Lesson Plan

Viruses & Malware 101

DENVER PUBLIC LIBRARY

Students learn what types of malicious software there are, how to tell if their computer is infected, and what they can do to protect their computer from viruses and spyware.

Lesson Objectives

At the end of the class, the student will:

- Know how to identify signs a computer may be infected with malicious software
- Be able to protect their computer using antivirus and antispyware software
- Understand what viruses, spyware, and Trojans are
- Know how to avoid inadvertently downloading malicious software
- Know how to use Antivirus software

Lesson Prep Work

(30 min, at a minimum, prior to student arrival)

- get in early to test for technology failure, because it will happen :-)
- pre-sign into accounts
- pre-load videos or web demos
    - http://www.commoncraft.com/video/computer-viruses-and-threats
- Load antivirus and spyware download sites
    - Avast! (http://www.avast.com/en-us/index)
- print handouts

Lesson Prerequisites

Basic familiarity with computers, the internet, and mouse control.

Lesson Outline

The lesson is completed in one (90) minute class session.

(5) Introduction

- Introduce instructor, students.
    - Ask students at introduction: Have you ever had a computer act strangely? Have you ever had a virus before?
- Let students know it is okay to take phone calls, but ask them to put their phone on vibrate and answer calls outside the classroom.
- Inform students that they can sit back and watch if the class is too advanced.
- Inform students they can go to the bathroom, they don't need permission.
- Show order in which class will happen. Explain scope of class.

- (20) Malware and how to beat it

- Malware
  - Explanation
    - Malware is the general term for malicious software. This can include things like viruses, worms, spyware, and hostage ware. The technical differences between them all aren't that important to know, just how to stop them.
    - Malware can do a lot of damage:
      - Erase files
      - Deny access to files
      - Create popups
      - Track keystrokes
      - Turn computer into spam email server
      - Disable computer completely
    - Malware can be spread through:
      - Email attachments
      - USB drives
      - Programs downloaded off the internet
      - Hackers exploiting vulnerabilities in programs running on your computer
  - Activity: Show video
    - Show video Computer Viruses and threats (http://www.commoncraft.com/video/computer-viruses-and-threats)
- Signs your computer may be infected
  - Discussion: What are the signs you should look for to see if your computer has been infected?
    - Your computer may slow down.
    - You are bombarded with popups or warnings that your computer may be infected from a program you didn't install.
    - New icons or wallpaper or toolbars show up.
    - Your default homepage or search engine starts redirecting to another site.
    - Files deleted or missing.
    - Updates and/or certain programs are disabled.
    - Your computer won't start up (this is most likely hardware related).
- Good practices to avoid infecting your computer
  - Explanation
    - Ignore pop-ups, or even better block them
    - Pop-ups from unknown or untrustworthy sites can have malware attached to them.
    - Watch out for download dialogue boxes, especially if you're not trying to download anything.
      - Only download files from sources you trust.
    - Update your software, specifically flash and Java. You should be prompted to update these at specific interval.
  - Demo: Show pop-up blocker in IE – tools -> Pop-up blocker
    - Go to popuptest.com and run pop-up test 1. Show what happens without pop-up blocker. Show warning bar when blocker is on.
    - Be especially careful with popups that claim your computer is infected or it needs to be scanned for errors.

- ALWAYS close popups by clicking on the red "X" – NEVER click on anything in the body of a popup.
    - *Teachers Tip: To be extra safe, don't click on anything in the window and use ALT + F4 (the red "X" can be faked).*
- Don't open spam email (unsolicited email)
- If you don't recognize an email address, don't open the email.
- If you do open it, REALLY don't open any attachments or click on any links.

- (40) How to protect yourself using Antivirus
    - Antivirus software
        - Explanation
            - Antivirus software scans your computer for malware and monitors your system for activity associated with viruses.
            - It's important to:
                - Update regularly – viruses are constantly evolving, so it's important your antivirus has the latest info to protect you.
                - Scan your computer once a week (or more).
                - Most programs can be setup to automatically update and scan for you.
            - Some good free Anti-virus options include:
                - AVG (http://free.avg.com/us-en/homepage)
                - Avast! (http://www.avast.com/en-us/index)
                    - Teachers Tip: Make sure the class knows that they should disable pop-ups with their new AV software.
    - Downloading and installing Antivirus software
        - Explanation
            - Today we're going to download and install antivirus software so everyone can participate in the process. We're going to download Avast because it has a free version and it is also highly rated.
        - Teachers Tip: Inevitably someone will ask why companies are making antivirus software available for free. Typically, the unpaid version will not contain all the features (like identity theft protection, etc.). Also, you may encounter advertisements in the product for the paid version as well. However, unless you are running a business and require technical support a free antivirus should work just fine.
        - Activity: Download Avast
            - Google Avast
                - Teachers Tip: Using Google encourages good searching skills, and in the off chance a student *doesn't spell the software correctly, they will still be* directed to the correct website.
            - Select Avast.com
            - Click on "Go to Download"
            - Click on the "Download" button under the Avast! Free Antivirus heading.
            - Select "Download free antivirus" on pop-up screen
                - Teachers Tip: Most free antivirus software has a paid version as well, and the pop-*up is asking if you'd like to pay for the more full featured* version of Avast. For most people, free antivirus is perfectly fine.
            - You will be redirected to cnet.com (aka download.com)

- Click on the green “download” button.
- Your download should begin

- Activity: Installing AVAST
  - Navigate to the downloads folder in “my documents”
    - *Teachers Tip: It’s good general knowledge for people to know where their* downloads go.
  - Double click on the “setup” file to install the software.
  - Click on “Run”
  - Click on “Regular Installation” (ignore the custom installation for now)
    - *Teachers Tip: Try to watch out for (and ignore) any extra’s that come with* software (like toolbars).
  - Click “next” on the following screen
  - Installation should begin
  - Click “done” once your installation is complete.
- Explanation
  - Avast will do a quick scan of your system automatically and requires no further input on your part. It is set by default to scan weekly (which is generally recommended). However, we are going to look at some of the settings and features to learn a little bit more about Avast.

- Using Avast
  - Explanation
    - You have some control over how Avast behaves, but you have to know how to navigate the Avast interface first.
  - Activity: Adjusting the settings in Avast
    - To open up the Avast user interface you can double click on the Avast icon in the system tools tray, or right click on the icon and select “open Avast! User interface”.
    - Note the other options available, such as:
      - Silent/gaming mode – which will disable all notifications from Avast.
      - Update – While Avast will stay updated by default, if you’re ever concerned you can manually update Avast via this option.
      - Avast! Shield Controls – Allows the user to disable Avast entirely (not recommended). This may occasionally be necessary if you’re installing certain software (it is still not recommended).
    - Your navigation tabs are on the left hand side
    - Select the scan tab on the left hand side (this is the most important one for our needs).
    - Explain scan types:
      - Quick Scan: Scans most commonly infected files, and is much quicker than a full scan. Most of the time this will suffice.
      - Full System Scan: This will scan everything on your computer. It can take a while, but it is recommended that you do this occasionally.
      - Removable Media Scan and Select Folder to scan: Scans specified external device or Folder.

        - Boot Time Scan: If you have a nasty piece of malware that won't allow your antivirus to run normally you can do a boot-time scan, which will run a scan before any other unnecessary software is loaded.
    - Select "Create Custom Scan" in lower right hand corner.
- Explanation
    - You have a lot of control over how scans are performed on your computer. Typically, it's best to leave everything the way it is. However, you may want to adjust how often your antivirus scans your computer.
    - Select "Scheduling" tab along left hand side.
    - By default, Avast will scan weekly on Sunday (at midnight).
    - Select "Schedule this scan" and you will be able to adjust the options.
        - Teachers Tip: Students who are unsure of what to do should just leave Avast as is.

- (20) How to protect yourself from additional threats
    - Install an anti-spyware and adware program and keep it updated
        - Explanation
            - Spyware and adware collect information on you without your consent, whereas a more traditional virus typically spreads software. Antivirus will protect against some spyware, but not necessarily all of it.
            - Most of the time, Antivirus is enough, but if you suspect you are infected and your Antivirus scan doesn't uncover anything, you may want to use some additional software.
            - Some good free options include:
                - Spybot Search and Destroy
                    - Navigate to Spybot Seach and Destroy web page
                    - Point out reviews at cnet.com
                - AdAware
                    - Navigate to Adaware web page
                    - Point out reviews at cnet.com
            - Just like antivirus, update regularly and scan once a week.
            - In the chance that your scans miss something and you think it's a virus, we recommend using Malware Bytes – it can often catch things other scanners cannot, and they have free tools that can get a scan and removal working when by viruses.
                - Navigate to Malware Bytes web page.
                - Point out reviews at cnet.com

(5) Conclusion

- Go over handout, review material, and emphasize contact info & further resources on handout.
- Any questions? Final comments?
- Remind patrons to practice; assign take-home-practice - remind them they can ask for help
- Remind to take survey.

<u>What This Lesson Does Not Cover</u>

- Computer maintenance and privacy concerns.

Key Decisions

1. Protecting your Computer has been broken into several parts. The first is a class solely dedicated to Anti-virus. The second is concerned with staying private online.

Appendix

http://download.cnet.com/Spybot-Search-Destroy/3000-8022_4-10122137.html - spybot search and destroy

http://download.cnet.com/Malwarebytes-Anti-Malware/3000-8022_4-10804572.html#editorsreview – Malware Bytes

http://download.cnet.com/Ad-Aware-Free-Antivirus/3000-8022_4-10045910.html - Adaware