

Cybersecurity - Being Safe Online

Presented for the
Tolland Public Library Foundation
December 9, 2015

Understanding digital terminology

- * I will try to keep it simple clarifying things by:
 - * How you can recognize what's occurring
 - * What consequences it could have
 - * What should you do about it
- * When the technology and concepts underlying a technical term are too complex for quick or simple explanations I will suggest where you can look, read and learn. (e.g. websites like Webopedia or
- * <https://www.staysafeonline.org/>
- * <http://www.dhs.gov/topic/cybersecurity>
- * <https://www.fbi.gov/scams-safety/>)
- * You can ask questions or for clarification at any time

What is Cybersecurity ?

- * What are cyber attacks?
- * How do they happen?
- * Who perpetrates the attacks?
- * How frequently do they occur?
- * What makes me vulnerable to an attack?
- * How do I know if I have been attacked?
- * How can I protect myself and my data?

What is “Cyber” ?

- * Cyber- is derived from "cybernetic," which is the "control of any system using technology"
- * Commonly cyber appears as a prefix to describe computer or network/internet related topics e.g. cyberspace, cybercrime, cybersecurity, cyberattack, cyberwarfare or cyberterrorism
- * “Cybersecurity is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide” (Definition from Wikipedia)

What are cyber attacks?

- * **Cyber-attack** is any type of offensive maneuver employed by individuals or an organization that targets computer information systems, computer networks, infrastructures, and/or personal computer devices that either steals, alters, or destroys a specified target by [hacking](#) into a susceptible system.
- * Cyber-attacks can range from installing [spyware](#) on a PC to attempts to destroy the infrastructure of an entire nation. (Definition from Wikipedia)
- * Americans' top fears - include government corruption (58%), cyber-terrorism (44.8%), corporate tracking of personal information (44.6%) - Chapman University's Study

How do they happen?

- * There are many ways your personal PC or device can be attacked including emails, clicking on webpage links or a “pop-up”, connecting an infected USB flash drive, a CD ROM disk with malicious software, a phone call from a criminal
- * Using fake "like" buttons, hackers trick people into clicking on a website link that installs malware
- * Cyberwarfare or terrorism target infrastructure and can severely cripple a nation. Internet connected computer systems are used for control systems, electric grid and natural gas, finance, transportation, telecommunications, and water facilities

Who perpetrates the attacks?

- * People who want to steal information or cause harm to others. Individuals, criminal, political or terrorist organizations (e.g. Hamas & Hezbollah), military &/or espionage units of governments (North Korea, China, Israel and the USA have conducted attacks)
- * Stuxnet was a software virus attack on Iran's nuclear centrifuges, likely by the US NSA / CIA & Israel
- * There is a “black market” for stolen data e.g. identity theft, and for the software & hardware tools used
- * There also are “warped” individuals who engage in this as a “sport”, electronic vandalism

How frequently do they occur?

- * **Nearly 1 million new malware threats are released every day**
- * Attacks on online systems are continuous 7/24/365 & global
- * Attacks on your individual PC or smartphone can occur anytime you connect to the internet or answer your phone
- * According to the FBI hackers stole \$1.2 billion from 7,000 businesses since October of 2013. Some examples are:
 - * JP Morgan bank - 76 million households and 7 million small businesses
 - * 80 million personal medical records from Anthem Medical Insurance
 - * 5.6 million fingerprints and 22 million personal records from the U.S. Government OPM system
 - * The IRS, Target, TJMaxx, Sony, T-Mobile, Amazon ,Vtech ... - compromised.

What makes me vulnerable to an attack?

- * Being online exposes us to cyber criminals and others who commit identity theft, fraud, and harassment.
- * Things that you do or fail to do like clicking on a link in an e-mail or not using up-to-date anti-virus security
- * Some organizations are not careful with our data, not doing enough to prevent unauthorized access and they didn't encrypt data to make it difficult to use if criminals did access it
- * This presentation will provide many more examples of what not to do and what will reduce your risk.

How do I know if I have been attacked?

- * The symptoms vary from slower response on the device to floods of Ads and Pop-ups, a ransom message to unlock your device, and others I'll describe
- * Browser hijacking restricts you to a malicious web site and prevents you from normal connections
- * You may not know unless a scan by a security suite with antivirus and malware detection tells you or you see unauthorized financial activity on your accounts.
- * You can search the InfoArmor database of Email compromised addresses & sign-up for free monitoring <https://pwnedlist.com/query>

How can I protect myself and my data?

- * *This presentation is intended to help you:*
- * Understand basic digital terms & concepts
- * Learn how to be safe in the digital environment
- * Learn to protect your privacy on social media
- * Continue to learn on secure websites
- * You must continue to keep aware of the dangers and consistently follow safe habits

Know the enemy ...

- * It's come to my attention that ignorance is, in fact, not bliss. (author unknown)
- * Computer Viruses, worms, spyware, “phishing” fraud and browser hijacking - What are these attacks and how can you protect your device?
- * Let's begin with some definitions so we all have a shared understanding of basic terms.

Operating System (OS)

- * The software on a device that manages the hardware interconnections of a device (PC, tablet, phone) and allows running the application programs. You should know what version your device has because the attacks and defense options can differ based on this. The most common are:
 - * Apple iOS for iPads, iPhones, iPods; Mac OS X versions
 - * Microsoft Windows 10, 8, 7, Vista, XP
 - * Android – Google developed for phones & tablets
 - * Google Chrome – Chromebook built-in malware & Antivirus protection with auto updates (Linux based)

Web Browser

- * The program you use to access an Internet web site. This could be Microsoft's Internet Explorer (IE), Edge, Mozilla FireFox, Google Chrome or Safari on an Apple device.
- * When you click on a web address e.g. <http://www.google.com> or file of type .html the web browser opens it just like Word opens files of type .doc or .docx

Virus

- * Disruptive programs that install without your permission and often send themselves to everyone in your e-mail address book.
- * **Worm** - A category of virus that replicates itself PC to PC over a computer network (LAN). Like other viruses it does damage, slows or shuts down your PC.

Trojan horses

- * **Trojan horses** are destructive programs that masquerade as a benign application. Unlike viruses and worms these do not reproduce by infecting other files or replicate themselves.
- * (Definitions based on Webopedia)
http://www.webopedia.com/TERM/T/Trojan_horse.html
- * The pop-up that claims it has discovered and will remove viruses from your computer but actually installs them is a classic example

Malware

Malware is short for malicious software; software designed specifically to damage or disrupt a system, electronic vandalism software, or steal information from you like credit card numbers. It installs without your permission, usually hidden in system folders.

Often unwanted software is installed at the same time as legitimate programs, beware of “bundling”

- * Microsoft has Malware Protection pages on FaceBook
<https://www.facebook.com/msftmmpc?fref=photo>

Malvertising (Malicious Advertising)

“One of the more common ruses is to redirect the viewer of the advertisement to a site that warns the user of spyware or malware on his or her computer and offers to scan it for free. Typically, clicking on the "scan my computer" or similar instruction actually places the malware on the computer.”

(This definition based on content at www.webopedia.com)

For iOS (iPad, iPhone) if your Safari browser gets stuck on a bad site disconnect from the internet with airplane mode. Kill Safari, then restart it. It will try to load the offending web site, but will be unable to do so and you will get an error message from a freed-up Safari. Either kill the tab with the offending web site or type in a different address.

Spyware

Dangerous and disruptive - Malware that has been unknowingly installed on a PC. Spyware can monitor your activity on the Internet and transmits that information in the background to someone else who will target you with pop-ups or steal your private data. The most dangerous look for and send your passwords or financial information.

(This definition based on content at www.webopedia.com)

Rootkit

- * Malware that has obtained root or Administrator access to a system. Full control over a system means that existing software can be modified, including software that could be used to detect or remove it.
- * Removal can be complicated or practically impossible, especially if the rootkit resides in the [kernel](#); reinstallation of the operating system may be needed.
- * The best detection is to shut down the PC, then check its storage by [booting](#) from an alternative trusted medium (e.g. a rescue [CD-ROM](#) or [USB flash drive](#))

Phishing fraud in an e-mail

“The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user’s information. For example, in one scam e-mails supposedly from eBay claims that your account is about to be suspended unless you click on the provided link and update the credit card information that the genuine eBay already has.”

(This definitions is based on content at www.webopedia.com)

Phishing fraud – Phone, text message or the Web

- * Did you get calls like – “This is Rachel from Credit card services ...” Most people realize this scam to collect their credit card and other information to make fraudulent charges.
- * Internet sites can have links that also attempt to get you to provide this info.
- * Scams on social platforms - People share videos or stories with their friends that include links to sketchy sites. This spreads fraud rapidly because people are more likely to click on something posted by a friend.

Browser Hijacking

Your web browser home page is changed to a web site loaded with ads you don't want. You can't easily undo this change or select Internet addresses you do want, just their junk. Repairing the web browser damage requires removal of the invader code and often uninstall / reinstall of the browser.

Most current browsers try to detect and warn you.

Try going back to a safe Windows Restore Point

Ransomware

“Ransomware” locks access to your files until you pay them for an unlock code.

You have to provide funds, usually by credit card, to an international account. Foreign organized crime and terrorist groups are generating these attacks.

Spam – Junk or unsolicited E-mail

- * Most Internet providers use programs at their central post offices that attempt to delete spam and viruses. You may get just a cover note saying a message from “sender name” was infected or spam.
- * Be careful where you leave your e-mail address and create / use a disposable e-mail for product registration.
- * **Don't try to Unsubscribe to Spam** - It just confirms to them your E-mail address is live and their message was opened

SPIM – SPAM and Phishing by Instant Messaging

- * Unsolicited advertising messages with embedded hyperlink link to a Web site
- * The best way to avoid SPIM is to never open or respond to an instant message from a person you do not know.
- * Keep your IM profile and username off public directories.
- * Beware of messages supposedly from Google that ask for your verification code, never provide that to anyone, use it only on the login page of your Google account.

Cookie

A small file placed on your PC when you connect to an Internet web site

- * Good / harmless Cookie – Used by a business to uniquely identify you when connecting to their web site, e.g. Amazon or LLBean welcomes you back and suggests items related to prior purchases or searches.
- * Bad Cookies – Used by adware and Spyware to track you

To Delete **all** cookies on the IE Browser menu Click the Tools bar Safety, and then click Delete browsing history. Select the Cookies and website data check box, and then click Delete.

(Programs like CCleaner and SlimCleaner do this well.)






Be Safe on Wi-Fi

- * At home encrypt your wireless internet connection with WPA2 and a key of more than 8 characters
- * Beware of public free internet wireless “hotspots” They can be OK at a hotel but at coffee shops there are people who setup hotspots to intercept your internet connection and steal your data and attack your device. Cell 3G/4G is safer in public space.
- * When moving around away from home turn Wi-Fi off

What's in a "Security Suite"

- * Antivirus – Blocks & scans for known & suspicious code
- * Instant Message Protection – As above Malware in IM
- * Firewall - Blocks malware from Up or downloading
- * Child filter (Parental Controls) - Block access to content and /or sites unsuitable for children
- * Privacy filter - Provides a warning when it thinks you unintentionally will disclose personal information
- * Anti-spam – Filters and/or flags what it thinks is junk
- * Browser toolbar – Attempts to provide safer searches
- * File Backup - Performs scheduled selected file backup

How safe are websites in a search result?

- * Norton Safe Web is a service from Symantec. Their servers analyze Web sites to see how safe they are. Using the Norton Toolbar installed on your PC, they let you know how safe a particular Web site might be before you view it. (Little green, red or grey tags)
- * **Norton Safe Web Site Ratings:** *display on search page*
- *  = Scanned Safe & Secure for online transactions
- *  = Scanned Safe
- *  = Risks Detected
- *  **Norton** = Site may contain low security risks
- *  **Norton** = Untested

Internet of Things - IoT

- * By 2020 close to 30 Billion connected things will be in use across a wide range of industries. (Gartner Report April 2015)
- * Programmable Logic Controllers (PLCs) are the computerized electronics that control motors, valves, or machines used to monitor and control large scale industrial facilities like power plants, dams, waste processing systems and similar operations.
- * These and home systems are at risk of attack, beyond security & privacy damage and harm can be done.

What is the “Cloud”

- * **“Cloud storage service, file hosting service, online file storage provider, are equivalent terms for an [Internet hosting service](#) specifically designed to store user files. It allows users to upload files that could then be accessed over the internet from a different computer, [tablet](#), [smart phone](#) or other networked device, by the same user or possibly others with the ID and password.”** (From Wikipedia, the free encyclopedia)
- * Some examples are:
 - * Music – iTunes or Amazon (distinct from listening - Pandora)
 - * Photos &/or Video –PhotoBucket or Flickr, Adobe CCloud
 - * File Sharing and Storage – Dropbox, Google Docs, iCloud, Carbonite

What is Safe “In the Cloud”

- * Photos, Videos, Music, school project files, E-Books, calendars, contacts, secure file backups, Pandora, ...
- * Do not put copyright protected content there for sharing with other people
- * Use only secure bank or brokerage accounts for your financial records. (Intuit and other services for tax & personal finance may be OK; I prefer local storage.)
- * Long term trend is that people will utilize storage in central Cloud services with the benefits, costs & risks
- * E-books for Nook, Kindle, iPad, PC have an uncertain future for long term transfer to friends or relatives

Staying safe in the digital environment

Safer Online Shopping

- * Buy from reputable merchants – e.g. Amazon, LLBean
- * Be sure you are in secure (encrypted) mode *https//* and look for the padlock icon near the address bar
- * Use a security “Suite” like Norton with Malware protection or install one like MalwareBytes
- * Keep your browser at current version to best protect
- * Use PayPal which does not disclose your credit card or linked checking account number to the seller
- * Never send credit card # or SSN by unsecure E-mail

Identity Theft Prevention

- * Criminals steal information about you such as your name, address, social security number, date of birth, phone numbers, banking and credit card information. If a thief is able to access this personal information, they can use it to commit fraud in your name. (based on information at Webopedia)
- * http://www.webopedia.com/DidYouKnow/Internet/2006/identity_theft.asp)
- * Protect your personal information. “Ask companies how they use your information, and for online transactions review a Web site's privacy policy. In offline transactions don't provide credit card numbers, financial account numbers, and personal identifying information over the phone unless you know the communication line is secure. Ideally, you should initiate the conversation.” **Be sure you know who you are dealing with.**

Parental Internet Safety, Control & Monitoring

- * **Set up Parental Controls in Windows (7, 8, 10)**
 - * Use separate IDs for the children, Standard Accounts
 - * Use settings within the Security Suite on your PC
- * A package like Net Nanny or WebWatcher provides filtering, blocking and monitoring capabilities. You can choose to block or monitor activity and control the time that children spend online. It also lets you control games, instant messaging and e-mail.
- * Apple has some restrictions for iPads/iPhones and you can add a tool like Net Nanny for iOS, Intego's [Family Protector](#)
- * These can safeguard unintentional risks & “mischief”

Organize & Secure Your IDs & Passwords

- * Do not use the same ID / password on multiple sites or services. So how can you keep track of these?
- * Simplest – Use a password protected Word document with a table of the Purpose/Organization, ID, Password, URL (web address)
- * Many Security Suites include secure storage for IDs
- * iCloud Keychain keeps your Safari website user names, passwords and credit card information
- * RoboForm Everywhere is subscription-based and synchronizes password management and form filling on multiple computers (You have to trust them).

Facebook – Deny “Public” Access

- * Select the padlock icon in the blue navigation bar to activate the Privacy Shortcuts dropdown menu
- * You can see who can view your posts, contact you, send you messages. **Do not set this to Public!**
- * At the menu bottom select See More Settings to limit who can look you up by phone number, email address
- * Limit what you put in your Profile information & Restrict access – Click on the Update Info button. This will allow you to set privacy settings item by item.
- * Your Facebook name & Profile photo are public to all

Facebook Mistakes to Avoid

From June 2010 Consumer Reports Magazine.

- * **Using a weak password** - No simple names or words
- * **Leaving your full birth date in your profile**
- * **Not using privacy controls to limit access**
- * **Posting your child's name in a caption (beware tags)**
- * **Mentioning that you'll be away from home**
- * **Letting search engines find you** - Be sure the box for public search results isn't checked
- * **Permitting youngsters to use Facebook unsupervised**
- * **(See consumerreports.org Facebook & your privacy)**

Protecting your privacy on social media

Facebook

- * **Disclose as little as possible** – Don't think that only your friends will be able to see what you post.
- * **Invest the time to read and understand what Facebook has posted on their Safety pages**
 - * <http://www.facebook.com/safety>
- * **How to Protect Yourself from Facebook Scams/Spam**
 - * This link is to pages you also should read and understand
 - * http://www.webopedia.com/DidYouKnow/Internet/protect_from_facebook_scams.html
 - * If you don't understand the precautions described be a cautious “reader” but don't post or contribute

Protecting your privacy on social media

Twitter

- * **Twitter also has Safety & Security Pages to read**
- * <https://support.twitter.com/articles/76036#>
- * Be careful who you follow or friend. Do you really know them? Cybercriminals use their profiles to spread spam and malware.
- * Be careful about what Twitter or Facebook apps you allow to access your profile information.
- * Twitter has searchable databases but I couldn't find an anti scam app

Mobile Phone & Tablet Safety

- * Enable & use phone passwords
- * Download apps only from official app stores like iTunes, Google Play or Amazon. (Safer but not 100%)
- * Require a strong password for purchases
- * Set-up built-in lost & found features & allow erase all if stolen
- * **Never share personal information with strangers**
- * Children should tell their parents if they receive inappropriate, upsetting or threatening messages
- * Apple claims an Antivirus is not needed for IOS (built-in), Android devices should have one installed (e.g. AVAST, Norton Mobile, 360 Security, ...). See reviews at: <https://www.av-test.org/en/antivirus/mobile-devices/>

Restrict what information Apps can access

- * Review the terms and privacy policy for each third-party app to understand how it uses the data it's requesting. You can turn off each app's access to a category of information (Contacts, Calendar, location)
- * For iOS Limit / Restrict Ad Tracking - Go to Settings > Privacy > Advertising. **Turn on Limit Ad Tracking** to prevent apps from sending you targeted Ads.

Protecting your privacy on the Internet

- * Use *InPrivate Browsing* to prevent Internet Explorer from storing data about your browsing session. This includes cookies, temporary Internet files, history, and other data. Toolbars and extensions are disabled by default. It is effective from preventing other people who have access to your computer from knowing what sites you have browsed. This does not hide your IP address, so the websites that you visit can still log your IP address (so stay off risky “adult” sites).
- * It does not prevent any network administrators from discovering which sites you have connected to, so don't go on bad websites at work/school (firewall rules and other safeguards may block these those locations).

Protecting your privacy on the Internet

- * Not Saved - History, Searches, Cookies, Temporary Files
- * Internet Explorer has InPrivate Browsing
- * Firefox calls it Private Browsing mode
- * Google Chrome calls it incognito mode
- * This is safer when you use a public computer and want to order something online or access you bank accounts for a transfer.
- * A privacy software package is needed to make you anonymous on the worldwide web. When privacy software conceals your Internet Protocol (IP) address and encrypts your connections, you are “cloaked”.

Software Licenses – It's Not “Their Fault”

- * **DISCLAIMER OF WARRANTY.** THE PRODUCT IS PROVIDED "**AS IS**" WITH ALL FAULTS. TO THE EXTENT PERMITTED BY LAW, *Software Vendor* HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED, ... THAT THE PRODUCT IS FREE OF DEFECTS, MERCHANTABILITY, FIT FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. **YOU BEAR ENTIRE RISK** AS TO SELECTING THE PRODUCT FOR YOUR PURPOSES AND AS TO THE QUALITY AND PERFORMANCE OF THE PRODUCT.
- * WILL NOT BE LIABLE FOR ANY INDIRECT ... DAMAGES ... LOST PROFITS, LOSS OF DATA, AND COMPUTER FAILURE OR MALFUNCTION, ...

Research Before you Download/Install

- * Make sure the download is from a “safe” source
- * The update function within a program is usually safe.
- * Check file properties to verify the digital signature
- * “Google” the APP to look for complaints about the program or its publisher, read the reviews. If you find significant problems don’t install it.
- * Be sure to scan any downloaded files for viruses and spyware before installing.
- * Read the iTunes reviews before updating an App. Often the new version has serious flaws, crashes or freezes for many people and you will see this in the reviews. Wait for a version that gets good reviews (or switch to another application if necessary).

What you think is safe may not be

- * Usually apps at Apple & Google Play are safe but ...
- * “**InstaAgent**, an app that claimed to tell you who viewed your Instagram account, stole passwords and may have hijacked a half million Instagram accounts before Google and Apple axed the malicious app.”
- * The app also used the credentials to hijack accounts and post unauthorized photos to Instagram profiles.
- * Uninstall the app and change your Instagram password immediately
- * From Computerworld | Nov 11, 2015

Windows System Restore Point

- * **Create a System Restore point before installing any software so that you can undo the changes**
 - Control Panel – System – System Protection –
Click the Create a System Restore Point button
- * Windows 7 and 10 automatically do this before installing a Windows patch / update.
- * You can restore to any of the saved points

Phil's Top Ten List

Prevention is the Best Protection

- * The top ten things you should do, with #1 being the highest priority.
- * I encourage you to use these as a checklist and see what you already are doing and what you need to do ASAP.
- * The effort to take precautions is very small compared to disruption impacts.
- * There are more attacks to Windows PCs than Macs or iOS devices so these points emphasize PC safeguards.

1. Make Backups regularly

How often should you make backups of your work / data files?

- * What would be the impact / cost of the loss of data be?
- * How much work / data do you want to risk loosing? (Photos, music, e-books, ...)
- * What is the effort & cost for backup? With external USB drives it's easy & inexpensive.
- * Based on your answers, you decide.

1.a Backup best practices

- * I recommend daily backup of work/data files or continuous to an external drive.
- * Full “Image” backups to an external drive.
- * Create a bootable recovery CD; that would allow a full restore of the Image backup.
- * Consider one backup set off-site perhaps internet hosted “cloud” backup. Multiple versions, carefully stored and labeled are best.

2. Use a Security Suite / Antivirus on your PC and keep it up to date

- * Security Suites combine protection for Virus/Firewall/Spyware-Malware
- * Updates should be automatic but verify that the definition files dates are current
- * Run automatic scans at least once a week (preferably daily background / idle time scans)
- * NEVER install more than one Antivirus

3. Keep your antivirus completely up to date

- * Be sure your PC has checked for / received antivirus updates before opening your e-mail and that attachments are scanned before opening them.
- * Definitions more than a day old are not safe (most do multiple updates daily).

4. Keep Windows & Utilities up to date

Apply the Microsoft automatic security and reliability patches (second Tuesday of every month)

For folks with high speed Internet connections getting critical patches will be easy if Windows on your PC is set for automatic download of the updates.

Adobe Reader, Adobe Flash, Java must be kept current because the patches close “backdoors” that allow Malware to control your PC or steal information.

5. Use a Firewall program

- * Security Suites that include this function will turn off the Windows firewall. A good firewall should warn you if something infects your PC and tries to communicate out to the Malware source.

6. Make your PC harder to attack

1. Use secure passwords and change them regularly. Secure passwords are at least 8 characters long, have a mix of upper and lower case letters, numbers, special characters (@#!\$.) and don't use your name or other words linked to you.
2. At night turn off your PC (not sleep mode) – That's as safe as it gets.

Password guidance

- * Avoid using simple passwords based on dictionary words
- * Never use the same password on multiple sites or services
- * Use a password protected document or electronic “vault” to store your IDs/pswds
- * Never click on ‘reset password’ requests in emails — instead go directly to the service

7. Use Pop-up blocking

- * Pop-ups are not just annoying, often they're a source of dangerous invaders.
- * Both Internet security suites and the browser settings can be used to block them. For Internet Explorer 11 choose Tools – Pop-up Blocker
- * You can also choose to allow pop-ups for sites that use them legitimately, e.g. on-line shopping to provide more specifics or a picture of an item
- * AdBlock Plus for Firefox is an “Ad-on” extension
- * Safari > Preferences, and then click Security. Turn on “Block pop-up windows.”
- * Google Chrome blocks pop-ups automatically

8. Don't click on links in e-mail

- * **Beware of Attachments and Links** these are prime methods for connecting you to a fraudulent web site. It is safer to leave e-mail and use your known browser favorites / bookmarks to log on to a business or bank. For example, E-Bay and PayPal warn about phony imposter sites that use this phishing trick.
- * Be sure attachments are scanned before opening them. Photos or safe files should scan as OK.
- * .ZIP files are dangerous and could contain malware

9. Browser Settings

- * **Be sure to enable safe web browsing features**
- * Set your browser to block "Third-Party Cookies" These come not from the web site you're on like Amazon or Yahoo, but from some other possibly malicious web site, often in a pop-up or banner ad. TOOLS – Internet Options – Privacy - Advanced
- * For Microsoft Internet Explorer, change the Security settings to Medium – High This will not download Unsigned Active X and prompt you to recognize and allow downloads

10.a Text e-mail is safer than HTML

Some may consider this paranoid but you can setup for just “dull” text without pictures. It will be less likely you’ll accidentally click on an icon / link that starts a dangerous program attachment or links to a nasty web site.

How to - In Outlook this is done by selecting
TOOLS – Options – Preferences Tab – e-mail
Options button and checking the
 Read all messages in plain text

This won’t stop Spam or junk e-mail so if you are getting lots of this change your address.

10.b Turn off E-mail preview

- * E-mail that is auto scanned before you view should be OK but it can be dangerous to auto display e-mail messages because it can auto start a potentially dangerous virus / spyware loaded in the message.
- * How to - In Outlook this is done by selecting VIEW – Auto Preview – Click turns On or OFF and VIEW – Reading Pane – Off.
- * This allows you to read the Subject Line and the Sender ID / From without opening or activating the message contents. (Outlook attempts to automatically block what it considers as dangerous attachments.) I prefer Mozilla Thunderbird E-mail.

Prevention is the Best Protection

The Technology Haiku
Yesterday it worked.
Today it is not working.
Technology is like that.

Technology is flawed, the internet is both useful & dangerous

"Let's be careful out there."