Protect the Future of Your Nonprofit's Data

By: Jennifer Chandler

With all the news about recent data hacks, why wait until October's National Cyber Security Awareness Month to consider best practices that can help secure the future of your nonprofit's data and online presence. Steps every nonprofit can take to protect online activities are featured in the IRS Small Business Information Security guide and in this toolkit (for small businesses but applicable to nonprofits). Perhaps circulate the following advice from the IRS and discuss it at the next meeting of your paid staff, volunteers, and anyone else who uses your nonprofit's computers:

- Be careful of email attachments and web links
    - Do not click on a link or open an attachment that you were not expecting. If it appears important, call the sender to verify they sent the email and ask them to describe what the attachment or link is. Before you click a link (in an email or on social media, instant messages, other webpages), hover over that link to see the actual web address it will take you to. Train employees to recognize phishing attempts and who to notify when one occurs.
- Use separate personal and business computers, mobile devices and accounts

    - As much as possible, have separate devices and email accounts for personal and business use. This is especially important if other people, such as children, use personal devices. Do not conduct any sensitive business activities for your nonprofit (like online business banking) on a personal computer or device, and do not engage in activities such as web surfing, gaming, downloading videos, etc., on business computers or devices. Do not send sensitive business information to personal email addresses.
- Do not connect personal or untrusted storage devices or hardware into computers, mobile devices or networks.
    - Do not share USB drives or external hard drives between personal and business computers or devices. Do not connect any unknown / untrusted hardware into the system or network, and do not insert any unknown CD, DVD or USB drive. Disable the “AutoRun” feature for the USB ports and optical drives like CD and DVD drives on business computers to help prevent such malicious programs from installing on the systems.
- Be careful downloading software
    - Do not download software from an unknown web page. Be very careful with downloading and using freeware or shareware.
- Watch out when providing personal or business information
    - Never give out usernames or passwords. No company should ask for this information for any reason. Also, beware of people asking what kind of operating system, brand of firewall, internet browser, or what applications are installed. This is information that can make it easier for a hacker to break into the system.
    - Social engineering is an attempt to obtain physical or electronic access to business information by manipulating people. A very common type of attack involves a person, website or email that pretends to be something it’s not. A social engineer will research a business to learn names, titles, responsibilities and any personal information they can find. Afterwards, the social engineer usually calls or sends an email with a believable, but made-up, story designed to convince the person to give them certain information.
    - Never respond to an unsolicited phone call from a company you do not recognize that asks for sensitive personal or business information. Employees should notify their management whenever there is an attempt

or request for sensitive business information.

- Watch for harmful pop-ups
  - When connected to and using the Internet, do not respond to popup windows requesting that users click “OK.” Use a popup blocker and only allow popups on trusted websites.
- Use strong passwords
  - Good passwords consist of a random sequence of letters (upper case and lower case), numbers, and special characters. The “best practice” recommendation is that passwords are at least 12 characters long. For systems or applications that have important information, use multiple forms of identification (called “multi-factor” or “dual factor” authentication).
  - Many devices come with default administration passwords – these should be changed immediately when installing and regularly thereafter. Default passwords are easily found or known by hackers and can be used to access the device. The manual or those who install the system should be able to show you how to change them.
  - Passwords should be changed at least every three months.
  - Passwords to devices and applications that deal with business information should not be re-used.
  - You may want to consider using a password management application to store your passwords for you.
- Conduct online business more securely
  - Online business/commerce/banking should only be done using a secure browser connection. This will normally be indicated by a small lock visible in the lower right corner or upper left of the web browser window.
  - Erase the web browser cache, temporary internet files, cookies and history regularly. Make sure to erase this data after using any public computer and after any online commerce or banking session. This prevents important information from being stolen if the system is compromised. This will also help the system run faster. Typically, this is done in the web browser’s “privacy” or “security” menu.

RESOURCES

- Background on cybersecurity for charitable nonprofits (National Council of Nonprofits)

- StopThinkConnect toolkit and resources for cybersafety
- Stay safe online activities (National Cyber Security Alliance)
- Reporting cybercrime (National Cyber Security Alliance)
- Cyberbullying and harassment (National Cyber Security Alliance)
- Identity theft and fraud online (National Cyber Security Alliance)
- Microsoft Secure blog (tips on staying secure online from Microsoft)
- Tip sheets in different languages (National Cyber Security Alliance)
- Nonprofit cybersecurity: Why pay attention? (Nonprofit Quarterly)
- It's 2018: Do you know where your nonprofit's cybersecurity is? (Nonprofit Quarterly)