connect cause
YOUR CAUSE. OUR MISSION.

Connect Cause works exclusively with nonprofits and other charitable foundations to improve their technology solutions, so that they can make an exponential impact and better serve their communities.

www.ConnectCause.com

The Nonprofit's Guide to Cybersecurity

Table of Contents

Introduction

Are Nonprofits Really at Risk of a Cyberattack?

In today's digital age, cybersecurity is not just a concern for large corporations—nonprofits are equally at risk. As a nonprofit organization, you handle sensitive data, including donor information, financial records, and possibly even personal information about the people you serve. Protecting this data is not only crucial for maintaining trust but also for ensuring that your nonprofit can continue its vital work without disruption.

Data breaches, ransomware attacks, and phishing scams can result in significant financial losses, operational disruptions, and damage to your nonprofit's reputation.

Cyberthreats are everywhere, and they are always evolving. Which means, it's not a matter of **IF** a nonprofit will experience a cyberattack, it's a matter of **WHEN** and **HOW BAD** it will be.

Important Facts About Cyberattacks

39

A cyberattack takes place every 39 seconds! This equates to more than 2,200 attacks per day across various industries--including nonprofits!

According to Security Magazine

72%

Between 2021 and 2023, data breaches rose by 72% and the cyberattacks show no signs of slowing down.

According to Forbes

$1.72 MILLION

The average cost of a data breach in the nonprofit sector is estimated to be around $1.72 million, a significant financial burden for nonprofits that rely on donor funding.

According to IBM

So how are you protecting your sensitive information?

Why is Cybersecurity Important for Nonprofits?

Protection of Sensitive Data

Nonprofits often collect and store sensitive information such as donor details, financial transactions, and client records. A breach could result in the loss of this data, leading to severe consequences including legal penalties, loss of donor trust, and damage to your reputation.

Compliance with Legal Requirements

Depending on your location and the type of data you handle, there may be legal requirements regarding data protection. Failure to comply with these regulations can result in fines and legal action against your nonprofit.

Operational Continuity

Cyberattacks can lead to significant downtime, disrupting your operations. This could mean a halt in critical services, delaying projects, and even losing funding opportunities. Ensuring your systems are secure helps maintain operational continuity.

Financial Impact

The cost of recovering from a cyberattack can be enormous. Apart from potential fines and legal fees, there are also costs associated with data recovery, system repairs, and loss of revenue due to downtime.

Preserving Donor Trust

Your donors trust you with their personal information. A breach can erode this trust, leading to a decline in donations and support for your cause.

Key Cybersecurity Terms You Need to Know

While this list is in no way comprehensive, here are some of the most common Cybersecurity terms that will help you navigate this topic.

Cyberthreat Actor

An individual or group responsible for carrying out a cyberattack. Cyberthreat actors may include hackers, cybercriminal organizations, or even disgruntled insiders who seek to exploit the nonprofit's systems or data for malicious purposes.

Cyberattack

A deliberate attempt by a cyberthreat actor to compromise the security, integrity, or availability of a nonprofit's digital systems or data.

Threat

Any potential event or action that could cause harm to a nonprofit's digital assets or operations. In a cybersecurity context, a threat could be a cyberthreat actor, a malware infection, or even a natural disaster that puts the nonprofit's data at risk.

Vulnerability

A weakness or flaw in a nonprofit's digital infrastructure that can be exploited by cyberthreat actors to carry out an attack. Vulnerabilities might include outdated software, weak passwords, or untrained staff.

Loss

The negative impact or damage suffered by a nonprofit as a result of a successful cyberattack. Losses can be financial or operational. Losses can also include reputational damage, leading to decreased donor trust and support.

Cyber Risk

The potential for loss or harm to a nonprofit as a result of a cyberattack or other cybersecurity threat. Cyber risk involves assessing the likelihood of a threat exploiting a vulnerability and the potential impact of such an event.

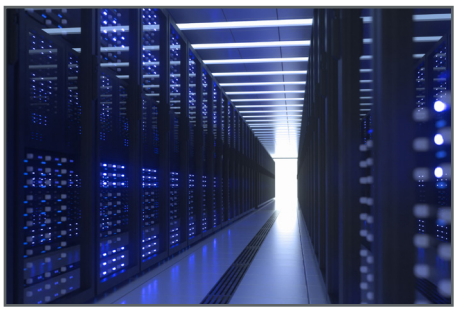
Common Cybersecurity Threats Face by Nonprofits

Phishing Attacks

Phishing is a common tactic where attackers send fraudulent emails designed to trick recipients into revealing personal information or clicking on malicious links. These attacks are often disguised as legitimate requests from trusted sources.

Ransomware

Ransomware is a type of malware that encrypts your data, making it inaccessible until a ransom is paid. Nonprofits are particularly vulnerable due to limited IT resources, making them attractive targets for ransomware attacks.



Data Breaches

Data breaches occur when unauthorized individuals gain access to your nonprofit's sensitive information. This can happen through various means, including weak passwords, unpatched software, or insider threats.

Social Engineering

Social engineering attacks exploit human psychology to manipulate individuals into divulging confidential information. This could involve impersonating a trusted colleague or using other tactics to gain access to sensitive data.

Tips to Keep Your Nonprofit Safe

Implement Strong Password Policies

Ensure that all staff and volunteers use strong, unique passwords and change them regularly. Consider implementing multi-factor authentication (MFA) to add an extra layer of security.

Regularly Update Software

Keep all software, including operating systems and applications, up to date with the latest security patches. Outdated software is a common entry point for cyberattackers.

Conduct Regular Security Training

Educate your staff and volunteers about the importance of cybersecurity and how to recognize potential threats. Regular training sessions can help prevent accidental breaches caused by human error.

Back Up Your Data

Regularly back up your data and store it in a secure location. Ensure that backups are not connected to your main network to prevent them from being compromised in the event of an attack.

Develop and Incident Response Plan

Have a plan in place for responding to a cyberattack. This should include steps for containing the breach, notifying affected parties, and restoring operations as quickly as possible.

Partner with a Trusted IT Partner

Working with an IT provider like Connect Cause that understands the unique needs of nonprofits can help ensure your systems are secure and compliant with the latest regulations.

How to Educate and Train Your Employees, Donors, Board Members and Volunteers

Start with the Basics

Overview Sessions: Begin with introductory sessions that cover fundamental cybersecurity concepts. Ensure everyone understands what cyberthreats are, why they matter, and how they can impact the nonprofit. Tailor content to the different audiences (employees, board members, volunteers, and donors) based on their roles and involvement with the nonprofit.

Common Threats: Explain common threats like phishing, ransomware, and social engineering, using real-world examples that are relevant to nonprofits.

Role-Specific Training

Customized Content: Develop role-specific training that aligns with the responsibilities of each group. For example, employees who handle donor data may need in-depth training on data protection, while board members might focus on governance and compliance issues.

Scenarios and Simulations: Use scenario-based learning and simulations tailored to each group. For instance, simulate a phishing attack and walk them through the steps to recognize and respond appropriately.

Regular, Ongoing Training

Scheduled Updates: Cybersecurity is an evolving field, so make training a regular part of your nonprofit's operations. Quarterly or bi-annual training sessions can help keep everyone updated on the latest threats and best practices.

Short, Frequent Reminders: Incorporate short, frequent reminders or micro-learning sessions to reinforce key points. This can be done through newsletters, emails, or during regular meetings.

Interactive and Engaging Methods

Workshops and Webinars: Host interactive workshops or webinars that allow participants to ask questions and engage with the material. Make the sessions hands-on by including exercises like identifying phishing emails or setting up multi-factor authentication (MFA).

Entertainment: Use entertainment techniques, such as quizzes, challenges, or rewards, to make learning about cybersecurity more engaging and memorable.

Create and Distribute Easy-to-Use Resources

Guidelines and Checklists: Develop easy-to-understand guidelines, checklists, and cheat sheets that cover best practices for password management, email security, and safe internet use. Ensure these resources are accessible to everyone involved with your nonprofit.

Video Tutorials: Create or share short video tutorials that demonstrate key cybersecurity practices, such as how to spot a phishing email or the importance of regular software updates.

How to Educate and Train Your Employees, Donors, Board Members and Volunteers (Continued)

Promote a Culture of Cybersecurity

Leadership Involvement: Encourage leadership, including board members, to actively participate in cybersecurity training. When leaders take cybersecurity seriously, it sets a tone for the rest of the nonprofit.

Encourage Reporting: Foster an environment where employees, volunteers, and even donors feel comfortable reporting suspicious activities or potential security issues. Make sure they know how and to whom they should report these concerns.

Highlight the Importance of Personal Cybersecurity

Extend Training Beyond Work: Educate participants on how cybersecurity practices at home can affect the nonprofit. For example, explain the risks of using the same passwords for work and personal accounts or the dangers of unsecured home Wi-Fi networks.

Empower Donors: While donors may not need in-depth training, offering tips on how they can protect their personal information when interacting with the nonprofit (e.g., securely donating online) can build trust and enhance overall cybersecurity.

Evaluate and Adapt Training

Feedback Loops: Gather feedback from participants to identify areas where training can be improved. Use this feedback to adapt and enhance future sessions.

Assessment and Metrics: Assess the effectiveness of your training programs by tracking metrics like participation rates, the number of reported phishing attempts, or completion of cybersecurity quizzes. Adjust the content based on these assessments.

Utilize External Experts

Cybersecurity Consultants: Consider bringing in external cybersecurity experts to conduct training sessions or workshops. They can offer specialized knowledge and provide insights into the latest threats and defenses.

Partnerships with IT Providers: Leverage your relationship with IT providers like Connect Cause, who specialize in working with nonprofits, to co-host training or provide resources that are specifically tailored to your nonprofit's needs.

Conclusion

Protect Your Data and Your Mission!

Cybersecurity is an ongoing process that requires vigilance, education, and the right tools. By taking proactive steps, your nonprofit can protect its valuable data, maintain donor trust, and continue its mission without interruption. At Connect Cause, we are dedicated to helping nonprofits navigate the complexities of cybersecurity. Contact us today to learn more about how we can support your nonprofit's IT needs.

About Connect Cause

The Connect Cause Difference

When you partner with a Managed Services Provider, you begin a relationship made up of equal parts technology and trust. The technology can be specified, but the trust must be earned. By partnering with Connect Cause, you will work with our expert technicians who are certified across all major systems, but with a model that has your nonprofit nonprofit's budget in mind.

Connect Cause helps nonprofits better serve their communities by transforming their technology. Your mission is our first priority, which is why we're dedicated to making sure technology is a success driver and not a roadblock. No matter what technology challenges nonprofits face, Connect Cause delivers the planning, project management and database & application development to help make it happen. Through our managed IT services, we support the entire technology infrastructure, in the cloud or on-premises, to ensure our nonprofit clients are supported and protected. From software and service deployment to support and maintenance, our nonprofit-focused experts provide strategic technology guidance that helps nonprofits do more with less.

Let's Partner Together

Contact Us

Connect Cause
9001 Aerial Center Pkwy
Suite 110
Morrisville, NC 27560

www.ConnectCause.com

(919) 925-5881

connect@connectcause.com

Follow Us

@ConnectCause @ConnectCause @ConnectCause @ConnectCause @ConnectCause1 @ConnectCause