Security for Non-Profit Organizations: 10 Tips to Help Those Who Help Others

Cheryl Biswas
March 26, 2015

After the massive breaches and attacks of last year, everyone has become far more aware of their vulnerability to being hacked. Security has taken on new meaning as people start putting defensive measures in place. Yet for many, especially those in the Non-Profit sector, this still seems a daunting task due to the perceived costs and skills required to know just what to do.

Like every other business, Non-Profits need to make information security a priority. They are just as much a target for cybercrime, just as susceptible to phishing attacks, ransomware and viruses. Ironically, like Healthcare, they are even more vulnerable because of the volume and sensitivity of the data they have on both donors and those they help. But the reality is that most just don't have the same budgets, skills and resources. How can we best help those who help others?

There's an old adage that goes "Give a man a fish, he'll eat for a day. But teach a man to fish and he'll eat the rest of his life." **Low budget/no budget should not preclude a solid security foundation.** Utilizing the shared wealth of information and experience currently available, there are affordable, manageable steps any organization can take and put in place. Here is a basic ten-step framework for Non-Profit Security.

1. *Support your local sheriff*. You need to have someone in-house who is in charge, ready not only to lay down the law, but to defend it regarding security matters. This person will be your key resource, and liaison with external support. They will know and understand what compliance and governance means for your organization, so that liability doesn't have to become a consequence.
2. *You've got to have a plan*. A Disaster Recovery/Business Continuity Plan. Daily news gives us all the reasons we need: fire, severe storms, acts of nature, and increasingly cyber attacks and ransomware. Putting a plan in place ensures that you have data saved from a recent point in time that you can restore from. That means being able to pick up where you left off so that you aren't losing donors, funding, and time. No more excuses for not having one. It doesn't have to cost much more than the time you invest in doing it. And it is the responsible thing to do.
3. *Back it up*. This is fundamental to your security and your ability to restore should something happen. Decide what data is most crucial and back that up daily. Other information can be done weekly. There are a range of flexible and affordable options utilizing cloud storage. The key is to backup frequently and have redundancy. Yes. More than one, in different locations. Because ransomware, system crashes, and acts of nature happen to backups too.
4. *Show them how*. Your staff needs guidance on what they can and cannot do while at work, or with remote access, or if they bring in their own devices. Your organization is accountable to the donors whose information is on record, as well as to your own team and their safety. Regular training sessions keep everyone well-informed and up to date on current threats like phishing emails, malicious links, dangerous websites, and ransomware. Because threats are constantly changing, sporadic or infrequent bouts of training are not effective. Everyone needs to play their part, and training is essential to explaining not just how but why.

5. *Stay current*. Keep your software and operating systems updated regularly. This is one of the most effective things you can do because it will limit system vulnerabilities that hackers find and exploit. Check for monthly security patches and then install them. Outdated software does not receive security patches or support, leaving you exposed.

6. *Invest in technologies like an enterprise level firewall*. This item is over and above the software firewall offered by Windows or extended anti-virus programs. But the cost is less than you think. Firewalls work to keep intruders out by blocking inbound internet traffic, and the risks are high when you connect via DSL or broadband cable and are always on. In addition, consider technologies such as Intrusion Detection Systems (IDS) - there are some open source free tools to consider.

7. *Restricted access*. Who has access to your data, especially the most critical or sensitive data? Is this data accessible remotely? You need to restrict access so that accidents don't happen via social engineering tactics frequently used by hackers. And you don't want this data to be copied onto portable media like CDs, flash drives or USB keys which can be lost, duplicated or stolen. Only a select few people should have access, with passwords being changed regularly.

8. *Passwords, encryption and VPNs*. These all put up safe barriers against unwanted intrusion. Passwords are the first line of defence but can only be effective if the basic rules are followed: Strong passwords that are 10 characters minimum, combining numbers, letters and special character, with alternating cases. Never use the same password for more than one purpose. And change up passwords because once a hacker finds it, they will keep using it. Do you encrypt what you send out? If not, you should be, particularly for sensitive data. Consider an email provider like Constant Contact or MailChimp to send email blasts and fundraising appeals. Encrypt stored data on site by using tools to encrypt the entire hard drive. Examples are Bitlocker for Windows and FileVault for Mac. VPNs or Virtual Private Networks allow you to securely send data between two points through a digital or virtual tunnel, shielding it from outside threats. These can be easily set up, and much safer than sending via the open Internet.

9. *Pay now or pay later*. How do you handle you online payment processing and payment processing in general? Your method needs to be secure, but it cannot be complicated because you don't want to discourage donors. While many non-profits use PayPal, it has suffered some security breaches in past. There are other third party services for nonprofits, such as Network for Good or Razoo. It pays to fully investigate your options on this.

10. *Secure Your Wireless Network*. Many small organizations use wireless routers. But they leave the default settings in place. Hackers know these and use them to get right into your network. Change your default SSID or wireless network name, and the default or admin password. And again, change up your password. Enable encryption.

Non-profits hold a special place in my heart because helping others is truly a wonderful thing. Helping secure those who help others – well, that's a reward in and of itself. Go on making the world a better place – you can stay safe while you do!

PS, there's also a nice website for non-profits, TechSoup, with how-tos and helpful articles of all kinds