Skokie Public Library Presents: Defending Windows with antivirus software, June 26, 2018

With all the computer viruses, worms, adware, spyware, and ransomware on the Internet, keeping your computer safe and clean is an important challenge. In this session we will discuss antivirus software as one layer of defense in keeping your computer safe and answer your antivirus software questions.

- Introduction, definitions, and basics
  - "**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/
  - What is malware?
    - Malware is short for malicious software. It is a broad term that refers to a variety of "malicious" programs. Malware can be as innocuous (but annoying) as pop-up adds or hijacking your browser search, or as menacing as monitoring keystrokes, stealing passwords, or encrypting and ransoming your data.
    - Common types of malware:
      - Virus
      - Trojan
      - Adware
      - Spyware
      - Ransomware
      - Bot
      - Worm
      - Rootkit
    - Malware myths
      - I will know when my computer is infected
      - I don’t go to shady sites, so I will be fine
      - I don’t have anything worth stealing on my computer
      - Macs don’t get malware
    - Resources
      - Malware - Wikipedia https://en.wikipedia.org/wiki/Malware
      - Common Malware Types https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101
      - Five Myths About Malware You Need to Know

http://www.zonealarm.com/blog/2014/03/five-myths-about-malware-you-need-to-know/

- How does one get "infected?"
  - Accepting without reading
  - Downloading infected software
  - Opening email attachments
  - Inserting or connecting an infected disk, disc, or drive
  - Visiting unknown links
  - Unpatched software
  - Pirating software, music, or movies
  - Online Ads
  - Links on Social Media sites
  - Resources:
    - 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/
    - How does a computer get infected with a virus or spyware?
      https://www.computerhope.com/issues/ch001045.htm
- Symptoms of an infected computer:
  - An infected computer can display a number of symptoms.
  - Or it could display no symptoms at all!
  - Resources:
    - 13 Warning Signs that Your Computer is Malware-Infected
      https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/
- How does Antivirus software work?
  - Traditional antivirus software works with virus "definition," i.e., signatures or patterns embedded in the files themselves. Virus signatures are always being updated, even hourly. This technique does not protect against "zero-day" exploits that take advantage of unknown or unpatched software flaws.
  - Resources:
    - HTG Explains: How Antivirus Software Works
      http://www.howtogeek.com/125650/htg-explains-how-antivirus-software-works/
    - How Antivirus works (Comodo)
      https://antivirus.comodo.com/how-antivirus-software-works.php
- Antivirus software potpourri
  - On-demand antivirus scanners and virus removal
    - **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/

- 22 Free On-Demand Virus Scanners (updated April, 2018)
  http://freebies.about.com/od/computerfreebies/tp/best-on-demand-virus-scanner.htm
- Microsoft Safety Scanner, free on-demand virus scan from Microsoft
  https://www.microsoft.com/security/scanner/en-us/default.aspx
- **Windows Defender Offline**
  https://support.microsoft.com/en-us/help/17466
- **Malwarebytes** for removing Potentially Unwanted Programs (PUPS)
  https://www.malwarebytes.com/

- Anti-Exploit software
  - Anti-Exploit software complements antivirus software. It typically protects against zero-day exploits that target browser and application vulnerabilities and defends against drive-by download attacks. Today there are very few stand-alone or single-function anti-exploit products however. Most have been merged into larger products.
  - Resources:
    - 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/
    - Malwarebytes
      https://www.malwarebytes.com/premium/
      - Since the release of v.3 in 2016 anti-exploit has been merged into the premium product.
    - Hitman Pro (now owned by Sophos)
      https://www.hitmanpro.com/
    - Microsoft's Enhanced Mitigation Experience Toolkit (EMET)
      NB: EMET is no longer supported as a separate tool. Much of its functionality has been incorporated in Windows 10 "exploit protection."
- Next-Generation Antivirus (NGAV)
  - Doesn't work with traditional AV signatures.
  - Specializes in trying to stop unknown exploits
  - Currently focused on the enterprise not on the consumer market
  - Examples: Barkly, Carbon Black, Cylance, Sentinel One, Traps
- Microsoft
  - Windows Defender Security Center
    - Beginner's guide to Windows Defender Security Center on Windows 10
      https://www.windowscentral.com/beginners-guide-windows-defender-security-center-windows-10
    - What's new in Windows Defender for Windows 10 Anniversary Update
      https://www.windowscentral.com/whats-new-windows-defender-windows-10-anniversary-update
    - New Windows Defender Security Center features in Windows 10 Fall Creators Update
      https://www.windowscentral.com/whats-new-windows-defender-security-center-windows-10-fall-creators-update
      - Controlled folder access

        - Exploit Guard
    - What's new with Windows Defender Security Center in the April 2018 Update
      https://www.windowscentral.com/whats-new-windows-defender-security-center-april-2018-update
        - Windows Defender Application Guard (WDAG)
          Starting with the April 2018 Update (version 1803), the feature is now available for devices running Windows 10 Pro with processors that support virtualization.
            - How to enable Microsoft Edge Application Guard on Windows 10 April 2018 Update
              https://www.windowscentral.com/how-enable-application-guard-microsoft-edge-windows-10-april-2018-update
- Resources
    - The most secure Windows ever - and built to stay that way
      https://www.microsoft.com/en-us/windows/comprehensive-security
    - Windows Defender Security Intelligence
      https://www.microsoft.com/en-us/wdsi
    - Microsoft antivirus and threat protection solutions
      https://www.microsoft.com/en-us/wdsi/products
        - Windows Defender (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/
        - MS Security Essentials (for Windows Vista and Windows 7)
          https://www.microsoft.com/en-us/safety/pc-security/microsoft-security-essentials.aspx
        - 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.
            - With Win10 Anniversary Update, Defender Offline is built into the OS
        - How to change Windows Defender Antivirus cloud-protection level on Windows 10
          https://www.windowscentral.com/how-change-windows-defender-antivirus-

cloud-protection-level-windows-10
        - Advanced Windows Defender settings documented https://answers.microsoft.com/en-us/protect/forum/protect_defender-protect_scanning-windows_10/is-using-windows-defender-as-good-as-avast-or/dc9390f9-d16d-4d2b-a262-881c5a1a0285
    - Consumer antivirus software providers for Windows https://support.microsoft.com/en-us/help/18900/consumer-antivirus-software-providers-for-windows
        - Windows Defender and Microsoft Security Essentials will turn themselves off if you install another anti malware program to protect your PC.
- Bonus Material
    - The user is the weakest link in the security chain!
        - Run as a regular user, not an Administrator
        - Check URL visually before clicking.
        - Question anything unsolicited in email, even if it's from someone you know.
        - Don't be quick to click, go slow, exercise your best judgement.
    - If you installed it, update it
        - Keep system, software up to date: enable automatic updates
    - If you don't use it anymore, uninstall it
        - No Flash; no Java (unless you actually do require it for some reason)
    - Protect your data!!!
        - keep multiple instances of your data
        - one instance should be offline or in cloud, with rollback assurance (Dropbox, for example)
    - Other useful software
        - Firewalls
            - Zone Alarm https://www.zonealarm.com/
            - GlassWire https://www.glasswire.com/
            - Simplewall https://www.henrypp.org/product/simplewall
            - Windows Firewall Control https://www.binisoft.org/wfc.php
        - Trusteer Rapport https://www.trusteer.com/ProtectYourMoney
            - Trusteer Rapport is offered for free to customers of select banking, brokerage, and retail websites.
            - Which attacks does Trusteer Rapport protect against? https://trusteer.secure.force.com/PKB/articles/en_US/FAQ/Which-attacks-rapport-protects?l=en_US
        - RansomFree https://ransomfree.cybereason.com/
            - a behavioral approach to stopping ransomware in its tracks
            - compatible with antivirus software

        - AdBlocking in browser
            - Ads can be an attack vector for malware
            - uBlock Origin is the one I use but there are others
- Final Thoughts
    - **Never ever run two 3rd party antivirus programs simultaneously!**
    - Is antivirus software going to save me?
        - "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
        - "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." Brian Krebs
        - Resources:
            - 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
            - 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
            - It might be time to stop using antivirus
            https://arstechnica.com/information-technology/2017/01/antivirus-is-bad/
            - Is antivirus software a waste of money?
            http://www.wired.com/2012/03/antivirus/
            - 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 non-recommendations:
    I don't provide professional recommendations, but I will tell you what I do.

        - I use the latest version of Windows 10 and rely on Windows Defender as my antivirus program.
        - If I were to use a third party antivirus program instead, I would probably pay the $40/year and go with either Kaspersky, Bitdefender, or Avast.
        - I occasionally run the free version of MalwareBytes (and don't get the real-time protection). The real-time protection may be worth the money for most people. If I was going to pay for one program, this would probably be it.
        - I also run a free program called RansomFree by Cybereason. It works fine with both Windows Defender and MalwareBytes
          https://ransomfree.cybereason.com/
        - Finally, I practice "safe computing."
- Additional Resources
    - What's the Best Antivirus for Windows 10 (is Windows Defender good enough)?
      http://www.howtogeek.com/225385/what%E2%80%99s-the-best-antivirus-for-windows-10-is-windows-defender-good-enough/
    - Antivirus software evaluation
        - Consumer antivirus software providers for Windows
          https://support.microsoft.com/en-us/help/18900/consumer-antivirus-software-providers-for-windows
        - AV Comparatives: Independent Tests of Antivirus Software
          http://www.av-comparatives.org/
        - AV Test
          https://www.av-test.org/en/antivirus/home-windows/windows-10/
        - 4 Places to find up-to-date antivirus test results online
          http://www.howtogeek.com/129624/4-places-to-find-up-to-date-antivirus-test-results-online-2/
    - Antivirus recommendations
        - Best Antivirus Software for Windows 10 in 2018
          https://www.windowscentral.com/best-antivirus-software
        - Best Antivirus Software and Apps 2018 (Tom's Guide)
          http://www.tomsguide.com/us/best-antivirus,review-2588.html
        - The best antivirus software for Windows Home User
          https://www.av-test.org/en/antivirus/home-windows/windows-10/
        - The Best Free Antivirus Protection of 2018 (PC Mag)
          http://www.pcmag.com/article2/0,2817,2388652,00.asp
        - The Best Antivirus Protection of 2018 (PC Mag)
          https://www.pcmag.com/article2/0,2817,2372364,00.asp
        - The Best 6 Free Antivirus For Your Windows 10 PC
          http://www.intowindows.com/the-best-6-free-antivirus-for-your-windows-10-pc/
        - The Best Free Antivirus Protection of 2018 (Tech Radar)
          https://www.techradar.com/news/the-best-free-antivirus
    - Antivirus and security awareness
        - Malware Tips
          https://malwaretips.com/
        - BleepingComputer Virus, Spyware & Malware Removal Guides
          http://www.bleepingcomputer.com/virus-removal/
        - Naked Security (blog)

https://nakedsecurity.sophos.com/

- Malwarebytes Lab (blog)
  https://blog.malwarebytes.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/
- Ransomware that's 100% pure JavaScript, no download required
  https://nakedsecurity.sophos.com/2016/06/20/ransomware-thats-100-pure-javascript-no-download-required/
- Standards for a highly secure Windows 10 device
  https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-highly-secure
- Google just added these antivirus features to Chrome for Windows
  https://www.zdnet.com/article/google-just-added-these-antivirus-features-to-chrome-for-windows/