Protecting Your Church from Online Threats

By Rollie Dimos

thinkstockphotos.com

On a regular basis, there are news stories about someone falling victim to an online scam, like the infamous Nigerian email scam (e.g., I have $500,000 to give you, but you need to send me $1,000 for legal fees) or promises of great investment returns that turn out to be Ponzi schemes (think Bernie Madoff). Unfortunately, fraudsters never stop trying to find ways to take advantage of unsuspecting people, and our churches are not immune. Consider these examples:

- Last year, Michael Winans, Jr., the Grammy-nominated gospel singer, was convicted of stealing $8 million dollars from Christians who were promised a quick return on their investment.

- One pastor's Facebook credentials were compromised because he clicked on a video link that someone sent him. He was redirected to the Facebook login screen and entered his login credentials. Unfortunately, this was not the real Facebook login site, and the scammers used his credentials to take over his Facebook page and scam others.

- A pastor in Oregon replied to an official-looking email from Yahoo which asked for her login information. She completed the form and was immediately locked out of her account. At the same time, her friends starting getting emails from "her" that said she had been robbed while ministering overseas and needed $1,400 wired to a specific account in order to get back home.

- One pastor fell victim to an email scheme and lost $48,000. An unsolicited email from his credit card company appeared authentic but was really a phishing scheme asking for personal account information. The pastor replied to the email, and the scammers immediately accessed his credit card account.

In today's digitally-connected world, we are constantly exposed to electronic threats. And your church is just as vulnerable.

Whether viruses, spam, trojans, malware, phishing or smishing schemes, hackers never stop trying to find ways to attack.

What can you do to keep your ministry and personal computing safe?

Here are some best practices to protect your church's computer systems.

1. **Get up-to-date.** Make sure you are using the most up-to-date operating software and anti-virus programs.

If using Microsoft Windows operating systems, make sure you are using the most current update. Microsoft releases new patches every Tuesday.

Are you still using Windows XP? If so, consider upgrading to Windows 7 or 8. Microsoft will stop supporting Windows XP on April 8. That means no more security updates. Unfortunately, some studies estimate 30% of Windows users are still using Windows XP, which could amount to 500 million computers. If that includes your church, your computer systems will be vulnerable to malware

Continued on next page...

Protecting Your Church from Online Threats (cont.)

and hacking. Other software that you rely on may stop getting patched as well if those software developers stop supporting XP too.

Be sure to keep antivirus definitions up to date. While some antivirus programs are free, others require annual subscriptions. Make sure your subscription is up-to-date, so that updates will be current. Microsoft Security Essentials is one program that is free and helps guard against viruses, spyware and other malicious software.

Another word of caution: If you are using Microsoft Security Essentials as your antivirus program AND Windows XP, your computer system will still be vulnerable after April 8. Microsoft will stop providing anti-malware signature updates for Microsoft Security Essentials running on Windows XP systems on July 14, 2015.

2. **Clean house.** Remove programs on your computer desktop that you no longer use. If they are not being used regularly, they are most likely not being updated or patched. Spyware, Trojans and hacks can attack these vulnerable programs and compromise your data, your network and your security.

Consider installing an automatic program updater. These automatic updaters will scan all your programs and let you know if you are running the latest versions. Two free solutions can be found at www.secunia.com (free for up to 5 computers) and www.filehippo.com.

3. **Be vigilant.** Scrutinize the sites you visit on the Internet. Some honest-looking websites can deliver malicious programs to your computer.

If you have multiple computer systems in your church, consider a company-wide policy on acceptable Internet usage. Install Internet blocking software on any computers that connect to your church's network.

Be wary of unsolicited emails, and never click on any links in suspicious emails. For example, if you get a suspicious email from your bank, don't click on the link embedded in the email. Instead, open your browser and manually type in the Web address to your bank, or call the bank for more information.

Lastly, don't open emails from people you don't recognize.

4. **Stay informed.** Keep abreast of current scams and attacks and ways to protect yourself and your church.

Visit OnGuardOnline.gov. This is the federal government's website dedicated to help you be safe, secure and responsible online. It offers resources to help you, your family and your business recognize and report scams, use technology safely and wisely, and protect yourself from identity theft.

If you want to dig deeper, visit the NSA's website (www.nsa.gov) for easy-to-read and user-friendly whitepapers on computer security or the Internet Crime Complaint Center (www.ic3.gov) for a regularly updated list of Internet schemes and prevention tips.

* * *

About the Author:
Rollie Dimos, CIA, CISA, CFE, is the Internal Audit director at the Assemblies of God National Leadership and Resource Center. As an auditor in the government and nonprofit sectors, Rollie has been helping leaders assess the strength of their organizational controls for over 20 years. If you have a question about this article, you can contact Rollie at 417-862-2781, or by email at rdimos@ag.org.