspace
6. Backup Codes and Account Recovery
7. Training Employees & Volunteers
8. Common Attacks MFA Stops
9. Policies for Small Businesses & Nonprofits
10. Quick Deployment Checklist

1. Why MFA Is Critical in 2025

- MFA blocks 99.9% of account-takeover attacks.
- Most breaches begin with stolen or reused passwords.
- Small businesses and nonprofits are now top attacker targets.
- MFA is the single most cost-effective cybersecurity control.

2. Understanding Google MFA

- Adds a second verification step to your login.
- Protects Gmail, Drive, Docs, Sheets, Photos, and Workspace apps.
- Stops attackers from accessing accounts even if a password leaks.

3. Step-by-Step Setup Instructions

- Sign into your Google Account.
- Open the Security section.
- Enable '2-Step Verification'.
- Choose Authenticator App, Google Prompt, or SMS.
- Download and store backup codes securely.

4. Choosing the Right MFA Method

- Authenticator App — best security option.
- Google Prompt — easy for non-technical users.
- SMS — acceptable but less secure due to SIM swap risk.
- Security Keys — strongest option for admins and high-risk users.

5. Admin Enforcement for Google Workspace

- Admins can enforce MFA for all employees and volunteers.
- Policies prevent accounts from operating without MFA.
- Set deadlines for MFA enrollment.
- Monitor MFA adoption using Workspace Security Reports.

6. Backup Codes and Recovery

- Backup codes prevent lockouts.
- Store codes offline — never in email.
- Provide recovery instructions to all users.
- Rotate and regenerate codes annually or after suspicion of compromise.

7. Training Employees & Volunteers

- Provide simple step-by-step MFA setup instructions.
- Explain why MFA protects donor and financial data.
- Train staff on phishing attacks designed to bypass MFA.
- Run tabletop exercises to test employee readiness.

8. Common Attacks MFA Stops

- Credential stuffing and password reuse attacks.
- Phishing-based account takeover.
- Business email compromise (BEC).
- Donation fraud and financial impersonation scams.
- Unauthorized access to cloud files and financial accounts.

9. Policies for Small Businesses & Nonprofits

- Require MFA for all employees and volunteers.
- Mandate MFA on all donor, finance, and HR systems.
- Require MFA on all admin and shared inbox accounts.
- Disable legacy authentication methods that bypass MFA.

10. Quick Deployment Checklist

- Enforce MFA for all accounts.
- Require Authenticator Apps instead of SMS.
- Disable legacy login protocols.
- Train staff on identifying phishing attacks.
- Store backup codes securely offline.
- Review MFA logs monthly.