Digital Resilience Toolkit for Nonprofits

Protecting Your Mission in a Digital World



Software for Good

1st Edition / 2025

LOVE / HUMANITY / ECOLOGY / CONTEXT / LIBERATION / STEWARDSHIP

About this Toolkit

Who is this for?

- Mission-driven nonprofits under increased digital and political threats.

How do I use this toolkit?

- Each section offers a practical “quick win” you can implement immediately.

Need more help?

- Click here to schedule a 15-minute discovery call if you need personalized guidance.

Why Digital Resilience Matters Now

In today's increasingly volatile climate, nonprofits and social impact organizations face unique digital challenges.

Beyond typical cybersecurity concerns, many mission-driven organizations must now navigate political pressures, targeted attacks, and platform dependencies that can threaten their very existence.

This toolkit offers **practical steps** to strengthen your organization's digital resilience—**ensuring your mission continues without interruption, compromise, or fear.**

5 things your nonprofit can do right now

1. Conduct a Data Inventory & Minimization Audit

Why it matters:

Every piece of unnecessary data you collect is both a **security risk** and a **potential liability.**



Action steps:

- ❑ List all the **types of data** your organization collects
- ❑ For each data type, ask: ***"Is this essential to our mission?"***
- ❑ Identify **sensitive** data that could put communities at risk if exposed
- ❑ **Create a plan** to securely delete unnecessary data
- ❑ **Revise intake forms** and processes to collect **only essential information**

Quick win:

Review your **most-used form** and remove at least one **non-essential** question.

2. Create Platform Independence

Why it matters:

Relying entirely on a single tech platform puts your organization at risk if that platform changes policies, increases prices, or shuts down.



Action steps:

- ❑ Identify which digital platforms are **most critical** to your operations
- ❑ For each critical platform, document:

  Cost, **alternatives**, and what would happen if access were **suddenly restricted**
- ❑ **Export** and **back up** essential data **monthly** from all third-party platforms
- ❑ Consider implementing **multi-platform** strategies for critical functions
- ❑ Prioritize **open-source** solutions where appropriate

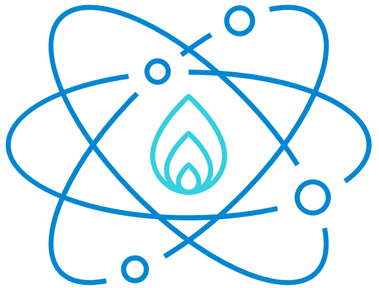
Quick win:

Set up automatic **monthly exports** of your **donor database, email list,** or other **critical data.**

3. Establish Operational Continuity Plans

Why it matters:

When digital systems fail, your community still needs you. Having backup plans ensures you can continue your essential work.



Action steps:

- ❑ Identify the **top 3 digital systems** that would create the biggest problems if brought down
- ❑ For each system, create **simple instructions** for an **alternative workflow**
- ❑ Designate and train **backup personnel** for critical digital responsibilities
- ❑ Create **offline copies** of essential contact information and procedures
- ❑ Test your continuity plans **quarterly** with simple drills

Quick win:

Create a **shared document with emergency contact information** for all technology vendors and support resources.

4. Strengthen Access Controls

Why it matters:

Most security breaches happen through **compromised accounts,** not sophisticated hacking.



Action steps:

- Implement **multi-factor authentication** for all critical systems
- Create a **password manager** account for your organization
- Audit who has access to what systems and **remove unnecessary access**
- Establish clear processes for **onboarding and offboarding staff/volunteers** from digital systems
- Create **tiered access levels** based on role and necessity

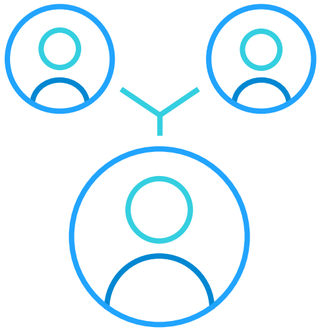
Quick win:

Enable **multi-factor authentication** on your organization's **email accounts** today.

5. Build Staff Security Awareness

Why it matters:

Your team is both your greatest security asset and potential vulnerability. Simple training can dramatically reduce risks.



Action steps:

- ❑ Schedule a **30-minute security basics session** at your next staff meeting
- ❑ Create a simple, **non-technical security guide** for staff and volunteers
- ❑ Establish clear procedures for reporting potential security incidents
- ❑ Recognize and reward security-conscious behavior
- ❑ Make security part of your **onboarding process**

Quick win:

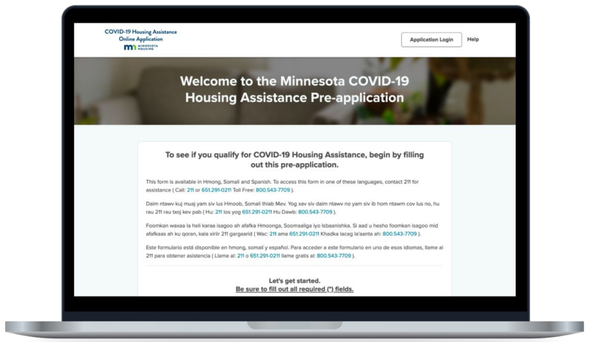
Share one specific phishing example with your team and discuss how to **identify suspicious messages.**

Real-World Examples of Digital Resilience

Case Study:

Emergency Housing Assistance During Crisis

When Minnesota needed to distribute over $70 million in housing assistance during the pandemic, Software for Good partnered with HousingLink to build a system designed with both security and accessibility in mind. By collecting only essential data and creating streamlined processes, the platform successfully processed 70,000+ requests while minimizing security risks.



Resilience principle applied:

Data minimization as a security strategy.

Case Study:

Reproductive Healthcare Access

As legal landscapes shifted around reproductive healthcare, abortion funds and justice organizations needed resilient digital infrastructure. By building decentralized, adaptable systems, these organizations ensured they could continue coordinating essential healthcare regardless of external pressures or platform restrictions.



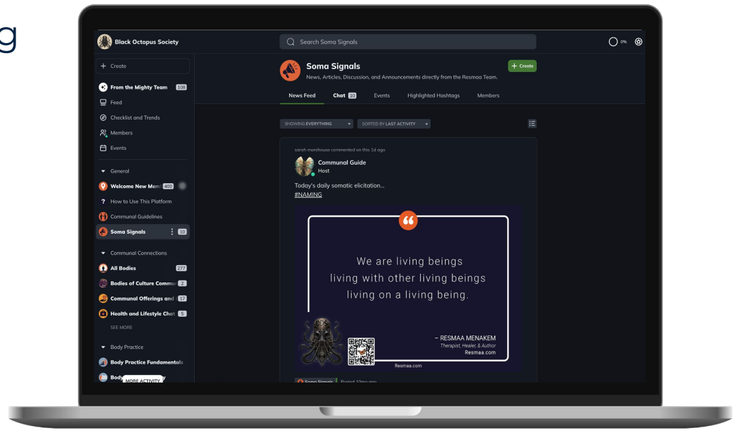
Resilience principle applied:

Operational continuity through system independence.

Case Study:

Black Octopus Society

For Resmaa Menakem's educational platform, building resilience began with platform selection. Instead of creating a fully custom system that might create dependencies, the organization chose a platform that ensured content ownership and control, with independent backups and multiple distribution channels.

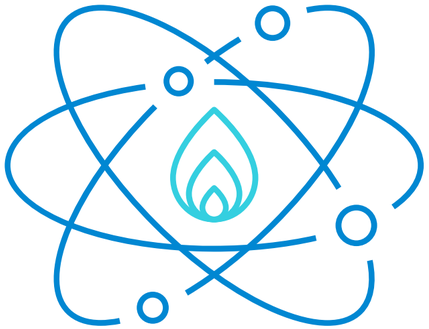


▶ Resilience principle applied:

Platform independence through strategic technology choices.

▶ Next Steps:

Building Long-Term Resilience



While the immediate steps above can significantly improve your organization's digital resilience, consider these longer-term strategies:

1. **Include digital resilience in strategic planning**
   Make technology decisions with an eye toward long-term independence and mission protection.

2. **Budget for security and resilience**
   Allocate resources specifically for maintaining and improving your digital infrastructure.

3. **Build technical capacity internally**
   Invest in training to reduce dependence on external support.

4. **Collaborate with peer organizations**
   Share resources, strategies, and even technology infrastructure with aligned groups.

5. **Develop relationships with tech allies**
   Connect with technologists who understand your mission and values.

A Final Note on Digital Resilience



Digital resilience isn't about preventing all possible problems—it's about ensuring your organization can adapt, recover, and continue its essential work no matter what challenges arise. By taking even small steps to strengthen your digital infrastructure today, you're protecting not just your organization, but the communities and causes you serve.

Remember: The most resilient organizations aren't necessarily those with the most resources or the most sophisticated technology.
They're the ones that approach digital systems with **intention**, **care**, and a **clear focus on their mission**.

This toolkit was developed by Software for Good, a technology partner that builds software with love to help organizations create positive change.

For more information on digital resilience consulting or other technology services, visit softwareforgood.com or write us at hello@softwareforgood.com

Thank you

Software for Good

SOFTWAREFORGOOD.COM

LOVE / HUMANITY / ECOLOGY / CONTEXT / LIBERATION / STEWARDSHIP