Protect Your Church (and Home) from Digital Threats

By Pete Tarka

"Good morning, this is Sam from Microsoft. We have gotten reports that your computer is infected with a virus and is running slowly. Would you have a moment that we could remotely connect to your computer and resolve this for you?"

Have you ever received a phone call similar to the one mentioned? How about a Facebook message saying, "Wow you won't believe the pictures I took of you at the party last night!" Or better yet, an e-mail stating that a Nigerian prince has left you $1.7 million and all you need to do to claim it is to send your bank account and routing number. Odds are that you, or people you know, have been a recipient or victim of such correspondence.

As you read the different ways that scams can infiltrate your computer and possibly your bank account, you may think, "Who would fall for such obvious scams?" Since 2013, more than 3,000 people nationwide have fallen for the fake IRS agents' scam harassing taxpayers to pay past-due taxes using prepaid gift cards. **(The Tampa Tribune, June 14, 2015)**

My original example of a phone call from "Sam at Microsoft" may seem farfetched to some; however, thousands of Americans in the past 4 years have lost millions of dollars in identity theft, stolen information, as well as frustration and inconvenience. (If you have fallen for the remote access phone scam, this article may be helpful in your road to recovery.)

So how do you protect yourself, your church, and your loved ones from these scams and malicious attacks?

Let's explore some of the various types of industry-known threats and ways to prevent them.

How to Avoid Scams

The world of technology may seem like a scary and dangerous place; and for good reason, it is. Unchecked use of technology and a lack of respect for your online presence can jeopardize your computer, your business, and your personal well-being.

The first step to protect your business, and your home, is to be aware of the potential risks and remain vigilant. Kimberly Palmer, U.S. News, provides some helpful tips in a timeless article about ways to avoid online scams (read the entire story here).

Continued on next page...

Protect Your Church (and Home) from Digital Threats (cont.)

Her recommendations include:

1. Don't click on hyperlinks in e-mails. These are links that will take you to another Web site. If you do not know who the link came from, simply delete the e-mail.
2. Avoid suspicious Web sites. If Web sites look cheap in design or have multiple pop-ups, it may not be legitimate.
3. Use caution when shopping on your smartphone. These devices lack virus protection which can leave you vulnerable when entering your payment information.
4. Keep your social security number to yourself. Legitimate businesses rarely ask for your SSN.
5. Stick with plastic. Credit cards usually come with fraud protection. This means if someone else fraudulently buys something, you can dispute the charge. A debit card does not work the same way, and you may find yourself trying to convince your bank to reimburse you.
6. Use strong passwords.
7. Don't "friend" strangers online. If you don't know the person "friending" you, simply decline the request.
8. Schedule a regular paperwork review, to include credit card bills and credit history. Credit card companies are more inclined to believe that you did not buy that 100-inch LED TV if you report the fraud quickly, rather than reporting fraudulent charges months later.

Computer Viruses

A computer virus is a manmade program, or piece of code, that is loaded onto your computer without your knowledge, and runs against your wishes. Viruses can also replicate themselves. A simple virus, that can make a copy of itself over and over again, is relatively easy to produce. Even a simple virus is dangerous because it will quickly use all available memory and bring the computer system to a halt. An even more dangerous type of virus is one that is capable of transmitting itself across networks and bypassing security systems.

Computer programs, or files that appear to be harmless but actually do damage, are called Trojan viruses. You may download a beautiful sunset picture for your computer wallpaper completely unaware that a Trojan virus is embedded within the file.

E-mail attachments can contain viruses as well. Here are some quick and easy steps to identify potential threats and avoid them:

1. **Look closely at the subject line.** A subject line is a summary of an e-mail. If you happen to get subject lines similar to: "Make.Money.Fast," most likely the e-mail contains a virus.
2. **Watch attached files.** Most of the time a file that is a virus has an .exe or .vbs file extension. (A file extension is a type of file.) What most hackers do is try to make the file

Continued on next page...

Protect Your Church (and Home) from Digital Threats (cont.)

seem legitimate by adding a familiar file type to the name such as blank.jpg.vbs. The first extension (.jpg) is just part of the name if followed by another (.vbs).

3. **Check the sender.** If the sender is someone you don't know, or a company you're not familiar with, the e-mail could contain a virus.
4. **Read the message.** Although it might be sent from someone you know, the message may leave you clueless about why it was sent. For example, the "here you have" e-mail virus simply says, "This is The Document I told you about, you can find it Here," followed by the virus' download link. If you view the document, the virus will send itself to everyone in your Microsoft Office address book and list you as the sender. These ambiguous messages are an obvious indication that the e-mail contains a virus.
5. **Know that e-mail viruses may pretend to be sent from an existing company.** It is important to read each e-mail thoroughly; an e-mail may seem to be sent from a legitimate company when it was really sent from a hacker. This is called forging e-mail. A forged e-mail may contain multiple spelling and punctuation errors, which is another indicator that the e-mail may contain a virus.
6. **Do not follow links unless assured or necessary.** Sometimes the virus is located on a Web site, rather than attached to an e-mail. The hacker requires the victim to follow the link to a Web site in order for the virus to be downloaded. If not contacted prior to receiving the e-mail with assurance that the link is safe, do not follow it.

Other Threats

Other types of viruses, spyware, and malware include:

Macro Viruses: A macro virus is a computer virus that "infects" Microsoft Word or a similar application. It can cause a sequence of actions to be performed automatically when the application is started or other actions occur.

Computer Worm: A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program.

Spyware: Spyware can track users through advertising that may pop-up on your computer. When you click on the pop-up, you will be taken to a Web site which can install a virus onto your computer without your knowledge. The virus can hijack your Web browser, making your home page a specific site, create dozens of additional pop-ups each time you try to open a new web page, as well as slow the performance and efficiency of your computer by using all of your memory and resources, and potentially render your computer inoperable.

Continued on next page...

Protect Your Church (and Home) from Digital Threats (cont.)

Scareware: Scareware are malicious computer programs designed to trick a user into buying and downloading unnecessary, and potentially dangerous, software such as fake antivirus protection. A pop-up window may say that your computer is infected and needs to be scanned. Once the scan is completed, it may say you have 10,467 infected files, and 6,875 potential threats, and that you need to download a program to clean your computer. However, once the program is downloaded and installed, it may contain other hidden installations which can hinder the performance of your computer.

Protect Yourself

Going online doesn't have to carry steep consequences, nor does downloading and installing a new version of Angry Birds have to keep you awake all night. Instead there are several basic preventative measures that can help ensure that you get back to safely throwing birds and updating your Facebook status.

1. **Virus protection.** This is number one on the list for good reason—it's important! Virus protection companies update their virus definition libraries daily to combat the onslaught of hackers and spammers that can cause your computer, and you, problems. Some of the most popular anti-virus software is:
   a. McAfee
   b. AVG (Free Version available)
   c. Microsoft Security Essentials (Free full version)
   d. Norton by Symantec

2. **Security updates.** Making sure your operating system is fully patched and current on all of its security patches is critical to its safety and well-being. Microsoft calls them service packs and windows updates. Apple calls them security updates, operating system updates, and firmware updates. More information can be found online at the websites for Microsoft and Apple.

3. **Malware protection.** Some anti-virus software has built-in malware protection; however it is my personal experience that software specifically designed to search and quarantine malware is a better solution. Some of the more popular anti-malware software is:
   a. Microsoft Malicious Software Removal Tool (Free)
   b. Malwarebytes (Free version available)
   c. Vipre

The above lists are not exhaustive and other solutions are available. I would recommend that you go online and do a bit more research to find which software meets your specific needs.

Continued on next page...

Protect Your Church (and Home) from Digital Threats (cont.)

The technological age we currently live in is an amazing and exciting time. We have instant access to information, constant communication, and shopping at 1:00 in the morning, if we so desire. With that being said, you must always be mindful of your online surroundings, as well as your information, and how you share it. The due diligence you put into protecting your personal information, your business information, and your computing devices, will not only enhance your online experience, but also build confidence that you are protected from potential pitfalls and threats.

About the Author:
Pete Tarka manages the IT Customer Care Department at the AG National Leadership and Resource Center. He has served the IT needs of the national office for over 12 years. If you have any questions about this article, you can reach Pete at ptarka@ag.org.

For information on how to keep your phone and computer data safe and encrypted, view his article here.