Smart Cybersecurity Measures Any Nonprofit Can Take

By Rachel Sams

Lead Consultant and Editor

Resource Type: Articles

Topic: Data Privacy, Tech Risk, Cybersecurity

The email came from someone I knew. It linked to a document I was expecting to receive. But the link looked bland and generic—the way examples of phishing scams look.

I was tired. I wanted to click, get the document and get on with my day.

I thought about the Take 9 campaign from Craig Newmark Philanthropies ("Take a 9-second pause and think before you click, download, share.") OK, I thought, I can take 9 seconds.

When those 9 seconds were up, I knew I should dial the phone, just to check. So I did. I left my contact a voicemail. They responded right away, sounding surprised to hear from me but glad to confirm they sent the document.

Double-checking where that link came from cost my nonprofit zero money and very little time.

I might click a malicious link or attachment someday. Anyone might. But plenty of free or low-cost steps like the one above can help your team strengthen its cyberdefenses and make it more likely that you can consistently keep your nonprofit's data safe.

Why Cybersecurity Matters

If you think your nonprofit doesn't have any data cybercriminals would want, think again.

All nonprofits collect personally identifiable information. Your digital and paper files are likely full of phone numbers, email addresses, and physical addresses of clients, team members, volunteers, and more. Somewhere in your systems, you likely store even more sensitive information, like credit card numbers and bank account data. You may have demographic information about the ethnicity or gender of participants, volunteers, and staff.

Every piece of that information belongs to a person: a valued team member or client. That means your mission includes protecting those people's data from misuse.

Common examples of cybersecurity breaches nonprofits experience include:

- Social engineering “phishing” scams like the one I suspected in the example above. If you’ve ever received an email that appeared to come from your CEO, pleading with you to issue gift cards to someone immediately, you’ve experienced a phishing attempt. Social engineering uses emails, texts or social media messages to prompt users to reveal sensitive information or access a malicious link or attachment. In “spear phishing,” attackers tailor these attempts to a person based on information from their public social media or publicly available profiles.
- Malware, or software that can disable computer systems, destroy or steal data, and more. This category includes ransomware, in which the attacker demands a ransom to get data back or systems operating again.
- Denial-of-service (DOS, or DDOS for larger-scale distributed-denial-of-service) attacks flood an organization with electronic traffic until its systems can’t respond to routine requests.

Start with Humans

How do you address the risks of those types of cyberattacks?

The human beings in your organization are its strongest and weakest link when it comes to cybersecurity. Your team members’ quick thinking could thwart an attack, while one seemingly small mistake could compromise your entire network and cost you millions of dollars. To fortify your cyberdefenses, it makes sense to start with your people.

If you don’t already send your team members phishing simulations, where a third party tests them on how they would respond to common social engineering scenarios, that’s a great place to start. Your IT provider may be able to provide these as part of your existing relationship, or you may be able to take advantage of these features in software like Microsoft Defender. You can also access free resources like KnowBe4’s option to send free phishing simulations to up to 100 users.

Some great cybersecurity practices to instill in your team:

- Hover over links and check sender addresses before responding to an email, clicking a link or downloading an attachment.
- Verify requests like wire transfers, gift cards or password resets through another channel. If the request came by email, reach out to the purported sender by phone or another means to confirm they sent the message.
- Create and share a clear process for how employees who suspect they’ve been phished or your systems have been compromised can report their concerns.
- Use free videos from your Internet provider or other credible sources to reinforce what your team is learning about cybersecurity.

Build on the Basics

Make sure your nonprofit has the basics in place on passwords and multifactor authentication to reinforce system security, too.

- Require long, complex passphrases.
- Don’t allow password reuse across systems, and don’t let employees share passwords with other users.
- Use a password manager like LastPass, 1Password or Dashlane to help team members create strong passwords and securely store them.

Multifactor authentication provides an extra layer of security for your organization’s accounts. At its simplest, multifactor authentication requires additional information beyond a login and password to access organizational systems—for example, a number entered from an authentication app. Multifactor authentication creates additional hurdles for outside actors to break into a system; they’d need not only your login and password, but also the authentication code.

Organizations should consider and address the potential for bias in multifactor authentication. Concerns about that have led some nonprofits to avoid authentication options that involve facial recognition. Of the major

biometric authentication methods in use, facial recognition is the least accurate, raises extensive privacy concerns, and current implementation of the technology “involves significant racial bias, particularly against Black Americans,” according to Harvard.

Here are some additional steps to strengthen your cyberdefenses.

Update software, firewalls, and email filters regularly. I know—it seems like those update messages pop up every day. But taking a few minutes for updates can save hours, days, or weeks of headaches down the road. Software updates can patch vulnerabilities hackers could use to get into a product. They also help protect the personal information on your devices. Encourage your team members to set reminders to download updates when they step away from their computer for lunch or a break.

Remove old user accounts when staff or volunteers leave your organization. Make sure you revoke all their accesses to your systems, from email to shared drives. Create a standardized process for this, so team members aren’t scrambling every time someone leaves.

Standardize where you store files in your organization. Store documents in approved cloud software with access controls rather than local copies on personal devices.

Create tiered data access. Make sure that only employees who need to access specific data, especially sensitive data, have the ability to do so.

Restrict who can install software on organizational devices. Check that your process is simple and seamless. Don’t incentivize the action you’re trying to avoid: staff downloading software on their organization-issued laptops because it ‘takes too long’ to get help from the colleague assigned to help.

Set security standards and protocols for employees who access your organization’s computer system from home or on the road. Make these standards and protocols simple, jargon-free and easy to access.

Collect only the data you really need. Stop collecting data you can’t or won’t use! And follow a practical schedule and protocol for data deletion. If your organization doesn’t collect it, hackers can’t steal it (at least not from you!)

Cyberbreaches: Get Ready to Be Ready

The bad news: Your nonprofit could take all the above steps and still experience a data breach. Cybercriminals are persistent, and they constantly evolve their tactics, including using artificial intelligence to help infiltrate systems.

The good news: If you’ve taken the above steps, you’re likely to incur less damage in a breach. And if you take a little time now to prepare for what you would do in the event of a breach, that stressful time will be less painful. Here are some steps to help.

Identify now who your team will call if a cybersecurity breach occurs. Cyber insurance providers often have “breach coaches” who can lead an insurance response for nonprofits. Put your legal counsel on the list of people to call, along with any cybersecurity law or forensic experts your counsel recommends. Your list might also include your information technology and security vendors, operations, human resources, communications, and management.

Identify which systems and data are mission critical. What systems would render your organization inoperable if you didn’t have access to them? Make sure you have backups in place on those systems. This may happen automatically through your software programs. Double-check whether it does, and if not, make the necessary backup provisions.

Craft a contingency plan. What work could you do if your organization’s major digital systems were unavailable? Who would lead your response to a cyberbreach, and who is that person’s backup?

Keep Learning, Keep Preparing

If you've read this far, you know cybersecurity isn't one and done. Like so many things in our nonprofit organizations, improving our cybersecurity is a journey. If you put some basic safeguards in place, create a plan to keep learning, and share and discuss what you learn, you'll be well on your way to improved cyberhygiene.

Rachel Sams is Lead Consultant and Editor at the Nonprofit Risk Management Center. She is a firm believer in the power of the firewall update on a lunch break. Reach her with thoughts and questions about this article at rachel@nonprofitrisk.org or (505) 456-4045.