10 Common Sense Technology Security Tips

By Val Steed, CPA, MA, CITP

In the last issue of *Today's CPA*, we covered some of the top technology mistakes I see on a regular basis and how to protect yourself from them. This issue, we'll discuss the instances of technology security breaches.

It seems appropriate to remind folks in the wake of recent ransomware attacks that often the simplest, most common sense steps work wonders to keep your technology safe. The WannaCry virus on May 12, 2017, was a worldwide cyberattack that targeted computers running the Microsoft Windows operating system, infecting more than 230,000 computers, in over 150 countries, within a day.

The WannaCry Ransomware cryptoworm attacked these operating systems by encrypting data and demanding ransom payments in Bitcoin cryptocurrency – which should send a clear signal to all of us about Bitcoin. However, the attack only succeeded when a user's operating system was out-of-date or if they were still using Windows XP. Good grief! It's been at least a decade since we were warned about Windows XP, right? Maybe now we'll actually listen. Here are some simple steps we can do to help prevent technology security breaches.

1. Keep Your Operating Systems Up-to-Date

Ask your IT folks if your systems are up-to-date. If they are not, demand clear answers as to why they are not keeping current. Many IT groups will lag behind in updates because they haven't tested how critical software in your organization will respond to the update. If this sounds like an IT practice in your organization, this should send a signal to you and your management team that there is a problem. You should always update as soon as possible after a security release – if not immediately, then within a few weeks at most.

2. Keep Your Antivirus Software and Licenses Current

If your antivirus software is out-of-date, it cannot keep up with the latest attacks, nor should you expect it to. I had a person complaining in class that a very popular antivirus software had failed them. When I asked to know more, they admitted the software was out of license at the time of the breach. Out-of-date or non-licensed antivirus software is unreliable at best and presents a serious security risk. Make sure to keep it current.

3. Notice Anything Out of the Ordinary

You need to know your system inside and out, so you can recognize when something is amiss. For example, a browser that starts blinking when it normally does not blink or an email that takes extra-long to open could be a sign that something is not right with your system.

The first thing you should do when you notice something's off is shut everything down and restart. Often simple application collisions in RAM can be reset with a restart. If the problems persist, then you'll know it's not a RAM issue and you may have a bigger problem.

4. Try Updating Your Antivirus if the Problem Persists

One of the first things an attack will do is disable your antivirus update, followed by disabling your antivirus software. Check and run the update and scan. I prefer to update my systems automatically at least once a day and scan at least once a day.

5. Consider Using a PC Cleaning Tool

If everything checks out after restarting and updating your antivirus, but your computer is still sluggish, you may need to use a PC cleaning tool to dig a little deeper and uproot the problem. Just keep in mind that all these cleaning tools will clear out cookies and at times require you to reset information. Use at your own risk. I recommend trying Cleaner Pro, because it's worked well for me in the past.

6. Be Wary of Open WiFi

I never do anything using a serious login on open WiFi. Instead, I will always turn on my own cell-based hot spots from my iPhone or iPad for serious work. Your cell phone hot spots are encrypted to the tower and offer much more protection than open WiFi connections. Keep a special eye out for Venmo, PayPal, bank transfers, etc. If a hacker can get side by side with you on an open network, they can track what you are doing.

7. Change Your Serious Passwords at Least Once a Year

More often would be better, but busy schedules make it easy to forget simple practices like this. Ask yourself if you've changed your

bank remote login in the past year? If you have, you're already ahead of the curve. If you're like most people, use this as a reminder and go change it right now.

8. Never Use the Same Password for Multiple Sites

Consider this – once a hacker breaks into your Facebook account, they will immediately test your bank login with the same password. Facebook and other social media platforms gather a lot of personal information about their users and if a hacker has access to your social media accounts, then they already have a good idea of where you bank.

9. Use Caution When Posting on Social Media

Phishing schemes now are incredibly sophisticated and will use information they gather about you to deceive you or others in your company. Don't post anything on social media that you don't want to be absolutely public, especially when it comes to business information.

10. Avoid Gmail, Yahoo, Outlook, Comcast or Others for Business Email

If you're in business, you should own your own domain and have it managed. This allows you to control the level of access and security for your business email. These email services work fine for personal stuff, but not business. I have enough very sad stories to fill pages that are all due to folks using these services for business email. Just don't do it. If you need help setting up a domain, get it. Look for a very sophisticated business email security solution like Mimecast.com. You can and should take a proactive stand on email.

Bottom Line

Most of these solutions won't cost you anything except a change in mindset. It takes a conscious effort to remember to change passwords or recognize when you're on public WiFi vs. using a hotspot, but it's a small thing in comparison to leaving yourself vulnerable to hackers or malware. The bottom line is be current, be aware and you should be fine. ■

Val Steed, CPA, MA, CITP is the CEO of K2 Enterprises, a national technology training and consulting organization. He has 12 years experience in public practice and has been involved with the accounting technology industry for more than 30 years.