



**In this article**

**Spam blocking with security suites**

How much protection do security packages offer **129**

**How spam filters work**

Spam probability is determined in several steps **131**

**Cover CD/DVD includes security package**

PCpro security package against spam and phishing attacks on cover CD (● PCP-Code: ANTISPAM)

# An End to Spam and Phishing

**In the second part of its major test of security suites, PC Professionell gave spam protection filters a lot to chew on. Over 35,000 junk mails and almost 30,000 clean messages had to be correctly identified.**

RÜDIGER PEIN

**E**-mail fraudsters cleverly manipulate their victims in order to coax them into transferring money or disclosing secret PINs or TANs. Phishing e-mails requesting you to update your account details are now perfectly laid out and written in correct English. On top of that, the sheer volume of junk mail plays into criminals' hands; who on earth has time to carefully look through over 500 e-mails a day?

**Protection from advertising and fraudsters**

That's why the security suites PCpro tested have spam filters that automatically sort out unwanted junk and phishing e-mails. But telling the difference between real and phishing e-mails is difficult even

for human readers, as the results of the first Mailfrontier Phishing Test ([http://german.mailfrontier.com/survey/phishing\\_de.jsp](http://german.mailfrontier.com/survey/phishing_de.jsp)), proved: only 11.1 percent of the approximately 25,000 participants were able to correctly assess all e-mails. In a similar test in the USA, only 3.0 percent of participants got it right. Due to their damage potential, most security suites therefore treat phishing e-mails similarly to viruses and work with regular signature updates (see also Issue 8/2006).

**Test winner in all fields**

The best spam filter is the one that recognises the most unwanted messages while at the same time filtering out the fewest real e-mails. Impossible, you say?

It's possible. Our test winner, G Data AVK Internet Security 2006, can do it. Even in phishing attacks it beat all other candidates we tested, achieving a detection rate of 98.6 percent.

**65,000 incoming e-mails**

Our PCpro testers bombarded the security suites with 65,000 e-mails. The trickiest part: All these e-mails were brand new (no older than 24 hours). Particularly the Panda and Softwin products had trouble detecting phishing e-mails. Computer Associates did worst in our usability test and would be well advised to follow the examples of F-Secure, G Data and Kaspersky when it comes to ease of use.

RPE

# Anti-Spam Tools in Detail

**A good spam filter will keep junk mail out of your inbox without removing important e-mails. Our test winner manages both.**

Modern spam filters use a multi-stage procedure to analyse incoming e-mails by various criteria and assign points for spam probability (see also »How Spam Filters Work« on page 131). If the total number of points exceeds a certain value, a message is classed as spam. Most programs allow you to choose this tolerance level yourself (see Features table on page 134). Our testers used the programs' default settings to determine detection rates. By the way, e-mails infected with viruses or trojan horses were not among the samples in our spam test. Those are already taken care of by the suites' anti-virus and anti-spyware modules.

## 100% spam detection is impossible

Spammers will try anything to camouflage their messages as harmless personal e-mails, so some junk mail will always slip through the filters. At best, it still adds up to 4.0 percent - test winner G Data detected 96 percent of junk mail without requiring



**The graph from McAfee reveals that adult content is the top spam subject**

any special configuration or having to be trained. An excellent performance compared to its competitors. Panda did worst, only detecting a meagre 68.4 percent.

G Data's excellent result is due in large part to its Spam Outbreak Shield. This module already blocks a significant share of unwanted and dangerous e-mails using current data from the servers of anti-spam specialist CommTouch ([www.commtouch.com](http://www.commtouch.com)), be it because hundreds of identical mails have already been sent from various servers or because the sender's address is from a bot network. Another advantage of this method is

that it uses little system resources on your PC, since the actual analysis already takes place on the CommTouch servers.

Ranked next for spam detection were F-Secure (90.1 percent) and Symantec (89.0 percent), trailing by a significant margin. With 86.9 percent, Kaspersky, winner of the anti-virus/anti-spyware test in our last issue, ended up in fourth place for spam analysis.

## Phishing Threats Identified

The detection rate of phishing e-mails was significantly higher for all products. One reason is that security firms put more effort into detecting these threats. Another is that they are often easier to recognise because they attempt to mask their target URLs. G Data again leads the field, this time with the same number of points as McAfee: Of 1086 phishing attempts, only 15 were not recognised; this corresponds to a detection rate of 98.6 percent. However, McAfee can only manage this in combination with its virus scanner, which already recognises a number of these fraud attempts by typical signatures.

F-Secure (97.1 percent) and Symantec (96.1 percent) also achieved very good results for phishing protection. Panda again brought up the rear of this test field with 80.4 percent of recognised fraud e-mails. At first sight that seems like quite a lot, but conversely it means that one in five phishing attempts reaches the intended recipient. This difference was particularly obvious in our PC Professionell test laboratory: Of the 1086 tested phishing e-mails, Panda left 213 in the inbox, compared to only 15 for G Data and McAfee – a poor show.

## Our recommendation

### G Data AVK Internet Security 2006

Impressive in all fields: G Data detects by far the most junk mail without erroneously classifying too many wanted messages as spam. If the standard settings aren't enough for you, the program offers extensive options that are comprehensively described in the user manual. PC Professionell therefore recommends the G Data security suite for spam protection.



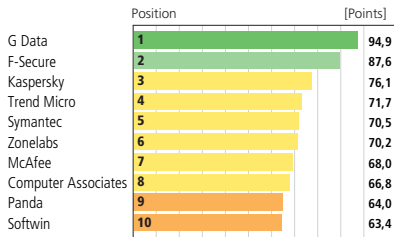
### The security suites with the best anti-spam modules

- 1 **G Data**  
AVK Internet Security 2006 . . . . . **94,9**
- 2 **F-Secure**  
Internet Security 2006 . . . . . **87,6**
- 3 **Kaspersky**  
Internet Security 6 . . . . . **76,1**
- 4 **Trend Micro**  
PC-Cillin 14 Internet Security . . . **71,7**
- 5 **Symantec**  
Norton Internet Security 2006 . . . **70,5**

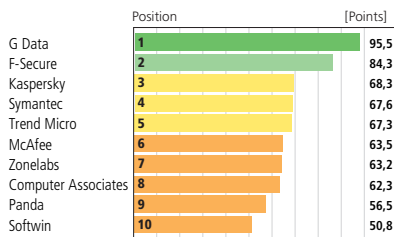
Manufacturer Product . . . . . max. achievable points: 100

## Ratings

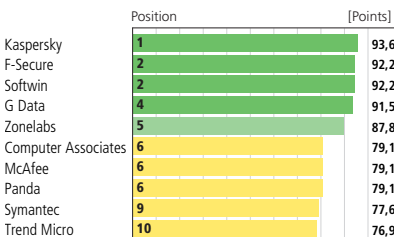
Overall rating 100 %



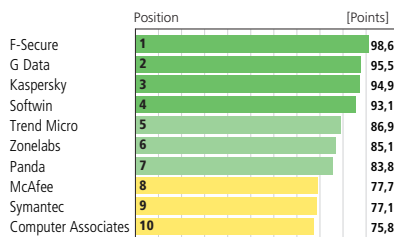
Performance 70 %



Features 15 %



User-friendliness 15 %



- very good ..... 90,0 to 100 Points
- good ..... 80,0 to 89,9 Points
- satisfactory ..... 65,0 to 79,9 Points
- adequate ..... 50,0 to 64,9 Points
- inadequate ..... 0 to 49,9 Points

**Performance (70%)** Detection rates for spam and phishing e-mails, proportion of e-mails erroneously classified as spam (false positives)

**Features (15%)** Integration with Outlook and other e-mail clients, user-defined customisation of tolerance levels for spam detection, separate settings for various spam types, reading address books into the whitelist, reporting and statistics functions

**User-friendliness (15%)** Ease of installation, user interface, quality of manual

## How we tested

PCpro testers unleashed approximately 35,000 junk e-mails and over 1,000 fraud attempts on the spam filters.

In the second part of our major comparison test, the filter modules of the ten security suites got to grips with unwanted spam and phishing e-mails. In collaboration with the AV-Test test laboratory ([www.av-test.de](http://www.av-test.de)), PC Professionell took a look at how reliably those unsolicited mails were detected and how well the security suites really work with different mail clients.

In order to collect as many current test samples as possible, various honeypot systems captured tens of thousands of dubious messages over a period of three weeks. At the same time, almost as many wanted e-mails, such as newsletters, were arriving on our testers' PCs. Double manual checks were used to verify which e-mails really were spam and which ones weren't.

### Fresh spam instead of old rope

At the time of testing, all e-mails were no older than 24 hours – this is important for detection by fuzzy checksum. In contrast to the signatures used by virus scanners, the data of previous spam waves are removed for performance reasons if it is unlikely that the same e-mails will be sent out again.

As phishing e-mails represent a particular risk, PC Professionell determined the detection rate for fraudulent e-mails of this type separately from that for other junk mail. This point was also weighted higher in the overall evaluation.

But keeping inboxes mostly junk-free isn't enough. If users regularly have to retrieve false positives, i.e. messages erroneously classified as spam, by hand, important e-mails can easily be overlooked. The lowest possible number of false alarms was therefore the most important test criterion. Like the average user, our testers left the default program settings for all tasks and made no entries into black- or whitelists.

When it comes to user-friendliness, how the spam filter is integrated is an important aspect. At least for Outlook and Outlook Express, this will generally be through a plug-in. Filters in the form of POP3 or IMAP proxies operate on a more universal level, allowing users to choose any e-mail client they want; in return, these spam filters have to be managed through a separate interface.

## Metrics

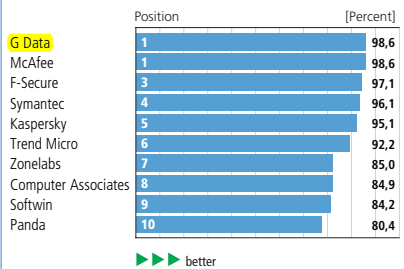
Spam detection

Test set of 34,376 spam e-mails



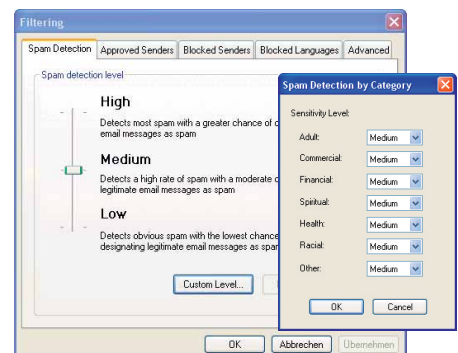
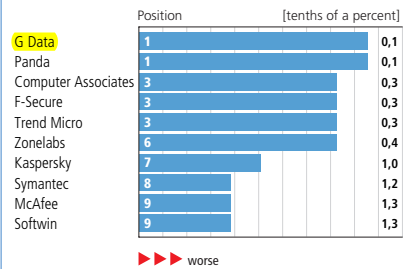
Phishing e-mail detection

Test set of 1086 phishing e-mails



False positives rate

Test set of 28,366 clean, wanted e-mails



Trend Micro allows you to set the spam tolerance level of your choice for each category.

# Security Suites – Anti-Spam Filters TEST



Product	InternetSecurity 2006	Internet Security 2006	Internet Security 6	PC-Cillin 14 Internet Security	Norton Internet Security 2006
Manufacturer	G Data	F-Secure	Kaspersky	Trend Micro	Symantec
Website	www.gdata.de	www.f-secure.de	www.kaspersky.de	http://de.trendmicro-europe.com	www.symantec.de
Price (one PC, one year)	45 very good	60 Euros	40 Euros	59 Euros	70 Euros
Upgrade (one PC, one year)	35 Euros	40 Euros	30 Euros	39 Euros	50 Euros
<b>Overall eval. (grade/points)</b>	<b>very good 94,9</b>	<b>good 87,6</b>	<b>satisfactory 76,1</b>	<b>satisfactory 71,7</b>	<b>satisfactory 70,5</b>
Performance (70%)	very good 95,5	good 84,3	satisfactory 68,3	satisfactory 67,3	satisfactory 67,6
Features (15%)	very good 91,5	very good 92,2	very good 93,6	satisfactory 76,9	satisfactory 77,6
User-friendliness (15%)	very good 95,5	very good 98,6	very good 94,9	good 86,9	satisfactory 77,1
<b>Summary</b>	<b>Clear test winner: Best at detecting spam and phishing e-mails, lowest false positives rate.</b>	<b>Consistently good performance in spam protection combined with user-friendly interface.</b>	<b>Good detection rates with default settings, but many false alarms; easy to use.</b>	<b>Good detection rates with default settings, but many false alarms; easy to use.</b>	<b>Good at detecting spam and phishing e-mails, but also many false positives.</b>

Metrics					
Spam detection rate	96,0 Percent	90,1 Percent	86,9 Percent	74,5 Percent	89,0 Percent
Phishing e-mail detection rate	98,6 Percent	97,1 Percent	95,1 Percent	92,2 Percent	96,1 Percent
False positives rate	0,1 Tenth of a percent	0,3 Tenth of a percent	1,0 Tenth of a percent	0,3 Tenth of a percent	1,2 Tenth of a percent

Functionalities					
POP3/IMAP proxy	yes/yes	yes/yes	yes/yes	yes/no	yes/no
Plug-in for e-mail clients	Outlook, OE	Outlook, OE	Outlook, OE, The Bat!	Outlook, OE	Outlook, OE
Adjustable spam tolerance	yes	yes	yes	yes	yes
Spam detection methods	Bayesian filtering, URL filter, online spam signatures, RBL, distribution patterns (outbreak shield), white-/blacklist	Bayesian filtering, URL/charset/graphics filters, local and online spam signatures, RBL, white-/blacklist	Bayesian filtering, URL/charset/graphics filters, local and online spam signatures, header analysis, white-/blacklist	URL/charset/graphics filters, local spam signatures, white-/blacklist	Bayesian filtering, URL filter, local spam signatures, white-/blacklist

Spam detec. methods					
Supported operating systems	Windows 98 SE/Me/2000/XP (018 01) 00 06 60 <sup>2)</sup>	Windows 98/Me/2000/XP (089) 787 46 73 67	Windows 98/Me/NT/2000/XP (08 41) 98 18 90	Windows 98/Me/2000/XP (09 00) 186 37 22 <sup>3)</sup>	Windows 2000/XP <sup>1)</sup> (09 00) 11 01 30 <sup>6)</sup>
Hotline					
E-mail support/form	hotline@gdata.de	support-de@f-secure.com	support@kaspersky.de	Online support form	Online support form



Product	Zonealarm Internet Security 2006	Internet Security Suite 2006	eTrust Internet Security Suite r2	Platinum Internet Security 2006	Bitdefender 9 Internet Security
Manufacturer	Zonelabs	McAfee	Computer Associates	Panda	Softwin
Website	www.zonelabs.de	www.mcafee.com/de	www.blitzbox.de	www.panda-software.de	www.bitdefender.de
Price (one PC, one year)	50 Euros	80 Euros	60 Euros	80 Euros	69 Euros
Upgrade (one PC, one year)	35 Euros	45 Euros	60 Euros	60 Euros	52 Euros
<b>Overall eval. (grade/points)</b>	<b>satisfactory 70,2</b>	<b>satisfactory 68,0</b>	<b>satisfactory 66,8</b>	<b>satisfactory 64,0</b>	<b>satisfactory 63,4</b>
Performance (70%)	satisfactory 63,2	satisfactory 63,5	satisfactory 62,3	satisfactory 56,5	satisfactory 50,8
Features (15%)	good 87,8	satisfactory 79,1	satisfactory 79,1	satisfactory 79,1	very good 92,2
User-friendliness (15%)	good 85,1	satisfactory 77,7	satisfactory 75,8	good 83,8	very good 93,1
<b>Summary</b>	<b>Moderate overall performance, option of inquiry e-mail to sender if message cannot be unambiguously identified.</b>	<b>Very good at detecting fraudulent e-mails, otherwise average performance, high false positives rate.</b>	<b>Low detection rate, few false positives and good integration into Outlook and Outlook Express.</b>	<b>Lowest detection rates in test, but very few false alarms; limited configuration options.</b>	<b>Highest false positives rate in the test, limited success in detecting spam and phishing e-mails.</b>

Metrics					
Spam detection rate	78,8 Percent	83,6 Percent	75,9 Percent	68,4 Percent	82,8 Percent
Phishing e-mail detection rate	85,0 Percent	98,6 Percent	84,9 Percent	80,4 Percent	84,2 Percent
False positives rate	0,4 Tenth of a percent	1,3 Tenth of a percent	0,3 Tenth of a percent	0,1 Tenth of a percent	1,3 Tenth of a percent

Functionalities					
POP3/IMAP proxy	yes/yes	yes/no	yes/yes	yes/yes	yes/no
Plug-in for e-mail clients	Outlook, OE	Outlook, OE, Eudora, Netscape	Outlook, OE	Outlook, OE	Outlook, OE
Adjustable spam tolerance	yes	no	no	no	yes
Spam detection methods	Bayesian filtering, blacklist, URL/charset/graphics filters, online spam signatures	Filters, URL/charset/graphics filters, local spam signatures, Sender Policy Framework (SPF), white-/blacklist	Bonded Sender method, Sender Policy Framework (SPF), whitelist	Bayesian filtering, URL filter, local and online spam signatures, RBL, white-/blacklist	Bayesian filtering, URL/charset filters, graphics, heuristics, local and online spam signatures, white-/blacklist

Spam detec. methods					
Supported operating systems	Windows 98 SE/Me/2000/XP (018 05) 33 97 90 <sup>4)</sup>	Windows 98/Me/2000/XP (09 00) 110 14 86 <sup>5)</sup>	Windows 98 SE/Me/2000/XP (09 00) 100 03 86 <sup>5)</sup>	Windows 98/Me/2000/XP keine	Windows 2000 SP4/XP (075 42) 94 44 60
Hotline					
E-mail support/form	emea_support@zonelabs.com	info_Deutschland@mcafee.com	support@blitzbox.de	technik@panda-software.de	support@bitdefender.de

<sup>1)</sup>includes Norton Internet Security 2005 for Windows 98/Me <sup>2)</sup>4.09 cents per minute <sup>3)</sup>62 cents per minute <sup>4)</sup>12 cents per minute <sup>5)</sup>1.50 euros per minute <sup>6)</sup>9 a.m.. to 6 p.m.: 59 cents per minute, 6 pm to 9am: 2.5 cents per minute