Avoiding Viruses and Malware

STAYING SAFE ONLINE
What is a Virus

- Software with malicious intent
- Meant to:
  - Steal Identity
  - Steal personal data (passwords, bank account info, credit card numbers)
  - Trick you into buying something (antivirus software)
  - Damage data or Operating System
- Often propagates itself
Malware vs. Virus

- Virus meant to do actual harm
  - Steal money
  - Destroy data
  - Damage network
- Malware meant to solicit
  - Buy our AV product
  - Buy these addons
  - Get this product upgrade
Where do they come from

- Email
  - Attachments
  - Pictures
  - Links
- Websites
- Third party software
  - Toolbars
  - Emoticons
What do they look like

- Most recent is fake Anti Virus Software
- Website will pop up a new window saying you are infected
- **Click here to clean your computer!**
- Clicking anywhere usually installs program
- You are then notified that you have to purchase full program to fully clean your computer
AntiVirus 2010/2011

Scanning your computer (Scanned - 39%)

- Started: 15.10.2010 18:50
- Duration: 06:01:37
-Remain: 06:01:58

Scanned objects: 5587
Threats detected: 3
Suspicious files: 0

Last scanned object:
C:\System Volume Information\_restore\B67800AA-8812-4BCC-BD37-6EAFE10C8519\RPS

<table>
<thead>
<tr>
<th>Path</th>
<th>Detected</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Program Files\Internet Explorer\explore.exe</td>
<td>Adware.Redirect.rt</td>
<td>Trojan detected</td>
</tr>
<tr>
<td>C:\Program Files\Outlook Express\msoe.dll</td>
<td>Email.Win32.Herond</td>
<td>Trojan detected</td>
</tr>
<tr>
<td>C:\Program Files\Windows NT\dailer.exe</td>
<td>Backdoor.Dialer.W32</td>
<td>Trojan detected</td>
</tr>
</tbody>
</table>

Remove selected  Remove all  Stop scan

PC is threatened! [Trial Licence, Threat Detected!] 3 threats detected and 0 bad files found

Fix Now!
AntiVirus 2010/2011

- Pops up when visiting infected websites
- Looks like actual Virus Scan or Windows alert
- Is actually a webpage

Symptoms
- Pop ups (continual)
- Browser hijacking (can only visit vendor page)
- Icon in system tray (warning message)
Removal of AntiVirus 2010/2011

- EXTREMELY difficult to remove
  - It buries itself very deeply into the computer system
- Must clean computer and registry
- Not recommended for average user
- Once disabled, clean with anti virus program or malware removal program
- Each version is different and requires different steps
How to Avoid Them

- Be cautious about what websites you visit
  - Go to well known sites before risky sites
  - Amazon over joesshoesforless.com
- If you see the popup, touch nothing!
  - If at work, call EdIT right away
  - If at home, press <ALT> + F4 and reboot
- Scan computer for viruses and malware
Tools for Avoiding and Cleaning

- Good AV software is a MUST
  - Microsoft Security Essentials  
    (http://www.microsoft.com/security_essentials/)
  - McAfee  
    (http://www.purdue.edu/securepurdue/download/index.cfm)
  - McAfee Site Advisor  
    - Included with McAfee Security Center
  - Malwarebytes  
    (http://www.malwarebytes.org/)
Microsoft Security Essentials

Computer status - At risk

Microsoft Security Essentials detected 1 potential threat on your computer.

Real-time protection: On
Virus & spyware definitions: Up to date

Scan options:
- Quick
- Full
- Custom...

Clean computer

Scheduled scan settings
Next scan: Sunday around 2:00 AM (Quick scan) | Change my scan schedule
Real or Fake???

Antivirus 2010

Microsoft Security Essentials
Viruses found
McAfee Site Advisor

- Helps block risky sites

![Image of McAfee Site Advisor]

**Rating Icons**
- **McAfee SECURE**: Tested daily for hacker vulnerabilities.
- **SAFE**: Very low or no risk issues.
- **CAUTION**: Minor risk issues.
- **WARNING**: Serious risk issues.
- **UNKNOWN**: Not yet rated. Use caution.

**Secure Search Icons**
- **SECURE SEARCH BOX**: Worry free searching.
- **BROWSER BUTTON**: Validates site rating.
McAfee Site Advisor
Malwarebytes

- Help clean computers of malware
Let’s Be Careful Out There

- The internet isn’t as safe as it used to be
- This doesn’t mean we should bar the doors and cower in fear
- Some simple steps will help us stay safe online
Good Practices

- Best defense is good judgment
  - Don’t click links in email
  - Don’t go to dangerous websites
  - Use programs to help protect yourself
  - Look at every screen when installing software
  - Don’t just click buttons when prompted to; take your time and look at everything
  - When in doubt, ask for help or shut down