Apparo

AMPLIFYING NONPROFIT IMPACT

Follow Apparo on LinkedIn

Subscribe to Apparo email

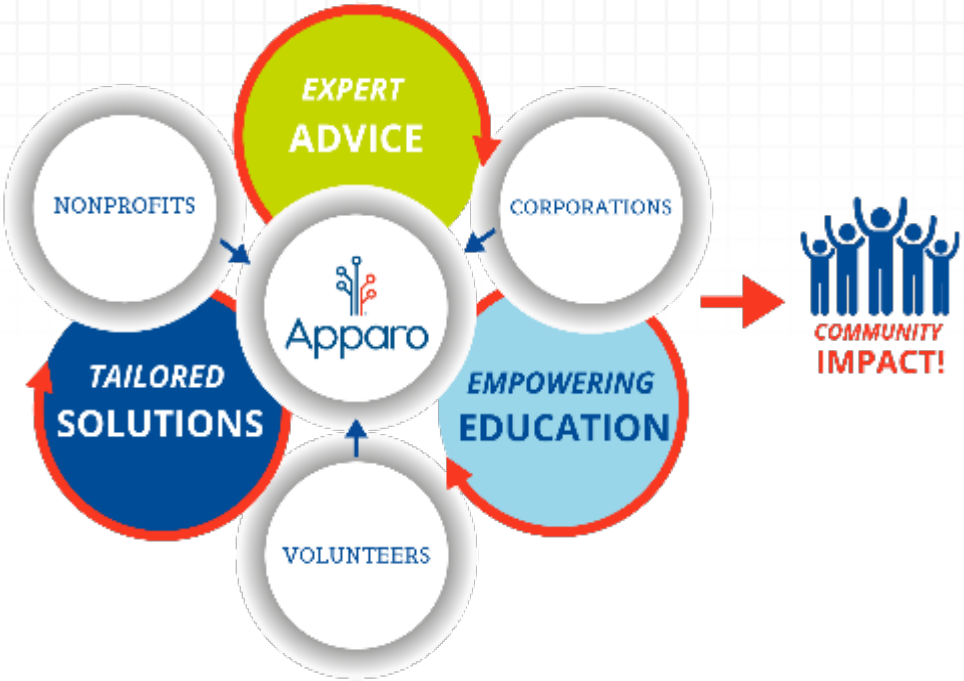
Bolster Your Organization's Cybersecurity

Apparo

AMPLIFYING NONPROFIT IMPACT

We believe that technology and passion can change the world.

Our Model Serves our Mission



Our mission is to transform communities by connecting nonprofits to technology expertise and resources that amplify their impact.

AMPLIFYING NONPROFIT IMPACT

Apparo Tech Therapy Team

Stephanie McKee

Jennifer Ray

Jerri Grant

Todd Reavis

AMPLIFYING NONPROFIT IMPACT

Today's Goals

- ✓ Understand cybersecurity threats
- ✓ Recognize common attack tactics and how to spot them
- ✓ Learn simple, practical steps to protect your organization
- ✓ Know what to do if an incident occurs
- ✓ Leave empowered to strengthen your nonprofit's digital defenses

AMPLIFYING NONPROFIT IMPACT

Why Cybersecurity Matters

Impacts of Cyberattacks on Nonprofits

- Loss of trust and reputation
- Financial losses and operational disruption
- Vulnerability due to limited resources
- Compliance and legal risks

Apparo

Why Nonprofits Are Vulnerable

- ✓ Limited Budgets
- ✓ Lack of Training
- ✓ Outdated Technology
- ✓ Small Teams
- ✓ Trusting Culture

AMPLIFYING NONPROFIT IMPACT

Apparo

Types of Cyber Risks

Phishing and Business Email Compromise (BEC)	Increasingly sophisticated phishing techniques Targeted attacks on nonprofit organizations
Ransomware attacks	Disruption of operations Potential financial losses
Insider threats	Employees or volunteers compromising data Intentional or unintentional actions
Third-party/vendor breaches	Weaknesses in vendor security
AI-driven scams	Use caution with entering confidential data into an AI tool

AMPLIFYING NONPROFIT IMPACT

Poll

Which of the following is the most common cause of cybersecurity breaches in nonprofits?

- Using outdated antivirus software
- Insider threats from staff or volunteers
- Phishing emails
- Lack of a cybersecurity budget

Phishing Emails

- Within the first 10 minutes of receiving a malicious email, **84% of employees** took the bait by either replying with sensitive information or interacting with a spoofed link or attachment.
- **13% of targeted employees reported the phishing attempts**. Employee failure to report phishing attempts limits the organization's ability to respond to the intrusion and alert others to the threat.

Apparo

Phishing Attacks: Recognize and Prevent

Definition of Phishing

- Phishing is a type of cyber attack where attackers impersonate legitimate entities to steal sensitive information.

Common Examples Relevant to Nonprofits

- Emails pretending to be from trusted organizations asking for donations.
- Fake invoices or payment requests.

How to Protect Yourself

- Verify Senders
- Think Before You Click
- Train Your Team
- Use Technology

AMPLIFYING NONPROFIT IMPACT

Phishing Red Flags

Urgent language

Creates a sense of urgency to prompt immediate action

Unusual sender address

Sender's email address looks suspicious or unfamiliar

Unexpected payment request

Request for money or payment that was not anticipated

Strange links or attachments

Links or attachments that seem out of place or irrelevant

Real Life Incident

Save the Children Data Breach (2017)

Phishing Attack

- compromised an employee's email
- attackers posed as a vendor requesting funds

Financial Impact

- $1M transferred to a fraudulent account

Vulnerability of Nonprofits

- smaller IT teams
- weaker cybersecurity budgets
- sensitive missions that pressure organizations to pay quickly

Ransomware: Holding Data Hostage

Understanding Ransomware

- Malicious software that encrypts data
- Demands ransom for decryption key

Impact on Nonprofits

- Disruption of operations
- Loss of sensitive data
- Financial strain

Prevention Strategies

- Regular data backups
- Use of antivirus software
- Employee training on phishing

Real Life Incident

OneBlood Ransomware Attack (2024)

Ransomware attack

Attackers encrypted data systems
Surgeries and procedures were delayed
Donor data was stolen

Vulnerability of nonprofits

Cybersecurity can directly impact mission delivery
Cyberattacks can interrupt services
Critical operations may stop entirely
Donor trust can be damaged quickly

Third Party Incidents

Real-World Example: Third-Party Breach

2020: Major ransomware attack on Blackbaud (nonprofit cloud service provider).

Donor, financial, and personal data exposed across hundreds of nonprofits.

Organizations had to notify donors and manage the fallout.

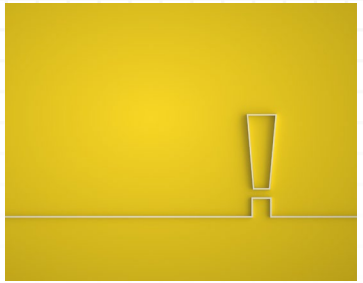
Even nonprofits with strong internal cybersecurity were affected.

Trust and donor relationships were deeply impacted.

Post-Incident Actions: What to Do After a Breach

Immediate Steps

- ✓ Notify leadership & relevant stakeholders
- ✓ Engage with experts for advice
- ✓ May need to reset passwords, disable certain accounts
- ✓ Begin the recovery process



Post-Incident Review

A support partner can help:

- ✓ Analyze the cause and impact of the breach
- ✓ Evaluate the effectiveness of the response
- ✓ Implement improvements to prevent future breaches
- ✓ Document lessons learned

Cybersecurity Basics: Protect Yourself

1. Stop & Ask
   - Pause before taking action
   - Question unexpected requests
2. Examine senders and links
   - Check email addresses carefully
   - Hover over links to see the actual URL
3. Be careful with downloads
   - Only download from trusted sources
   - Scan files for malware
4. Verify payments
   - Confirm payment requests through a separate communication channel
5. Be suspicious of urgency

Common Starting Points

Not everything—just where many organizations begin

- Multi-factor authentication (MFA) on key systems
- Password manager
- Basic phishing awareness
- *Not everything—just where many organizations begin*

AMPLIFYING NONPROFIT IMPACT

Multi-Factor Authentication (MFA)

What is MFA?

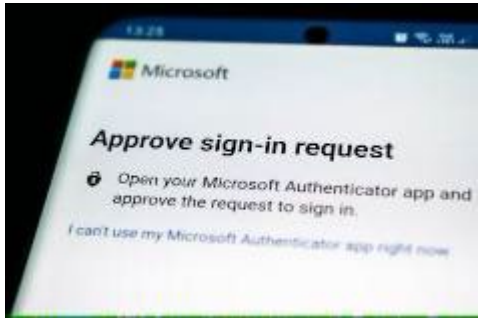
- MFA stands for Multi-Factor Authentication
- It is a security system that requires multiple forms of verification
- Enhances security by requiring more than one method of authentication

Why use MFA?

- Provides an extra layer of security
- Helps protect sensitive information
- Reduces the risk of unauthorized access

Steps to get started with MFA

- Choose an MFA method (e.g., SMS, email, app)
- Set up the chosen method on your account
- Verify your identity using the selected method



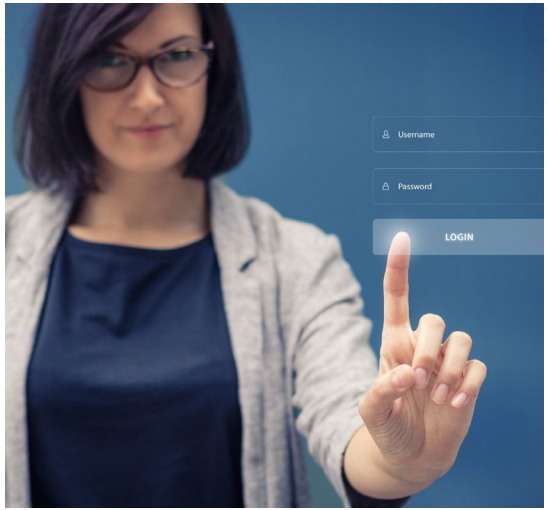
Password Management

Password Managers

- Securely store and manage passwords
- Generate strong, unique passwords
- Reduce risk of password reuse

Key Practices for Passwords

- Use complex and unique passwords
- Enable two-factor authentication
- Regularly update passwords
- Avoid using easily guessable information



Staff Training: A Key Line of Defense

Importance of Training

- Enhances employee skills and knowledge
- Improves organizational performance

Key Training Activities

- Regular cadence
- Interactive online courses
- Hands-on practice

Free Resources

- Utilize platforms like CanIPhish
- Access to a variety of training materials

Apparo

Cybersecurity Quick Wins

Enable MFA

Multi-factor authentication adds an extra layer of security

Use a password manager

Securely store and manage passwords

Train your team

Educate staff on cybersecurity awareness & best practices

Keep systems updated

Regularly update software to patch vulnerabilities

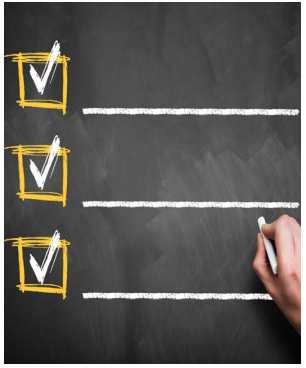
Access controls

Establishing clear policies and procedures

Set permissions

Regular backups

Keep multiple copies of data in different locations



AMPLIFYING NONPROFIT IMPACT

Apparo

Minimum Viable Security

The smallest set of practices that meaningfully reduce risk

- Focus on impact, not completeness
- Prioritize what's realistic
- Build over time

AMPLIFYING NONPROFIT IMPACT

Free and Affordable Resources

- CanIPhish – Free phishing simulator
- CISA - Cybersecurity and Infrastructure Security Agency
- National Cybersecurity Alliance
- FCC - Federal Communications Commission
- Internet Crime Complaint Center
- Apparo Basic Cybersecurity Assessment

Apparo

Q&A

Apparo

AMPLIFYING NONPROFIT IMPACT

Please stay connected with us.

Learn more, Contact for help

Follow Apparo on LinkedIn

Subscribe to Apparo email

Review Apparo on Google