TRUST NO ONE! – 11.19.15

As I've been speaking to most of you and reading the Tech Blogs, I am very disconcerted about the way hackers or miscreants are trying to get into our computers.

I have seen the following:

1. Phone calls to YOUR homes indicating that
    a. This is a Follow Up to something they have already worked on
    b. Something is wrong with your computer and they need access to help you

2. Pop Ups from the following sources indicating that your Computer requires immediate attention.
    a. MacKeeper (BAD)
    b. Tune Up My Mac (BAD)
    c. Other sources

3. Spoof Emails that look real but aren't from:
    c. Facebook
    d. iCloud
    e. PayPal
    f. Google
    g. Ebay

4. Spoof Emails from MYSELF - yes - they are addressed to me BY me with my correct email address in the From field.

At any rate, my main advice to you is to TRUST NO ONE! IF you receive an email from your bank or from any other source that is asking you to verify your information, DON'T! Either call the bank or the other source or go directly to their website and check it out directly. Do NOT click on any links.

Also, if you are constantly getting redirects or popups on your computer, it means you've been infected with MalWare. My recommendation is to go to the site www.adwaremedic.com and install malwarebytes and scan your computer. If the redirects are so bad that you can't get there, call me and I can clean your computer

enough so that we can scan it and clean it up. If you want to read more about MalWare and the latest news on new malware, look at www.thesafemac.com. You can install malwarebytes on your PC as well as Mac.

In addition, I have recently read articles about "ransoming" mac computers. While this is more prevalent at the Corporate and PC level, there has been recent news about it possibly infiltrating Mac computers. I will keep an eye on this, but here's an article if you are interested in learning more about it:

http://www.macworld.com/article/3003987/business-security/ransomware-for-mac-is-nothing-to-worry-about-for-now.html#tk.nl_macwk

Another way to infect or bring malware onto your computer is to download applications for third party sites. A lot of time when I come to your homes and I see malware, I always ask, do you share your computer with your kids? To make your computer a little bit safer against unwanted downloads, go to the Apple (upper Left corner), choose System Preferences/Security & Privacy/General - then check Allow applications downloaded from Mac App Store and identified developers. At least if your kid tries to download something, he/she will need the computer password to do so. Here's an article about the perils of downloading from an inappropriate site:

http://www.macworld.com/article/3000984/mac-apps/never-download-software-from-software-download-sites.html#tk.nl_macwk

A friend of mine who works at DropBox told me that if you are a Pro Subscriber, you should be all set in terms of hijacking because of their extended version history feature: https://www.dropbox.com/en/help/113. I am currently slowly moving my data over to DropBox and can help you if you are interested. I have about 1.5 terabytes of files to move over.

At any rate, good luck and stay safe!