8 Expert Tips: Cyber Security on a Nonprofit Budget

October 30, 2015

By Annabelle Baxter, Senior Manager, External Communications, Alliance Data

Cyber crimes cost the global economy more than $445 billion annually, and the cost is only expected to continue to rise. For the business community, that cost can have a material impact, but for nonprofits with extremely limited budgets, every dollar used toward cyber security is a dollar that can't be used to make an impact on the community. Nonprofits are increasingly being targeted by hackers, so security awareness is just as important for their operations as any other business.

We asked two experts to share their thoughts on how nonprofits can increase their cyber awareness.

Joel Rothermel is the technology director for CNM Connect, which has focused for more than 30 years on strengthening nonprofits, helping them be better connected, engaged and equipped. As technology director, Joel manages CNM's information technology operations and facilities, and also advises nonprofits on technology issues.

Collin Harrison is vice president of finance and information technology for Alliance Data, where he manages a team of over 75 professionals who support enterprise technology systems and information security. Collin has more than 18 years' experience leading technology innovation and transformation across several industries. Collin recently joined CNM's board of directors, with the goal of helping the organization achieve its strategic objectives through the use of modern, secure technology.

For CNM Connect's Joel Rothermel, cyber security has become an important part of the advice and counsel he provides to nonprofits. Here are his five top tips for how nonprofits can be more prepared and cyber aware:

1. Protect Your Network

Have and use a firewall on your network and don't forget to properly restrict outbound traffic too. Your sensitive information should be protected from unwanted visitors.

2. Change Your Passwords

Changing the default passwords on all of your software, firewall and wireless routers should be the first action you take with any technology. Make sure passwords are long enough, complex enough and are changed on a regular basis.

3. Stay Up to Date

Ensure you are always installing the latest patches. Don't forget to patch applications and plug-ins as well as the operating system. Most applications and operating systems have auto-update capabilities. Turn them on. If possible, run the latest version of operating systems and applications to help ensure full vendor support.

4. Everyone is Unique

Avoid sharing logins and passwords within the nonprofit. Everyone needs a unique account. It makes it easier to remove access when someone leaves. Treat accounts and passwords the same as you would your personal bank account, which you wouldn't share with co-workers.

5. Limit Access

Only give people access to information that is in line with their job responsibilities. While it's easier from a support perspective to give everyone administrator access, it will cause more issues in the long run.

We asked Collin Harrison to share his tips for nonprofits as well, and here are the 3 additional insights he shared:

1. Respond to Events Promptly and Correctly

Ensure your employees know who to contact when they think something suspicious has happened. Attempts from an untrained employee or volunteer to try to fix the situation themselves could spread malware, or leave you with a false sense of security that the problem has been resolved.

2. Have a Robust Backup Strategy

Backing up files is critical to ensure timely recovery in the event of an infection.

3. Run Software Only from Trusted Locations

Developing software restriction policies and, more importantly, communicating those to nonprofit employees is critical. Never download or add software without knowing the source. This will also help ensure better control of a malicious program that is running on the computer in case of an incident.

Cyber awareness is the first, and maybe the most important, step in protecting any organization from cyber crimes. For nonprofits with a smaller budget, vigilance takes on even more importance, as, just like everything in life, prevention is much simpler (and economical) than responding to a cyber security event.

— — — — — — — — — — — — —