**President's Corner: September, 2014**
**Know with Whom You are Dealing**
**By Eric Moore**

As many people are using Internet, it is no surprise that criminals are seeking new, innovative ways to scam you into giving up access to sensitive data and your computer devices for their own use. They know that many users are not very savvy about computer security and how to detect a scam, so they will continually try to trip up anyone they can through spam, counterfeit websites, text messages, unsolicited phone calls, and fake security alerts. There are many ways they will try to trip you up, and no one is beyond fooling if the ploy is well-designed, and new scams are being devised every year. Your best weapon is to be very cautious and skeptical. Although this short article is not an exhaustive list of the ways you can be fooled and robbed, it will hopefully arm you with basic information that you need in order to protect yourself.

**Verify with Whom You are Dealing**

A cardinal rule to keep in mind before giving out personal data, money, or access to your computer, is to verify with whom you are dealing. In October 2005, my predecessor, Jamie Leben, gave an excellent presentation on computer security. To protect yourself and your assets, you should always confirm that anyone you deal with by email, chat, text, or phone is who they claim to be, and that they have a right to the information they request of you. If you receive a phone call about a problem with your banking or credit card count, or a security problem with your computer, or anything else that requires you to give up your personal data or provide access to your computer, hang up. If you receive electronic communication such as a text or email, do not respond. If you are concerned enough to follow up, then look up the person's or company's contact information from a trustworthy source. If it has to do with your bank or credit card, then call the phone number listed on your bank or credit card statement. For computer products or services, look for contact information or a web site address in the product documentation, invoice, or on the product packaging. For a government agency, look it up in the phone book or an official publication. Be careful of searching for a company's web site on the Internet, as scammers set up websites with a URL that is similar to that of a legitimate company, and then gladly fleece you for sub-standard support, or to gain control of your computer. As a rule, never give up any information—name, birth date, credit card number, banking information, password, or anything else—to someone you do not know.

A common scam that has been around for a while, operating out of call center in India, is one in which someone calls you out of the blue, claiming to be with Microsoft or a company affiliated with Microsoft. The reason for the call is that they supposedly detected a malware infection on your computer and will assist in “cleaning” it. They will attempt to convince you to allow them remote access to your computer, which they may then infect with software that will collect your personal information or perform any other of number of functions. They will also attempt to convince you to give up payment information such as a credit card number or PayPal account, so they can then steal your money, ostensibly as payment for “services” or to “renew” an expired Microsoft license. Microsoft does no such thing, nor do any of their legitimate affiliates.

**Pop-ups**

Malicious websites can produce pop-ups that make a variety of claims such as your computer is infected, the registry is “poor,” your computer is running slow, etc. Don't believe it. It is too easy for

someone to concoct a website pop-up that looks sophisticated enough to be a legitimate warning. I have even seen one that contained animated graphics of what appeared to be an active scan of the user's hard drive for malicious software. No web site is checking your computer for problems. Do not click on the pop-ups—close them. Do not call a phone number listed on the pop-up or purchase any software you supposedly need. Do not trust a pop-up for a product you've never heard of and never installed on your computer. If you cannot close a pop-up, it may be safest to shut down or reboot your computer to get out of the site. Then be certain not to return to the website. Other pop-ups may be produced by malicious software that is installed on your computer by a "drive-by download." These can be more troublesome, as they can take up residence on your computer and not go away no matter what you click or even if you reboot. Some, such as fake warning that you supposedly did some criminal, thus necessitating the FBI to lock you out of your computer, can be especially difficult to close or remove.

As a rule, you always want to be certain you have a current anti-virus program installed before you connect to the web. The program should automatically download and install updates when they become available, and should always have an active subscription. (You should also keep up-to-date with the latest software updates for your operating system.) Some programs may require you to renew your subscription every year, so be certain to do so. In addition to having good anti-virus software, I have found the free version of Malwarebytes Anti-Malware to be a good additional tool for finding and removing troublesome software that other anti-virus software may miss. The free version does not constantly run in the background, so it won't interfere with other software such as Norton AntiVirus, which is always running. You should also be careful of the websites you visit. If you do not know what a site is about, it is best not to go there. But then, even legitimate sites can be hacked into to serve up malware to visitors, so be certain your anti-virus software is up-to-date. Some browsers such as Google Chrome and Mozilla Firefox can warn you if they detect the site may be dangerous.

**Email Security**

Don't believe everything you receive in email. If it sounds too good to be true, it is. A common scam is the "Nigerian 419" scam in which a person supposedly from Nigeria or other foreign country needs help moving millions of dollars from a bank account to another account overseas (never mind that it would be illegal to do so). All you need to do is to give your account information so they can transfer the money and leave you with a tidy fee for your assistance. A variation of this scam is that someone has supposedly died and left no heirs, so you have been chosen because of your reputation to be the lucky recipient of the money. Do not fall for them. Too many people have lost money, which is why these scams are profitable and continue to be propagated. Never share sensitive personal or financial information by email; you might just as well write it on a piece of paper and post it on a public bulletin board for the world to see.

File attachments are another concern. Too often times, you may receive email with an important attachment to be opened. The message may be "spoofed" to make it appear to be from someone you know or from a legitimate company. The scam runs the gambit of a picture of a promising romantic match, an airline ticket you supposedly purchased, an invoice for an online purchase, a form for claiming an undeliverable shipment, details about an ACH transfer, an important Windows update, etc. As a rule, never open a file attachment from someone you do not know; just delete the email. Never open a file attachment that appears to be from someone you know, if you did not expect to receive the file. If you think you know the person, call or write to confirm that the attachment is legitimate. Unless you can confirm it is legitimate, do not open it.

As for "official" communications regarding unpaid taxes, money transfers, failure to show up for jury

duty or a court case, or other governmental or financial matters, you should expect to receive it as U.S. mail, not as an email message or attachment. Also, be suspicious of email that appears to be from a company or government entity with whom you know you have never shared your email address.