Four Simple Steps to Improve Cyberhygiene at Your Nonprofit

By Rachel Sams

Lead Consultant and Editor

Resource Type: Risk eNews

Topic: Data Privacy, Tech Risk, Cybersecurity

Many nonprofits possess huge amounts of valuable data. Plenty of hackers would love to get their hands on the personal data of your employees and the individuals your organization serves, as well as confidential information pertinent to your operations.

Over time, your organization will likely experience countless hack attempts. As we look ahead to National Cybersecurity Awareness Month in October, this article offers a cyberhygiene refresher inspired by guidance from the Cybersecurity and Infrastructure Agency and the National Cybersecurity Alliance. Take some time this month to nail down these cybersecurity basics. While a data privacy breach can happen to even the best-protected organization, these steps will help your nonprofit become a less vulnerable target.

Recognize phishing and report it.

"Phishing," a type of social engineering, uses email and, often, the names of trusted individuals to seek personal information. Nonprofits and all types of businesses face phishing frequently. If you've ever received an email that looks like it's from your boss urgently asking you to click a link, you've experienced a phishing attempt. Provide employees with regular training and reminders on how to recognize phishing. Watch out for suspicious sender addresses, generic greetings, and urgent requests to open or download an attachment. Never click on a link or attachment in such emails, and never provide personal or organizational information unless you're sure a request is legitimate. If a communication from someone whose name you recognize looks off, call them to ask if they really sent the message. Forward any suspected instances of phishing to the person who handles technology for your organization so they can warn others.

Enable multifactor authentication.

Multifactor authentication provides an extra layer of security for your organization's accounts. At its most basic, multifactor authentication requires additional information beyond a login and password to access organizational systems—for example, a code sent to your cell phone. 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 need to consider and address the potential for bias in multifactor authentication. Such concerns 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.

Mandate strong passwords.

Require all passwords for organizational software to be at least 12 characters long. A strong password should include both uppercase and lowercase letters, numbers, and symbols. Do not use a word that can be found in the dictionary in any language. Do not allow employees to use passwords similar to their previous ones. Don't reuse passwords for multiple sites. Encourage employees to use a password manager.

Update software, firewalls, and email filters regularly.

I know—it seems like those update messages pop up every day. Before I wrote this article, I'd clicked the X to postpone a software update every day for weeks. 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 device.

These simple practices can help your organization become cyberwise and keep employee, client, and your organization's information secure. They may require members of your team to build new habits and routines. Resolve to take some time during *National Cybersecurity Awareness Month* to do that. I finally did that software update, which took about 20 minutes. Join me by doing the same!

Rachel Sams is a Consultant and Staff Writer at the Nonprofit Risk Management Center. She'd love to know how your organization keeps basic cybersecurity top of mind. Reach her at 703.777.3504 or rachel@nonprofitrisk.org.