Five Things Worth Doing in January

President, Ministry Business Services, Inc.
Reprinted from *MinistryTech Magazine*

January, 2018! The start of a new year! New beginnings are part of the Christian life, and January is a great time to make certain a few IT items are ready for the New Year. Let's focus on protecting systems and data….

Firewalls
The most common entry point for malware and other system ills is the internet. The best way to protect your system and data from bots, rascals, and compromised websites is to be certain your firewall is adequate and is current. Some points worth examining:

- Is your firewall adequate? There are many options to consider when buying firewall solutions–whether hardware or software. My firm's preference is SonicWALL firewalls (we don't sell or benefit from our hardware and software recommendations). We find the features and price point are a good 'sweet spot' for churches and ministries. Yes, you can buy more expensive and capable firewalls, but very few churches and ministries benefit from any features beyond what SonicWALL includes in their firewalls. We also recommend purchasing their Total Secure package, which can filter internet content.
- Is your firewall subscription current? Regardless of which firewall you use, make certain that if it requires a subscription to stay current, your subscription is current and in force. Not doing so is the equivalent of welcoming intruders, rascals, bots, and malware that have developed new methods for gaining access to your systems and data.
- Make certain there is no connection from your systems to the internet that don't go through your firewall. We have seen many churches and ministries mistakenly connect their internet connection directly to their network switch. The internet connection should connect to your firewall, and then your firewall to your switch so that all internet traffic MUST go through it.

SPAM
The second most common way for malware to access your systems and data is via email attachments and links. SonicWALL is not our preference for this important role; we prefer the Barracuda SPAM Filter. It is best of breed and a best practices solution.

My firm inexpensively hosts SPAM filtering for many churches and ministries. I don't mention that to try to sell our service, but to point out that we were surprised to see how many users of Microsoft O365 email use our hosted SPAM filtering solution (yes, we use a Barracuda SPAM Filter, model 600). We moved our email to O365 for six months and were shocked at how much SPAM got through Microsoft's filter! Now we know why so many O365 users have their email scrubbed by other solutions!

Anti-Malware
Protecting systems and data requires multiple layers. An important one is your anti-malware

solution. And simply purchasing and installing it is not enough! These solutions also have subscriptions that keep them updated and identifying new methods used to cause harm. It is essential that the subscription on your anti-malware not be allowed to lapse– the same as your firewall subscription. I know churches and ministries that have been hit by new ransomware methods because they didn't keep their subscriptions current.

The anti-malware my firm recommends is Thirtyseven4.com. It is capable, and it is reasonable in cost.

BTW… it should be installed on every Windows and Mac computer– whether notebook, tablet, desktop, or server. Some say it's not necessary on Macs, but that isn't true. Even though few anti-malware threats are written to impact Macs, Macs can be carriers that infect shared data drives and more.

Passwords
What is your password policy? Here are some quick thoughts on this important topic:

- Passwords should be strong (minimum of 7 characters that include uppercase and lowercase alpha, numbers, and common punctuation).
- Passwords should not be required to periodically change! Our firm has been saying for many years that forcing users to change their passwords actually *lowers* system security. In 2016 the U.S. Federal Trade Commission agreed with us based on two studies! You can read about it at https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes.

Backup
Some say protecting the integrity of system data is IT's most important responsibility. Do you have a comprehensive backup strategy? And do you test it? An untested strategy is dangerous! Here's what we recommend:

- Establish a strategy that makes certain all important data is on your server. This is worth doing because 1) it is the organization's data, and 2) it eliminates the requirement that all systems need to be connected to the network (facilitating notebooks, etc).
- Backup all system data nightly to an appropriate device. LTO tape is the most affordable and durable technology for this, and is preferred by most of corporate America. Our favorite backup solution is Veeam. It's powerful, easy to use, and they offer churches and ministries very reasonable pricing.
- Take a copy of your backup tape off-site weekly to protect your organization from a larger disaster.
- Create a monthly task in whatever task tracker you use (like Outlook) to test the backup. You can do this by restoring a random file or folder, and then confirming that the restored files are intact.

These five things will likely take less than an hour to check, and can help ensure that your organization's systems and data are well-protected for 2018! Happy New Year!