Defending Windows with Antivirus Software, December 7, 2017

With all the dangers lurking on the Internet, keeping your computer safe and clean is an important challenge. In this 90-minute session we will discuss strategies and technologies for keeping your computer safe in a networked world, with the emphasis on antivirus software.

- Malware
    - The term malware is a contraction of malicious software. Put simply, malware is any piece of software that was written with the intent of doing harm to your data or device.
      https://www.avg.com/en/signal/what-is-malware
    - Brief history
      https://en.wikipedia.org/wiki/Antivirus_software
        - The roots of the computer virus date back as early as 1949, when the Hungarian scientist John von Neumann published the *"Theory of self-reproducing automata."*
        - First computer virus ("Creeper") appeared in 1971
        - Term first coined in 1983.
        - Before the Internet, computer viruses were typically spread by infected floppy disks.
        - The late 80's and early 90's saw the birth of antivirus industry
    - Common Malware Types
      https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101
        - Viruses, Worms, Trojan horses, Ransomware, Spyware, Adware, Rootkits, etc...
    - Malware symptoms
        - While the different types of malware differ greatly in how they spread and infect computers, they all can produce similar symptoms. Computers that are infected with malware can exhibit any of the following symptoms:
            - Increased CPU usage
            - Slow computer or web browser speeds
            - Problems connecting to networks
            - Freezing or crashing
            - Modified or deleted files
            - Appearance of strange files, programs, or desktop icons
            - Programs running, turning off, or re-configuring themselves (malware will often reconfigure or turn off antivirus and firewall programs)
            - Strange computer behavior
            - Emails/messages being sent automatically and without user’s knowledge (a friend receives a strange email from you that you did not

send)

        - 14 Warning Signs that Your Computer is Malware-Infected
          https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/
    - Five Myths About Malware You Need to Know
      http://www.zonealarm.com/blog/2014/03/five-myths-about-malware-you-need-to-know/
        - I will know when my computer is infected
        - I don’t go to shady sites, so I will be fine
        - Macs [Android OS] don’t get malware
        - I don’t have anything worth stealing on my computer
        - I can just wipe the computer and restore from backup
- How does a computer get "infected?"
    - Accepting prompts without reading them
    - Downloading infected software
    - Opening e-mail attachments
    - Inserting or connecting an infected disk, disc, or drive
    - Visiting unknown links
    - Unpatched software - not running the latest updates
    - Pirating software, music, or movies
    - Online Ads (malvertising)
      protect your browser with an Ad-blocking extension
    - Social media
    - Additional References:
        - How does a computer get infected with a virus or spyware?
          https://www.computerhope.com/issues/ch001045.htm
        - 5 Hidden Ways Viruses Infect Your Computer
          http://www.businessnewsdaily.com/6365-virus-infections.html
        - How You Can Be Infected via Your Browser and How to Protect Yourself
          http://www.howtogeek.com/138667/how-you-can-be-infected-via-your-browser-and-how-to-protect-yourself/
        - From where did my PC get infected
          https://malwaretips.com/blogs/from-where-did-my-pc-got-infected/
        - Ransomware that’s 100% pure JavaScript, no download required
          https://nakedsecurity.sophos.com/2016/06/20/ransomware-thats-100-pure-javascript-no-download-required/
- How does Antivirus software work?
    - Virus definitions and heuristics
        - Traditional antivirus software relies heavily upon signatures to identify malware. These virus signatures or "fingerprints" are added to the software's "dictionary." Every file access is matched against the dictionary to see if it matches one of the signatures. Although the signature-based approach can effectively contain malware outbreaks, malware authors have tried to stay a step ahead of such software by writing "oligomorphic", "polymorphic" and, more recently, "metamorphic" viruses, which encrypt parts of themselves or otherwise modify themselves as a method of disguise, so as to not match virus signatures in the dictionary.

https://en.wikipedia.org/wiki/Antivirus_software

        - Viruses mutate in different strains called variants. While it may be advantageous to identify a specific virus, it can be quicker to detect a virus family through a generic signature or through an inexact match to an existing signature. Virus researchers find common areas that all viruses in a family share uniquely and can thus create a single generic signature. This is heuristic detection.
          https://en.wikipedia.org/wiki/Antivirus_software
    - On-Access Scanning vs On-Demand system scanning
    - Additional References:
        - How Antivirus Software Works (How-To Geek)
          http://www.howtogeek.com/125650/htg-explains-how-antivirus-software-works/
        - How Antivirus works (Comodo)
          https://antivirus.comodo.com/how-antivirus-software-works.php
- Microsoft Windows security and antivirus solutions
    - Windows Defender Security Intelligence (**Microsoft's "security" portal**)
      https://www.microsoft.com/en-us/wdsi
    - Microsoft antivirus and threat protection solutions
      https://www.microsoft.com/en-us/wdsi/products
        - Windows Defender (antivirus software for Windows 8 and Windows 10)
          https://support.microsoft.com/en-us/help/17187/windows-10-protect-your-pc
            - Windows Defender, built into Win8 and Win10, is completely different from the identically-named “Windows Defender” in Vista and Win7. The former is a relatively good front-line anti-malware application; the latter is a much simpler tool that should never be relied on as your primary defense against malware.
            - Windows Defender Limited Periodic Scanning (available in Win 10 Anniversary update)
              https://blogs.technet.microsoft.com/mmpc/2016/05/26/limited-periodic-scanning-in-windows-10-to-provide-additional-malware-protection/
            - Windows Defender Exploit Guard: Reduce the attack surface against next-generation malware
              https://blogs.technet.microsoft.com/mmpc/2017/10/23/windows-defender-exploit-guard-reduce-the-attack-surface-against-next-generation-malware/
                - Stopping ransomware where it counts: Protecting your data with Controlled folder access
                  https://blogs.technet.microsoft.com/mmpc/2017/10/23/stopping-ransomware-where-it-counts-protecting-your-data-with-controlled-folder-access/
            - Configure Windows Defender Security Center in Windows 10
              https://www.winhelp.us/configure-windows-defender-security-center.html
            - What's new in Windows Defender for Windows 10 Anniversary Update (Aug. 2016)
              http://www.windowscentral.com/whats-new-windows-defender-windows-10-anniversary-update
            - New Windows Defender Security Center features in Windows 10 Fall Creators Update (Sep. 2017)
              https://www.windowscentral.com/whats-new-windows-defender-security-center-

windows-10-fall-creators-update
    - MS Security Essentials (antivirus software for Windows Vista and Windows 7) https://www.microsoft.com/en-us/safety/pc-security/microsoft-security-essentials.aspx
  - Windows Threat Protection https://docs.microsoft.com/en-us/windows/threat-protection/
- Third Party Software
  - Consumer antivirus software providers for Windows https://support.microsoft.com/en-us/help/18900/consumer-antivirus-software-providers-for-windows
  - Traditional antivirus software, stand-alone or as part of a security suite
  - Next-Generation Antivirus (NGAV)
    - Doesn't work with traditional AV signatures.
    - Specializes in trying to stop unknown exploits
    - Examples: Barkly, Carbon Black, Cylance, Sentinel One, Traps
    - Currently focused on the enterprise not on the consumer market
    - "Next-Gen" Antivirus Vs. Antivirus: Is there a difference http://www.intelligonetworks.com/blog/next-gen-av-vs-av
  - Anti-Exploit software
    - Malwarebyes Antiexploit beta https://www.malwarebytes.com/antiexploit/
      - Malwarebytes Anti-Exploit is now part of the premium version of Malwarebytes 3.0
      - Malwarebytes will continue to test cutting-edge anti-exploit technology in a free beta version of Malwarebytes Anti-Exploit.
    - Microsoft's Enhanced Mitigation Experience Toolkit (EMET) (end of life July 31, 2018) https://support.microsoft.com/en-us/help/2458544/the-enhanced-mitigation-experience-toolkit
      - a utility that helps prevent vulnerabilities in software from being successfully exploited. EMET achieves this goal by using security mitigation technologies. These technologies function as special protections and obstacles that an exploit author must defeat to exploit software vulnerabilities. These security mitigation technologies do not guarantee that vulnerabilities cannot be exploited. However, they work to make exploitation as difficult as possible to perform. https://support.microsoft.com/en-us/kb/2458544
      - Moving beyond EMET https://blogs.technet.microsoft.com/srd/2016/11/03/beyond-emet/
      - CERT warning: Windows 10 is less secure than Windows 7 with EMET https://betanews.com/2016/11/24/windows-10-security-emet/
    - Use an Anti-Exploit Program to Help Protect Your PC From Zero-Day Attacks http://www.howtogeek.com/223228/use-an-anti-exploit-program-to-help-protect-your-pc-from-zero-day-attacks/

    - [Noteable] Anti-Malware software
        - MalwareBytes
          https://www.malwarebytes.com/
        - SpyBot Search & Destroy
          https://www.safer-networking.org/
        - Zemana Anti-Malware
          https://www.zemana.com/
        - RansomeFree
          https://ransomfree.cybereason.com/
    - IBM Security Trusteer Rapport (to protect your online banking)
      https://www.trusteer.com/ProtectYourMoney

        - Rapport is provided to you to help protect your online banking sessions and other non-enterprise related websites, for example, e-commerce and online email. Rapport is advanced security software that helps to protect your online banking communication from being stolen by criminals. Rapport is highly recommended and offered by your bank as an extra layer of security to any antivirus or security software you already use. By creating a tunnel for safe communication with your bank's website, Rapport helps to block malicious attempts to steal money from your account.
          https://www.ibm.com/support/knowledgecenter/SS7MJT_1804/ug/c_What_is_Rapport_URGuide.html
- On-demand antivirus scanners
    - Microsoft Safety Scanner
      https://www.microsoft.com/security/scanner/en-us/default.aspx
    - 22 Free Stand-Alone/Portable Antivirus Scanners
      https://www.geckoandfly.com/10007/complete-list-of-9-free-standalone-antivirus-scanner/
    - VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.
      https://www.virustotal.com/
- Malware Removal
    - **Depending on the severity of the infection, the safest bet might be to reinstall Windows from scratch!**
    - For simple PUPs (potentially unwanted programs) I use the free on-demand version of MalewareBytes
    - Emsisoft Emergency kit (Programs that can be used without installation to scan and clean infected computers)
      https://www.emsisoft.com/en/software/eek/
    - Windows Defender Offline (WDO)
      https://support.microsoft.com/en-us/help/17466/windows-defender-offline-help-protect-my-pc
        - Runs before OS loads. When you launch Defender Offline, it closes your current Windows session and starts a limited version of the OS. Once the scan is done, your system reboots and returns to normal operation.
        - Built into Windows 10 version 1703 (Anniversary Update); free download for older versions of Windows
    - 14 Free Bootable Antivirus Tools [rescue disks]
      https://www.lifewire.com/free-bootable-antivirus-tools-2625785

    - BleepingComputer Virus, Spyware & Malware Removal Guides
      http://www.bleepingcomputer.com/virus-removal/
- How effective is Antivirus software?
    - Detection Rates and False Positives
        - Bad News: Your Antivirus Detection Rates Have Dramatically Declined in 12 Months. January, 15, 2017
          https://blog.knowbe4.com/bad-news-your-antivirus-detection-rates-have-dramatically-declined-in-12-months
        - False Positives
          A "false positive" or "false alarm" is when antivirus software identifies a non-malicious file as malware.
    - Comparing Antivirus software
        - AV Test
          https://www.av-test.org/en/antivirus/home-windows/windows-10/
        - AV Comparatives: Independent Tests of Antivirus Software
          http://www.av-comparatives.org/
    - Industry Recommendations
        - The Best Antivirus Protection of 2017 (PC Mag)
          http://www.pcmag.com/article2/0,2817,2372364,00.asp
        - The Best Free Antivirus Protection of 2017 (PC Mag)
          http://www.pcmag.com/article2/0,2817,2388652,00.asp
        - The Best Malware Removal and Protection Software of 2017 (PC Mag)
          https://www.pcmag.com/roundup/354226/the-best-malware-removal-and-protection-tools
        - The Best Free Antivirus Protection of 2017 (Tech Radar)
          http://www.techradar.com/news/software/applications/best-free-antivirus-1321277
        - The Best Free Anti-Malware Software of 2017 (Tech Radar)
          http://www.techradar.com/news/software/applications/best-free-anti-spyware-and-anti-malware-software-1321656
        - Best Antivirus Software and Apps 2017 (Tom's Guide)
          http://www.tomsguide.com/us/best-antivirus,review-2588.html
        - What's the Best Antivirus for Windows 10?
          http://www.howtogeek.com/225385/what%E2%80%99s-the-best-antivirus-for-windows-10-is-windows-defender-good-enough/
    - Additional References:
        - Is antivirus software a waste of money?
          http://www.wired.com/2012/03/antivirus/
        - It might be time to stop using antivirus
          https://arstechnica.com/information-technology/2017/01/antivirus-is-bad/
        - Disable Your Antivirus Software (Except Microsoft's), January 26, 2017
          http://robert.ocallahan.org/2017/01/disable-your-antivirus-software-except.html
        - Google Chrome engineer says Windows Defender "the only well behaved AV"
          https://www.onmsft.com/news/google-chrome-engineer-says-windows-defender-the-only-well-behaved-av
        - You can't depend on Antivirus software anymore
          http://www.slate.com/articles/technology/future_tense/2017/02/why_you_can_t_depend_on_antivirus_software_anymore.html

- My advice and non-recommendations*:
  *I won't give professional recommendations as to what specific software you should use, but I will tell you what I do.
  - Backup your data!
    Your insurance policy against infection.
  - Don't install two antivirus competing antivirus products. They usually don't "play" well together.
    But you can install two or more complementary security products.
  - Educate yourself and stay informed
    The human element is usually the weakest link in the security chain.
    - Naked Security (blog)
      https://nakedsecurity.sophos.com/
    - Graham Cluley (newsletter, blog)
      https://www.grahamcluley.com/
    - Krebs on Security (newsletter, blog)
      http://krebsonsecurity.com/
    - Knowbe4 (Free tools, newsletter, awareness training)
      https://www.knowbe4.com/
  - Use multiple layers of security
    - "Security is all about layers, and not depending on any one technology or approach to detect or save you from the latest threats. The most important layer in that security defense? You! Most threats succeed because they take advantage of human weaknesses (laziness, apathy, ignorance, etc.), and less because of their sophistication." Brian Krebs
      http://krebsonsecurity.com/2014/05/antivirus-is-dead-long-live-antivirus/
    - 10 Step Security Guide to Keeping your Computer Virus Free
      https://www.groovypost.com/howto/groovytip/security-guide-keep-your-computer-virus-free/
    - So much more ...
  - I run Windows 10 on all my computers and rely on Windows Defender
    If I were to install a third party antivirus program, I would probably pay the $40/year and go with either Avast, Bitdefender, Kaspersky.
    - What’s the Best Antivirus for Windows 10? (Is Windows Defender Good Enough?)
      https://www.howtogeek.com/225385/what%E2%80%99s-the-best-antivirus-for-windows-10-is-windows-defender-good-enough/
  - I have MalwareBytes installed but am using the free version in on-demand mode.
    - Malwarebytes is good at finding “potentially unwanted programs” (PUPs) and other junkware. As of version 3.0, it also contains an anti-exploit feature, which aims to block common exploits in programs, even if they are zero-day attacks that have never seen before—like those nasty Flash zero-day attacks. It also contains anti-ransomware, to block extortion attacks like CryptoLocker. The latest version of Malwarebytes combines these three tools into one easy-to-use package for $40 per year.
      https://www.howtogeek.com/225385/what%E2%80%99s-the-best-antivirus-for-windows-10-is-windows-defender-good-enough/
  - I also run RansomFree by Cybereason. It is made to complement antivirus software.

https://ransomfree.cybereason.com/

  - Cyberreason's RansomFree is a ransomware protection program that silently runs in the background looking for ransomware activity on a computer. If activity is detected, such as the encrypting of certain files, it will automatically terminate the program to prevent your data from being encrypted. RansomFree utilizes canary files, which are folders of files created throughout the computer. These files are then monitored for any changes by an external program. If RansomFree detects that a file has been modified, it will display a prompt asking if you wish to terminate the program that is trying to access these files.
    https://www.bleepingcomputer.com/download/ransomfree/

- Final thoughts
  STAY SAFE
  - Do I really need antivirus software? "Antivirus is getting increasingly useless these days. Ransomware attacks in many cases sail right through all the filters because they rely on social engineering the end-user and contain no malware in either the body or the attachment. The bad guys can easily find the email addresses of your users, called your 'phishing attack surface'". Stu Sjouwerman
    https://blog.knowbe4.com/cyberheistnews-vol-6-27-intel-thinks-antivirus-is-s-and-dumps-useless-mcafee
  - "In short, as I've noted time and again, if you are counting on your antivirus to save you or your co-workers from the latest threats, you may be in for a rude awakening down the road. Does this mean antivirus software is completely useless? Not at all. Very often, your antivirus product will detect a new variant as something akin to a threat it has seen in the past. Perhaps the bad guys targeting you or your organization in this case didn't use a crypting service, or maybe that service wasn't any good to begin with. In either case, antivirus remains a useful — if somewhat antiquated and ineffective — approach to security." Brian Krebs
    http://krebsonsecurity.com/2014/05/antivirus-is-dead-long-live-antivirus/
  - "Remember that no antivirus solution is a replacement for good browsing habits. Make sure you trust an application before you install it and test it in a safe environment if you need to. Learn how to spot a scam and don't click on everything you see. The more you can spot malicious software before it ends up on your computer, the less your antivirus programs have to clean up."   Eric Ravenscraft
    https://lifehacker.com/5865356/the-best-antivirus-app-for-windows