An Updated Survey of Anti-Virus Software – from Published Test Results and Evaluations

Compiled by Gary Patrick
Lexington, Massachusetts Senior Center
Computer and Technology Group
July 14, 2015

This presentation consists of two .pdf files, text material, and graphics, separately.
(This is the text material portion)

Table of Contents:

(Examples of Test Result charts from major test houses are given in the accompanying graphics-content .pdf file).

The first anti-malware advice to give you today is:
Do one of the following, to protect your data backups and disk image backups:
1) Configure your backup program to hide its storage from Windows Explorer, (Windows 7 or 3rd Party Backup Software can do this), or
2) Disconnect your backup storage device from your p.c. except when actually making a data or image backup.

Why? To reduce the risk that Malware called "Ransomware" (such as Crypto-locker) could encrypt your backup device files too.

Variants of Crypto-locker have become increasingly sneaky this year.

1) When first infecting your computer it may encrypt your data files but hide this activity from you for days or weeks, by decrypting individual files while you are using them, and re-encrypting them as these files are closed.

2) Crypto-locker finds your files by whatever shows up as if you were to run Windows Explorer. If your backup device is displayed in Windows Explorer, your backup files could get ensnared.

3) After the "incognito" period ends, Crypto-locker leaves your files encrypted and demands a ransom to give you the decryption key.

Further explanation of these defenses:

Strategy 1) Most backup software can be configured to hide your backup device, including Windows 7 Backup, but not Windows 8.

Strategy 2) A disconnected storage device disappears from Windows Explorer listing:

USB-interface devices such as an external hard disk drive, or Flash memory (thumb drive), are ideal for manual disconnect.

(If you are still using Windows XP, it is recommended to invoke the “Eject Device” icon in the Windows System Tray before physically disconnecting the external device).

Strategy 3) If you are using Cloud storage, and it offers “versioning,” use that feature to keep greater depth to your backups automatically.

(slides 3-5 revised 7/21/15)

Here are some methods by which ransomware can infect your p.c.

Most ransomware infections arrive via email attachments or phishing attacks. Ensure that your email service has filtering enabled to remove malicious attachments.

Malicious websites might piggyback onto news links on a web page you are visiting.

Anti-virus software may or may not be able to catch ransomware. Sometimes it is hidden in a .zip (compressed) file inside another .zip file.

Visit only trusted websites on a p.c. containing sensitive information; do your casual browsing on another device such as a tablet or Chromebook.

Reference: Windows Secrets Newsletter, April 23, 2015:

www.windowssecrets.com/how-to-defend-yourself-from-ransomware/

Windows Secrets Newsletter (7/09/2015) weighs in with advice to be a savvy p.c. user:

1) If you receive a 'phone call from someone reporting your p.c. is infected and needs to be fixed by an online download, it's a scam. For example, Microsoft never makes 'phone calls; you are expected to take the initiative to visit their support page, if you want or need Microsoft Corp. help.

2) Another example – you receive a bogus email about delivering a product you never ordered (and most of the time you'll recognize you didn't order it.)

3) If you receive an email from someone you know, with an attached file, call the person to verify it's legitimate if you have any doubts. Determined hackers can spoof a sender's email address – some malicious site stole a Gmail, Hotmail,or Yahoo contact list to get it.

4) Never, ever open a ZIP attachment unless someone has told you in advance it will be delivered that way.

5) If there's a file you really feel you need to have checked out, there are websites, such as TotalVirus, to which you can send the file for diagnosis. The Windows Secrets Newsletter July 9th issue has a full article about TotalVirus and other tools for vetting a possibly dangerous file.

Reference: www.WindowsSecrets.com/top-story/tools-for-foiling-malicious-links-and-files

6) Stay informed about the latest malware trends by reading the Krebs and Ouch Newsletters:

www.krebsonsecurity.com , written by Brian Krebs, former Washington Post technology reporter.

www.securingthehuman.org/resources/newsletters/ouch/2015, written by volunteer staffers

The most effective 2015 Anti-virus and Security Suite products have been identified by test results and commentary by a number of independent test houses, such as AV-Test, AV-Comparatives, Dennis Labs, ICSA Labs, West Coast Labs, and Virus Bulletin.

1) The leaders in the category of free antivirus programs are Avira, Avast, and AVG.

   Of the three, Avira scores highest in Consumer Reports overall opinion, and is supported by other independent test results.

2) The leaders in the category of Internet Security Suites are ESET, Symantec's Norton Security, BullGuard, G Data, Kaspersky, and BitDefender.

Refer to my spreadsheet of test scores, in slide # 10, as an aid to identify the top quality Anti-malware software.

In my personal opinion, the best AntiMalware Programs for a Windows p.c. for 2015 are:

1) ESET Smart Security 8 (for a fee of $80/year)

Pros: Clean user interface, excellent firewall,

free technical support by U.S. personnel, including hands-on virus removal if needed, (except $50 if virus present prior to ESET installation).

Cons: Displayed text small and cramped in some places

2) Avira Free (if you want a free anti-virus program)

Pros: Malware detection better than most (even counting security suite programs),

Cons: Annoyance of daily pop-ups urging you to buy their premium product.

Is Anti-virus software only, not including extra features an Internet Security Suite has, such as anti-phishing or firewall.

The spreadsheet on the next page is a compilation of the test results from several sources, to assist in comparing the effectiveness of this year's security products:

The free products are listed first, then the for-pay ones.

Each year, Neil Rubenking, a senior editor at PC Magazine (PC Mag online) studies the test results on Anti-virus and Internet Security Products by a number of independent laboratories, and conducts some tests of his own design to reach his conclusions, published by PCMag online. Some rows in the spreadsheet, tagged “PCMag”, contain his categories and results.

Other rows, tagged “C.R.”, quote particular test scores from the Consumer Reports 2015 evaluation; the Consumer Reports summary chart from its July 2015 issue is slide # 3 in the accompanying graphics slides .pdf file.

Thirdly, some rows are quoted from PCAntivirusReviews scores.

A Composite Summary of Lab Test Evaluations for 2015 Anti-virus Software, and Internet Security Software						
Free Anti-Virus Software, tested by Consumer Reports and/or PC Mag. (a)	Avira Free Antivirus	AVG AntiVirus Free	AVAST Free AntiVirus	Microsoft Windows Defender (in Windows 8.1)	Panda Free AntiVirus	BitDefender Anti-Virus Free Edition (2014)
Consumer Reports Overall Score (to 100)	58	54	54	38	-	-
PC Mag Overall Score (scale of 1 to 5)	no report	3.5	3.5	no report	4.5, and is an Editors' Choice	4.0
Details of Product Evaluation, by Test:						
PC Mag Aggregate Lab Rating	no report	3	3	no report	4	5
Threat Blocking (C.R.) (scale = 5)	4	4	4	2	not tested	not tested
Malware Blocking (PC Mag) (scale = 10)	not tested	7.8	9	not tested	8	9
Malicious URL Blocking (PC Mag), percent	not tested	38%	72%	not tested	64%	(not applicable)
Malware Scan (C.R.) (scale = 5)	4	4	3	2	not tested	not tested
Use of Resources (C.R.)	3	3	4	5	not tested	not tested
Updating (C.R.)	5	4	5	4	not tested	not tested
Response to Threats (C.R.)	5	5	2	5	not tested	not tested
Firewall (C.R.)	1	1	2	1	not tested	not tested
Ease of Use (C.R.)	4	3	3	3	not tested	not tested
Anti-Phishing (C.R.)	1	1	2	1	not tested	not tested
Informative Help (C.R.)	Yes	Yes	No	No	not tested	not tested
Startup Repair (C.R.)	Yes	Yes	No	Yes	not tested	not tested
footnote (a): PCAntivirusReviews did not test the free versions.						
For-Pay Internet Security Suites Product Tested by Consumer Reports:	ESET Smart Security 8	Symantec - Norton Security	BullGuard Internet Security	G Data Internet Security	Kaspersky Internet Security	BitDefender Internet Security
Product Tested by PC Mag:	(same)*	(same)	BullGuard Premium Protection	(same)*	(same)*	(same)*
Consumer Reports Overall Score (to 100)	69	69	68	67	65	65
PC Mag Overall Rating (scale of 1 to 5)	3.0	4.5, and is an Editors' Choice	3.0	3.0	4.0, and is an Editors' Choice	4.0, and is an Editors' Choice
PCAntivirusReviews.com (scale = percent)	94%	88%	(not rated)	(not rated)	78%	84%
Details of Product Evaluation, by Test:						
Detection (PC Mag) (Scale = 5)	5	(not rated)	5	5	5	5
Cleaning (PC Mag)	4	4	4	4	5	5
Protection (PC Mag)	5	5	5	5	5	5
Threat Blocking (C.R.) (Scale = 5)	5	4	4	5	5	4
USB Virus Protection (PCAntivirusReviews)	Excellent	Average	(not rated)	(not rated)	Excellent	Excellent
False Positives (PC Mag)	5	5	5	5	5	5
Malware Blocking, percent (PC Mag)	94% (2014)	89%	94% (2014)	92% (2014)	83%	86%
Malicious URL Blocking (PC Mag), percent	41% (2014)	51%	30% (2014)	(not tested)	10%	18%
Malware Scan (C.R.)	4	4	4	5	4	4
Use of Resources (PC Mag: "Performance")	3	5	4	2	5	5
Use of Resources (C.R.): "Efficiency"	4	4	3	4	4	3
Updating (C.R.)	5	4	5	5	5	5
Response to Threats (C.R.)	3	5	5	5	5	5
Firewall (C.R.)	3	5	4	3	1	2
Ease of Use (C.R.)	4	3	3	3	3	2
User Interface/ Usability (PCAntiVReviews)	Very Good	Excellent	(not rated)	(not rated)	Average	Average
Anti-Phishing (C.R.)	3	3	2	2	4	4
Informative Help (C.R.)	Yes	Yes	No	Yes	Yes	No
Technical Support (PCAntivirusReviews)	Excellent	Average	(not rated)	(not rated)	Average	Poor
Startup Repair (C.R.)	Yes	Yes	No	Yes	Yes	Yes
Subscription Price, 3 p.c. bundle	$80	$80	$60	$50	$60	$80
* = PC Mag also tested a more extensive version	←	a green cell indicates best in class;		←	pink flags poorer behavior than most	

Should you change if you are running something other than one of the top-rated ones?

There are two anti-virus products I recommend be replaced:

1) Microsoft Defender (built into Windows 7 and Windows 8, or Microsoft Security Essentials, if you are using it, as an add-on to Windows XP), because it has scored poorly not only in testing by Consumer Reports but by other test houses.

2) McAfee products: McAfee was purchased by Intel Corporation 5 years ago, and has not kept up with the competition, as evidenced in test results by Consumer Reports and others of the test houses. Intel has renamed McAfee "Intel Security," and the McAfee name will be dropped. One may speculate Intel might even drop out of the consumer anti-virus business in favor of continuing an Intel Security product set for businesses.

Otherwise, if you are content with the security package you have, keep it. It may be a good idea to check these test rankings to see if the company has kept up with the best.

Consumer Reports has some advice on the subject of changing, capsuled on the next page.

Additional help to decide whether a free or for-pay product is right for you is provided by Consumer Reports

"Free software, such as Avira Free Antivirus 2015, is good enough for most users.

1) ample protection against websites that deliver malicious software,

2) quick to identify new types of malware.

3) make sure you download it from the official manufacturer website, and double-check that you're not grabbing a fee-based product by mistake."

"The freebies do lack a few features some users might regard as important.

a spam filter for email (but it's built into many Web-based email services).

parental control over websites that can be visited

little or no protection against phishing, (where cyberthieves try to trick you into giving up credentials such as your password and log-in.) That's easy to fix with a free toolbar like McAfee Site Advisor or Netcraft. These add a bit more protection than most browsers provide. Site Advisor, for example, puts site-legitimacy icons right into search results. Depending on how well your e-mail program sorts out junk mail, you may also want to add anti-spam to your free security package. Consumer Reports likes SPAMfighter.

a firewall, but for most users Windows' built-in firewall offers enough protection, keeping malicious software from being downloaded onto your computer. The Windows firewall is turned on by default for Windows XP and later.

some users may benefit from the two-way firewall included in a fee-based suite such as Symantec's Norton Security."

Best alternate choices depend upon some particular features:

You might choose Norton Security over ESET because:

Norton Security has versions for Apple Mac and Android devices as well, giving you the consistency of the same software on all your devices, and all managed in a single online account.

Norton Security has the best firewall of any.

Norton's ranking in tests by independent review houses has improved dramatically versus recent years.

Explanations of Consumer Reports' Terms for its Product Evaluation, and User Comments collected (next page):

Consumer Reports Overall Score is based on performance detecting and blocking both online and offline threats, ease of use, and effective response to newly-discovered malware.
Updating score indicates how soon the product was able to protect against new malware.

Startup Repair provides a way to recover operation of your p.c. when malware stops your p.c. from booting up, even if you haven't created a repair disc with the software (which you should do).

Use of Resources measures the software's use of memory, impact on boot-up time, and tendency to slow computer operation when performing a scan for malware.

Ease of use rating covers installation, changing settings, and interacting with the software.
Firewall rating: how well the software and its firewall stopped rogue connections to and from the internet.
Malware scan measures the effectiveness scanning the p.c. for malware, both online and offline

Response to Threats rating indicates the appropriateness of the suggested or default response to a detected threat

Threat Blocking score shows how well the product protected against live exploits from websites and local drives.

CR users comments on Norton - very good, and has become easier to use over the years
does not remove cookies very well, so use another program for that.
Backup feature can be a pain once you have maxed out your basic (storage)

CR user comment on AVIRA - daily pop-up ads that try to get you to upgrade to the paid service are annoying. Trying to block the ads creates a separate warning message that a service has been blocked which is just as annyoing.

CR user cmment on G Data: G Data recently updated its system, and it is now top notch.
No user feedback on ESET or Bullguard.

CR User commenst on Kaspersky - 2 of 3 had problems and complaints (April and May 2015)
"Firewall is poor; doesn't stop spyware or malware; viruses come through all the time; always having to reboot to disinfect - losing info and mail etc. It used to work great but it can't keep up with the latest issues out there.."
"I have a basic, no-frills Dell, running Windows 7 Home Edition. I had nothing but problems after buying and installing this product. It crashed after four days, forcing me to re-install. It then slowed my computer to a crawl, to the point that I was getting error messages from other programs. Then, the financial protection portion crashed. Uninstalled and got a refund."
No CR suser reviewss on BitDefender IS, or on AVG, Avast, or Win Defender free ones. or F-secure or Panda IS.

CR k user report on McAfee - Avast Free found 7 infected files McAfee missed. conflicts with Minecraft sw

PC Mag mapping of test house results into categories:

Distilling the meaning of each of Neil Rubenking's six characteristic-summary ratings.

Detection << VB100 + 2 file detection tests by AV-Comparatives; detection certification by ICSA and West Coast Labs can boost rating (but not having it doesn't detract).

Cleaning << AV-Comparatives Malware Cleaning test, possibly boosted by ICSA and/or West Coast certification of vendor's cleaning technology.

Protection << real world test by Dennis Labs + Dynamic Test by AV-Comparatives + protection component from AV-Test.

Efficiency in Use of Resources << AV-comparatives + AV-Test Neil's "Performance" category

False Positives << Dennis Labs FP score + AV-comparatives downrating (if any) + a piece of usability rating from AV-Test.

Neil's own Malware Blocking Test

Overall summary rating

Most Internet Security products can be downloaded directly from the company website: (the safest way to obtain it)

Avast Free: download.cnet.com/Avast-free-antivirus-2015/

Avira Free: http://www.avira.com/en/downloads

AVG Free: http://www.avg.com/us-en/download

BitDefender: http://www.bitdefender.com/Downloads/

BullGuard: http://www.bullguard.com/downloads.aspx

ESET: http://www.eset.com/us/download/home/, for a free trial.

G Data: https://www.gdata-software.com/home-solutions/

Kaspersky: http://www.kaspersky.com/downloads/internet-security

Norton: http://us.norton.com/norton-security-antivirus

Product Support Websites for the major AntiMalware Companies:

Avast: http://www.avast.com/support
AVG: http://www.avg.com/us-en/support
Avira: http://www.avira.com/en/support
BitDefender:
http://www.bitdefender.com/site/KnowledgeBase/consumer/
Bullguard: http://www.bullguard.com/support.aspx
ESET:
http://kb.eset.com/esetkb/index?page=home&locale=en_US&option=none
G Data: http://www.gdata-software.com/support
Kaspersky: http://usa.kaspersky.com/support/
Norton: http://www.symantec.com/norton/support/index.jsp
Panda: http://www.pandasecurity.com/homeusers/support/

Installing a new or different anti-virus (general guidance).

The download offered is usually an installer file. It may be offered as a free trial, or you can purchase it online.

Save this installer file to a folder where you know you can find it using Windows Explorer (File Explorer in Windows 8)

Disconnect from the internet.

Uninstall your existing anti-virus product, using an uninstall option when the program is open, or if not evident, then

Turn off or disable the existing anti-virus program, and use the Windows Uninstall program to remove this old anti-virus sottware.

Find the installer file you downloaded in Windows Explorer, and right-click Run as administrator. You may have to re-connect to the Internet during this process if the installer needs additional files from “Home.”

Verify that the installation is complete by viewing a status display, or message that indicates “you are protected.”

With an Internet Security product, look at the setup options for the additional features to accept or modify the defaaut behavior of the fiirewall, malicious URL filtering, spam filtering, parentlal control, or whatever.

A site called EICAR provides a virus -like sample you can test your system:

The eicar.org site describes it as a "legitimate DOS program, and produces sensible results when run (it prints the message "EICAR-STANDARD-ANTIVIRUS-TEST-FILE!")."

The program is completely harmless and is designed to help people test their antivirus software.

The EICAR site says,
"...requests come from exactly the people you might think would be least likely to want viruses 'users of anti-virus software'.

"They want some way of checking that they have deployed their software correctly, or of deliberately generating a 'virus incident in order to test their corporate procedures, or of showing others in the organisation what they would see if they were hit by a virus'."
If you fall into this category and want to test your antivirus software, EICAR is the "right" way to do it.

References:

1) Consumer Reports, Anti Virus Software, July 2015 Issue (available online by logging into the Minuteman Library system Databases with your Cary Memorial Library membership card).

2) PC Magazine online: about Security Suites: http://www.pcmag.com/article2/0,2817,2369749,00.asp

about free antivirus programs:

http://www.pcmag.com/article2/0,2817,2388652,00.asp

3) PCAntivirusReviews website articles: http://www.pcantivirusreviews.com/Internet-Security-Software/