SAFE TO WORSHIP™

20 CHURCH COMPUTER TIPS FOR STAYING SAFE ONLINE

1. Don’t run Windows XP. Use Windows 7, 10 or Mac OSX.
2. Do regular Windows or OSX updates. Don’t wait to apply these critical security patches!
3. Your staff smart phones are handheld computers so make certain everyone you are going to allow on the network for any length of time applies those patches, also.
4. Update Java, Adobe Flash and Silverlight on all church computers regularly. Set them to automatically update if you can. These programs are notoriously hacked.
5. When you download and install software from the internet, avoid installing extras like Google Tool Bar and Chrome Browser. Some software will try to sneak these in on you. Have people uncheck these if they see them.
6. Run only one Anti-Virus program. Pay to keep it updated, if you must, and update it regularly. Don’t trust anti-virus exclusively. Safe surfing habits are the best way to prevent infection. The best anti-virus is the one you and your staff use and keep updated.
7. When you download a program or file from the internet, scan it with your anti-virus before you open it. Often this is a simple right-click action to perform.
8. Download and install **CCleaner** free version. It cleans a lot of unwanted junk off your computer. Only download it from *www.piriform.com*. Run the cleaner once a week.
9. Download and install **MalwareBytes** free version. It is a good anti-malware detector. It has to be updated before you use it the first time. Download it only from *www.malwarebytes.org.* Keep it updated and run it once a week.
10. VirusTotal at https://www.virustotal.com is a great place to check files and links for viruses.
11. Use the **FireFox** web browser *www.mozilla.org*. It is a great independent browser and the organization is big on privacy. Keep any browser your church uses up to date.
12. FireFox’s greatest feature is the many plug-ins that can be installed to enhance its security. If you feel comfortable with adding plug-ins, consider **Ghostery, NoScript, Adblock, uBlock and HTTPs Everywhere**. These can go a long way to protect your privacy on-line but remember, the more security you add to your browser, the less beautiful your on-line experience will be. This is why many people just choose to ignore security.
13. Children can be a big security threat to your computers. They want to play on-line java based games like MineCraft. Minecraft is a great game and is truly educational but restrict downloads people can do on your network. Kids may try to download mods to the games, and many mod sites are bad.
14. Teach your church kids about on-line safety, not just from hackers but also child predators. *www.netsmartz.org* is a great site for kids to learn about on-line security. Also, *https://staysafeonline.org* is a great resource.
15. Educate your church parents that they can get a free internet filter for their home at *https://www.opendns.com/home-internet-security/* They will need to read and follow the instructions, but it can go a long way to keeping their kids safe online by filtering out adult content.
16. Teach your staff about phishing, even on social media sites.
17. Consider obtaining a VPN https://www.expressvpn.com for the church. A VPN can keep your internet surfing from being snooped on by various groups and sold to marketing companies.
18. Use a password manager like **1Password** and use multi-factor authentication.
19. Incorporate multi-factor authentication in every program that offers it for security.
20. Close all computers down at the end of the day. Do not leave a computer active and running for someone to simply sit down and begin to use.

Source: Modified with permission from "*21 Home Computer Tips for Staying Safe Online*,"
by Mr. Tim Leonard, SVP, CIO, Commercial Bank of Texas, N.A.