VISUAL NEWSLETTER – SEPTEMBER 2017

Libra Retirement Planning

Libra's Accounting System has been around since the late 1970's. During that time it has been used by a number of small, medium and large companies that found the functionality and ease of use excellent for its time. While it still works well for many companies it has become more difficult to maintain in recent years. Most of my larger clients have either completed the conversion to newer software or are in the process of doing so. With complex systems this conversion can take several months, or in some cases a number of years to complete, so significant planning is required.

Since I am considering retirement sometime in the next few years, companies are encouraged to consider an eventual replacement for both Libra Accounting Software and the various services that I now provide. There is no hard timetable for this retirement at present and I will support it for as long as I am able.

Determining what software your competitors or other companies in a similar business are using is a good first step in this process. Making some connections and attending some presentations will help to narrow down the eventual software selection. I don't think that there is any need to rush this transition but you should give some consideration to getting the process started.

For many clients, I also currently provide computer equipment, hardware setup and associated support services and I can continue to do so for the near future. Replacing hardware support, should it become necessary, is less ominous as many companies can provide these services. The problem, as with software, is to find a good company that you can rely on when something goes wrong. Many remote clients just run their computers to Staples or Best Buy for service.

It's actually fairly rare these days to find one company that can support both your accounting software and your hardware setup and support needs and this is not 100% necessary, but it can avoid significant finger pointing should anything ever go wrong.

So for now, not a lot will change, but I do recommend that you have a software migration plan in place. I will certainly assist you, where possible, to make the transition as smooth as possible when the time comes to make the change to new software. We can often export data via Excel into a format that the new system can import and save a lot of time and effort in setup.

Microsoft Fake Virus Warnings

In the last month, several users have fallen for a scam whereby links on a web-site triggers a trap. A pop-up indicates that Microsoft has detected a virus on your computer and that the failure to call the supplied phone number immediately could result in permanent damage to your PC. To make things worse, the site plays warning bells and locks your Internet browser so you cannot easily exit the site. Microsoft issues no such warnings and this is purely a scam to get you to pay for some services that you really don't need.

You can usually get out of this trap by simply pressing CTRL/ALT/DELETE and selecting logoff or sign out as determined by your version of Windows. Once you do this the problem should be resolved but it wouldn't hurt to do a couple of scans with your Anti-Virus and Malwarebytes just to make sure nothing remains.

Ransom / Crypto Viruses

In the last few years, there have been a large number of people hit by a category of Virus known as a Ransom Virus. In its most simple form, it locks up your computer and demands money to unlock it. For people with Windows 7 the usual fix is to power off, start up in Safe Mode and use System Restore to take Windows back a day in time to remove the nuisance virus. Users of Windows 8 and Windows 10 will require a recovery CD / DVD to do this, due to enhanced boot routines.

The latest wave of these sort of viruses go through your computer and encrypt all of your critical files. Typically, they go after Word & Excel files, PDF files and JPG picture files. Again there is often a message stating that if you pay the asking fee they will fix your files for you. This almost never happens even if you do give the crooks your money or credit card information. These viruses can hit you regardless of the type of anti-virus you have installed. They usually reside on the web in poisoned web-sites and in links from within unsolicited e-mails that promise something that our innate curiosity draws people to click on.

Some form of encrypted and off-site backups are your best defence against the sort of damage these viruses can inflict as there is almost no way to un-encrypt these files without a bank of Super Computers to do the work. A backup product like Crash Plan is a cheap insurance policy to protect you from these file losses.