Radio Days – 2013-05-11

Tip of the Week – Think, Don't Click

A recent client posed two questions just as I was leaving. He asked if it was safe to reply to a spam message saying *Get lost!* or something similar and he also asked if it was safe to click on a link in an email from an unknown sender. Two excellent questions; same answer.

Replying to a Spam Email

One of the most valuable things that a spammer can get is an email address which is known to be active. These addresses can be sold, and there is an ongoing market for such addresses. If you reply to a spam email you are stating that your email address is active and that you reply to unsolicited emails, otherwise known as *Spam*.

If you want to fill your email inbox with spam the best ways to do so are to reply to all your spam emails and to subscribe to all the email newsletters that you see on the internet. Both of these actions will allow you to get all the spam email that you want and then even more.

Do ***NOT*** reply to spam emails!

If you find that there are too many spam emails in your inbox then the best way to stop them coming is to use a program called *MailWasher*. There are two version of MailWasher: Free and Full. The free version allows you to check one email address (enough for most of my clients) while the full version allows you to check an unlimited number of email addresses.

MailWasher allows you to see emails before they reach your computer. This means that you can delete them before you download them; it also means that you can *bounce* unwanted emails.

Bouncing an Email

If you remember the olden days when letters arrived in an envelope which was sealed with sealing wax after being written with a quill pen on parchment you may also remember the times that you received an unwanted or wrongly-addressed letter. These letters were usually returned to the sender with a message written on the envelope saying something like *Please return to sender: not at this address*.

You can do a similar thing with emails: you may even have received a bounced email after having sent one with the wrong address. You can easily simulate this process using a program like MailWasher to bounce unwanted emails.

My client asked the obvious question: will you never get another email from this sender? Unfortunately the answer is *No* because not every spam email sender removes unknown email addresses from their address list. It will, however, reduce the number of spam emails you get.

Clicking On Links

My client's other question: *Is it safe to click on a link in an email from an unknown sender?*

The answer to this question is also ***NO!*** I showed him that, if you move the mouse pointer over the link in the email, you will see the address that this link will take you to. In the email that my client had on his screen the address in the link and the address in the pop-up box were different. This means that the link was not genuine.

Never click on a link in an email from somebody you do not know.

Even be suspicious if the email is from somebody that you know: it could be a fake or the result of a virus attack on your friend's computer. Always check links by moving the mouse pointer over the link and checking what address shows in the pop-up box.

Protecting Your Data

I had two separate incidents this week where people had lost data. One person lost data by not following the rules, the other lost data because of a virus.

Neither person had a backup!

Follow The Rules!

The person who didn't follow the rules was copying data from a camera's card to a USB stick. The card was a Secure Digital card and he had not switched the protection switch to *Lock*. This meant that the computer could write to the SD card and could delete all the files on the SD card. The USB stick also had no protection.

This meant that there was nothing to stop her from losing all her data if something went wrong, and something did go wrong.

He had copied some of his photos from the SD card to the USB stick. While copying these photos he decided that he had finished the copying so pulled both the SD card and the USB stick out of the computer.

This is something that all the books warn you against!

The reason for the warning is that, because Windows is still accessing a card or stick, it can accidentally delete everything from the card or stick. It doesn't happen every time (which is why people can do it many times and get away with it) but, when it does happen it is usually disastrous. And disaster struck my client with a vengeance!

Because Windows was actively reading and writing both the SD card and the USB stick when they were pulled from the computer all the data was wiped from both devices! I asked him to replace both of the devices in the computer and we checked them: both had lost all their data!

I installed my favourite program for recovering data: it is called *Recuva*. Like so many of the programs which I use there are a number of versions, and I use the free version because it is so good. Despite all my previous experiences with Recuva, it did not manage to recover any of the lost data.

This meant that my client had lost all the photos from a weekend family trip to the high country around Bright.

How to Prevent This From Happening Again

This sort of disaster is preventable, but it involves a little knowledge and a little patience. There are several places where, if my client had stopped and allowed things to take their course the disaster would have been prevented.

1. Use the write-protect switch on the SD card. This is a little lever which sits in an indent on the side of all SD cards: push it towards the small arrow towards the word *Lock* written on the card. This prevents Windows (or any other program) from writing to the card or deleting anything from the card.
   This would have kept his photographs safe until all other steps had been completed.
2. Wait until Windows had finished copying his photographs from the card to the stick, then use the little green button to release both of these devices before removing them from the computer.
   This would have warned him that these devices were still in use.
3. Do the first copy to the computer's hard disc. This would have meant that only one device was likely to become corrupted by premature removal. After copying all his photos to the computer's hard disc he could then have copied his photos to his USB stick in safety.
   This would have given him a second copy of his photos in case something went wrong.

Virus Kills Data!

My second disaster of the week was a client who started his computer only to find that his desktop photo had disappeared and most of the icons on his desktop had also gone. Further investigation showed that his data had also disappeared. His *My Documents* folder was empty as was his *My Pictures* folder. This was a major disaster for a dedicated photographer (and no, these things do not only happen to photographers!) and, as expected, he did not have a backup!

I have used Recuva to recover lost photos on two occasions in the past with great success. On each of those occasions the data was recovered from a USB stick or camera memory card to a computer's hard disc. This option was not available on this occasion for two reasons:

- Installing Recuva to my client's hard disc could well have written over one of the photos which we were trying to recover. Whenever you write anything to your hard disc you run the risk of overwriting a piece of data. Usually this data is just a piece of temporary data which had been deleted in the normal course of your computer work.
- When recovering data from any device (removable or fixed) you must always write it back to another device to prevent the risk of overwriting another piece of data on the original device. This means that you must recover data from your hard disc to another hard disc, and this means that you must install your computer's hard disc into another computer. This is a task which I cannot perform so I always advise my clients to take their computer to a competent repair shop.

Backup, Backup, Backup

The best, cheapest and easiest backup program that I have come across is called SyncBack. It, like many other programs on the internet, comes in a free and full version. There is also a professional version for larger organisations but I recommend the full version because it has the ability to keep a number of generations of files. This is useful for many people, especially those who create files which change. Examples of files which change are accounting program files, written documents and photographs which are improved using programs like Picasa and Photoshop.

Most people keep most of their files in the standard places: Documents, Music, Photos and Videos. There are many others who keep important files on their desktop and a few who even keep important files in the Recycle Bin. This is perhaps the most stupid place because Windows can, and does, delete files from the Recycle Bin when it becomes too full.

If you backup the files in your four standard places and on your desktop you will probably get the most important files in your computer. The files which you will miss are your emails and your address book because these are usually stored in the most unexpected places.

Because setting-up and running SyncBack backups is so simple I am surprised at the number of people who still do not do a regular backup of their important files.

Please get your backup created and run now. If you only get most of your important files it is better than having none of them stored after an accident.

Please remember that there are two types of people: those who have lost data and those who are just about to lose their data.

Further Information

MailWasher Free	www.mailwasher.net
MailWasher Full	www.firetrust.com
Recuva	www.piriform.com
SyncBack (Free & Full)	www.2brightsparks.com