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

compiled by Gary Patrick

Lexington, Massachusetts Senior Center Computer & Technology Club

January 16, 2013, and amended March 19th and March 26th, 2013

Note: As last year, this survey is intended for users of Microsoft Windows personal computers. It does not address the question of Anti-virus protection for Apple computers.

[Here's an Apple Support Communities discussion that recommends either of two products: https://discussions.apple.com/thread/4468450?start=0&tstart=0 ;
For a tabular list of anti-virus products available for Mac, with some test scores: http://mac-antivirus-software-review.toptenreviews.com/
I recommend a Google search if you need more information.]

Index to the pages in this Talk Slide Set

A mini-glossary for this year:

"Zero-day" virus or malware: newly discovered, for which an antidote has not yet been released by the anti-malware companies.

"In-the-wild:" a virus or malware that is circulating on the internet.

Virus Bulletin has an extensive glossary of computer security terms:
http://www.virusbtn.com/resources/glossary/index

(page added 1/20/2013)

Meeting Agenda

Anti-Virus Software Recommendations – (revealing the conclusions ahead of the evidence)
(see page 4 in this document)
The supporting evidence –
User Ratings and Comments *(beginning on page 6)*
Test Report Summaries from four organizations *(see pages 16 - 18)*
Virus Bulletin
Consumer Reports
AV-Test
AV-Comparatives
(refer to accompanying slide set .pdf for computer screen shots of their website data)
plus help of a PC Magazine review as well.
Local Computer Repair and Maintenance Businesses

Maintaining Security beyond Anti-virus Software

(much additional reference material beyond this was not reached in the meeting March 20th)

Anti-Virus Product Recommendations – considering test results and user opinions

All these programs are significantly more complex than in years past, trying to counter the volume and sophistication of malware now, and will start and run slowly enough on older computers to be really noticeable, even with Windows 7 or 8.

At this time, nearly all have been revised to be compatible with Windows 8, but may not yet take advantage of all the advancements available in Windows 8. e.g. ELAM (early launch hook for anti-malware software).

Free Anti-Virus:

Avast Free Antivirus 2013 – performs reasonably well, with fewer complaints from users than for Avira Free or AVG Free. Avira is not compatible with Windows 8.

A change in recommendation from last year – be wary of Microsoft Security Essentials; protection level has fallen; I would recommend running something else instead. For example, MSE 4.0 & 4.1 both failed to achieve AV-Test Labs' certification.

Fee-based Anti-virus or Security Suite:

Bitdefender – agreement on its strength by results from multiple test houses, but is resource-intensive; not for Win-XP, and not the best at offering help. Does have startup repair.

Kaspersky – also top-performing, except slightly lower in VirusBulletin RAP score. User satisfaction is 77%, although not without some complaints on support and renewal.

G Data – least expensive, very good at almost every task, but not tops in repair, no startup repair capability. Runs 2 scanning engines, slows down older computers.

Norton (Symantec) – competent, although not quick at protecting against newly discovered malware, and its firewall is poor. If you have Windows Vista, 7 or 8, use the Windows

firewall instead. It does integrate with ELAM in Windows 8.
Norton is an enigma – it is well liked by professional evaluators; is a PCMag Editors' choice, but annoys customers on a number of issues, such as the Identity Safe for storing your passwords (solution –just don't use it) and non-helpful support.
If you currently are using a Norton product, stay with it. To change to something else one must uninstall Norton, and even so it leaves behind remnants that can trip up the installation and operation of the next anti-virus/anti-malware product. Complete removal of Norton remnants is very difficult.

F-Secure – quickly protects against newly discovered malware, very good firewall, but has dropped from ADV+ to ADV rank at AV-Comparatives. Easy to use and novice-friendly.

Webroot – may be the up-and-coming dark horse. The most recent tests at AV-Test show marked improvement, and earned PCMag Editors' Choice. User satisfaction is 84%.

Some Data-mining concerns in trusting these reports -

1) On what version of Windows was it tested ?
(example: Virus Bulletin runs MS Windows Server products as well as Windows XP & 7)
Some of the test houses have results already for Windows 8 (AV-Test for example, and VirusBulletin is part way into Windows 8 testing)
2) What version (nominal year of release) of Anti-virus product was tested ?
3) What level Anti-virus product was tested (Anti-Virus, vs. Security Suite, etc) ?
This concern negated if the AV engine is the same across products

User Ratings and Comments on Internet Security Suite Products

(abbreviations for sources: AZ = Amazon.com, CR = Consumer Reports, CN = cnet.com)
Users' rating is an average, on a scale of 1-5, obtained from the number of reviews indicated.
Satisfaction Histogram, if given, is numbers of votes (or percent) in five ranks from Excellent to Poor.

Free Antivirus software: (presented in order of rank by performance test results)

AVG Free Antivirus

Users' rating (from CR) 1.3 from 3 reviews; none would recommend it to a friend

Users' comments: (from CR)

foreign Internet AVG Technical Support is no good. They are NOT knowledgeable at all! AVG constantly lets thru malware.

things started happening with my computer. Malware had invaded it via my e-mail. It nearly crashed my computer completely.

after download and install, we learned that it was free for only 29 more days.

Avast Free Antivirus 2013

Users' rating (from CR): 4.2 from 13 reviews; 85% would recommend Avast to a friend.

Users's comments: (from CR)

Avast found threats to my computer, when the other high priced anti-virus products didn't.

needs to improve its malware scan; misses TROJANS that malware software is able to detect.

doesn't have any of the pop-ups that annoy people about Avira.

Of 13 reviews 7 of them flagged: Easy to navigate; 4 flagged: Fast and powerful.

Avira Free Antivirus 2013

Users' rating (from CR): 2.4 from 18 reviews; 28 % would recommend Avira to a friend.

Users' comments: (from CR)

presents a number of annoying pop-ups to buy the full version.

makes my pc so slow I end up turning Avira off.

my computer speed slowed drastically and crashes were more frequent; Replaced with Avast and problem solved.
not compatible with Windows 8.
Of 18 reviews, 4 flagged: Fast & powerful; 3 flagged Easy to navigate

Pay-for-Service Internet Security Suites (presented in order of rank by performance test results)

Bitdefender Internet Security 2013

Users' rating (from AZ) 4.0 from 17 reviews; Satisfaction Histogram: Excellent - 8, 4, 3, 1, 1 – Poor
i.e. 47%, 24%, 18%, 6%, 6%

Users' comments (from AZ): two said it slows a computer less than Kaspersky does.
calls for a re-start computer almost every day for updates.
an extremely resource intensive program. If you're using a computer old enough to be running XP, you probably shouldn't be running it.
scanning your system constantly when resources are available, negating the need for a separate scan. (no scheduling is provided)
a pro service person said Bitdefender 2012 was a good antivirus, but 2013 is known for a lot of problems so far.

Kaspersky Internet Security 2013 [Consumer Reports did not test Kasperski]

Users' rating (from AZ): 4.1 from 320 reviews, Satisfaction Histogram: 63%, 14%, 5%, 6%, 12%.
Users comments (from AZ): 11% say easy to install and works well
11% said non-invasive product, very reliable and not a resource hog.
one review complains Digital River (that handles renewals via credit card) is a hassle.
a couple of recent comments reported installation trouble, and support seemed technically weak.
Users' rating (from CN): 3.52 from 25 votes; Satifaction Histogram: 44%, 12%, 12%, 16%, 16%.
Users' comment (from CN):
Very good protection, very reliable, highly customizable, few false positive alarms.
It just made the system unstable, I don't know how they wrote that it is Windows 8 compatible.
Don't install it ..3/4 memory eater and 100% cpu usage from first start up. You need an i7 processor to

use this antivirus.

Pray that you never have a real problem, as support is slow and solutions are not forthcoming.

Kaspersky needs to list suggested requirements for the product. If you have a fast pc with lots of memory you will not notice anything. If you have a slower pc and minimum memory it probably will not please you.

It takes a long time to start up and connect, which leaves you unprotected for a little while which is not a good thing.

F-Secure Internet Security

Users' rating (from CN): 5.0 from 2 votes; 3.7 from 135 votes on all (past) versions.

Users' comments (from CN):

easy to use & novice friendly. uses the Windows firewall and adds modules to the firewall for extra protection, and might be vulnerable. there are no log files.

Very slim feature set for a paid suite. Very good product support via email, phone & chat.

[Read more: http://download.cnet.com/F-Secure-Internet-Security/3000-18510_4-10205368.html]

[No user feedback was found for F-Secure on Amazon.com]

Norton Internet Security 2013

Users' rating (from AZ): 4.2 from 636 reviews; Satisfaction Histogram: 61%, 21%, 6%, 2%, 10%.

Users' comments (from CN):

Support is not readily helpful. If you try online help, "Nathan" inundates you with lame solutions rather than allowing you to email the problem to them.

If computer is idle long enough for Norton Background Tasks to cut in, it's a hog, slowing your ability to resume doing work, processor busy.

Slows the loading of Windows, and opening any program.

Norton Identity Safe locks up all web browsers on which it is used, making it unusable.

Local Norton Internet Safe in 2012 and earlier is moving one's data to cloud Vault, and failed to get it all for one user; lost a major portion of passwords data.

One cannot import the Vault contents to back it up locally.

Wouldn't install on a Windows-XP laptop without crashing it, where NIS 2012 ran flawlessly.

I would summarize it as: don't use Identity Safe, don't choose this product if you are likely to need help from Norton; use it only on a relatively fast p.c.

Users' comments, cont. (feedback to a product review by Neil Rubenking at PCMag.com)

Identity Safe is a major issue for many early users (of Norton 2013). If you do an upgrade you can keep it local for now but that option will go away in the future. If you do a clean install there's no way to store your information locally; it can only be stored on the cloud! Many users, including myself, don't feel comfortable having our information stored on the cloud.

G Data Internet Security 2013

Users' rating (from AZ): 4.0 from 2 reviews (one 5.0 and one 3.0)

User comments (from AZ):

The reason why Gdata is so good is because it runs dual antivirus engines (AVAST and Bit Defender engines) in tandem. 5*

G Data ran fine on my Dell XPS but brought my older Dell and Compaq laptops to their knees. 3*

User rating (from CN): 4.5 from 2 reviews

User comments (from CN):

Easy to use; signature files delivered every few hours and uses dual scanning.

GUI maybe not as impressive as some competitors.

User comment (from CR): and rated it 3.0.

G-data Slowed my computer down. It now takes 10 minutes for the computer to start up. Also, I have rarely been able to use my chrome browser since I installed G-Data (not too big of a problem, I just switched to Mozilla).

The Security worked great, much better than Norton (which I was using before), also way simpler to use and understand than Norton.

AVG Internet Security 2013

Users rating (from AZ): 3.8 from 6 reviews; Satisfaction Histogram: 66%, 0, 0, 17%, 17%

Users comment (from AZ):

one complaint it interfered with POS software (business customer)

one complaint it slowed startup by 100% on a new computer. switched to Webroot.

Bullguard Internet Security 2013

Users' ranking (from CN): 2.0 on only one review, current version; 3.7 on all (past) versions

Users' comment (from CN):

Reasonably intuitive and user friendly. Doesn't seem to keep up as well as other programs with the latest viruses, started letting in some really nasty stuff even though I am a careful about which sites I visit. Firewall started blocking favorite games, can't be user adjusted.

[Read more: http://download.cnet.com/BullGuard-Internet-Security/3000-18510_4-10134873.html]

Webroot SecureAnywhere Complete 2013

Users' rating (from AZ): 4.7 from 90 reviews; Satisfaction Histogram: 84%, 7%, 4%, 0, 5%

Users' comments (from AZ): 20% cite very easy to use

Webroot does not slow my machine's response time as much as Norton 360 Premier.

Webroot has a community support forum, answered by experiences tech folks.

Primary tech support feature is the ticketing system, which has turnaround delays from uploading your logs, their analysis,and advice to come back.

They should employ a message system that allows the caller to leave a name and phone number to receive a call-back, rather than have the caller remain on the line for what can be an intolerably long wait time.

Sites where download of Anti-virus and Anti-malware products can be obtained:

Free antivirus products: www.cnet.com and www.filehippo.com

Paid Antivirus/Internet Security products: from the website for the product itself, or from www.cnet.com, www.amazon.com or www.newegg.com.

What are the most popular Internet Security products?

Number of Internet Security product downloads from C-net, last week (ending 3/15/2013?)

		Cnet users' Average rating (on a scale of 1-5)
Avast Internet Security	10,956 downloads	4.5*
Kaspersky Internet Security	4,852 downloads	3.5*
Norton Internet Security 2013	4,655 downloads	3.0*
Trend Micro Titanium AntiVirus Plus 2013	4,193 downloads	3.0*
ESET Smart Security 6	2,383 downloads	4.0*
Agnitum Outpost Security Suite Free 32 bit	2,276 downloads	3.5*
Agnitum Outpost Security Suite Free 64-bit	1,133 downloads.	3.5*
Avira Internet Security 2013	1,910 downloads	4.0*
Bitdefender Total Security	1,570 downloads	3.0*
Bitdefender Internet Security 2013	625	2.5
Avast Premier	979	5.0* (only two votes) turn off webrep
McAfee Internet Security	342	3.0*
Panda Internet Security	275	2.5*
Webroot SecureAnywhere Complete	246	3.0*

Read professional reviews by website and online magazine editors

Cnet: downloads.cnet.com or reviews.cnet.com

PC Magazine (excerpts from ? issue, see page www.pcmag.com

PC World Magazine online: www.pcworld.com

Index to Screen-Shot Slides "2013AVtalkSlideSet.pdf" – Website pages of Four Test Labs
With *some explanatory comments (in italics)*.

Slide 1) Title page

2) Virus Bulletin, two-dimensional "RAP" chart – "Reactive And Proactive" Test Results
July 2012 through February 2013, although each test batch collects 4 weeks of data.
Reference: http://www.virusbtn.com/vb100/rap-index.xml. "The RAP Test measures products' detection rates over the freshest samples available at the time the products are submitted to the test [*indicated by the Reactive Test score*], as well as samples not seen until after product databases are frozen [*indicated by the Proactive Test score*], thus reflecting the vendors' ability to handle both the huge quantity of newly emerging malware and their accuracy in detecting previously unknown malware."
Proactive test scores are obtained on malware samples gathered in the week after the Product-under-test was submitted to Virus Bulletin Lab, i.e. constituting "in the wild" viruses and malware unknown to the Product-under-test.
Reactive test scores are obtained with an ensemble of samples gathered in the three weeks prior to the submission of the Product-under-test.
(slide 3 presents a magnified view of the upper right quadrant of this chart).

3) Virus Bulletin, magnified view of the upper right corner of performance slide 2.
Obviously, dot locations up-and-to-the-right indicate better products.
Product name in red means the product represented was tested only once during the period covered by the chart. *Are Avira Free and Coranti really the stars? The other test houses don't show Avira as quite that stellar.*

Note: Norton (Symantec) products are absent from Windows XP, Win 7 & Win 8 tests.
Notice how a number of products are clustered together as "best in class," with Reactive test score over 95%, and Proactive score at about 84% or higher.

By adding a set of vertical grid lines, I was able to interpolate numerical score readings from the version of this graph that presented May-December 2012 test results, and listed them as my representation of Virus Bulletin results in my Summary Table that appears two pages onward in this MSWord text document. (Table update now needed)

4) Virus Bulletin, Summary Table of their "VB100" certification test results, http://www.virusbtn.com/vb100/archive/summary, shown by product tested and Windows system tested.

VB100 certification means

a) a product detects all malware listed as 'In the Wild' by the WildList Organization during the review period, and

b) generates no false positives when scanning a set of clean files.

(references: http://www.virusbtn.com/vb100/about/100procedure.xml www.wildlist.org)

5) Consumer Reports Test Summary Chart for 2013 Free Anti-Virus software, and Paid Internet Security Suites.

Explanation of Column Headings (Specific Performance Measures) on the Consumer Reports Chart:

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

b) Ease of use covers installation, changing settings, and interacting with the software.

c) Malware Scan score rates effectiveness scanning the PC for malware, both online and offline.
d) Resource Drain measures use of memory and tendency to slow computer operation during a scan.
e) Firewall Test shows how well the software and its firewall stopped rogue connections to and from the Internet.
f) Updating shows how quickly the product is able to protect against new malware.
g) Anti-phishing measures the ability to block websites known to host malware.
h) Response to threats indicates appropriateness of the suggested or default response to a detected threat.

6) AV-Test, Test Results Summary by Product, Windows Environment, and Date.
7) AV-Comparatives, Chart of Test Results by Product, Type of Test, and Date.
AV-Comparatives ranks its results into three levels, STD, ADV, and ADV+.
One * = STD, ** = ADV, and *** = ADV+ certification.
8) AV-Comparatives, Table of Contents for their downloadable Summary Report, 2012
This listing names the seven types of tests they perform (some of which are the Column labels on the slide 6 Chart).
9) AV-Comparatives, description of how they obtain virus and malware samples to test.
10) AV-Comparatives, description of the Test Result Thresholds to achieve ADV+ vs. ADV vs. STD level certification; includes consideration of false alarms.
11) AV-Comparatives (speaking of false alarms) False Alarms Bar Chart by Product.
For all of the AV-C charts that follow, I chose the most recent test date available.
The Product names across the bottom are, left to right, AhnLab, Avast, AVG, AVIRA, BitDefender, Bullguard, eScan, ESET, F-Secure, Fortinet, G Data, GFI Vipre, Kaspersky,

McAfee, Microsoft, Panda, PC Tools, Sophos, Trend Micro, and Webroot.

12) AV-Comparatives, defining “few” vs. “many” (false alarms) quantitatively
13) AV-Comparatives, Real World Protection Test, Bar Chart of Results
    Additional products Quihoo-360 and Tencent-QQ show up here.
    (unclear – meanings of “compromised” and “user dependent” not evident)
14) AV Comparatives, Bar Chart of Heuristic (and) Behavioral Test Results by Product
    (unclear what is the distinction between heuristic and behavioral)
15) AV-Comparatives, Bar Chart of (Malware) File Detection Test Results by Product
16) AV-Comparatives, Bar Chart of Performance Test (Burden on Computer System)
    (unclear what the PC Mark Score or AVC score mean.)

(pages 12-15 added 1/22/2013)

Test Results Summary table: augmented upon the summary table for AV-Test that appears in PC Magazine, Dec. 2012

Company	AV-Test Lab Scores. All are for Internet Security Suites, except Avast is the free version				AV-Comparatives		Virus Bulletin VB100 testing May-Dec 2012		Consumer Reports Online	PC Mag. Editor's judgment	Windows 8 ?
	Total	Protec	Repair	Usabil	Citation & Rank		Proact.	React.	Score		
Bitdefender	16.8	5.8	5.8	5.1	Prod. of Yr.	1	84	97	56	Excellent	Y
Kaspersky	16.2	5.7	5.6	4.9	Top rated	2	78	96	no test	Excellent	Y
F-Secure	15.6	5.8	4.6	5.2	Top rated	3	80	94	64	Excellent	Y
Norton (Symantec)	15.0	5.6	4.4	5.0	(not tested)		(not tested)		50	Excellent	Y
G Data	14.7	5.8	4.5	4.5	Top rated	7	85	99	67	Excellent	Y
AVG I.S.	14.4	5.2	4.6	4.6			76	96	51	Good	Y
AVG Free * (a)	14.1	5.0	4.2	4.9					49		Y
BullGuard	13.9	5.7	3.5	4.7	Top rated	5	84	97	53	Excellent	Y
Avast *	13.7	4.6	4.1	5.0	Top rated	8	76	97	58	Good	Y
Webroot	13.4	4.9	3.9	4.6					no test	Fair	Y
Avira Free *	13.3	4.6	4.6	4.1	Top rated	4	89	97	55	Good	
Trend Micro	13.2	4.9	3.8	4.6					54	Fair	Y
GFI	12.4	4.3	3.5	4.6					no test	Good	Y
Microsoft SE *	12.4	2.3	4.7	5.4			77	89	43	Good	
PC Tools	11.7	4.7	3.2	3.9			64	85	no test	Fair	
McAfee	11.6	4.1	3.0	4.6			77	83	53	Good	Y
Norman	11.6	3.8	3.6	4.2			70	95	no test	Good	Y
ESET	11.5	3.6	2.6	5.3	Top rated	6	78	91	66	Good	Y
Zone Alarm Free AV+F'wall (Checkpoint)	15.5	5.3	5.0	5.2	(not tested)				no test	Excellent	Y
	only 3 tests run by AV-Test										

* = free products; note (a) = only 5 tests run by AV-Test on AVG Free. Windows-8-ready reported on AV-Test site.

Notes to Understanding the Test Table on the Previous Page:

First, there is an update of the Test Table just preceding, on page 18, attempting to show changes in product performance from testing performed in the first quarter of 2013 vs. last quarter of 2012.

Product Tested: the table is somewhat split as to what was tested, by test house.

AV-Test (columns 2-5) – all were Internet Security Suites except Avast and Microsoft Security Essentials are free products

AV-Comparatives (columns 6-7) – all were Internet Security Suites

Virus Bulletin VB 100 testing –

Consumer Reports Online, sampled 3/15/2013 – Avast, Avira, and AVG are the free versions, and Microsoft Security Essentials is a free product. The other scores are for paid Internet Security Suites.

Explanation of Columns:

AV-test Total Score is the sum of the next three columns, Protection, Repair, and Usability.

The scores are from a summary of 22 months of tests, from

(to be continued)

Test Results Summary Table (as above) with AV-Test Nov-Dec 2012 results on Windows 7 added (2nd row)

Company	AV-Test Lab Scores. All are for Internet Security Suites, except Avast is the free version				AV-Comparatives		Virus Bulletin VB100 testing			PC Mag. Editor's judgment	
	Total	Protec	Repair	Usabil	Citation & Rank		Proact.	React.			
Bitdefender	16.8 16.5	5.8 6.0	5.8 5.5	5.1 5.0	Prod. of Yr.	1	84	97		Excellent	
Kaspersky	16.2 16.0	5.7 5.5	5.6 5.5	4.9 5.0	Top rated	2	78	96		Excellent	
F-Secure	15.6 15.5	5.8 6.0	4.6 5.0	5.2 4.5	Top rated	3	80	94		Excellent	
Norton (Symantec)	15.0 16.0	5.6 5.5	4.4 5.5	5.0 5.0	(not tested)		(not tested)			Excellent	
G Data	14.7 14.5	5.8 5.5	4.5 5.0	4.5 4.0	Top rated	7	85	99		Excellent	
AVG I.S.	14.4 14.0	5.2 5.0	4.6 4.0	4.6 5.0			76	96		Good	
AVG free *	14.1 14.0	5.0 5.0	4.2 4.0	4.9 5.0							
BullGuard	13.9 14.5	5.7 5.5	3.5 4.0	4.7 5.0	Top rated	5	84	97		Excellent	
Avast *	13.7 14.0	4.6 4.5	4.1 4.5	5.0 5.0	Top rated	8	76	97		Good	
Webroot	13.4 15.5	4.9 6.0	3.9 5.5	4.6 4.0						Fair	
Trend Micro	13.2 15.5	4.9 6.0	3.8 5.5	4.6 4.0						Fair	

Maintaining Security beyond Anti-virus/anti-Malware Software

(Anti-Virus/Anti-Malware protection for your computer is only one aspect of establishing computer and user security.)

An article in PC World Magazine, December, 2012 addresses a number of aspects.
As a summary list, it offers pointers -

- Enable Automatic Windows Updates
- Be sure your Firewall is enabled – maybe enhance it with Internet Security SW feature
- Keep non-Windows software up to date – the following are bigger hacker targets than others:
  - Web Browsers
  - PDF readers
  - Adobe Flash and Adobe Shockwave
  - Java – January has brought the announcement of a security vulnerability in Java -
    - Uninstall it unless you need it, or be sure to upgrade to Java version 7, update 11.
    - Even so it may be wise to disable it in the browser you use most, and leave it enabled in an alternate browser that you use not for surfing, but to see known websites that require it.
    - Refer to: http://www.java.com/en/download/help/disable_browser.xml (read to the end)
  - "Unplug Java . . .doc"
  - Apple Quicktime, iTunes, etc
- Wireless Router:
  - Be sure you have at least WPA2-Personal security set
  - Use a strong password in WPA2 setup
  - Enable encryption
- Encrypt sensitive files on your hard drive, or encrypt the whole hard drive
- User tips:

Don’t click on a link in an email unless you know it’s a legitimate site

Check that your browser connection to a URL is using SSL encryption for sensitive data

Clue: “https” at the beginning of the URL display window.

Maintaining Security beyond Anti-virus/anti-Malware Software, continued

Reference: An article in PC World Magazine, February 2013 issue, titled
"Beyond Antivirus Software: Eclectic PC Security Tools," by Eric Geier, Link:
http://www.pcworld.com/article/2013814/beyond-antivirus-software-eclectic-pc-security-tools-for-system-wide-audits.html. (dateline 11/13/2012)

"Use strong passwords; keep your system, applications, and browser plug-ins up-to-date; and make sure your firewall is doing its job by blocking all intrusions."

Advice on better passwords:
http://www.pcworld.com/article/227023/how_to_build_a_better_password.html

"A number of tools and services can simplify all the extra security precautions that modern PCs require. All of the following are free for personal computer users. (in increasing order of user sophistication) Here are five to check out:

1) Qualys Browser Check.

   free service

   scans your Web browser(s) to find outdated or insecure versions of some popular plug-ins or add-ons (such as Adobe Reader, Adobe Flash, Java, and Windows Media Player.)

   Two versions available: run real-time within current web browser, or download & install it

   Installed version checks multiple browsers you have installed on your p.c.

   Supported browsers include Internet Explorer (IE), Mozilla Firefox, Google Chrome, Safari, Opera, and Camino.

   Lists plug-ins it scanned, indicates any insecure versions, and if any updates are available.

Provides links to where you can download the newest plug-in version

2) Secunia Personal Software Inspector (PSI for short)

[user feedback on some sites complains Version 3 is too obtuse, prefers Version 2]

Version 2 may still be available

3) Password Security Scanner , by NirSoft

scans for passwords stored by Windows applications and Web browsers, and tells how strong they are.

runs on Windows, and it will scan passwords stored by Internet Explorer, Mozilla Firefox, Microsoft Outlook, Windows Live Mail, and MSN/Windows Messenger, as well as your dial-up and VPN passwords.

4) Shields Up web-based computer-port scanner

tests your Internet connection for possible security holes, such as incorrect firewall settings.

might be a bit over the head of average computer users

If results show open ports, can investigate firewall settings of your router or PC and try to close or secure them.

5) Belarc Advisor (for techies more than for usual home users of a p.c.)

scans your PC's hardware, network connections, software, antivirus status, Windows Updates, and Windows

security policies for insecure settings and other security vulnerabilities.

generates a report in HTML that you can view in your browser.

provides details on the scanned items and any detected issues,

provides links on how to fix them, but it doesn't automatically fix them for you.

Updated programs announced in January, 2013 PC World:
Firefox 17 and Thunderbird 17, Apple iOS 6.0.1, Safari 6.0.2, and Quicktime 7.7.3, to correct security issues.
Adobe Flash Player, and Cold Fusion

Websites that have test data shown as reference material
(from Paul) West Coast Labs Real-time 28-day summary:
http://westcoastlabs.com/realTimeTesting/article/?articleID=1. Has animated score reports

Commentary on the individual free Anti-malware Programs (in alphabetical order)

Avast: West Coast Labs Real-time Test score 89%, and commentary by West Coast Labs:
Version 6.0 looks almost identical to the last new version, that had a new interface that vastly modernised the application's overall look and feel, but builds even further on the functionality with some nice improvements. We should note that Avast automatically updated itself to version 6.0 during the testing period.
The interface, as mentioned, is well designed and easy to follow,
Wants you to promote the program to friends, by putting a "like Avast" social networking button on the page.

Avira: WCL RTT score 90%, and their commentary:
highly intrusive program, sticking a big advertising window in your face every time it updates
- Still true in the latest version 10.
Updates every day, by default
performance has dropped off mildly from previous versions, that achieved consistently excellent detection rates
pleasingly frugal resource usage.
In our group test, AntiVir missed 10 unique files, putting it in fourth place on that rating
(Of course, this is only 10 files out of the just over 4000 that comprised the testing across FTP, HTTP, and P2P)

AVG: WCL RTT score 89%
has long been our recommended free security package, thanks to its impressive malware detection and generous feature set.
This year's upgrade, however, doesn't add any interesting features to speak of.
PC Analyzer module is disabled in the free edition.
a gadget for Windows 7 and Vista is provided, but it replicates the function of the System Tray icon and is much more obtrusive.

Continued next page.

PC Tools Free Version: WCL RTT score 83%

The 2010 edition of the paid full suite was near the top of the class in previous tests
and the free version has usually been a solid alternative to paid suites.
But, more than once the software allowed current malicious executables to install and run on our test system without raising the alarm,
Missed a rather large number (25) of unique files.

[end of West Coast Labs material]

Testing Organizations' Explanations of their testing methods and sources of samples:

AV Comparatives, e.V.: http://www.av-comparatives.org/images/stories/test/docs/methodology.pdf
Page 7 explains where and how they gather malware samples.
See my screen-capture
Pages 15-16 explain the criteria for their Standard, Advanced, Advanced+ ranking of anti-malware.
See my screen-capture

PC Magazine, explanation of test and evaluation method for results of the other labs, by Neil Rubenking, 2012

How PC Magazine's Editor Interprets Antivirus Lab Tests, 2012 edition (Neil Rubenking)

When reviewing an antivirus or security suite product, I always perform hands-on testing of the product's ability

1) to clean up malware-infested systems, and
2) to protect a clean system against attack.
3) To supplement my own tests, I look at results from five major labs, all of them associated with the Anti-Malware Testing Standards Organization (AMTSO), because I'm just one person, I can't come near the exhaustive evaluations performed by the independent testing labs.

My charting and interpretation of these tests necessarily must evolve as the labs introduce new testing methods. Another article explains the system I applied in earlier reviews.

Two Kinds of Test, Static vs. Dynamic

A traditional static antivirus test simply presents the product with a huge number of viruses and other malware samples and records the percentage detected. That's not a situation that occurs in the real world. The ordinary user doesn't keep a folder containing 100,000 viruses on hand, after all.

Malwarebytes, Kaspersky, Trend Micro, Symantec, and other security vendors have been pressing me to include more dynamic testing of extremely current malware. These vendors argue, quite reasonably, that dynamic testing better reflects a product's actual protection than static tests.

Dynamic testing is much more labor-intensive, but fortunately some of the labs have devised automation methods and other techniques to make dynamic testing feasible. I've modified the lab tests chart that I include with each review to clearly distinguish static and dynamic tests.

Static Tests

West Coast Labs and ICSA Labs will check the ability of a vendor's technology to detect a vast number of malware samples, and will separately evaluate how well it cleans up the infestation. Virus Bulletin regularly tests security products against their list of viruses in the wild. To attain the VB100 certification, a product must detect all the threats without erroneously flagging any good programs. I look at the percentage of successful certifications in the ten most recent tests. If a vendor's security technology has achieved VB100 certification in all ten, that's an impressive achievement.

Researchers at Austrian lab AV-Comparatives.org run two specific types of test several times a year. The on-demand tests check a vendor's ability to detect a large collection of viruses and other malware samples. The retrospective tests force each product to use virus definitions from before the first appearance of the samples, thus testing the product's ability to detect new and unknown malware. They rate each tested product ADVANCED+, ADVANCED, or STANDARD; occasionally a product fails to even meet the criteria for a STANDARD rating.

Dynamic Tests

AV-Test.org, based in Germany, keeps inventing new and better tests. Their latest set involves certifying products for antivirus protection under Windows XP and Windows 7.*[Note: AV-Test eliminated Windows Vista certification in 2011.]* Each product can earn from 0 to 6 points for protection, repair, and usability, with a total of 12 required for certification. A surprising number of products have failed to reach certification in one or more tests. Others have scored as high as 17 of 18 possible points in all three.

The whole product dynamic test run by AV-Comparatives challenges a collection of security products to defend test computers against very new real-world malicious Web sites. An impressive automated system crawls the Web to find malicious URLs every day. The end result is a report with the percentage of threats successfully blocked, threats entirely missed, and threats for which successful protection requires a correct decision by the user.
Ongoing results are published monthly, with a full wrap-up twice a year. The summary report rates each product as ADVANCED+, ADVANCED, or STANDARD, just as in this lab's other tests.

Interpreting Results

When looking over results from the labs I have to consider the vendor rather than a specific program. Different tests may use different products or versions from the same vendor, so I take each test as an evaluation of the vendor's technology.
ICSA and West Coast Labs report on a vendor's certification only after success is achieved. Having their certifications is definitely good, but not having them typically means the vendor just didn't choose to participate. Likewise some vendors choose not to participate in Virus Bulletin's testing.
Because of the intensive nature of their testing, AV-Test.org and AV-Comparatives.org typically include just 15 to 20 products in a test. Here again, if a product isn't included I can't count its absence against it. On the other hand, I'm impressed with a product that all five labs consider important enough to test.
Keeping these facts in mind I've devised a system for aggregating test results into a rough overall score. This system will change as the labs invent new tests, naturally. For AV-Comparatives.org I take the average of the on-demand and retrospective scores, counting ADVANCED+ as 3 and STANDARD as 1. I map the average of the three AV-Test.org results onto a range from 0 to 3. For Virus Bulletin I calculate the percentage of VB100 successes in the ten latest tests and also map that to 0, 1, 2, or 3. Then I average the three ratings. If a product doesn't have at least two of these three ratings I consider that there's just not enough information.
As noted, I have more confidence in a product that's tested by many labs. To account for that, I add to the average one tenth of a point for each lab that tested the product. At present, that's how I reach the aggregate rating of POOR, FAIR, GOOD, or EXCELLENT.

New Chart Style

In addition to distinguishing static and dynamic tests, I've also replaced the simple Y for a tested product with numeric values in most of the column. Only ICSA Labs and West Coast Labs retain the simple Y.

For AV-Comparatives static tests the chart shows the average of the on-demand and proactive scores, up to 3 (ADVANCED+). It reports on the dynamic test in the same way. The number in the AV-Test column is the average total score in the most recent three tests.

This system will continue evolving with time, but I believe it does offer an easy way to summarize what the various labs have to say.

AV-Comparatives' List of Its Tests

At AV-Comparatives we limit the number of participants in our tests to usually around 16-20 vendors and where possible we include only good and reliable products/vendors. Due to this, we have devised various requirements in order to take part, which also aids us identifying and filtering out rogue anti-virus vendors.

1) Whole-Product Dynamic ("Real-World") Protection Tests:

2012 winners – BitDefender, 99.7%; Gdata, 99.6%; Kaspersky, 99.3%; with few false positives.

This section contains full product long-term dynamic test reports. These tests evaluate the suites "real-world" protection capabilities with default settings (incl. on-execution protection features). It is our aim to do these tests rigorously. Due to that, these tests are time and resource expensive, so only products chosen for the yearly main test-series are included. Results are released monthly (from March to June and from August to November), together with two overview reports (July and December) covering four months each.

2) File Detection Test – evaluates the static file scanning engine, one subset of the protection features provided by security products.

2012 winners – Avira, 99.6%; Kaspersky, 99.3%; Bitdefender and F-secure, each 98.9% (percentages are the average achieved in two tests, March and September, 2012); awarded the Advanced+ rating

This is a malware detection rate (file scanning) test. The file detection rate is still one of the most important and reliable factors in determining the effectiveness of an anti-virus engine which works without asking for user interaction, decision or opinion. The file detection tests show the detection rates of products over an actual and full malware test set from the previous months. This test also takes into consideration the false positive rate.

3) Proactive / Retrospective Tests

2012 Winners – Bitdefender and Kaspersky, 97%; F-secure, 91%; G-data, 90%; few false positives.

The retrospective tests evaluate the products against new and unknown malware to measure the proactive detection capabilities (e.g. through heuristics, generic signatures, etc.), without internet access. This test also takes into consideration the false positive rate. Starting from 2012, the remaining malware files are also being executed, so that the proactive protection provided by e.g. behaviour blockers is evaluated.

4) False Alarm Tests

2012 winners – Microsoft SE, 0; ESET, 6; Bitdefender and Kaspersky, each 14 (the sum of false positives from both FP tests,

This section contains details about the false alarms discovered during the File Detection Tests.

5) Overall Performance Tests

2012 winners – Webroot, ESET, and Avast; Lower impact on system performance than others.

These tests evaluate the impact of anti-virus software on system performance.

6) Malware Removal / Cleaning Tests - 2012 winners – Bitdefender, Kaspersky, and Panda, received an Advanced+ rating.

These tests evaluate the cleaning / malware removal capabilities of anti-virus products.

For this test we use mainly prevalent, "in-the-field" samples from infected PC's of customers.

7) Anti-Phishing Tests

2012 winners – blocking rate - Bitdefender, 97.4%; McAfee, 97.0%; and Kaspersky, 94.8%

These tests evaluate the protection provided against known or suspected phishing websites. (Phishing websites attempt to steal money from their victims, by the victim's response to viewing the website, commonly incorporating a "bait" link to a fraudulent website.)

The graphs of all these tests are available at: http://chart.av-comparatives.org/chart1.php

Progress vs. time charted by individual company: http://chart.av-comparatives.org/chart2.php
(shows STD vs. ADV vs. ADV+ status overall)

AV Comparatives' Summary Report 2012 - found in:

http://www.av-comparatives.org/comparativesreviews - this year and past years offered.

the 2012 report:

http://www.av-comparatives.org/images/docs/avc_sum_201212_en.pdf (5 megabytes) is a comprehensive report, well worth reading, as the later sections have a full critique of each product tested.

Contents:

- Overall Winner for 2012 -
- The other top-rated Anti-Virus software for 2012
- Top performers in each category of test (the categories just listed above)
- User Interface Review Section – complete write-up with screenshots of product operation (see my screenshot)

Six test houses best known. (all independent from one another)

AV-Test (www.av-test.org/en/home/)

AV-Comparatives (www.av-comparatives.org)

Virus Bulletin (www.virusbtn.com)

NSS Labs (www.nsslabs.com)

ICSA Labs (www.icsalabs.com)

West Coast Labs (www.westcoastlabs.com/checkmark)

CheckVir (www.checkvir.com)

For further reading:

PC Magazine's latest article on Security Suite Software (Dec. 29, 2012, by Neil Rubenking
http://securitywatch.pcmag.com/none/306431-security-suite-endurance-test-winners
need to excerpt this article.

NSSLabs has a library of reports that are informative and well explained.
https://www.nsslabs.com/reports/categories/endpoint-security
For example, specific test-results reports:

1) Degree of Protection provided against Exploits (i.e. malware) by Consumer Anti-virus Software
https://www.nsslabs.com/reports/consumer-avepp-comparative-analysis-exploit-protection
2) Degree of Protection provided against Exploit-evasion (i.e. mutations of malware), by AV Software.
https://www.nsslabs.com/reports/consumer-avepp-comparative-analysis-exploit-evasion-defenses
3) General Malware Blocking compared for four browsers – Internet Explorer, Chrome, Firefox, and Safari
https://www.nsslabs.com/reports/your-browser-putting-you-risk-part-1-general-malware-blocking

Focus on Individual Products (starting with PC Mag's written reviews

Bitdefender Internet Security: pc Mag article - http://www.pcmag.com/article2/0,2817,2410717,00.asp

Bitdefender Internet Security 2013 includes everything found in the company's feature-rich antivirus and adds a no-hassle firewall, accurate spam filter, and cloud-based parental control.

PROS

Excellent results in antivirus lab tests and our own malware cleanup tests. Effective phishing protection. Accurate antispam. Remote management through MyBitdefender portal. Quiet firewall. Multi-device parental control. File shredding.

CONS Cleanup of infested systems can take a long time. In testing, cleanup caused some collateral damage. Some impact on system performance.

rated ADVANCED+, the top rating, in all tests by AV-Comparatives
outscored nearly all others in real-world tests by AV-Test.
PC mag total score = 6.4 points

PCmag own tests - on malware cleanup test, Bitdefender detected 87 percent of the threats. That's quite good, though Norton Internet Security (2013) andKaspersky Internet Security (2013) detected 89 percent.
Also puts as much protection as possible in the entry-level antivirus product, Bitdefender Anti-virus Plus 2013, $39.95, rated 4.5 (of 5.0) by PC Mag.
Quiet Firewall included, actively identified and blocked over 60 percent of thirty exploits generated by the Core IMPACT penetration tool. blocks hack attacks silently and decides for itself whether to block any program's Internet access.
Spam Filtering - Bitdefender does a better job than most, missing just 6.8 percent of spam.
didn't mis-file a single valid personal message or valid bulk message in the spam folder.
Cloud-Based Parental Control
Small Impact on Performance

Kaspersky Internet Security 2013:
PCmag own tests - on malware cleanup test, Kaspersky detected 89%
Kaspersky, Norton Internet Security 2013, Bitdefender Internet Security 2013, and G Data Internet Security 2012 are almost perfect at anti-phishing protection, distinctly better than all the others (pop up comparison provided)

Norton Internet Security 2013:
Editor's choice at PCMag (tied with Webroot SecureAnywhere Complete).
PCmag own tests - on malware cleanup test, Norton detected 89%
Norton (and Webroot SecureAnywhere Antivirus 2013) tied for first place with 6.6 points