

Anti-Malware for Your PC

Virus Protection
"Spyware" Protection

FOCUS

- Anti-Malware Protection for Windows OS
- Why? Because Windows is #1 target on INet
- System Settings to Check & Set
- Products & Software
 - Anti-Malware: Anti-Viruses & Anti-Spyware
 - Rootkits & Rootkit Revealers
 - Excluding Firewalls

Checking Windows Security

- Internet Explorer (on XP w/SP2)
 - Tools | Internet Options... | Security (tab)
 - Set Zones to DEFAULT
 - Tools | Internet Options... | Privacy (tab)
 - Set to DEFAULT
 - Block Pop-ups

Checking Windows Security

- Outlook Express (on XP w/SP2)
 - Tools | Internet Options... | Security (tab)
 - Normal is “Restricted sites zone”
 - Warn when send mail as me
 - ** Not allow attachments to be saved or opened **
 - Block external content in HTML e-mail

Checking Windows Security

- Turn off services you don't need
 - Windows Messenger
 - Tools | Options | Preferences (tab)
 - Disable run messenger when Windows starts
 - Disable allow messenger to run in background
 - MS Outlook – disable messenger
 - Tools | Options... | Other (tab)
 - Disable instant messaging in MS Outlook

Checking Windows Security

- Turn off services you don't need
 - GRC's 3 Musketeers
 - <http://www.grc.com/default.htm>
 - <http://www.grc.com/unpnp/unpnp.htm>
 - <http://www.grc.com/dcom/>
 - <http://www.grc.com/stm/shoothemessenger.htm>
- XP's Control Panel settings
 - Windows Security Center
 - Automatic Updates

Anti-Virus (AV) Products

- Test site - <http://www.av-comparatives.org/>
- Test & report types method
 - <http://www.av-comparatives.org/seiten/ergebnisse/methodology.pdf>
 - In-The-Wild (ITW) – active & spreading on Internet
 - Zoo – all other known viruses
 - Retrospective test – measures detection of unknown viruses
 - False positives not tested
 - Tests focus on detection, not cleaning
 - Because backup restoration is best fix

Anti-Virus (AV) Products

- Test site - <http://www.av-comparatives.org/>
 - Test & report types method (cont'd)
 - Minimum performance of listed AV's
 - 85% detection of Zoo viruses
 - 100% detection of ITW viruses
 - FAQ section

Anti-Virus (AV) Products

- AV Comparison
 - <http://www.av-comparatives.org/>
 - On-demand test
 - Retrospective / proactive test
 - Performance classification – std, adv, adv+
 - Historical results are dynamic

Anti-Virus (AV) Products

- Free AV products
 - Avast: <http://www.avast.com/>
 - My current choice
 - AVG: <http://www.grisoft.com/doc/1>
 - Crashes Win98 after each update
 - AntiVir: <http://www.free-av.com/>
 - No incremental update; no e-mail scan
 - BitDefender: <http://www.bitdefender.com/>
 - Free is on-demand scan only; no real-time

Anti-Virus (AV) Products

- AV organizations
 - <http://www.eicar.com/>
 - <https://www.icsalabs.com/>
 - <http://www.aavar.org/>
 - <http://www.ipa.go.jp/security/index-e.html>
- AV certification list
 - <https://www.icsalabs.com/> + select AV

Anti-Spyware Products

- What is?
 - <http://www.webopedia.com/TERM/s/spyware.html>
 - Legal wrangling (Leo Laporte KFI podcast)
- Ref: <http://spywarrior.com/>
- Eric Howes
 - <https://netfiles.uiuc.edu/ehowes/www/>
 - Malware guidelines
 - Email guidelines
 - WWW guidelines
 - Other PC protection guidelines

Anti-Spyware Products

- 2004 test results
 - <http://spywarewarrior.com/asw-test-guide.htm>
- Software features comparison
 - <http://spywarewarrior.com/asw-features.htm>
- Recommendations
 - <http://spywarewarrior.com/asw-features.htm#table>

Anti-Spyware Products

- My recommended freebies
 - Microsoft AntiSpyware
 - <http://www.microsoft.com/athome/security/spyware/software/default.mspix>
 - Best overall performance as Giant AS
 - But, MS AS doesn't check cookies
 - For XP/2000 only; not Win9x/ME

Anti-Spyware Products

- My recommended freebies (cont'd)
 - Ad-Aware SE Personal
 - <http://www.lavasoft.de/>
 - Add-ons at <http://www.lavasoft.de/software/addons/>
 - Messenger-Control (Ref: Slide #6)
 - OE/W Messengerctrl

Anti-Spyware Products

- My recommended freebies (cont'd)
 - An integrated pair no longer
 - Spybot S&D version 1.4
 - <http://spybot.safer-networking.de/>
 - Turn on Advanced mode & TeaTimer in Resident Tool
 - Check Immunize settings after each update
 - No longer initiate SB update from Immunize window
 - SpywareBlaster (SB)
 - <http://www.javacoolsoftware.com/spywareblaster.html>

Anti-Spyware Products

- Beware of ROGUE products
 - http://www.spywarewarrior.com/rogue_anti-spyware.htm

Rootkits

- What is a RootKit?
 - <http://www.sysinternals.com/Utilities/RootkitRevealer.html>
 - <http://www.f-secure.com/blacklight/>
- Example
 - http://www.sysinternals.com/blog/2005_10_01_archive.html
- Detection - rootkitrevealer.zip, blbeta.exe
- Removal – a problem; restoration best

Q&A

- Your questions PLEASE
- THE END