TOGETHER TUESDAY
Tech Capacity and Security Toolkit

A Supplement for Strengthening Organizational Resilience

On **June 23, 2026**, millions of people will take action for **TogetherTuesday**. This guide helps your organization turn that energy into digital resilience by connecting with a skilled volunteer to complete high-impact, time-bounded projects.

🛡️ Getting Started: The Collaboration Handshake

Before beginning, the Volunteer and Nonprofit Lead should agree on these ground rules:

1. **Safety First:** No data or accounts will be deleted without explicit, verbal confirmation from the Nonprofit Lead.
2. **Privacy:** The Nonprofit Lead will enter all administrative passwords; the volunteer should not view, store, or "own" these credentials.
3. **The Continuity Plan:** For any configuration changes (like MFA), the volunteer will walk the Lead through the "undo" process before any settings are applied.

Project 1: The Equipment & Asset Baseline (1.5–2.5 Hours)

Goal: Create a verified record of your hardware to identify security vulnerabilities and plan for future equipment needs.

1. Preparation (Nonprofit Lead)

- **Gather:** Collect existing spreadsheets, purchase orders, or hardware invoices.
- **Physical Access:** Ensure all laptops and tablets are on-site or reachable via a scheduled screenshare.

2. Guided Assessment (Volunteer to Nonprofit)

Record the following details for each device in a master spreadsheet. **(Download an Inventory Template here)**

1. **Identification:** What is the unique Service Tag or Serial Number?
2. **Primary User:** Who is the staff member responsible for this device?
3. **Operating System:** Is it running Windows 11, or an older version? (Check your version here).
4. **Ownership:** Is this organization-owned or a personal device (BYOD)?
5. **Sign-in Security:** Does the device require a password, PIN, or biometric to unlock?
6. **Cloud Sync:** Are the Desktop, Documents, and Pictures folders syncing to OneDrive or Google Drive? (Look for the cloud icon in the taskbar).
7. **Storage:** Is the hard drive more than 90% full?
8. **Physical Health:** Are there signs of battery swelling (bulging case) or frayed chargers?
9. **Antivirus:** Is a security suite (e.g., Windows Defender, Sophos) active and updated?
10. **System Readiness:** When was this device last fully restarted? (Check "Up time" in Task Manager).

3. Final Output: The Asset Roadmap

Volunteer: Before completing the session, provide a 1-page **"Asset Roadmap"** that summarizes the following:

- **Executive Summary:** A total count of workstations, laptops, and tablets identified during the session.
- **Inventory Management Scoring System**
- **The "Red List" (Critical Security Risks):** List the Serial Numbers and users of any devices running Windows 10 or older. *As of June 2026, these devices no longer receive security updates and represent a significant risk.*
- **Maintenance Flags:** Note any devices with physical health issues (bulging batteries, frayed chargers, cracked screens) or critically low storage space.
- **Replacement Priority List:** Instead of a budget, provide a "Tiered Priority" list for the nonprofit to use when requesting funds or donations. Rank devices based on:
  a. **Immediate Risk (Tier 1):** Devices with unsupported OS or hardware failure signs.
  b. **Security Gaps (Tier 2):** Personal/unmanaged devices used for sensitive work.
  c. **Performance Gaps (Tier 3):** Aging devices (5+ years old) that slow down staff productivity.

Tip for Volunteers: Record specific staff quotes about performance in your spreadsheet (e.g., "The fan is loud and it takes 15 minutes to open Excel"). These anecdotes are highly effective when the Lead presents the Roadmap to their board.

Project 2: Securing Your Accounts with MFA (1–2 Hours)

Goal: Close your organization's single largest security gap by enabling Multi-Factor Authentication (MFA).

1. Implementation Steps

Volunteer: Ensure the organization has the tools to manage this long-term.

- **For Microsoft 365:** Enable Security Defaults for smaller teams, or implement a baseline **Conditional Access** policy for larger groups.
- **For Google Workspace:** Deploy 2-Step Verification. Set the "Enforcement" date to 48 hours in the future to allow staff time to set up their devices.
    - Note, a "grace period" can be enabled on enforcement if there's concern about certain staff struggling to properly enroll. It's not recommended to extend this beyond one to two weeks.

2. Final Output: The Enrollment Guide

Volunteer: Hand over a "MFA Quick-Start Sheet" including the following three items:

1. **The Staff Message:** Provide a copy-paste email for the Nonprofit Lead (see template below) to send to the team.
2. **The Enrollment Runbook:** A 3-step bulleted list for employees on how to download the authenticator app and scan their first QR code.
3. **The Admin Recovery Protocol:** A clear, written instruction for the Nonprofit Lead on exactly how to reset MFA for an employee who gets a new phone or loses their device.

3. Staff Welcome Template

Volunteer: Customize this message and have the Lead send it to all staff immediately:

Subject: Action Required: Securing our community's data

To protect our mission and our donors, we are enabling Multi-Factor Authentication (MFA) today as part of our TogetherTuesday action.

How to get started:

- Download the **Microsoft Authenticator** or **Google Authenticator** app on your phone.
- Log in to your email on your computer. You will be prompted to link your phone.
- **Important:** Save your "Backup Codes" in a secure place during the setup.

If you have any trouble, [Admin Name] is available to assist you!

Final Step: Celebrate your progress! Share a photo of your session on social media with **#TogetherTuesday** and tag **@GivingTuesday** and **@TechSoup**.

Project 3: The Basic Security Check (2–3 Hours)

Goal: Identify high-impact security and safety gaps to strengthen your organization's security.

1. The Essential Checklist (Volunteer & Admin)

The volunteer will verify these items within your Admin Portal (Microsoft 365 or Google Workspace):

Identity Protection	Is Multi-Factor Authentication "Enforced" or "Enabled" by default for the products you're orgs using? Are 100% of your users required to complete a two factor 'challenge' in order to sign in to your resources?"
Emergency Access	Is there one "emergency" admin account without MFA, for which the login credentials are stored in a physical safe? (This prevents total lockout if a primary admin loses their phone).
Account Hygiene	Are there active accounts for staff or volunteers who have left the organization?
Backup Verification	Do the cloud providers your organization uses offer "point-in-time" or "version history" of the documents created by users? If not, does the org have a "recovery" strategy for lost content?"
Data Encryption	Is there any encryption software (like a BitLocker or File Fault) to protect data in case a device is lost?
Permissions	Are staff using "Standard" accounts for daily tasks? (No one should use an "Administrator" account for daily email or web browsing).
Legacy Access	Does your organization use, or is it required to use as part of an existing software platform, MAP/POP3 or basic SMTP AUTH? **If so, it's important to note these protocols can allow for bypassing of Multi-Factor Authentication (MFA).**

2. Final Output: The Security Roadmap

Volunteer: Create a "Security Traffic Light" document summarizing the checklist findings:

- 🔴 **Immediate Improvement (Action Required):** List the specific items that failed the check (e.g., "3 former staff accounts are still active"). Provide one clear sentence explaining the risk (e.g., "Former staff could still access sensitive client files").
- 🟡 **Strategic Improvement (Plan Required):** List items that meet baseline safety but require a plan to improve (e.g., "Backups are happening, but we haven't tested a recovery this year").
- 🟢 **Secure:** List the areas where the organization is currently following best practices.

Need more than just the basics?

TechSoup is here to help your organization adopt and optimize technology.

Get specialized training at the **Microsoft Digital Skills Center,** join **TechSoup Plus** for deep consultative support, or browse our full range of services at **TechSoup.org.**

Questions?

GIVINGTUESDAY
info@givingtuesday.org

techsoup
www.techsoup.org