Computer Security

Discussion September 29, 2016

- Everyone will tell you a good Malware or Internet Security program is essential.
- While this is true, because of the current nature of threats
  - As essential as a good antimalware software, is a good backup software.
  - The BEST Security protection is actually a GOOD BACKUP PROGRAM.
- No matter what antivirus or Internet Security software you use,
  - NOTHING will protect you 100% from malware.
    - Malware creators now depend on us doing something foolish, and bypassing the Security protection.
    - And **Zero-day attacks** can never be stopped entirely.
  - The wrong click or following the wrong link, and WHAM!
    - You are infected.
- Regimented and/or Scheduled Backup protects from:
  - Malware
  - Ransomware
    - Particularly Encryption Ransomware
  - User Error
    - Accidentally overwriting files
    - Corruption of Windows by critical file deletion
  - Physical damage
  - Device failure
  - Change of hardware
- Free backup programs
  - AOMEI: http://www.backup-utility.com/free-backup-software.html
  - Easeus: http://www.easeus.com/backup-software/personal.html
  - Comodo: https://www.comodo.com/home/backup-online-storage/comodo-backup.php#tab-features
- Backups provide disaster recovery.
- Backups reduce fear of disaster.
- Most people NEVER backup until they have lost everything at least once.
- Data Recovery services are very expensive, and not necessarily successful.

Computer Security

Discussion September 29, 2016

Malware Protection

- Most free or retail antiviral software will protect from most **known** threats.
  - These free programs do not usually offer firewall protection.
- Retail antiviral/Malware providers, or "pro" versions of free programs, offer firewall protection as well as antivirus.
  - Firewall software protects malware from sending out critical data by notifying you when an unknown program attempts to use the Internet.
    - It asks if it is OK for the program to use the Internet.
    - Blocks the Internet access until you respond.
  - Antiviral protection only prevents malware programs from entering the computer, or getting installed:
    - If we do not give it permission.
- Windows does provide a rudimentary incoming firewall.
  - But no outgoing firewall.
- A physical **Router** (for wireless signal as example) also provides additional incoming firewall protection.
- Windows 8 and 10 also provides basic antiviral protection.
  - But because of the nature, it is the most likely to be targeted for vulnerabilities.
  - Thus it is equivalent to most free programs.
- Window 7 and earlier can download a free version of the same Microsoft malware protection, called Microsoft Security Essentials.
- Don't confuse this with Windows Essentials.
  - Side Note: Microsoft will end support for Windows Essentials 2012 in January next year (2017).
- Today it is a good idea to have both an installed and constantly monitoring antivirus.
  - But also a second Malware scanning software to run periodically.

The way most protection software works

- Two components
  - An active always watching "auto-protect" component, and if provided, firewall protection.
  - Scheduled periodic scans looking for threats
- It is the Auto-protect and firewall components which can potentially interrupt or prevent proper installation or performance of software.
- Scans are both scheduled and manually requested.
  - Three or four choices for scanning for threats.
    - **Quick Scan** scans the most likely affected files and folders.
    - **Full scan** scans all files, folders, registry, and startup programs for malicious activity
    - Directed or **Custom scan** scans only the files or folders you wish.
    - **Independent scan** of a select file or folder
      - Such as a downloaded file or program BEFORE installation.
      - This can usually be initiated with a right-click on the file or folder, and choosing "Scan with" and choosing your antiviral software.
      - Or choosing to scan the file from a right-click Program named menu, or by opening the program itself from the Notification area.
  - How does it scan?
    - All antiviral or malware programs scan, looking for "**Signatures**".
      - Signatures are recognized aspects or traits, (such as filename, location, registry change, etc.) for **known** malware.
      - These Signatures are essentially what is contained in the **virus definitions** that are updated at least daily.
      - For the threat to be recognized, the threat must have previously been discovered by the company, and definitions created.
    - However, "**Zero Day**" threats are new, and have no such "definitions".
    - Today, new threats are appearing constantly at a feverish rate.
      - So much so, normal scanning techniques can no longer keep up.
      - To attempt to thwart such attacks, antiviral software performs **Heuristic** scans.
      - **Heuristic** scans are scans that look for malicious types of behavior, rather than looking for known files or folders.

Computer Security

Discussion September 29, 2016

Types of threats

- **Scams** are everywhere!
  - Email, a website, or a pop-up congratulates you for a trip you won; warns the IRS is hunting you; or informs you, you are about to be arrested; your computer is throwing out errors.
  - They direct you to websites, or phone numbers to call to remedy the situation.
  - Computer help scams are common
  - Any time you google (search) for help phone numbers, you must be careful to verify they are legitimate. Be skeptical.
  - Is this number truly affiliated with the service I am requesting help for?
    - Expect to pay for help provided to assist with free software or services.
    - But confirm it is actually the desired entity providing support (help).
    - They will all claim they are affiliated.
    - Because sites like Google, Yahoo, Gmail, etc. are free services, they do not offer technical support by phone readily.
  - Most phone numbers you retrieve from a search are not direct support, but instead private enterprises claiming to provide support.
    - And they do for a fee.
    - Problem is you can't be sure whether you are contacting a valid help service or a merely a crook.
    - And sometimes there is little difference.
    - These services like to "pad the bill" and offer unnecessary services.
  - Be wary of letting a stranger connect remotely to your computer.
    - Unless you have directly connected a legitimate manufacturer's support staff.
    - They may install Trojan or unwanted software either designed to create problems, or require a fee to remove (uninstall).
  - NEVER let anyone from a "cold call" take control of your computer.
  - Be hesitant to provide any passwords to your tech support. Put them in yourself.
  - Refer to Microsoft.com and go to Support, then Safety and Security Center (link towards the bottom) for more information.

- **Ransomware**
  - Video about Ransomware: http://www.symantec.com/tv/products/details.jsp?vid=1954285164001
  - Early Ransomware merely locked up your computer, requesting money.
  - Newer varieties of ransomware encrypt your files.
  - Don't pay the ransom!
    - You cannot be sure the criminals will provide access to your files or computer.
  - You can regain access to your computer merely by using the proper tools to remove the virus.
  - However, once your files are encrypted, you cannot unencrypt them.
    - You will need to restore them from a backup.
    - You CAN remove the malware, but that doesn't decrypt the files.
    - Kaspersky does have tools to try, but you must get lucky.
      - https://noransom.kaspersky.com/
  - Understand malware which encrypts your files can also encrypt your backup files **if your backup drive is connected while infected**.
    - Authorities recommend NOT KEEPING your backup drive connected.
    - If you do daily backups and don't want to plug and unplug:
      - **At least have a one regular backup on a device which is connected only during backup.**
      - Or use Cloud backup for that purpose.
  - If you discover you are infected:
    - **Immediately shut the computer down** with a hard shutdown (hold down the power switch until it goes off).
    - Immediately unplug your backup drive.
      - It takes time for the malware to encrypt all the files.
      - Your computer works continuously as it encrypts.
      - You may have saved some of the backup.
      - This may prevent damage to some files as well.
    - Immediately disconnect from the network
    - Restart in Safe Mode. This program is then often removed by standard scanners (Malwarebytes, etc.), or by registry tweaks
      - But disinfection will not restore encrypted files.
      - Must restore encrypted files from backups.
  - Ransomware or other infections may not let you enter Windows to perform standard scans.
    - Try using System Restore from a Safe Mode with Command prompt
      - Then doing complete scans to remove any infected components.
    - Removing the infection may require a pre-boot scan (a scan prior to Windows loading) using HitmanPro Kick, or Kaspersky Rescue disk, or similar program you boot to from either CD or USB.

- This will require another computer to download necessary files.

How we acquire these threat infections? Malware doesn't just happen.

- Essentially all antivirus and firewall products, free or retail, protect the computer satisfactorily from the classically encountered malware.
- The real problem today is our own online activity and habits.
  - We are the weak link in the protection!
  - We use all those links our friends send us, often without thought, or in a hurry.
  - We often surf from website to website, increasing the chances of "Drive by downloads".
    - A malicious site set up to invoke some browser security vulnerability (flaw) begins a download either automatically, or by an innocent click of the mouse, or accidental tap of the touchscreen.
- If you remember nothing else but these few practices about keeping your computer secure, whether it be a **text message**, an **email**, a **social** networking communication (Facebook, Twitter), or an unverified **flash drive** file:
  - Never click on an email or a website link without knowing where it is going!
    - We receive links to, or encounter links to other websites constantly.
  - Links can be masked. The text does not always depict the real destination.
  - Use the lower left side of the status bar to see where a link is actually directed (not where it is labeled CLAIMS it is going to.
    - This function is present on both the browser AND the email.
    - But you must be sure the Status bar has been turned on.
    - For example, don't trust "tinyurl… , as it hides the real destination.
  - Pay attention to the **primary domain** (the dot com or dot org, etc.)
    - Malware referred to as **Scareware** tries to make you think you need a scan, a false program or update, the phony offered protection.
  - Only access directly any financially and personal information-related sites.
  - Do not go through email links, or website links.
  - Never open an attachment which is unexpected, or has not been personally acknowledged or identified.
    - If unsure, **reply** to the sender and confirm the sender intended to send it.
    - Similarly, never SEND an attachment without accompanying it with a clearly personal acknowledgement. Don't trust a "generic" comment or just a friend's name.
  - Never provide personal security information to an email, unsecured website, or message, any "cold" request of any kind. Go directly to the site.
  - Social Media sites infect by clicking a link or accepting files.

- We all get in a hurry, or become complacent, and click without thinking.
    - It may even be a click to close the unwanted and unsolicited item.
- Unless having a specific problem with your computer, no unrecognizable update is ever needed immediately.
    - It will show up again if truly needed.
        - Although so may malware requests.
- Device Protection also involves keeping the computer, Windows operating system, and its Apps and programs up-to-date.
        - Updates offered by confirmed suppliers and providers frequently are plugging vulnerabilities discover BEFORE they are used for attack.
- Updates you always want:
    - Device Manufacturer supplied or advised, such as same version OS updates
    - Windows (Automatic) Updates
    - Installed program or App updates
    - Most of the above are providing to stop security vulnerabilities.
- Note that New OS versions are often providing new features, not security fixes.
    - The new version MAY provide increased security, but can sometimes introduce new and yet undiscovered or "fixed" vulnerability (security flaws).

Computer Security

Discussion September 29, 2016

How can you suspect you're infected?

- Hard drive is quite active even when you aren't.
    - Backups, antivirus scheduled scans, and scheduled computer maintenance can be performing legitimate tasks in the background.
    - But malware also can be performing malicious tasks in the background.
    - Task Manager can be a help determining which it is.
        - Access Task Manager with a right-click on the taskbar (not over an icon).
- Unexplained excessive data usage (notices from carriers you pay by the GB)
- Receiving a lot of returned email
    - This can be simply a matter of cloned email address, but warrants a scan.
- Sluggish computer performance
    - Internet is taking longer than usual
    - Programs are opening slowly, or not at all.
    - Again, Task Manager's performance tab can be helpful.
- Problems with repeated computer restarts
    - Repeated Crashes, or failures to start
- Repeated messages of infection
    - Can be warnings from your antivirus.
    - Or can be fictitious warnings from acquired malware infections.
        - Or unwanted legitimate programs installed alongside something else
            - Adobe, Java, and free antivirus installations are common culprits.
            - Watch for the checks to remove during legit installations
        - If you have unwanted legitimate programs, remove (Uninstall) them.
- Unable to open Task Manager, msconfig (Configuration Utility), Windows Update, Computer manufacturer's site, or any security source site.
    - Suggests something doesn't want you to be able to scan or investigate.

- What to do if you suspect a malware infection, (or just want to rule one out)
    - Download and install a free malware scanner such as
        - Malwarebytes Anti-Malware (malwarebytes.org)
        - Super Antispyware (superantispyware.com)
        - Do not use the installed antivirus software yet, as it may already be “ignoring” the infection.
    - Run the scan, Quickscan is usually sufficient unless it finds items.
        - If so, after removing or quarantining found items, run a full scan.
        - Repeat scanning until it comes back clean.
        - Malwarebytes often finds PUP… something.
            - These are not serious malware.
            - The PUP stands for Potentially Unwanted Programs
            - Remove them or leave them, depending on whether it is a program you use or not.
            - I personally first try to uninstall them from Programs and Features, before just removing the unwanted files, so the entire folder is removed.
        - Super Antispyware finds tracking cookies as well, again usually not serious threats.
    - **If your initial scan (Malwarebytes or Super Antispyware) scan finds nothing, run your installed antivirus.**
        - **If it also finds nothing, you are not likely infected.**
    - If the malware software finds items, Run the malware scan until it finds no unwanted entries.
        - Be particularly interested in removing Registry entries.
    - Now run a scan using your existing (installed) antivirus software.
        - The icon to initiate this is usually in the Notification area.
        - If it now finds infected files, let it remove or quarantine them.
        - Run it again repeatedly also until it no longer finds items.