Let's Schmooze

Other issues of *Let's Schmooze* can be found on the web at www.heirling.com

Primer on Internet Safety

They're getting a lot more aggressive about hacking into our computers. Computer hackers are looking for personal and financial information ~ and those almighty passwords ~ so that they can loot our banking and investment accounts, our e-mails, and even our personal identities. Call it "robbery by keyboard" ~ today the most lucrative way to steal someone else's goodies.

A while back, we ourselves experienced a source code hack attempt. It was blocked from executing by our real-time anti-exploit software. The hack attempt was a zero-day *radECCE3.temp* file buried in a seemingly innocuous Microsoft Word document attached to an incoming e-mail. If the hacking file had not been blocked, it would have corrupted and taken over our entire system.

Everybody is at risk ~ individuals, businesses, global corporations, banks, governments, etc. No one is immune to being hacked. Even the super-powerful United States federal government is constantly plagued by these pestilent scoundrels. Everyone, at every level of society, must be unremittingly on guard against these remorseless thieves. State-sponsored hacking can be extremely difficult to defend against, even for trained professionals.

However, there are simple steps that one can take to make it difficult for the hackers to break into one's personal information. We can't wait for the big companies and government to do it. There are things that one can do to protect oneself. Once they are put into place on your device, you can rest easier. Here are some steps.

First, keep your operating software up-do-date. Today's operating systems ~ provided by manufacturers such as Windows, Apple, and Google ~ provide a lot of realtime protection, including both malware and firewall safeguards. You can usually set your device to update the operating system automatically. Do that. Not updating automatically can leave you vulnerable to newly engineered malware.

Second, run additional protection. For those of you who are running Windows 10, that operating system includes a malware protection package called Windows Defender. Consider running a second malware protection software ~ in real time ~ that won't conflict with Windows Defender. Manually force both Windows Defender and your second line-of-defense to run deep, comprehensive scans at least monthly. The automatic daily scans tend to be quick scans.

Third, never use the same password on more than one account, and change passwords at least quarterly or yearly. Make sure that your passwords are a random mix of uppercase letters, lowercase letters, numbers, and special characters. Eight to thirteen characters would be great. Keep your passwords in a safe, secure location where you and only you have access to them.

Fourth, use 2-factor authentication whenever it is offered by a web site vendor, especially on financially sensitive accounts. This adds a second layer of security to your passwords, and makes it doubly hard for hackers who might run across your password on another site. With 2-factor authentication, they will need more than your login and password to access your accounts.

Fifth, clean out your browser histories at least once a day. That includes all histories, including cookies and saved passwords. If a hacker made it into your browser, you don't want any sensitive information waiting to be plucked and used against you. If you are concerned about cookies being silently sent to your device, running a protection package specializing in spy-ware removal would be a good idea.

Sixth, have a virtual private network (VPN) up and running in real time. Set your VPN to load whenever your device boots up. For those who really want to go far out on the security-and-privacy limb, it would be a good idea to start running important or sensitive applications through a VPN. There are a lot of good VPNs out there.

Essentially, when a VPN is utilized, a restricted "tunnel" is created through the Web that only you can utilize. It is as if one was standing in the public square, but talking in a language foreign to the surrounding bystanders. No one around you would have the foggiest idea what you were talking about. That's the security and privacy that a good VPN can offer.

Seventh, have the HTTPS Everywhere browser extension running in your browser(s). This will force most web sites to use maximum encrypted security when you are accessing and using them.

Eighth, power down your device at least once every 24-hour period, and leave it off for at least five to ten minutes. That will force the operating system to cold-boot with all the latest changes and updates, and it will also force the VPN provider to randomly reassign a new IP address to your device. Hackers ~ and advertisers ~ hate that.

Hacking is increasingly a serious threat, and we all need to get far more serious and vigilant about unceasingly guarding against it. It's not fun to lose one's hard earned wealth to a thief, nor is it any fun to lose one's personal identity to nefarious characters.

Once it happens, it is extremely difficult to regain what was so insidiously taken. Let's avoid that pain!

Hackers are like any other thieves ~ **they like easy pickings**. If you make your internet "house" close to impregnable, thieving hackers will go somewhere else ~ where they don't have to work so hard to break in.

~ *til we meet again* ~