SEO DETAILS:

Page Title: Training Nonprofit Staff to Safeguard Against Cyber Threats | [INSERT RELATED SERVICE] | [INSERT FIRM NAME]

Meta Description: [NAME OF FIRM] addresses common sources of cybersecurity threats and offers tips on how nonprofit organizations can train their staff members to be prepared.

Headline: Training Nonprofit Staff to Safeguard Against Cyber Threats

BODY COPY:

Cybersecurity is no longer a niche subject relegated to IT departments. Nearly every type of nonprofit organization now faces threats of cyberattacks like data breaches or ransomware and needs to get everyone on their staff involved in preventing or responding to cybersecurity threats. Every employee has a role to play, starting with learning what types of threats the organization faces and how they might inadvertently contribute to those risks. The following article addresses common sources of cybersecurity threats and offers tips on how nonprofit organizations can train their staff members to be prepared.

Understanding the Causes of Data Losses

When people hear terms like “cybersecurity” or “data breaches,” they might think of brute-force attacks by hackers to break into a system and steal data. This is only one way, however, that bad actors can gain access to nonprofit organizations’ computer systems. Common cyber threats may include the following:

- Employee errors or carelessness;
- Social engineering, including phishing scams and other fraudulent efforts to obtain information; and
- Malware, ransomware and other malicious software.

Many nonprofits store a considerable amount of data relating to donors or members on servers or in cloud accounts. This data could be quite valuable to hackers involved in identity theft and other criminal schemes. Nonprofits have a responsibility to keep this information safe. They risk losing not only important and valuable data but also the trust of their members and their community.

How to Train Staff to Avoid or Respond to Cyberattacks

Nonprofit employees need to be part of a comprehensive plan to prevent cyberattacks. They also need to know what to do if they discover that a cyberattack has happened or is in progress. A nonprofit organization’s cybersecurity policy needs to include training guidelines for all staff members.

Types of Threats The Organization Faces

Each nonprofit organization faces a unique set of cybersecurity risks and threats. Employees need to know which types of threats affect their organization. They might not need extensive technical training on issues like how ransomware works, but they should understand the nature of the threats.

Recognizing Social Engineering Attempts

Social engineering is an increasingly common method of gaining illicit access to nonprofit organizations' data. While security software receives regular updates to address new threats, human nature remains mostly the same. Malicious actors may pose as someone in a position of authority or trust. Phishing scams do this through email communications. Other forms of social engineering include:

- Vishing, which uses telephone or other voice communication to trick an employee into revealing sensitive or confidential information; and
- Smishing, which tries to achieve the same ends via text messaging.

Maintaining Up-to-date Software

Employees who have their own work computers or mobile devices need to keep all software up-to-date. This includes regular updates and security patches.

Keeping Work and Personal Systems Separate

The commingling of work and personal matters on a single device can lead to cybersecurity vulnerabilities. This can be especially true for remote workers. Employees need to be aware of any policies regarding personal use of an organization's devices.

Avoiding Risky Environments

Certain environments present greater risks of data breaches. Public locations with unsecured Wi-Fi networks are a prime example. Employees need to know about the risks, as well as the potential consequences of carelessness.

Password Security

Hackers may be able to gain access to an organization's data by obtaining or guessing someone's password. Employees should be aware of best practices for password security, such as:

- Changing passwords often;
- Choosing long passwords that combine letters, numbers and symbols;
- Choosing passwords that are difficult to guess based on an employee's personal information; and
- Never divulging a password to another person.

Frequent Backups

Ransomware attacks can be particularly devastating since they could cut off an organization from all of its data. Regular backups can help mitigate that risk. Employees need to know how they can help this effort.

What to Do if a Cyberattack Happens

Every organization needs a plan for how to respond to a cyberattack. This might include notifying key personnel and providing them with essential information. Employee training should include each person's responsibilities in this process. Every employee should know whom to call should an attack occur.

Learn How to Prepare for the Risks

Nonprofit organizations face more risk of cyberattacks than ever. The threats keep changing and adapting, as do the efforts to prevent and combat them. Staff members need to be aware of

the threats that their organization faces. They need to know what they can do to prevent attacks, and what to do should an attack occur. Help is available for organizations looking for resources and strategies to get their teams working together to keep their digital assets secure.

CLOSE:

If you have any questions or would like additional information, please contact [NAME] in our [DEPARTMENT] at [NUMBER] or [EMAIL].

SUGGESTED IMAGERY:

https://stock.adobe.com/images/cyber-security-concept-authentication-screen-on-computer-confidential-business-data/173503359?prev_url=detail