(//www.donorsearch.net)

(//www.donorsearch.net)

(//www.donorsearch.net/held-to-a-higher-cyber-security-standard/)

0 Share

By DonorSearch

The new normal brought on by the COVID-19 pandemic has us working (and interacting) online for much of our waking hours. It's also a time cloaked in chaos and uncertainty – two factors that cybercriminals rely on to prey on all sectors of society – from governments to hospitals to individuals– and *especially nonprofits*.

Opportunistic cybercriminals see nonprofits as the juiciest and lowest hanging fruit–for two main reasons:

1. **No/Limited Cybersecurity Measures in Place.** Limited staffing and/or budge dedicated to cyber security.
2. **Valuable Data.** The data nonprofits collect on individual donors, corporate contributors, partners, vendors, and charities are a gold mine. Personally identifiable information such as names, addresses, credit card details, email, and phone numbers are all there.

Nonprofits are also held to a higher standard for preserving privacy. Keeping data safe can cost. The July 16, 2020 *NonProfit Times* headline, "Blackbaud Hacked, Ransom Paid (https://www.thenonprofittimes.com/npt_articles/breaking-blackbaud-hacked-ransom-paid/)" was a quake felt around the nonprofit industry. While the company handled the situation well, informing their clientele, ensuring the data was not leaked, instituting stronger controls–we're ***all*** still feeling the aftershocks.

MEASURES TO TAKE

1. DEPLOY MULTI-FACTOR AUTHENTICATION (MFA)

MFA is an extra layer of security that requires users to login using their username and password, plus a passcode generated by an authenticating device, an authenticator app, or a text message sent to the user mobile phone. Without the passcode, the account can't be accessed even if the username and password are correct. A hacker would need to have access to the target's mobile phone or authenticating device to be able to breach the account.

2. DEVELOP AND DOCUMENT A CYBERATTACK RESPONSE STRATEGY

Having a robust and comprehensive cybersecurity solution can help mitigate the risks and reduce the impact of a cyberattack. A security policy can help improve response times and provide employees with concrete steps to address the issue.

3. ONLY USE A SECURE DONATION PLATFORM

Nonprofits that rely heavily on fundraising and donations are at higher risk of cyberattack occurring during volatile societal circumstances, like a pandemic. Organizations that collect and store donor information are more at risk. Any data breach could result in a loss of trust and finances. Look for a donation system that

- Has built-in safety features that can detect and guard against fraud.
- Is protected by SSL/TLS encryption technology to ensure that the checkout process is secure at all times.
- Is PCI compliant (global standards for authentication and tokenization for credit card and bank account data–nothing should be stored in your system!

4. TRAIN YOUR STAFF

Training your team on best practices and online/computer hygiene (e.g. using strong passwords, etc.) to shore up weaknesses in your cyber security.

5. CREATE BACKUPS AND REDUNDANCIES

Have multiple instances of crucial data and system redundancies both in a physical server and the cloud (many organizations use super-secure services like Amazon Web Services/AWS or Microsoft Azure), so if one instance gets compromised, you have backups ready to be deployed–saving your work, saving your mission.

6. MAKE YOUR SYSTEM ATTACK-RESISTANT

Harden your system by using security software such as a firewall, VPN, and antivirus. *Do a security assessment to see where you are most vulnerable and get software or tools to help shore up your defenses in these trouble areas.* A firewall can help keep the bad guys out. If they *do* get in, an antivirus or anti-malware solution can help protect your system from infection by flagging dangerous emails and infected drive-by websites.

7. UPDATE YOUR OPERATING SYSTEM AND PATCH ALL SOFTWARE

Make sure your systems are running the latest OS version and that all software has been patched against known vulnerabilities. Make it a point to conduct regular updates to ensure you're not running anything that a hacker can exploit.

8. HAVE A DEDICATED IT EXPERT OR CONSULTANT

If you have the budget, hire a professional in-house IT staff to handle your cybersecurity, someone monitoring your system and network can help detect and repulse threats as they arrive and do weekly checks and monthly security audits. *If you **don't** have the budget to add an FTE, then look for a vendor to provide you with this service on a contract basis. You can't afford not to.*

Nonprofits are trusted by their donors to fulfill their missions of delivering aid, helping vulnerable members of society, and making the world a better (and safer) place. That's why it's ***essential*** that they keep that trust with a strong cybersecurity protocol.