Computer Security

Computer Security

- What you don't know can lead to personal and computer security issues
  - Nobody told me
  - Not understanding how things work
- Many computer users encounter security issued because of
  - Curiosity
  - A lack of discipline
  - A lack of common sense
- Here are a couple of pretty good computer security rule
  - Be careful what you click on
  - If you don't have to do it, them don't do it.

Computer Security

- What are the threats
  - Viruses
  - Malware
  - Phishing
  - Spoofed email
  - Improperly configured programs
  - Pop-up boxes
  - Social networking
  - Hidden or double file extensions
  - Shortened Uniform Resource Locator (URL)
  - Email attachments
  - Scareware
  - Unsafe download sites

Antivirus Programs

- Viruses – antivirus program
  - Avast Free Antivirus 6.0
  - AVG Anti-Virus Free Edition 2011
  - Avira AntiVir Personal – Free Antivirus
  - Ad-Aware Free Internet Security 9.0
  - Microsoft Security Essentials 2.0
- Never have more than one antivirus program installed
- Configure the program to automatically update when you start your computer
  - How can you confirm that the data base has been updated

Antivirus Programs

- Check the program settings
  - Make sure all of the program features are operational
  - Check email
  - Check attachments
  - Check web pages
  - Check downloaded programs
  - Check files that are opened
  - Scan everything on the hard drive including compressed files
  - Use heuristic scanning
  - Check for updates to the program

Malware Detection Programs

- Malware – malware detection and removal program
- Use multiple programs to protect against this threat
  - Ad-Aware Free 9.0.5.0
  - Malwarebytes Anti-Malware 1.51.1.1800
  - Spybot – Search & Destroy 1.4
  - SuperAntiSpyware Free Edition 4.55.1000
  - Windows Defender 1.1.1593 – part of the Vista and Windows 7 operating systems
- These are programs that you start, update and run

Malware Detection Programs

- Some programs have an active monitoring feature
  - Part of the program starts when you start your computer and runs in the background
  - If you have two or more programs with this feature
    - Decide which active monitoring feature you want to use
    - Turn off this feature in the remaining programs
- Check the settings to make sure the program is properly configured
  - Data and program updates
  - Scanning
  - Use heuristic scanning (if available)

Phishing

- Phishing – common sense
  - Usually a legitimate-looking email from a trustworthy business
  - Can contain links to legitimate-looking web pages
  - Attempting to obtain personal and financial information
  - Information obtained used for
    - Identity theft
    - Fraud
    - Gain access to an email account
- Information can also be obtained by using
  - Pop-up boxes or windows
  - Intercepted email messages

Spoofed Email

- Creating an email that appears to be from someone other than the actual sender – common sense
  - Requires entering code that changes the information that appears in the “From” field
  - Used by phishers
  - Will probably ask for personal information
  - Personal email can also be spoofed
    - You can receive email that appears to be from friends or relatives
    - Your friends and relatives can receive email that appears to be from you

Other Security Issues

- **Pop-up boxes – discipline and knowledge**
  - Boxes that pop up on the screen while you are on the Internet
  - Advertise products or services
  - No red [X] in the top right corner
  - There might be a button labeled “Close”
    - Do not click on anything in the box
    - Hold down the Alt key and tap the F4 key
    - If that doesn’t work close the browser
    - If the box is still there
      - Shut down the computer
      - Wait thirty seconds before restarting

Other Security Issues

- **Social networking – knowledge and common sense**
  - Facebook
  - Twitter
- **The current breeding ground for malicious activity**
  - Phishing
  - Harvest personal information
  - Infect your computer with malware
- **Locate the security settings for these sites and select the most secure settings**
- **Don't post personal information for the whole world to see**

Other Security Issues

- File Extensions – knowledge and discipline
  - You should have your computer configured to show file extensions
  - The following file types are executable
    - .exe
    - .com
    - .bat
    - .bin
- Never attempt to open a file with a double file extension
  - .exe.docx
  - .com.ppt

Other Security Issues

- Beware of shortened Uniform Resource Locators (URL) – knowledge and discipline
  - Technique that shortens web addresses to accommodate texting
  - Procedure accomplished on a web site like Google URL Shortener (goo.gl)
  - www.bvcompclub.org can be shortened to http://goo.gl/NWAld
  - Can be easily spoofed
  - Before you click on a hyperlink in an email or word document check to see where it is going to take you

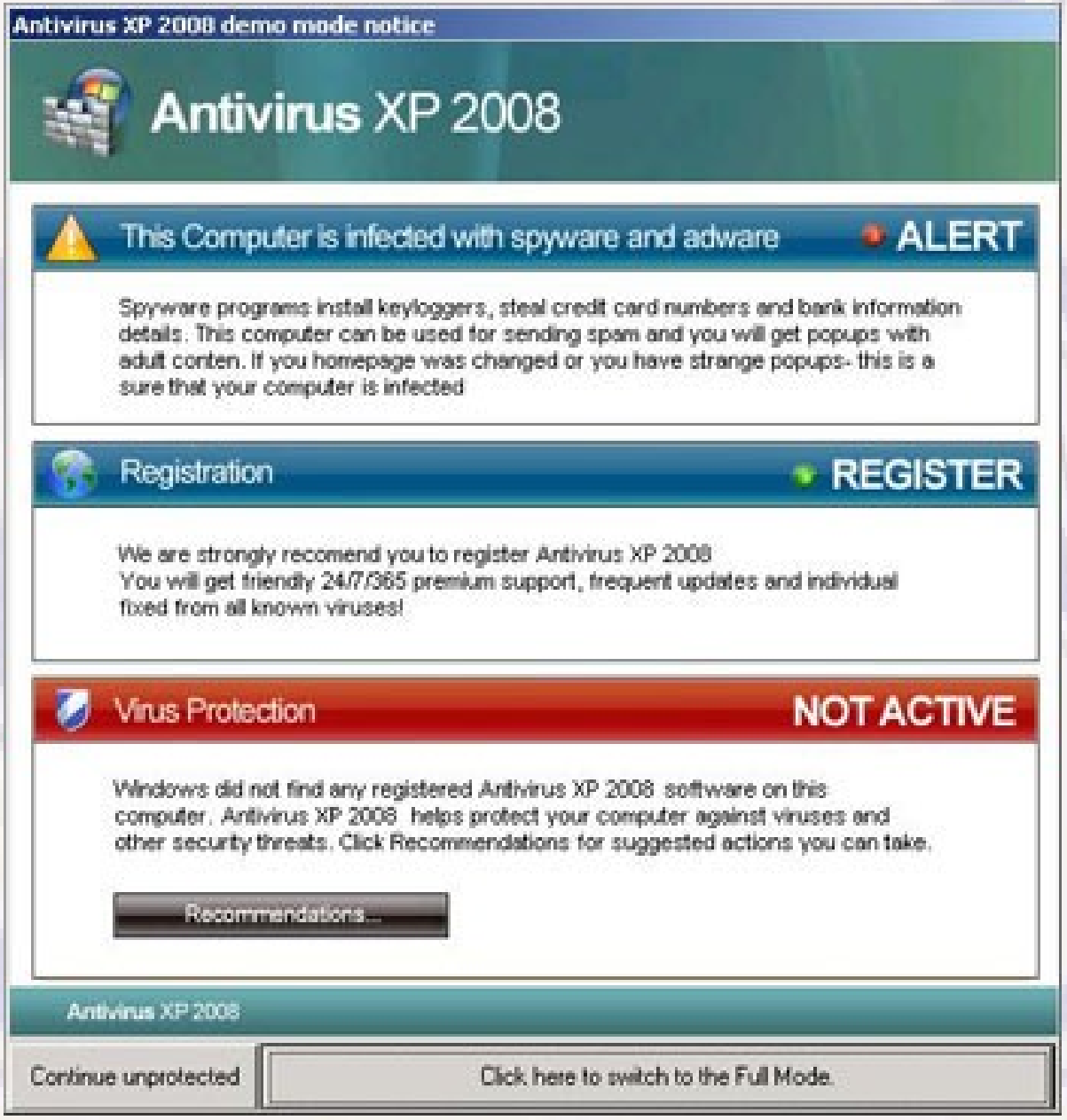
Other Security Issues

- Email attachments – discipline and knowledge
  - Verify the authenticity of an email message before opening an attachment
  - If you can't verify the authenticity of the email
    - What is the attachment
    - Save the attachment to a folder on the hard drive (ie. Working)
    - Have your antivirus program scan the attachment
      - Make sure your antivirus is up to date
      - If the scan does not detect anything it is probably safe to open the attachment

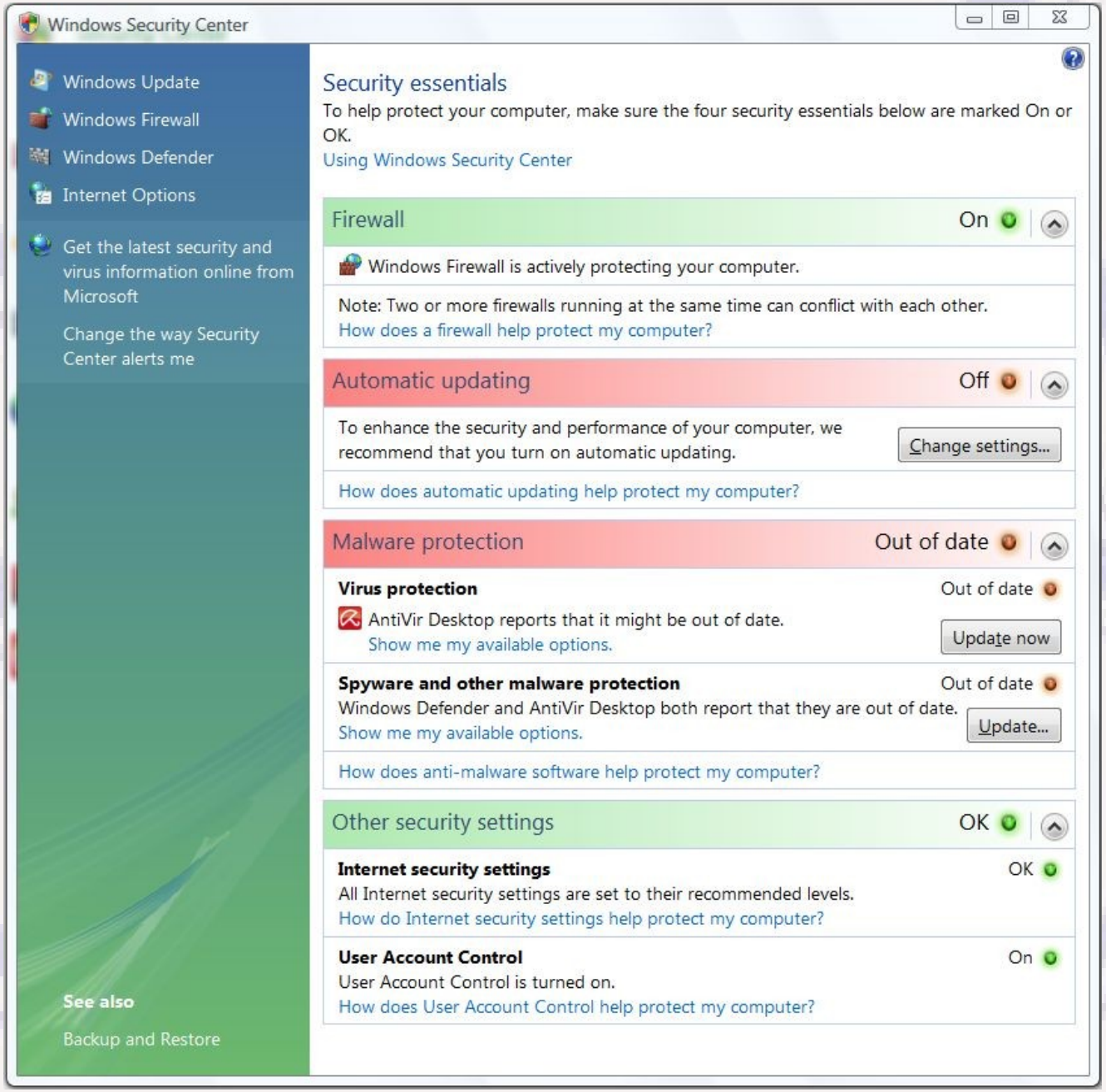
Other Security Issues

- Scareware – messages, pop-up boxes, and email messages that indicate you have a computer problem (Rogue Security Software) – discipline, knowledge, and common sense
- This is currently one of the most dangerous issues
  - Your system may be infected – Free Scan Now!
  - You need to download a file update from Microsoft
  - Critical error message – registry damage and corruption
  - Warning – 183 privacy violations found
  - Windows is scanning your system for threats. The scanning is provided by our official partner Internet Antivirus Pro

Other Security Issues



Other Security Issues



Other Security Issues

Do's and Don'ts

- Use only one antivirus program that is properly configured and updated every time you start your computer
- Make sure the firewall is on
- Make sure the pop-up blocker is on and properly configured
- If you have high speed Internet use a router
- Install the updates from Microsoft (3 categories)
- Use several up to date spyware detection and removal programs to scan your computer on a regular basis
- Make sure your computer displays file extensions
- When reading an article on a web page do not click on anything that is not within the text of the article

Do's and Don'ts

- Review and edit new email before reading
- Do not use the Preview Pane Or Reading Pane
- Be suspicious of all attachments
- Immediately delete any email that has an attachment with a double file extension
- Do not open unsolicited email (Spam)
- Do not click on anything in an unsolicited email
- If you must look at a suspect email use the back door
- There are a lot of free programs on the Internet that are or contain malware so be careful
  - The safe web site to download programs from is – http://download.cnet.com

Spybot's List of Malicious Products

- **If you have Spybot – Search and Destroy you can view all of the malicious programs the program blocks or removes**
  - **Open the program**
  - **On the menu bar click Mode and select Advanced mode**
  - **In the Warning box click the Yes button**
  - **At the bottom of the left column click Settings**
  - **In the left column click Ignore products and you will see a list of all the malicious programs the program blocks or removes**

Going in the Back Door

- To use the back door to read an email
  - Right-click the message header and select Properties
  - Click the Details tab
  - Click the Message Source… button
  - You can now read the email message
  - You can not view attachments
  - You can return to the Inbox by clicking the red X (two times)
  - Using this procedure does not open the email message