

Top Five Technology Mistakes

By Val Steed, CPA, MA, CITP

I've been using accounting technology and other forms of technology for more than 30 years, both in my business and personal life. I've taught countless classes on the business benefits of using technology, but I've also seen all kinds of mistakes that users make. I've compiled a list of the top five technology mistakes I see on a regular basis and how you can protect yourself from making them.

Out-of-Date Antivirus and Antispyware

I can't tell you how many times people tell me they're unsure or have no idea which antivirus or antispyware they're currently using – if any at all. Many users run out-of-date software or let their licenses expire because they forget to update. Some even say they are too busy working on a project to allow the update to happen. This is extremely dangerous.

Every computer should run antivirus and antispyware software at all times. You should check and update your software daily and allow it to scan for malware at least as often, to ensure that you're protecting your system and your information. Many top products will have multiple updates per day, so you need to make sure to adjust your settings and allow your software to update and scan daily.

Identifying if You're at Risk

Daily scans can also help identify whether your system has been compromised. If your system does not allow an update for your anti-virus, it could be an indicator that there's a problem. The number one hint that you have a problem is when your antivirus software will not update. If you notice your antivirus will not update, you need to get help immediately and shut down that system.

Know Your Software

Get familiar with the software you're running. Learn what the update, scan and diagnostics screens look like and how to read them so you can pick off spyware scams before they install a virus on your machine.



This includes Mac users not running antivirus software.

Ask any Mac user and you will probably hear some comment about how secure the Apple OS is compared to Windows. While I generally agree, there are a few things to keep in mind. Although Apple is not as big of a target as Windows, they still have vulnerabilities.

Almost all Mac users will begrudgingly tell you they are not running any anti-virus software. This is a big mistake. Many Mac users handle Windows files on a regular basis, without knowing – or caring – whether these files are infected, because a PC virus won't harm a Mac. Although the individual Mac isn't affected, they can become a carrier of Windows viruses in their environment.

I recommend fixing this issue by installing one of two, free antivirus solutions for Mac:

- www.sophos.com
- www.avast.com

Mac users reading this will find that these two products run very well and will not muck up their machine. Many Mac users

actually report finding multiple Windows trojans and viruses during their first scan after installing these antivirus solutions. Dear Mac folks, please trust me on this one. I am an Apple person myself.

Allowing Unwanted Location Services to Track You

When you allow technology to track your location, you are proclaiming your location to the world. This is most common with social media, like Facebook or Instagram. Even text messages can be tracked to GPS origins if you do not turn that feature off on your mobile device.

You may think you're only sharing with your own contacts or friends, but many times when those friends "like" or "share" your original post, it broadcasts to a wider network of people. This means people you don't know suddenly know if you're on vacation or away from your home, opening yourself up to potential risk.

Be extremely careful with location services. Make sure you monitor and choose exactly which applications will be allowed to use location and which ones will not.

Table 1: Return on Investment

Return on Investment for	Results
One Year:	106%
Two Years:	212%
Three Years:	319%
Four Years:	425%
Five Years:	531%

Poor Password Management

Poor password management may be the most common account technology mistake that I see. And a lot of it stems from needing to remember so many passwords.

Here are a few examples of poor password management:

- Using the same password on multiple sites
- Using weak or common word passwords
- Using obvious passwords like family or pet names

Probably the best advice is to look to a password manager, such as Password Depot, RoboForm or the like. These will help you keep your passwords secure and allow you to differentiate your passwords across all your log-ins.

Ignoring Software Updates

Many software updates fix known vulnerabilities in the existing software. Simply updating your software can go a long way in keeping your information secure. This is most critical with Windows, but most applications become more vulnerable to attack when not updated on a regular basis.

I often hear “tech experts” claim that it is best to turn off Windows and Office updates. Unless you’ve been specifically instructed by your IT department, I don’t recommend this. There are some cases where an update can cause problems with corporate applications and the IT department may have other protective measures in place for your company, but as a general rule, always check with your IT department before ignoring software updates.

For the rest of us, it’s in our best interest to keep the updates flowing for Windows,

Office and other applications. There are times when I will manually control QuickBooks, Adobe products and tax software updates, but I make sure to update QuickBooks and Adobe products at least once a month and tax software at least once a week.

Lack of Professional Training

Proper training on solutions and software that you use every day will make your job easier and more productive. Obviously, this may seem a little self-serving because we sell training, but I’ve seen the difference between a professionally trained user and someone who has used Google to “self-train.” That’s not a knock on Google. It is a fantastic

resource for many things, but to ensure that you’re not selling yourself short, I recommend seeking professional training for accounting technology. Following is an example of why I do.

Let’s say you attend a full-day class on Excel. This class gives you skills to save you five minutes of work per day. With an annual salary of \$70,000, working 208 days per year, the ROI for a \$350 out-of-pocket class is shown in Table 1.

This is just a very small example of the power of professional training. Clearly, in the bigger picture it’s worth the investment to ensure you have the knowledge and skills to help you succeed. This training can be anything from how to use Excel to the top five technology mistakes to avoid. ■

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.



2017 TAX PRACTITIONER WORKSHOPS

October, November and December

General Income Tax
(2 days - \$300)

Advanced Income Tax
(2 days - \$300)

Fiduciary Income Tax
(1 day - \$235)

Texas State Tax Issues
(1 day - \$235)

Partnership Tax Issues
(2 days - \$425)

Agricultural Tax Issues
(1 day - \$235)

Ethics for Texas CPAs
(4 hours - \$120)

16 Hrs CPE, 13.5 Hrs MCLE credit for 2-day workshop
8 Hrs CPE, 6.75 Hrs MCLE credit for 1-day workshop
TSBPA Sponsor #00139; IRS Approved CE Provider #NXR57

www.taxworkshop.com

for dates, times, and online registration

Sponsored by the Texas Extension Education Foundation, Inc.