A RESOURCE FOR MISSION DRIVEN ORGANIZATIONS

Nonprofit Guide to Cybersecurity

Your community trusts you to provide them services and to protect their private information. But cybercriminals are actively targeting nonprofits just like yours, knowing that one successful phishing email can expose years of hard-won trust. This guide walks through our **Protect, Train, Respond** framework. Built for organizations that need enterprise-grade security without the enterprise price tag.

PROTECT **TRAIN** **RESPOND**

---

1 IN 3

nonprofits report experiencing a cyberattack

24HRS

the window that determines your reputation after a breach

3 STEPS

that's all it takes to start

Is your organization actually as secure as you think?

At We Love Philly, we don't believe cybersecurity should be an enterprise-only luxury. We've designed our **Protect, Train, Respond** framework specifically for mission-driven organizations to secure their operations, without the enterprise price tag.

1 The Protect, Train, Respond Framework

Protect
Implement technical safeguards such as multi-factor authentication and encrypted connections to stop threats before they happen.

Train
Educate staff and volunteers through regular awareness training and simulated exercises to recognize social engineering, phishing, and red flags.

Respond
Build a clear, step-by-step incident response plan so your team knows exactly who to call, how to contain threats, and what to communicate if a breach occurs.

2 Immediate Quick Wins for Security

Action	Why It Matters
Enforce MFA (Multi-Factor Authentication)	Stops attackers from accessing accounts even if they possess your password — essential for email and administrative portals.
Hardened Email SPF / DKIM / DMARC	Validates that emails claiming to be from your domain are legitimate, preventing domain spoofing and phishing campaigns targeting your donors.
Regular Backups	Provides a recovery path if you are hit by ransomware; ensure backups are off-site and immutable (cannot be altered).
HTTPS Enforcement	Ensures all content, including styles and scripts, loads over a secure connection, preventing "mixed content" warnings and interception of site data.
Plugin / Theme Management	For WordPress users: remove unused themes and plugins, and strictly enforce updates. Every active third-party plugin is a potential attack surface that needs regular patching.
Staff Phishing & Security Awareness Training	Technology can't catch everything. Running a regular, simulated phishing test and establishing a clear, no-blame reporting rule turns your human error factor into a strong defensive line.

3 Understanding Email Authentication

A hardened email setup rests on three protocols working together. Here's what each one actually does:

SPF — Sender Policy Framework

A protocol that allows domain owners to publish a list of authorized IP addresses or subnets that are permitted to send email on behalf of their domain.

DKIM — DomainKeys Identified Mail

A method that adds a cryptographic signature to outgoing emails, verifying that the email actually originated from the claimed domain and ensuring the message content was not altered in transit.

DMARC — Domain-based Message Authentication, Reporting & Conformance

Builds on SPF and DKIM. It instructs receiving mail servers on how to handle emails that fail those checks (quarantine or reject) and sends reporting feedback back to the domain owner.

4 Building Your Incident Response Plan

The first 24 hours determine your reputation.

Contact List:

- **Internal:** IT Lead, Executive Director, and Legal Counsel.
- **External:** A vetted Managed Service Provider (MSP) for technical forensic help, your insurance provider, and local authorities (if data theft or financial crime is confirmed).

Communication Team:

- **Transparency:** Prepare draft templates for donors, staff, and beneficiaries that explain what happened, what steps you are taking, and how they can protect themselves.
- **Speed:** Aim to communicate within 24 hours of confirming a breach to preserve organizational reputation.

Containment Steps:

1. **Isolate:** Disconnect affected machines from the network to stop the spread of malware.
2. **Credential Reset:** Force a password reset for all administrative and user accounts across the impacted environment.
3. **Forensic Preservation:** Before wiping a machine, document the state of the system; this trail is essential if you need to report the incident to law enforcement or regulators.
4. **Service Triage:** Temporarily take public-facing pages offline if they are actively serving malicious content, rather than leaving them compromised while waiting for a fix.

5 The Top 5 Security Threats to Nonprofits

Ransomware Attacks:
Hackers deploy malware to lock organizations out of their critical systems and data, demanding payment to restore access. This is devastating for nonprofits because operational downtime directly stops their services and fundraising efforts.

Phishing and Social Engineering:
Cybercriminals send deceptive emails or texts impersonating trusted donors, vendors, or colleagues to trick staff into revealing sensitive passwords, transferring funds, or downloading malware.

Business Email Compromise (BEC):
Hackers compromise or spoof a legitimate employee's email account to redirect legitimate invoices, payroll, or donor refunds into attacker-controlled bank accounts, resulting in direct financial loss.

Third-Party Vendor Vulnerabilities:
Nonprofits rely extensively on third-party platforms for donor management, accounting, and cloud storage. If one of these vendors suffers a data breach, the nonprofit's connected ecosystem and sensitive data are immediately exposed.

Donor Data Exposure
Nonprofits collect highly sensitive personally identifiable information (PII) and payment details. Hackers target this information to sell on the dark web or to execute highly personalized spear-phishing campaigns against high-net-worth donors.

6 Real Philadelphia Nonprofits Hit by Cyberattacks

(And how we can protect you.) These lessons highlight common failure points and the specific, actionable steps that could have mitigated or prevented them.

Philadelphia Corporation for Aging

The Incident: A prominent Philadelphia nonprofit serving seniors announced a cybersecurity incident where an unauthorized party gained access to their network. The breach potentially exposed sensitive personally identifiable information (PII) and protected health information (PHI) of an unknown number of individuals.

PREVENTATIVE FIX — STRICT ACCESS CONTROLS & NETWORK SEGMENTATION
By applying the principle of least privilege, the organization could have limited the "blast radius" of the unauthorized access, ensuring the attacker could not move laterally into sensitive PII/PHI databases. Multi-Factor Authentication on all network entry points would have likely blocked the initial unauthorized entry.

Equilibria Mental Health Services

The Incident: A distinguished Philadelphia-area mental health and behavioral services provider announced a data breach after a highly targeted phishing attack compromised two employee email accounts — exposing names, addresses, health insurance plan details, and sensitive PHI, including explicit self-reported medical reasons for seeking treatment, for approximately 2,000 individuals.

PREVENTATIVE FIX — STAFF TRAINING & ADVANCED EMAIL FILTERING
Regular, simulated phishing training would have better equipped employees to recognize and report the deceptive email before clicking. Advanced email filtering could have identified and quarantined the malicious link or attachment before it ever reached their inboxes.

These examples demonstrate that robust security isn't just about expensive technology, it's about combining human education (training) with technical safeguards (MFA, filtering, and access controls). By integrating these defensive layers, nonprofits can significantly harden their posture against the threats they face today.

— The We Love Philly Cybersecurity Team