



The Nonprofit's Guide to Digital Hygiene

What's Inside the Guide:

Inside, you'll discover 10 practical habits your team can start using immediately:

- ▶ How to spot suspicious emails before damage is done
- ▶ Why password habits matter more than you think
- ▶ The easiest way to protect your accounts (in minutes)
- ▶ Simple backup practices that save organizations
- ▶ How to reduce risk without slowing your team down

Each Section Includes:

- ▶ Clear explanations
- ▶ Real-world nonprofit scenarios
- ▶ Actionable steps anyone can follow

This Guide is Perfect For:

- ▶ Executive Directors & leadership teams
- ▶ Operations & admin staff
- ▶ Program managers handling sensitive data

Simple Habits That Prevent Big Problems

Most IT issues in nonprofits do not start with major failures.

They start with small, everyday habits:

- ▶ A rushed click on an email
- ▶ A reused password
- ▶ A delayed system update

Individually, these actions seem harmless. Over time, they create risks that can lead to downtime, data loss, or security incidents.

The goal of digital hygiene is not to add complexity. It is to create simple, repeatable habits that keep your organization secure, stable, and focused on its mission.

This guide gives you 10 practical habits your team can start using immediately. With no technical background required.

▶ 1) Pause Before You Click

What To Do:

Treat all emails with caution. *Especially* the unexpected ones.

Simple Actions:

- ▶ Check the sender's full email address
- ▶ Hover over links before clicking
- ▶ Verify requests through another channel if you are unsure

Why it Matters:

Phishing is one of the most common ways nonprofits are targeted. A single click can expose your systems, donor data, and more.



► 2) Use Strong, Unique Passwords

What To Do:

Never reuse passwords across systems.

Simple Actions:

- Use a password manager
- Create long, unique passwords for each account
- Avoid sharing login credentials

Why it Matters:

One compromised password should not unlock your entire organization.

► 3) Turn On Multi-Factor Authentication (MFA)

What To Do:

Add an extra layer of protection to your accounts.

Simple Actions:

- Enable MFA on email, finance tools, and databases
- Use an authenticator app when possible

Why it Matters:

Even if a password is stolen, MFA can stop unauthorized access.

► 4) Keep Systems Updated

What To Do:

Install updates regularly.

Simple Actions:

- Turn on automatic updates when available
- Restart devices weekly
- Do not delay updates for long periods

Why it Matters:

Updates fix known security issues that attackers actively look for.

The Hidden Cost of “We’ll Deal with It Later”

In most nonprofits, IT problems don’t start as emergencies. They start as minor inconveniences that get postponed.

- “That’s annoying. I’ll fix it later.”
- “It’s probably nothing.”
- “We don’t have time for this right now.”

Here’s what happens next: Small issues compound quietly.

- A skipped update becomes a vulnerability
- A workaround becomes a risky process
- A “temporary” exception isn’t revisited

Over time, these stack into:

- Increased exposure to security risks
- Slower systems and frustrated staff
- Higher costs when something breaks

A better standard. Shift from:

“Is this urgent?”
to
“Does this increase risk if ignored?”

That one question changes how decisions get made and prevents issues from quietly growing into disruptions.





► 5) Back Up Your Data

What To Do:

Make sure your data can be recovered.

Simple Actions:

- Use automatic cloud backups
- Test backups periodically
- Keep backups separate from your main systems

Why it Matters:

Backups are your safety net if something goes wrong.

► 6) Limit Access to What's Necessary

What To Do:

Only give access based on job roles.

Simple Actions:

- Grant access based on responsibilities
- Review access regularly
- Remove access when staff/volunteers leave

Why it Matters:

Less access reduces the risk of mistakes and exposure.

► 7) Train Staff in Small, Consistent Ways

What To Do:

Keep cybersecurity awareness training ongoing.

Simple Actions:

- Share quick tips monthly
- Discuss real scenarios in meetings
- Encourage questions and reporting

Why it Matters:

Awareness fades quickly. Small reminders keep your team alert.

Quick Self-Check: How Resilient Is Your Organization?

☐ We can access all critical systems without relying on one specific person

☐ We know who to contact (internal or external) when something tech-related goes wrong

☐ Our team is comfortable flagging suspicious or unusual activity without hesitation

☐ We have a clear process for reporting tech issues (not just informal Slack/email messages)

☐ We can quickly tell what tools/systems we currently use across the organization

☐ We have confidence that former staff no longer have access to our systems

☐ We know which data is most sensitive or mission-critical

☐ We have a shared understanding of "what's normal" vs. "what's suspicious" behavior

☐ We could continue basic operations if one system went down temporarily

☐ Leadership has visibility into technology risks (even at a high level)

☐ We don't rely on guesswork to make decisions about tools or access

☐ At least one backup person can step in for critical workflows if needed

How to Use This:

10-12 checked: You're operating from a strong foundation

6-9 checked: There are gaps that are worth addressing before they become issues

0-5 checked: You're more exposed than you think





► 8) Secure and Track Devices

What To Do:

Treat devices as part of your security system.

Simple Actions:

- Lock screens when stepping away
- Avoid using personal devices for sensitive work
- Keep track of organization-owned devices

Why it Matters:

Lost or unsecured devices can expose sensitive information.

► 9) Document Key Processes

What To Do:

Write down important IT-related steps.

Simple Actions:

- Create onboarding and offboarding checklists
- Document basic procedures
- Store instructions where the team can access them

Why it Matters:

Consistency improves when processes are clear and repeatable.

► 10) Be Proactive, Not Reactive

What To Do:

Address issues before they become urgent.

Simple Actions:

- Schedule periodic check-ins
- Review systems before major events
- Ask for help early

Why it Matters:

Early action prevents stress, downtime, and last-minute problems.

Digital hygiene isn't about perfection. It's about consistency. When these habits become part of your daily operations, you can spend more time focused on what matters most: **your mission.**

About Connect Cause

Accredited Managed Services Provider
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%

IT For Nonprofits

Connect Cause works exclusively with nonprofits, so we understand the unique IT needs of organizations like yours.

 www.ConnectCause.com

 (919)925-5881

 connect@connectcause.com

