Home Network Security and Protecting Against Internet Scams

There's a saying that harkens back to the days of street vendors and door-to-door salesmen that goes, “There's a sucker born every minute!” For the scam artist, however, no truer words have ever been spoken. In our rapidly changing world of information access, mobile communications and creative marketing, consumers are exposed to a flurry of 'round-the-clock sales solicitations like never before. And the online scam artist is always there waiting, looking for new ways to con un-suspecting shoppers out of their hard earned cash.

Before the Internet, most households received sales solicitations through news print, direct-mail, television or radio advertisements. Today's advertising environment is far different from what it was a mere decade ago thanks in no small part to the rapid growth in Internet access and mobile communications. Moreover, nuisances such as cookies, pop-up ads and spam email that were once limited to home computers are now in your face 24/7 compliments of cellular phones that are Internet accessible. Making Internet security matters more complicated are the small computer programs called “apps” (short for “applications”) many cell phone users download daily as a matter of convenience for everything from online gaming to tracking your online shopping habits. It goes without saying that *going mobile* has forever changed how the world communicates. However, as advances in mobile communications technology pushes us more and more to “stay connected”, the threats to our online security, privacy and our wallets are sure to increase drastically! As members of this new and intriguing wireless communication world, it is incumbent on us as consumers to take every necessary precaution to stay ahead of the scam artists and protect ourselves from online security threats. Hopefully by the time you're done reading this chapter, you'll be better prepared to protect yourself against online privacy invasion, security threats and Internet scams that threaten to make your online experience a disaster!

Domestic Internet Access

In 1997, only 18 percent of all U.S. households with computers had Internet access. By 2009, nearly 70 percent of all U.S. households had Internet access[1] and by 2015 that figure had increase an additional 8 percent. However, Internet access is no longer limited to just the home computer. Today, mobile communications devices such as the iphone*, smartphones and other portable devices have made the Internet more accessible than ever before. This broader access in wireless communications also comes with an

1 [1]U.S. Census Bureau, “Population Survey” report; release date February 2010

increase in online security risks. According to leading experts, the aim of cyber security attacks is to steal data and/or personal identify information from unsuspecting, unprotected Internet computer users in an attempt to make money through their illegal use. It stands to reason then that the best way to protect yourself against cyber attacks is to configure and use your wired and wireless devices in ways that prevent unwanted access. The following sections provide helpful guidance on how to protect yourself from cycber attacks.

Note: The suggestions offered herein should be viewed as a guide to help protect you from unwanted Internet intrusion and not be considered as an all inclusive list of things-to-do, nor should they be viewed as 100% fail-safes to prevent unauthorized access to your wired and wireless devices. However, the hope is that the tips provided will help you to protect your computing and mobile communications devices from unwanted virus attacks and keep you from being scammed.

*The iphone and ipad are Apple® Computer brand model devices. Most cellular phone companies offer smartphones to their customers for mobile cellular phone communications; however, most experts on the Internet attribute the iphone as the mobile device that changed the way consumers use mobile communications devices to access the Internet. Therefore, the author refers to the "iphone" rather than the smartphone when addressing Internet access using a mobile communications device. Thus, the "iphone" and "smartphone" are used synonymous throughout this text. Nonetheless, it should be noted that smartphones are also widely used to access the Internet.

Internet Security Measures

- *Upgrade Your Web Browser* - The easiest protective measure you can take concerning Internet security is to upgrade your web browser. The two most common web browsers available today are Microsoft's Internet Explorer and Mozilla's Firefox, but others such as Google's Chrome are quickly gaining in popularity. As of this writing, the latest version of Internet Explorer is version 9; for Mozilla's Firefox it's version 8.0.1. Both web browsers have an auto-update option which when activated sends the most up-to-date features directly to your computer automatically when they come available.
- *Turn Off Auto-Fill/Auto-Display features* - For many Internet users, the convenience of reducing the number of keystrokes to complete common tasks such as filling in the log-in password to your favorite online forum is appealing, but leaving such features active leaves your computer open to security

vulnerabilities. Cyber security experts suggest turning this auto-fill feature off because it leaves the door open for computer hackers to invade your privacy and steal your personal information.

- *Pop-up Blocker* - One of the most annoying advertising tools that makes surfing the web so frustrating for many Internet users is pop-up ads. These small "click-through" ads were designed to replace traditional banner advertisements. Although pop-up ads have proven to be very cost effective for online businesses, they've also proven to be big annoyances for Internet surfers. Thankfully, this annoyance can be virtually eliminated by turning on the pop-up blocker feature in your web browser.

For Internet Explore (version 7 and higher): Go to "Tools>Pop-up Blocker>Turn on Pop-up Blocker".

For FireFox: Go to "Tools>Options>Content" and check the "Block Pop-up Windows" option.

- *These Aren't Grandma's "cookies"* - Another common advertising tool that can present security problems for Internet users are "cookies". An Internet "cookie" is simply a string of coded information a website uses to identify one computer user from another. In one respect, Internet cookies are a win/win for both the Internet users and the host website. For the visitor, cookies help load your most frequently visited websites faster. For the host website, they help "refresh" web content faster based on your previous visit(s) to the host site. There has been an ongoing debate, however, as to whether or not cookies pose a risk to Internet privacy because they track your Internet movements and browsing habits. To help avoid this, both aforementioned web browsers allow you to delete your browser history as a matter of routine if you suspect foul play. To activity the "delete browsing history" feature in both Explore and Firefox:

For Internet Explore: Go to "Tools>Delete Browsing History" or "Tools>General" tab, check the "Delete browsing history on exit" box or click

the "Delete" button under "Browsing History".

For FireFox: Go to "Tools>Clear Recent History" or "Tools>Options>Privacy" and either check the "Tracking" box to tell FireFox you don't want the browser to track the website you visit or click the links on the dialog box to either clear the entire browser history or select individual cookies to remove.

- *Use In-Privacy Browsing* - "In-Private Browsing" is a privacy feature that is relatively new to the Internet browsing experience. In-Private browsing basically allows you to surf the web without your browser collecting tracking information such as cookies, temporary Internet files, browsing history or other data about your Internet browsing experience. Internet Explore, FireFox and Google Chrome all offer this type of privacy protection and is easy to activate:

For Internet Explore: Go to "Tools>InPrivate Browsing"

For FireFox: Go to "Tools>Start Private Browsing"

For Chrome: Select "New Incognito Window" from the menu option

- *Network Security Measures* - Spyware, malware, auto-loaders, trojan horse and worm virus are types of malicious software that can render your computer as useless as paper weight atop a stack of papers in a wind storm. Protecting your computer against such threats requires you to take, at a minimum, the following security precautions:

  - Keep Your Operating System Up-to-date - Keeping your computer's operating system up-to-date is your first line of defense against network security threats. Microsoft Windows, one of the world's leading operating systems, has made this process easy by embedded a security feature within its operating system called "Automatic Updates". This feature allows you to set your computer to install essential software and security updates to featured components of your operating system at a pre-set interval (i.e., each Tuesday at 11:00 PM). However, you can manual search for updates as necessary. For Microsoft

Windows, auto-updates can be activated in the "Control Panel" under "Security and Security".

- Put a Firewall up between your computer and the rest of the world - Just as a brick wall helps to protect your home against unwanted intrusion, a network firewall helps protect your home network from unauthorized access. A firewall is basically a network access protocol that authorizes the exchange of data between your computer, your Internet Service Provider and the Internet. Once authorization has been confirmed, data is allowed to flow between your home network and the Internet. Some firewalls are built into your computer's operating system (such as Windows XP or higher). However, a firewall can also be a standalone hardware devices. Regardless of what type of firewall you use, ensure to keep it turned "ON" to help reduce the odds of unauthorized access to your computer.

- Use robust anti-virus software - Anti-virus software is essential for keeping your computer, if not your entire home network, secure from unwanted computer viruses and other malicious computer threats. Although free anti-virus software does a fine job of helping protect your computer against such threats as spyware, malware, auto-loaders, trojan horse and worm virus, they aren't as robust and can be easily manipulate should a hackers gain access to your computer and realize you're not protect by a fully loaded commercial anti-virus program. That's not to say that free versions of leading anti-virus software aren't affective at preventing unwanted virus intrusion. However, it does require diligent attention-to-detail to ensure your virus definitions are always up-to-date. To ensure your computer is well protected against potential security threat, it is highly recommended that you have a full commercial version of anti-virus software installed on your computer. It should be noted, however, that venders of operating system software such as Microsoft Corporation are now making anti-virus software like Windows Security Essentials® part of their operating system in an effort to stay a step ahead of computer hackers.

Note: Windows Security Essentials comes standard with Windows Vista and Windows 7 and runs in the background. As long as Window's automatic updates features is activated, Windows Security Essentials will check for security threats and update anti-virus definitions automatically at pre-set intervals you select.

Home Network Security and Protecting Against Internet Scams

Wireless Communications

Wireless communications is nothing new. The technology goes back as far as the late 1800's with the invention of the radio telegraph but gained prominence during World War II with the use of portable hand-held radios (more commonly known as the "walkie-talkie"). However, early wireless communications devices had one drawback - they only allowed for one-way communications reminiscent to today's "push-to-talk" hand held radios. Wireless communications took a giant leap forward with new mobile communications devices such as the car phone and the cordless telephone. Both devices were considered pioneers in early wireless communications technology. Today, the iphone (and similar wireless communications devices such as the ipad) dominates the wireless communications airwaves. But where wireless Internet access is concerned, the wireless router remains king! Except for cell phones, most wireless devices use a wireless router to access the Internet. A security breach to your wireless home network can typically be attributed to vulnerabilities in the configuration of your wireless router. As such, it is very important that you familiarize yourself with the setup procedures and security features of your router in order to protect your wireless network from unwanted intrusion. This section will cover basic steps you can take to better protect your wireless home network from unauthorized access.

- *Wireless Security* - As more and more people go from wired to *wireless* Internet access, establishing a secure connection to the Internet becomes critical to your web browsing experience. For example, laptops and online gaming systems, such as Microsoft's Xbox or Sony® Playstation, are capable of accessing the Internet using a wireless access point such as a wireless router or Wi-Fi hot spot. Regardless of how you access the Internet whether through a wired connection or a wireless access point, it is important that you take the proper security measures to protect your wireless devices from unauthorized access. This not only means finding networking hardware that's compatible with each wireless device in your network (such as ensuring the frequency setting for your wireless adapter meets or exceeds frequency standards of your wireless router (i.e., 802.11g is standard, but there are wireless adapters that broadcast at higher frequency ranges)), it also means ensuring that your wireless access point and your wireless devices are properly configured to minimize potential security risks. We've address ways to protect your computer against such threats. Now, let's outline ways to help keep your wireless home network secure.

Home Network Security and Protecting Against Internet Scams

- *Use Strong Password Protection* - One of the easiest security measures you can take to protect your wireless home network from unwanted intrusion is to set your network (router) password using a combination of numbers, letters in both upper and lower case, and symbols (i.e., #123AbC*Z). Most network security experts recommend using a password string between 8-15 characters long. The goal is to create a password that's difficult for hackers to figure out. DON'T use your birthday, anniversary, child or pet's name, street address or *any* part of your Social Security number as your password. (You'd be surprise to learn how many people actually use these common personal characteristics, in whole or in part, as their password and how quickly they are hacked!)
- *Wireless devices have MAC Addresses, too!* - A MAC (Media Access Control) Address is a 6-part, dual-digit alpha-numeric code that is unique to each network interface whether a network adapter card or portable network antenna. This address is different from your Internet Protocol (IP) address which is acquired from your Internet Service Provider (ISP). Your IP address tells your modem (for direct Internet connections) or your router (for network Internet connections) which service provider to use while your MAC address tells your router which wireless devices are authorized to access the Internet over your network. The MAC address for each network interface is set by the manufacturer. A typical MAC address might look something like this:

Example: 01:A3:FF:3B:4B:33

When setting up your wireless home network, the first MAC address you'll need is that of your wireless router. The MAC address is usually imprinted directly on the device. Next, access your wireless router by entering its default web address into your web browser. For most wireless routers, the default web address is http://192.168.1.1. From there, find the setup page that asks for the MAC addresses of the wireless devices in your network and enter each address here. Be sure to enter each MAC address correctly otherwise your wireless device will not be detected by your home network.

Home Network Security and Protecting Against Internet Scams

- *Give your wireless network a real name* - The default name of your wireless home network (or SSID which stands for "Service Set Identifier") will likely take on the name of your wireless router, i.e., Linksys.net, which is fine if you wish to try to remain anonymous in the big bad world that is the World Wide Web, but what happens when there's more than one "Linksys.net" broadcasting in your neighborhood? To work around this identifier problem, change your SSID to something more familiar so that you can distinguish your home network from others out there. It's also a good idea to check the "Do Not Broadcast my SSID" box during the network configuration process to help prevent unwanted access to your wireless network. If hackers can't find you, they can't harm your network.
- *Change your Pass-Through password routinely* – As mentioned in the above section on Using Strong Password Protection, having a strong administative passwork on your router is the first step in protecting your home network from unwanted intrusion. However, your router also provides internal security measures to help prevent unwanted access to your home network from outside invaders. Your pass-through code is a manual code you enter during the setup process when installing your router. This code allows authorized users access to your home network and keeps outside intruders out. To ensure hackers don't get a fix on your pass-through code, it's a good idea to change your pass-through code occasionally (once a month is ideal). Be sure to share your new code with all authorized users of your home network. (See *Wireless Devices have MAC Addresses, Too!* above).
- *Make Break-In and Entering Tougher for Hackers!* - Another step you can take to protect your wireless network from unauthorized access involves setting your router's security encryption to the highest level possible. This requires ensuring that your encryption is identical on both your router and your wireless devices. Most wireless routers come standard with WiFi Protected Access 2 (WPA2) level encryption. However, as stated previously you should try to find networking hardware that is compatible with each wireless device in your network. This is especially important when selecting a wireless router and a wireless antenna (one per wireless device) that meet the highest encryption protocol. For this reason, it is highly recommended that you choose wireless hardware with a minimum encryption level of WPA2. However, don't be put off should you find wireless hardware that combine encryption standards, i.e.,

Temporal Key Integrity Protocol (TKIP) w/Pre-Shared Key (PSK) (i.e., TKIP-PSK) or w/WPA2 (i.e., TKIP-WPA2). If in doubt as to which encryption protocol to use, consult your wireless hardware manufacture's instructions or your electronics retail specialist. (Best Buy has an outstanding computer troubleshooting and repair department.)

- *Automatic -vs- Static IP Address Configuration* - In a typical home network, the host computer is assigned an IP address by your local Internet Service Provider (ISP). Your ISP then issues a series of lower level IP address in range of the host IP address. In most cases, this automatic assignment is sufficient to cover all wireless devices in your home network and allow them to access the Internet. But occasionally the need arises where entering a "static" IP address is preferable for added security or because you're experiencing difficulty connecting to the Internet using an auto-assigned IP address. If you experience such difficulties, you should contact your local Internet Service Provider with details of your connectivity problems. If all troubleshooting steps fail even after contacting your wireless hardware manufacture, your ISP may issues you a static IP address as a go-around to resolve your Internet connectivity problem.

- *Put all wired/wireless devices to sleep* - There's one final step that needs to be addressed in protecting your wireless home network from unwanted intrusion and it's the easiest and perhaps the most ignored step of all...set your host computer and other wireless network devices to hibernation mode (or more commonly referred to as "power saver" or "sleep" mode) after a specific interval of non-use, if possible. This is different from activating your screen saver. While screen savers help to keep background images from "burning" into your screen particularly with flat-screen monitors, hibernation mode turns your computer off after a specific period of non-use. This may seem like an obvious thing to do, but most home computer users are accustomed to leaving their computer on for long periods sometimes for days on end. This habit stems from the old wives tale that suggests that turning your computer on and off frequently could damage your hard drive. Today's computer hard drives are very durable. Not only does activating hibernation mode help to conserve energy, it also removes your computer(s) from the World Wide Web temporarily. Thus, if hackers can't find you online they can't hack into your computer or your network. To activate hibernation mode in the latest version of MicroSoft Windows (Vista or Version 7):

Go to: Start>Settings>Control Panel>Power Options

A Power Schemes dialog box should appear. Select the features you wish to turn on including setting the time interval your computer goes into hibernation mode when not in use. And that's it! Assuming you've followed the manufacturer's instructions for your computer and other network devices and you've made the proper security settings, your home network should be as safe as it can be to surf the Web...short of operator errors, of course. Which now takes us to online scams.

- *Online Scam Prevention measures* - There's a saying that goes, "If it's too good to be true, changes are it's a rip-off!". I'm here to tell you that if you don't do your due diligence and investigate the validity of an advertised product or service, chances are you may learn the hard way that what you thought was a bargain turns out to be worthless! When faced with debt particularly during hard economic times, may people become desperate to get out of their financial situation. The stress of being in debt and having to answer the constant barrage of phone calls from creditors is more than enough to keep most consumers tossing and turning at night. As such, many unsuspecting consumers find themselves the victim of scam artist who just ripped you off for their last dime while attempting to get out of debt only to find their debt woes just got worse! #@$!! But fear not; there are ways to beat the scammers and protect yourself from being ripped off, but it starts with paying closer attention-to-detail to questionable sales solicitations.

  - Leave those odd, but interesting advertising links alone. Ever come across a link to an online advertisement you couldn't resist? You click on it only to become bombarded with multiple adware, spyware or autoloader (trojan) programs? Momma always said, "curiosity killed the cat." That cat may have eight more lives, but chances are if your computer gets hit with a virus it may be the last time it works again...at least until you can get the virus cleaned from your computer's hard drive. Actually, that's kind of an understatement. Today's computer hackers are getting more sophisticated. No longer is it just your hard drive that's the target of computer hackers. Viruses can now be embedded onto your computer's RAM ("random access memory) or BIOS

("basic input/output system") rendering your computer virtually useless. Fortunately, there are programs out there that can help clean your computer once infected (i.e., full versions of anti-virus software) or you can seek the assistance of a free online diagnostic service to diagnose and repair you computer problem (i.e., Bleepingcomputers.com – *outstanding source for online help in computer virus diagnostic and removal*; their staff is very helpful and extremely knowledgeable). Of course, if you can just resist clicking on unfamiliar links you might be able to prevent being infected in the first place.

- Don't open suspicious email or their attachments! Most of us are keenly aware that email attachments from unknown sources have the potential of containing a computer virus. Therefore, it should go without saying, *"DON'T open email or their attachments from unfamiliar sources."* Unfortunately, many people still take the risk and open questionable emails and/or their attachments anyway. A common email scam involves a process call "phishing" where scammers send out a seemingly legitimate email that gives the impression of originating from a reliable source, i.e., a bank, a popular department store or even the email server from your job, in the hopes of convincing you to part with your personal information. The scam usually involves you receiving an email notification offering you a special prize from a "sweepstakes" or "lottery" winning, or requires that you verify your social security or bank account number before you can receive your prize or have funds released to you. I can't make it any clearer than this: "*A legitimate bank, credit card company or retail stores (where department store credit cards are concerned) WILL NOT ask you for your social security number or account number!*," especially not via email. Of course, why would they since they already have this information in their company database? The term "phishing" means exactly like it sounds like; the scammer is "fishing" for your personal information in order to commit identify theft. And once he/she gets a hold of your personal information, it's very likely you'll either see a significant decline in your checking account balance in short order or questionable charges to your credit card account. So, how does one go about determining a legitimate email from a potential scam? There are a couple of safeguards you

can take to limit your risk of exposure depending on which email program you use.

- ✓ Use the Preview Pane. Some of the more popular email programs, such as Microsoft Outlook and Lotus Notes, use a preview pane that allows users to *view* email before actually opening it. The preview pane won't allow you to view the contents of email attachments, however. But atleast you get to read the email content and then decide if the attachment is worth opening or downloading.

- ✓ Scan it before you open it! The surest way to prevent exposing to an email virus is to scan the attachment before opening it. Most anti-virus software will allow you to scan a document or a specific folder to check for viruses. If the attachment passes the virus scan, chances are it's safe to open. But one word of caution: *Ensure your anti-virus software is up-to-date*; there's always the off-chance a new variant of an old virus is out there...waiting to bypass an out-dated anti-virus program.

❖ Security threats to smartphones/iphones. Accessing the Internet using our cell phones is fast becoming commonplace. As more and more people use their cell phones to connect to the Internet, network security will become more problematic. Security threats that were once limited to computers – adware, spyware, malware, viruses - have slowly begun to migrate to cellular phones. The primary reason behind this increasing migration is that not only do computers and cell phones access the same World Wide Web, they also use the same eCommerce advertising tools - hyperlinks, email and icons - to access information or review advertising content. Making matters worse is the flood of “apps” - mini-programs activated by clicking on small pictorial images similar to computer icons – to do most of our “computing-by-phone”. Although cell phone companies take great care to screen apps for security threats prior to making them available to the public, experts predict it will become more difficult to distinguish legitimate apps from those associated with online scams as corporations become more aggressive in their advertising campaigns and scam artist become more clever in how to use apps and/or cell phone network technology to their benefit. Already, there's been an increase in hybrid “phishing” scams cropping up directed specifically at the iphone market. The first is called “smishing” which uses text messages to lure

unsuspecting cell phone users to respond to either the number listed in the text ad or a toll-free number. The other is "vishing" which uses voice mail to solicit the scam. In this scam attempt, the unknown caller leaves a seemingly legitimate voice mail message in your in-box with a toll-free number for you to call back in the hopes that you'll provide your personal information.

- ❖ Social Media Confirmation. Social Media sights, such as Microsoft Outlook (formerly "Hotmail") and Facebook, are now using text messaging confirmation to verify the identidy of individuals to ensure that only authorized uses and have access to social media sights. The process works alittle like this: You access a social media sight from a remote location other than your usual location (i.e., home or wireless hotspot while traveling). The social media sight will ask for the standard user ID and passwork and possibly a "secret question" only you can answer. But even if you enter all information correctly, you're still not done. A confirmation code is sent to your cellphone or email asking you to further confirm your identidy and assess to the social media sight with a twist: You have to enter the confirmation code within a specified period of time (usually a few seconds). Otherwise, the confirmation code changes. Entering an expired confirmation code after a few incorrect attempts can lock you (and/or the unauthorized user) out of your social media account.

So, what should you do if you suspect you might be being scammed?

- ➢ *Be cautions of answering phone calls, text messages or responding to voice mail from unknown sources*. Generally speaking, most cell phone users will add the names and telephone numbers of friends, family or other known contacts to their Contact List. However, with the increase in smishing and vishing activity, odds are it's only a matter of time before you're contacted by an unscrupulous source pitching their sales scam. If you receive a phone call, text or voice mail solicitation from a suspicious or unknown source, try to get as much information as possible about the soliciting company (i.e., name, address, call-back number, business license number, etc.) and contact your cell phone provider or your local Better Business Bureau (BBB) to verify the legitimacy of the company. Chances are notifying your cell phone provider is the only way they become aware of a potential cell phone hacking or sales scam. Therefore, it is

extremely important that they hear from you - their customers - concerning unsolicited sales contacts. You can also contact your local Chamber of Commerce as they often can tell you if a company is a registered business in your area. If you do not receive a favorable report either from your cell phone provider, the BBB or Chamber of Commerce, chances are the suspect company isn't an entity you want to do business with let alone share your personal information. *Always verify the source of the cell phone communication before giving out your personal information*.

- *Unsubscribe from unwanted email subscription lists*. It's not uncommon for your contact information to be sold as part of a master sales database. It's part of doing business. The only way to reduce and/or eliminate unwanted solicitations is to opt-out of every annoying online solicitation you receive in your email Inbox.
- *Use the Internet to verify the scam*. In short, "Google it!" You can also use scam reporting websites, such as ScamBusters.org, to obtain the latest information on online scams.
- *Be alert!* Look for "the oddities"...things that just don't look or sound right.

Remember: If it sounds too good to be true, chances are it's a scam! So, do your due diligence and always be alert of odd emails, cell phone calls, text messages or any pop-up advertisement that just doesn't seem right to you. Ask yourself obvious questions, i.e., "why would my bank be asking me to verify my bank account information" or "I don't recall entering any contest or answering a survey". If you get that nagging sensation in the back of your mind telling you something's not quite right, chances are your instincts are serving you well.

So, stay alert, ask questions and verify the legitimacy of the source before giving out any personal information. Taking such prudent steps can save you tons of money and hardship down the road.