Tech Hints. Elsa Sell

These all take time and usually money and that input is rewarded.

Backing Up Files, Photos, etc.

Have you ever lost irreplaceable photos or files because of a hard drive failure, a computer crash, or disaster? If not, you're lucky. If yes, what a struggle you've had.

The solution? Back up everything.

How? There are several options. You may be able to accomplish these on your own or you may need to ask a techie friend for help, or pay for the service. Any option is safer than no option. The internet has information on programs or companies offering these services. It is wise to select one that provides phone support.

- Use an external hard drive to back up files, software, and even operating system. This requires software.
- Use a cloud company – e.g., Carbonite, iDrive, Spider Oak. Some have free versions. Amount of storage varies, as does number of computers, and ability to access your files from anywhere. Some of these also let you backup to a local hard drive. The first download may take days if you have many gigabytes of information to move. After that, the continuous updates are quick.
- A USB thumb drive. Large amounts of storage (e.g., 64GB) are inexpensive.

I backup all three ways and have been saved more than once from disastrous loss.

Downloading Software

I use lots of software programs. One, Filezilla, is a free FTP program for moving files to Mail Chimp, Survey Monkey, and BeaCon's web site. When my computer hard drive crashed this summer, I reinstalled all software programs – including Filezilla. It had been at least 3 years since I downloaded Filezilla, so I went to the site, started the download, and watched. There were things downloading that I hadn't requested. By then, it was too late. My computer had acquired malware. One of the malware programs took over my browsers and redirected all my requests to one place; it also inserted a regenerating malicious code somewhere in the operating system.

It required many days to clean up and plenty of frustration. This can happen with other software downloads, even some that are paid for. It is essential to download from a legitimate source.

The solution(s)?

- Google the software – "is it safe to download ****?"
- One windows legitimate source is Ninite (ninite.com). It has a limited number of software apps available for free download.
- Install a malware detection program on your computer. Read reviews that were created using professional labs and technical research.

I had both an antivirus/firewall program and a malware program running during the download; both missed the malware from the Filezilla download (later I learned not from a really legitimate source). I obtained Malwarebytes anti-malware and haven't had a problem since. No doubt there are others as good.

Prevent Hacking of Accounts (email, social networking, other online accounts)

There are ample recommendations online. Hacking is reportedly due more often to password theft (e.g., malware silently installed on your computer; somebody reading a printed list of your passwords, or that sticky on the side of the monitor!), bad passwords, or reuse of passwords than hacking the email provider.

- E-mail accounts
  - Use a secured account
  - Make the password hard to guess (see below)
  - Keep your password confidential
  - Be careful responding to messages that your email account has been hacked. In the last 5-6 years, I have never received a legitimate notice that my email account was hacked, although at least 1 message of this type comes in weekly
  - Better to not use your email address as your log in ID
- Social networking
  - Have a secured account
  - Keep password secure
  - Don't use a public computer to check in
  - Be quite careful of any third party apps on social networks
  - Use the account's security settings for more safety
  - Consider using privacy settings to limit who can see your information
- Sensible password precautions
  - Include symbols, numbers, uppercase letters, lowercase letters
  - Exclude similar characters (e.g., 0 [zero] and O [capital letter o]
  - Use long passwords (at least 8 or 9 characters)
  - Avoid using names of family, friends, pets, phone #, postal codes, social security number, or dictionary words
  - Change passwords often – every 3 to 4 months
  - Use a different password for every account
- General
  - Keep all passwords secure however you choose
  - Don't reply to any emails sent to your spam folder
  - Scan your computer and other devices regularly for viruses and malware
  - Don't click on "remember me" after logging in unless it is your own home computer

If it all seems like too much effort, remember that if a hacker gets your log in information, your whole web life could be wiped out. An ounce of prevention is worth a pound of cure (Benjamin Franklin).