

The Nonprofit's Guide to MFA

About Connect Cause

Accredited Managed Services Provider that Works Exclusively with Nonprofit Organizations

State-of-the-Art Operations Center with Cutting Edge Technology

24 / 7 / 365 Remote Help Desk and On-Site Support

24 / 7 / 365 Real-Time Network Monitoring

Experienced, Certified Technicians and Engineers

Dedicated Account Managers

Predictable Monthly Cost, Scalable Level of Service

Remote Resolution of Issues More than 90% of the Time

Easy to Understand Graphical Reporting of Performance

Reduces IT Operational Costs by Up to 70%

Cybersecurity threats are on the rise, and nonprofits are not exempt. From donor data to staff credentials, mission-driven organizations often hold sensitive information that cybercriminals want. One of the simplest and most effective ways to protect that information is by enabling Multi-Factor Authentication, or MFA.

This guide walks you through what MFA is, why it matters, how to implement it, and how to ensure your team is on board. Whether you're a small nonprofit or a large organization, MFA is a practical, low-cost step you can take today to strengthen your digital defenses.

► What is Multi-Factor Authentication (MFA)?

MFA adds an extra layer of protection to your accounts. Instead of logging in with just a password, users must verify their identity with a second factor, such as:

- A one-time code sent to a phone or email
- A push notification from an authentication app
- A biometric factor like a fingerprint or face scan

This second step makes it much harder for attackers to access your systems, even if they've stolen a password.

► Why MFA Matters for Nonprofits

- **Protects Sensitive Data:** Safeguards donor information, financial records, and beneficiary details.
- **Reduces Risk:** Prevents more than 90% of account-based attacks.
- **Builds Trust:** Demonstrates to funders, donors, and board members that you take cybersecurity seriously.
- **Compliance-Ready:** Helps meet security standards often required by grants and partnerships



► How to Implement MFA at Your Nonprofit

► Start with a Risk Assessment

- Identify which systems hold sensitive data (email, donor databases, file storage, etc.)

► Enable MFA on Key Platforms

- Start with email and cloud accounts like Microsoft 365 or Google Workspace
- Look at CRM platforms, accounting software, and donation portals

► Choose the Right Authentication Methods

- Authentication apps like Microsoft Authenticator, Duo, or Google Authenticator
- Backup options like SMS or email codes

► Train Your Team

- Provide step-by-step guidance on setting up MFA
- Explain how MFA protects your mission and the people you serve

► Monitor and Adjust

- Ensure MFA stays enabled
- Gather feedback from staff and volunteers and make improvements

► Common Myths About MFA

► “It’s too complicated.”

Most platforms make it easy to set up with just a few clicks.

► “It’ll slow us down.”

MFA adds a few seconds to logins, but saves hours in cleanup from a data breach.

► “Our passwords are strong enough.”

Even the strongest passwords can be stolen or leaked.

► Need Help?

Connect Cause has helped nonprofits of all sizes implement MFA quickly and smoothly. If you’re ready to get started, or just need support along the way, contact our team at connect@connectcause.com.

Protect your data. Build trust. Secure your mission.

MFA Implementation Checklist

- ☐ Identify high-risk accounts (email, donor systems, finance platforms)
- ☐ Confirm your software platforms support MFA (Microsoft 365, Google Workspace, etc.)
- ☐ Select an authentication method (app, SMS, hardware token)
- ☐ Communicate the change to your staff and explain the why
- ☐ Provide instructions or training on setup
- ☐ Require MFA for all staff accounts
- ☐ Test the process internally
- ☐ Monitor compliance and address any access issues
- ☐ Review and update policies annually

Pro Tip

Consider requiring MFA for board members and volunteers with access to sensitive systems. Anyone with login credentials should be included in your security plan.