Protecting Your Computer (Anti Virus/Security Options)

John Campbell
March 23, 2007
Jampbell@highstream.net

Scope

- **Threats/history**
- **Choices – my goal**
- **Anti Virus Software Sources**
- **Anti Virus Software – reviews**
- **Additional Security – Firewalls/Anti spyware**
- **How to tell if it's working – updates/scanning**
- **Final thoughts**

Threats:What are We Dealing With

The following are some of the more common security threats with a more complete listing In reference 2.

- **Virus – program code - attaches and replicates**
  - from disks, e-mail attachments, internet, shared stuff

- **Trojan horse – malicious programs disguised as useful**
  - can have a time-bomb program
  - not self replicating

- **Worm – network virus or replicating program**

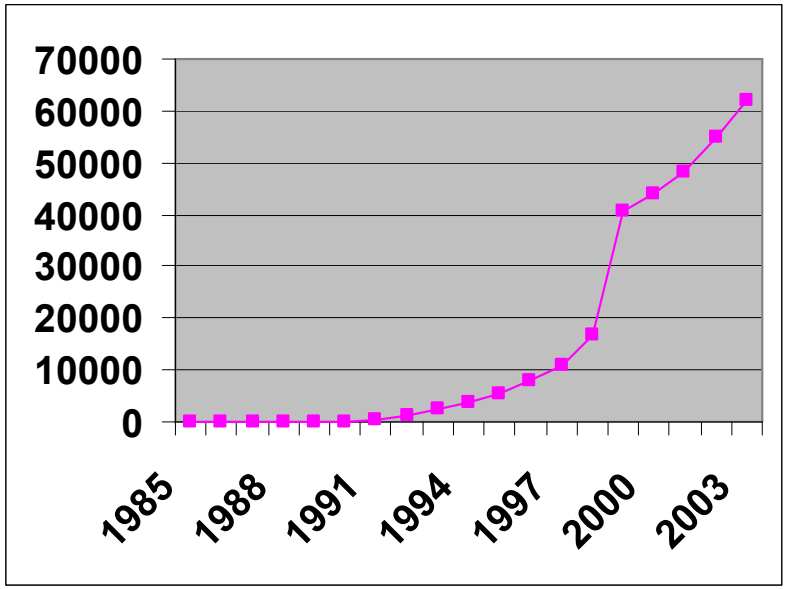
- **Phish – e-mail masquerading as legitimate business to obtain user information**

References 1,2

Record of Infamy

A time line of virus history and frequency as described in reference 3.

1983 – Fred Cohen created term
1985 – 1st Virus created in Labs
1987 – Spread to Universities
1987 – Friday 13th, Stoned, Cascade
1990 – Bulgaria (Dark Avenger)
1991 – Michelangelo (3/6/1491)
1992 – Virus Creation Tools
1998 – 1st BIOS based Virus (CIH)
1999 – NT VIRUS &Melissa (EMAIL attack)
1999 – Ping Virus (Network attack)
2000 -- Love Bug ($10 billion damages)
2001 -- Code Red, Nimda, SirCam
2002 -- Klez, Yaha, BugBear



Reference 3

Choices

Many choices present themselves and internet reviews can be confusing. Many seem unduly (in my opinion) on performance against esoteric threats, hence I believe the differences lie mainly in ease of use and customer service. Please note that if you are happy with your current security system, I would not change…..ie don't fix if not broken.

- **Choices:**
  - **full featured suite (antivirus, firewall, spyware & spam protection) provide convenience**
  - **a la carte (may) offer best of each category or ability to avoid unwanted options**
  - **free vs pay**
  - **internet reviews – data overload!! – bias**
    - **most do a good job on AV**
    - **focus on ease of use, customer service**
  - **no reason to change if current program works!!**

Suite strength depends on components

Anti Virus Software - Free

An excellent source of free security software is through your internet service provider as shown below. In addition, AOL provides a very attractive free package with an active security monitor that provides a snapshot view of your computer's security state. The active security monitor can be used separately (Reference 8). Other free options are also listed and are reviewed on the next slide.

Internet Service Providers

- **Comcast – McAfee Antivirus/Firewall/Privacy service**
- **Embarq DSL - Security suite (earthlink)**

Software Providers

- **AOL Safety and Security (AV/Firewall/Spyware/Spam)**
  - **McAfee/Computer Associates based**
  - **requires AOL e-mail address**
- **AVG – grisoft**
- **Avast**
- **Avira AntiVir**

Reference 8

Run Only One AV!!!

Free Anti Virus Performance

Three good free AV sources are listed below, AVG being the one mentioned frequently at the VCC meetings. I have used free AVG with great success. The download sites are listed in the references.

(2007 CNET)	Editor	Use
Avira AntiVir	-	90
Avast Home Ed	100	90
AVG Free	80	85
BitDefender	(60)	80

- **CNET – best user oriented review**
- **AVG free – large customer base/good reviews**

3 Good Free AntiVirus Options

References 4,5,6,7,8,9

Pay AntiVirus Performance

As noted before, the performance of the AV packages is very similar with the greatest differences showing up in ease of use and customer service. Norton has a long history of customer service issues and of being a resource hog. However, reviews of the 2007 product suggest that Norton has resolved many of these problems but customer service remains an unknown.

(3/2007 review)	Ratings	Service	Use
Bitdefender	100	100	100
Kaspersky	100	100	100
TrendMicro	100	75	85
McAfee	100	62	75
Norton AV	100	80	65
Panda AV	85	50	67
AVG	100	85	100

- **Customer service and use differences!!!**
- **VCC discussions on Norton issues – 2007 improved**

Choice based on service and ease of use

References 10,11

Security Part 2: Firewall

A good 2 way firewall is an important part of a security package and 2 good free options are listed below. It is important to block incoming and outgoing traffic to prevent a program from accessing an unwanted site or sending out information. The XP firewall is incoming blocking only with Vista being 2 way although some postings suggest that careful examination of the Vista firewall settings is required. Only 1 firewall should be used.

- **Firewall important to block hackers in and out**
  - **XP firewall block incoming but not out going**
  - **Vista firewall is in/out – but watch rules**

- **Several good free firewalls**
  - **Zone Alarm (long history)**
  - **Comodo personal firewall 2.0 (also offering free AV – no reviews)**

References 12,13,14,15

Security 3: Malware/spyware

Several good free spyware/malware scanning programs are available and in contrast to firewall and AV programs, several should be used. AVG offers a free trial of their anti-spyware program with reduced functionality after the trial period.

- **Several very good free programs**

	Review	User
Adaware (lavasoft)	**100**	**90**
Spybot	**60**	**90**
AVG AntiSpyware	**-**	**80**
Windows defender	**80**	**70**

- **Many security suites include anti spyware**

Use more than One

References 16,17,18,19

Pay Security Suite Performance

Security suites off all-in-one convenience and in addition to the pay versions reviewed below, AOL safety and security (free!!) is an excellent option. Windows Live Onecare has improved greatly with the latest release and has worked very well for Fred Whitson.

(3/2007 review)	Ratings	Service	Use
Shield pro	83	93	83
Bitdefender	83	67	83
Kaspersky 5.0	83	83	50
Norton AV	83	50	67
McAfee	83	50	75
TrendMicro	83	50	67
Zone Alarm	83		95

- **Windows live onecare – mixed reviews**
- **Zone Alarm, Kaspersky, shield pro good**
- **Norton 2007 improved - top rated with Zone alarm**

Reference 20

Choice based on service and ease of use

Advanced Options

- **Anti-phish and popup blocking**
  - part of Firefox 2 and IE 7

- **Password diligence – secure storage**
  - write down rules not passwords
  Typing phrase# = t1q2b3f4j5o6t7l8b9d10

- **Data encryption**
  true crypt (free) – excellent – file storage
  Ax crypt (free) – for individual files

- **File removal/shredding**
  Evidence eliminator $$
  Eraser (free)

References 21,22,23,24

Bottom Line

In assessing security options, I was interested to look at options once my laptop trial subscription (trend Micro PC-Cillin AV) runs out. I currently run AVG free, ZoneAlarm firewall and several spyware programs on my desktop but rather than just installing the same on my laptop, I wanted to look at options. Since these all scored very well in recent reviews that is the way I will go with my laptop, also because of my familiarity with the programs. However, I gave serious consideration to AOL's safety and security suite and had it not been for my desktop experience I would have gone for the AOL free option.

- **Internet performance reviews – beyond average user**
  - watch for ease of use and customer service

- **Many free good AV options – AOL suite**
  - AVG,AOL,Avast, Avira standouts
  - AVG/Microsoft link

- **Pay AV/suite Options**
  - Norton good performer but history of user issues
  - Norton 2007 improving (less memory hog)
  - Windows Live One Care – current suite excellent (FW)
  - Zone Alarm Security - high marks

Free Security – requires ISP version, AOL or a la carte

My Choice – AVG free/Zone Alarm/Adaware, AVG

Scope

- Threats/history
- Choices – my goal
- Anti Virus Software Sources
- Anti Virus Software – reviews
- Additional Security – Firewalls/Anti spyware
- **How to tell if it's working – updates/scanning**
- **Final thoughts**

Is it Working Real Time?

The way to verify if the AV program and firewalls are working is to look for the respective icons In the applications tray (lower right corner of the screen). The AVG icon turns grey if there is a problem and on Windows XP a balloon will appear showing that security is lacking.

Applications Tray Monitor

- **AVG**

Anti Virus – if inactive icon color changes

AOL Security

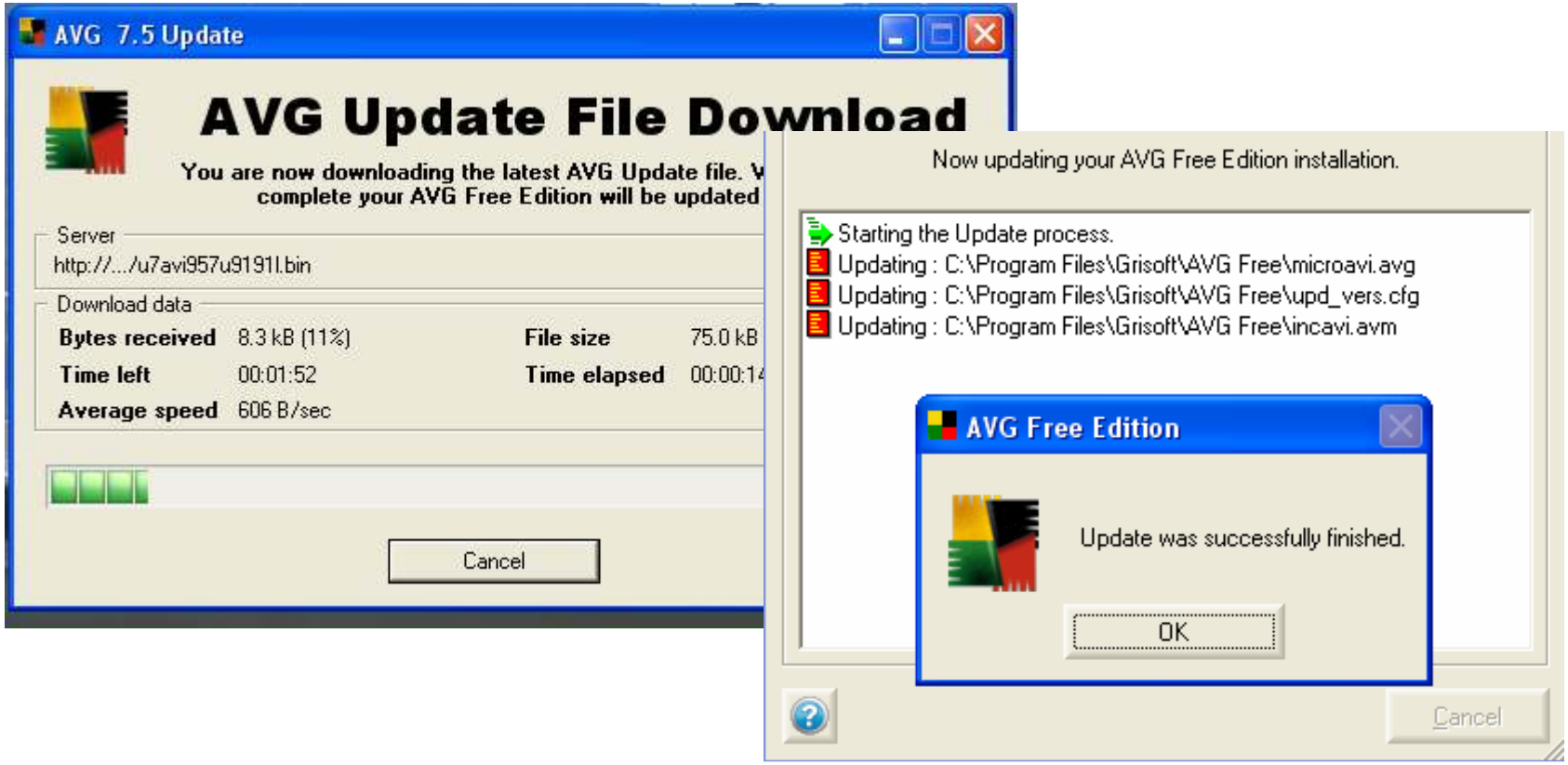
AVG Spyware

Run Only One AV!!!

Is it Working – Updates?

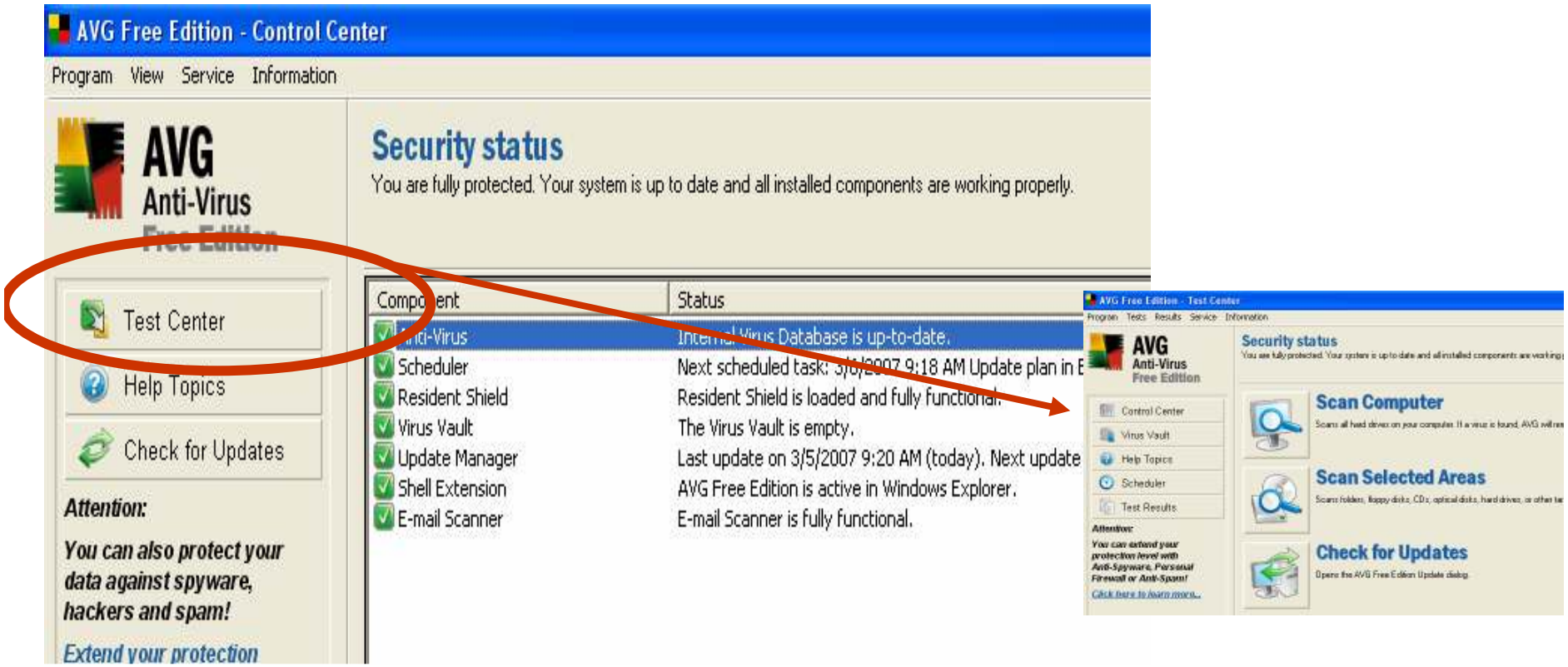
Part of good AV security is ensuring that updates are performed. In the case of AVG, every day on computer startup I see the update download shown below. It is also possible to do a manual update by clicking the AVG icon and then the check update option. AVG updates daily, a good procedure in my opinion

- **Should see update process on startup**



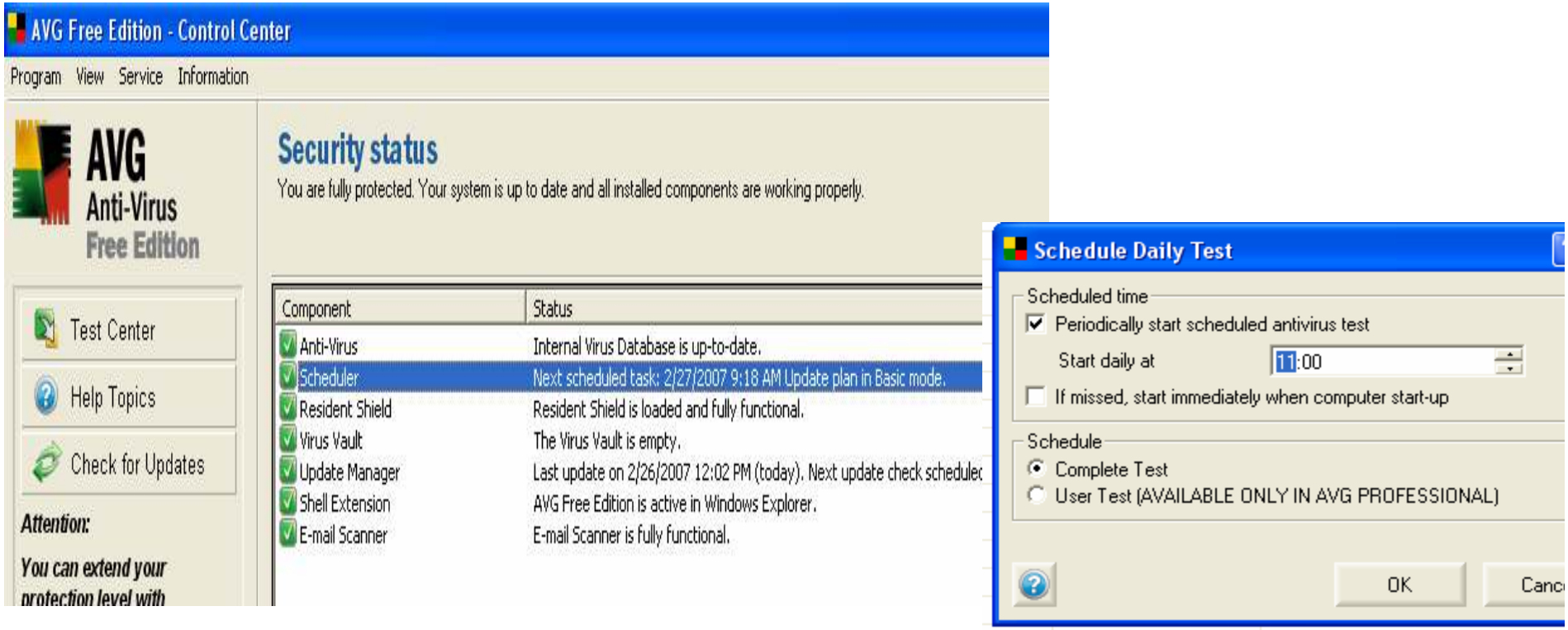
File Scanning

Clicking the AVG icon in the applications tray brings up the control center page. Selecting test center allows for manual scanning and updating. E-mail scanning can also be set – I use only incoming e-mail scanning.



Is it Working – Scanning?

In a similar fashion, the schedule for automatic scanning can be set although I prefer to do it at my convenience to avoid slowing down the computer.

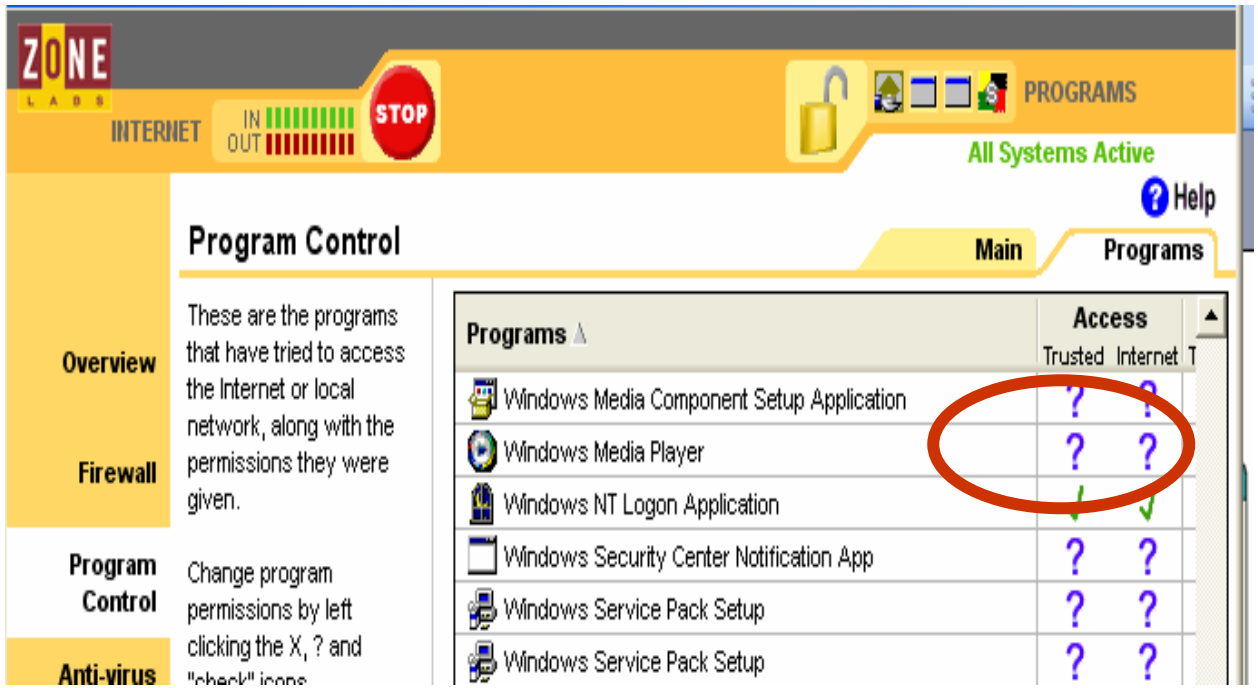


Firewall (Zone Alarm) Processes

Zone Alarm (free) provides notification of a program trying to perform an outgoing operation - in this case accessing the internet. Clicking the Zone Alarm application tray icon allows one to set program control so that alerts aren't received for trusted programs (eg Firefox, internet Explorer, e-mail…..)

- **2 way notification of incoming and outgoing attempts**

Outgoing



Final Thoughts

A list of references is shown on the next 2 pages and details my sources for the reviews as well as sites for free downloads (also mentioned in previous VCC presentations – see Bob Petrilak's)

- **Lots of good free options**
- **Run 1 AV and firewall – make sure AV is working/current**
- **Use several antispyware/malware programs**
- **Be vigilant!**
- **My choice: AVG free/Zone Alarm/Adaware-AVG AS-spybot**

…….enjoy safe computing

Resources/References

General Interest

1.(definitions): http://www.smartcomputing.com
2.(definitions): http://news.com.com/The+A+to+Z+of+security/2009-7355_3-6138407.html?tag=hed
3.(virus history): http://www.myitforum.com/forums/tm.asp?m=20539

Reviews and free AV downloads

4.(CNET free AV): http://www.download.com/3120-20_4-0.html?tg=dl-20&qt=free%20antivirus%20&tag=src
5.(free Kaspersky download trial): http://usa.kaspersky.com/downloads/trial-versions.php
6.(free avira download): http://www.free-av.com/
7.(free AVG download): http://free.grisoft.com/freeweb.php/doc/2/
8.(free AOL safety and security): http://daol.aol.com/safetycenter/virus
9.(free avast download) :http://www.avast.com/eng/download-avast-home.html#DownloadAvastHomeEdition

Reviews – Pay AV

10. (Pay AV review): http://anti-virus-software-review.toptenreviews.com/
http://antivirus-software.6starreview.com/?Refer=GoTA&Keyword=BantivirusSsoftware
11.(extensive AV data):http://www.av-comparatives.org/seiten/ergebnisse_2007_02.php

Reviews and free firewall downloads

12.(firewall reviews):http://www.pcmag.com/article2/0,1895,2090808,00.asp
13.(free comodo firewall download):http://www.personalfirewall.comodo.com
14.(Vista firewall comment):http://reviews.cnet.com/4520-3513_7-6690672-1.html
15.(Zone Alarm free download):http://www.zonelabs.com/store/content/company/products/znalm/freeDownload.jsp

Resources/References

Reviews: security suites and free spyware downloads

16.(spyware review):http://www.download.com/3120-20_4-0.html?tg=dl-20&qt=adaware&tag=srch:
17.(free Adaware download):http://www.lavasoftusa.com/products/ad-aware_se_personal.php
18.(free spybot download):http://www.spybot.info/en/download/index.html
19.(free AVG spyware download):http://free.grisoft.com/doc/20/lng/us/tpl/v5
20.(windows live onecare review):http://www.pcmag.com/article2/0,1895,2100528,00.asp

Advanced security options

21. Password storage:http://sourceforge.net/project/showfiles.php?group_id=41019
22. Encryption(true crypt):http://www.truecrypt.org/downloads.php
    (Ax crypt):http://www.axantum.com/AxCrypt/
23. File shredding(review):http://privacy-software-review.toptenreviews.com/?ttreng=1&ttrkey=Evidence +Eliminator
    (eraser download):http://www.heidi.ie/eraser/
24. Smart Computing Article: compute 911:security lockdown