Hackers are Targeting Nonprofits: How Can You Protect Your Organization?

Be sure you're cyber-secure.

By Joseph Steinberg

Nonprofits handle a great deal of sensitive information, which often resides on Internet-connected computers and networks. Donor details, programs, people receiving aid, employee and payroll records, and many other forms of data are of value to criminals.

Hackers know that nonprofits' computer systems are often several years old and designed before digital attacks became common. Cyber-thieves understand that such systems contain vulnerabilities and lack cyber-defenses, making them easier to hack than many systems in the commercial sector.

> Nonprofit systems are often easier to hack than those in the commercial sector.

The consequences of compromised security may not be small. Bad press, fines from credit card companies for failure to conform to security requirements, confidentiality breaches, and identity theft can be catastrophic.

Some cases have made the media. When cyber-criminals breached the Aid to the Church in Need organization, for example, they pilfered approximately 2,800 credit card numbers and associated confidential information.

> Require log-ins with passwords that aren't easily guessable or found in the dictionary.

What can you do to ensure that your organization remains cyber-secure? Here are several pointers:

- Commit to cyber-security in an active way. The cost—in terms of time, money, and aggravation—will likely be far less if you take a proactive approach.
- Create policies governing who has access to which resources. Develop rules and technology to enforce these policies. Access to systems and information should always be on a "need to know" basis. Systems should be used only for their intended purposes—not for reading personal e-mail or accessing Facebook. Ensure that all systems require log-ins with passwords that aren't easily guessable or found in the dictionary.
- If wireless (or wired) Internet is provided for guests within a facility, activate it on its own separate network, isolated from any nonprofit systems and networks. Visitors have no need to access any internal systems. Don't let them.

> When in doubt, encrypt.

- Branch office managers should ensure that they conform to all security policies of the parent organization. They should implement security to assure that a breach at another branch, or at the main office, doesn't prorogate to their location.
- Ensure compliance with all credit card security rules. Unless truly necessary, don't store credit card data after processing transactions. Never store credit card security codes or debit card PIN numbers.
- Store all sensitive data—including donor information, employee data, documents related to programs, and so on—in encrypted formats. When in doubt, encrypt.
- Implement security technology to meet functional and security requirements—and keep all technology up to date. All major recent cyber-security breaches have occurred to organizations running firewalls, anti-virus software, and other security products. You need to go that extra step.
- Leverage the services of a cyber-security professional to design your cyber-security plan. Remember, cyber-criminals have technical expertise. Shouldn't you have it to defend your organization? ■

Joseph Steinberg, CISSP, ISSAP, ISSMP, CSSLP (www.josephsteinberg.com) is an author, inventor of several cyber-security technologies, lecturer on topics related to cyber-security, and CEO of Green Armor Solutions, a leading provider of information security software.

Nonprofit World • Volume 30, Number 1, January/February 2012.
Published by the Society for Nonprofit Organizations
P.O. Box 510354, Livonia, Michigan 48151
734-451-3582 • www.snpo.org