SEO DETAILS:

Page Title: How to Protect Your Nonprofit Organization from Cybersecurity Threats | [INSERT RELATED SERVICE] | [INSERT FIRM NAME]

Meta Description: Though many nonprofits have moved cybersecurity to the back of their threat list, [NAME OF FIRM] covers why it should be at the top of yours. As cyberattacks become more sophisticated and complex, it's much easier to accidentally end up with a data breach of your employees', clients' or patrons' private information.

Headline: How to Protect Your Nonprofit Organization from Cybersecurity Threats

BODY COPY:

October was Cybersecurity Awareness Month, which emphasizes the high level of risk that cybersecurity issues pose to nonprofit organizations, especially as they become more sophisticated. Given the leaner than usual work environment existing in many nonprofits today because of the COVID-19 pandemic and economic concerns, cybersecurity has often taken a back seat to other operational concerns. However, shifting your organization's cybersecurity into a lower priority or no priority situation can make the problem even worse.

If your organization is depending on simple firewalls and policies to deal with the situation, your organization may be at grave risk as cyberattacks become both more frequent and more complex. Because of the advancements being made in technology and workflow automation, this risk is increased significantly, especially for organizations that have been forced to have workers use home-based systems or personal devices to complete their tasks. Vulnerabilities and the urgency with which these systems were established as the pandemic swept through our world have allowed potential issues to remain unaddressed by IT teams, leaving workers' home networks, personal computers and private finances vulnerable to cyberattacks, and your nonprofit susceptible to significant risk.

But why are criminals and hackers now targeting nonprofits? What do they have to gain in the process? Because your systems contain a range of sensitive information about your workers, donors and clients, that information can be used in identity theft, with information such as Social Security numbers, driver's license numbers, names, birth dates, government ID numbers and similar details. They can also see information about your donors, potentially including their credit card numbers, bank routing and account information and similar details. What about medical or other confidential and protected data from your clients, patients or employees? Any type of data breach and data loss can seriously damage your nonprofit's reputation and ability to continue its mission.

For this reason, your nonprofit needs to regularly review and assess the existing digital environment, including virtual infrastructure, no matter what type, level of sophistication or size of your nonprofit. This system needs to be a regular conversation point during board and management meetings. Everyone in the organization needs to be working collaboratively with both your external IT vendors and internal IT professionals to ensure that they have a solid understanding of the company's potential vulnerabilities.

So what should you do to make sure that your nonprofit is protected from these kinds of attacks? Here are three separate areas where you can take significant action to improve the situation, along with recommendations of what to do to get started:

IT Team

- Add multifactor authentication to vulnerable accounts
- Use encryption on all hard drives and storage devices
- Ensure all firewall software and firmware is kept current and configured properly for your needs
- Confirm the presence and functionality of antivirus and malware software on all devices
- Regularly review and patch any organization devices requiring updates
- Conduct periodic baseline systems scans, reviewing the results to discover any new vulnerabilities
- Create and monitor the logs for network events to detect, prevent and recover more easily from cyberattacks

Human Resources and Operations

- Conduct baseline phishing attacks on your own system, addressing any issues that may arise
- Create standard approaches for cybersecurity risks
- Provide cybersecurity training as a portion of your onboarding process
- Conduct regular cybersecurity educational opportunities and training for your employees
- Annually review all user logins and user access rights to all applications, data and software

Policies and Processes to Incorporate

- Require all users to sign off on your computer user policies
- Decide, communicate and enforce which devices or software programs can come into contact with your organization
- Review available cyber insurance or similar coverage and purchase a protection policy
- Encourage cybersecurity professional development on an annual basis for tech leaders and key organizational personnel
- Review cloud-based security agreements annually to ensure you're protected
- Audit and assess your third-party cybersecurity assets
- Take time to review and update your organization's continuity strategy
- Ensure you have a solid document retention and destruction plan in place

By understanding the threat that cybersecurity issues can pose to your organization, you'll be better positioned to avoid these threats and minimize their potential damage to your organization's reputation. Take a few minutes to review your current policies, practices and

procedures with your management team, then discuss ways that you can improve on your existing plan of action to ensure better cybersecurity moving forward.

CLOSE:

If you have any questions or would like to discuss how to best protect your nonprofit from cyberattacks, please contact [NAME] in our [DEPARTMENT] at [NUMBER/EMAIL].

SUGGESTED IMAGERY:

https://stock.adobe.com/images/cyber-security-and-protection-of-private-information-and-data-concept-locks-on-blue-integrated-circuit-firewall-from-hacker-attack/267969101?prev_url=detail