Anti-Spam Test

Anti-Spam Test
(Consumer Products)

Language: English

March 2016
Last Revision: 20th April 2016

Commissioned by PC Magazin

www.av-comparatives.org

Table of Contents

Tested Products

The following products were tested in March 2016 for their ability to filter out spam emails. We always used the most up-to-date product version available. The selection of tested products is based on suggestions by the German computer magazine *PC Magazin*.

- Avast Internet Security 2016
- AVG Internet Security 2016
- Bitdefender Internet Security 2016
- BullGuard Internet Security 16.0
- ESET Smart Security 9.0
- F-Secure Internet Security 2016
- G Data Internet Security 2016
- Kaspersky Internet Security 2016
- Lavasoft Ad-Aware Pro Security 11.1
- McAfee Internet Security 2016
- Microsoft Outlook 2013
- SuperSpamKiller Pro 6.30
- Symantec Norton Security 22.6

Introduction

Spam can be defined as unsolicited emails sent *en masse*[1]. These may be sent for advertising purposes, in which case they may be seen as irritating but harmless. However, many spam mails are clearly malicious. They may attempt to deceive the recipient into sending money to the scammer; typical examples are pretending to be a friend or relative who has lost their wallet while abroad, and so needs money to get home, or claiming that by paying a relatively small administration fee, the recipient will receive a much larger sum as lottery winnings. Other malicious spam emails may contain links to phishing pages or malware, or simply include malware as an attachment. The Spamhaus Project explains the difference between spam and legitimate bulk email[2]. Users should note that not all emails they regard as unwanted can necessarily be defined as spam. We ensured that all the mails used in our test *are* indisputably spam, please see details of the test procedure below.

Research by Kaspersky Lab in 2012[3] suggested that overall spam might be falling due to an increase in legal advertising opportunities on the web, resulting in a reduction of non-malicious advertising spam.

Recent research by Trend Micro[4] finds a more sinister reason for the reduction in overall spam levels. It suggests that malicious spam mails are now being more carefully targeted at specific known addresses, rather than using an email address generator that will produce huge numbers of potential email addresses, many of which will not actually exist in practice.

Another 2015 report, in this case from Symantec[5], notes that spam affecting business users is currently at a 12-year low. Whilst this sounds encouraging, we note that the analysis is based on the percentage of all emails received by business that have been classified as spam; this might mean that fewer spam mails have been sent, or that more legitimate mails have been sent, or some combination of the two.

The aim of this test is to provide readers with a guide to the effectiveness of some popular consumer programs with antispam features. Please consider the following limitations of the test, which focuses only on the spam-filtering capabilities of the products tested. It does not consider any other features of the products (such as malware detection); however, as 12 of the 13 products tested include malware protection, it is possible that some spam mails containing malware attachments were deleted by a product's antimalware feature before they could be marked as spam.

The test was performed in March 2016 under Microsoft Windows 7 SP1 64-Bit (English), using Microsoft Outlook 2013 as the email client. Over 127,000 spam mails were used for this test.

---

[1] https://www.spamhaus.org/consumer/definition/
[2] https://www.spamhaus.org/whitepapers/mailinglists/
[3] https://securelist.com/analysis/kaspersky-security-bulletin/36843/kaspersky-security-bulletin-spam-evolution-2012/#2
[4] http://blog.trendmicro.com/the-decline-of-email-spam/
[5] http://www.informationweek.com/software/enterprise-applications/spam-hits-12-year-low-symantec-report-finds/a/d-id/1321367

Test procedure

In 2015, we tested the products (with default settings) internally over a 6-month period, using spam mails provided by Abusix[6]. Vendors received examples of misses, to check that our testing methods work, and to provide feedback. Several products had very low scores in the internal test run, and several bugs in the spam-filters and products were discovered and had to be fixed by the vendors. In some cases, poorly-performing third-party spam-filters were fixed or even replaced. In March 2016, we ran this public test.

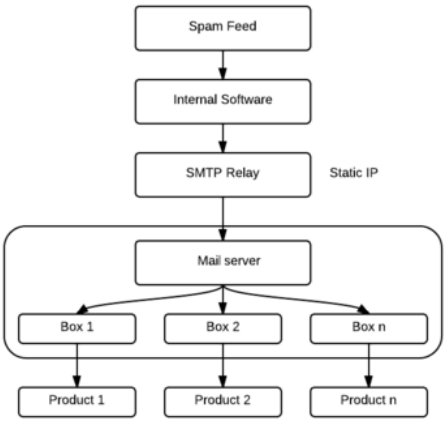
With any detection test (including spam detection), it is important to test for false alarms. In this case, it should be considered that some programs automatically increase their sensitivity when spam mails make up a large percentage of total mails received. We conducted a short-term false alarm test for this report, by running each product for one week on a customer machine and inspecting afterwards if there were legitimate mails classified wrongly as spam (there were none for any of the products tested). A large-scale test with genuine emails would be impossible without breaching privacy; although this was not as statistically significant as we would like, we feel this was sufficient to demonstrate that none of the tested programs was prone to FPs.

In the review of each program, we have checked to see if it adds its own tools to the Outlook ribbon, whether any configuration is needed to activate the antispam component, and what settings can be changed. We also looked for an option to clean the Inbox of any spam mails that were received before the product was installed/activated.

Readers should note the following points:

- We tested consumer products (almost all other antispam tests involve corporate antispam software)
- The products we tested were not allowed any form of training
- We disabled Outlook's own spam-filtering feature on test machines running an additional antispam product
- Any pre-filtering done by email-service providers (like Gmail, Yahoo, etc.) is not taken into account

Overview



[6] https://abusix.com

Environment

Each product receives emails from a POP3 mailbox (one mailbox per product, exclusive access). The products can use the domain and IP-address information in the received header of each mail; however, as the emails are provided by one SMTP relay with a fixed IP address, the address of the relay cannot be used for spam filtering.

Sent Emails

Emails are collected and transferred by Abusix. The spam feed is then pre-filtered (only valid emails are taken). All emails are forwarded without any changes to the main text, but the headers are rewritten, so that it appears to the receiver that the mail has been sent directly. The original recipient is replaced by the email address of the tested product, such as "Recipient <product_id@internal_server.tld>". All other fields remain untouched and are used as they come from the spam traps. Mails which had corrupted headers etc. – for whatever reason – were not counted in the results. Some of the emails in the Abusix spam feed have been anonymized (e.g.: xxx@xxx.xx or alice@xxx.xx). Such emails are also not used for testing. Only emails from senders with a full and valid email address are taken for the test. We also removed emails which did not contain at least one Received field with an IP address in the header.

After filtering, the resulting set of emails is larger than is required for the test; mails for the feed are selected at random at the rate of one every three minutes.

Additionally, the following lines will be added by the intermediate mail server:

```
Delivered-To: product_id@internal_server.tld
X-Original-To: product_id@internal_domain.tld
Return-Path: <sender@internal_server.tld>
Received: from localhost (internal_domain [ww.xx.yy.zz]) by
server1.internal_domain.tld (Postfix) with ESMTP id unique_id for
<product_id@internal_domain.tld>; Thu, 13 Feb 2014 16:33:51 +0100 (CET)
```

The following conditions apply:

- Product ID ... unique ID for each participating product.
- internal_server ... the hostname of the mail server
- internal_domain ... the domain to which the mails will be delivered
- unique_id ... unique id for each mail (will be generated by the mail server)
- Timestamp in the "received header" ... the time the mail is received by the mail server

127,800 spam mails have been used for this one-week test.

Sources of spam emails

The spam mails for this test were provided by Abusix, who provide the following explanation of their spam-collecting procedure[7]:

"Abusix has a huge network with several domains and thousands of email accounts. The spamtraps we generate within this network are administrated entirely by us. We do not use traps from other parties. The email addresses and the domains have never been used for any purpose other than for traps. No signups or subscriptions have ever been made with these addresses. Therefore, every email that hits these traps is a 100% spam. Senders that send to these addresses have likely found the domains registered within the domain whois, and then automatically created a range of similar email addresses, and started to send. This spam technique used by spammers is called "dictionary attack". Another way we use to spread email addresses are different types of harvester techniques. Regardless of the method, both identify non-permitted spam behavior in a precise and reliable manner."

Future tests

Home Users

Several vendors are thinking of removing the antispam feature from their consumer security products, as nowadays most users make use of webmail or mobile apps, and most antispam products/components work only with dedicated desktop email clients (SuperSpamKiller Pro is the only exception amongst the products in our test). Additionally, most consumer email service providers filter spam mails both as they are sent and as they are received. The same is true of hosted email services for business.

Corporate / Business Users

However, many companies still run their own email servers, which do not benefit from any sort of cloud-based antispam services. Antispam products and services for such in-house mail servers are as relevant as ever, and security-software vendors are concentrating on this area. So, future antispam tests will focus on such products. Enterprise products are typically a lot more functional than consumer products and often work at a different layer in the network.

[7] https://abusix.com/faq.html#a4

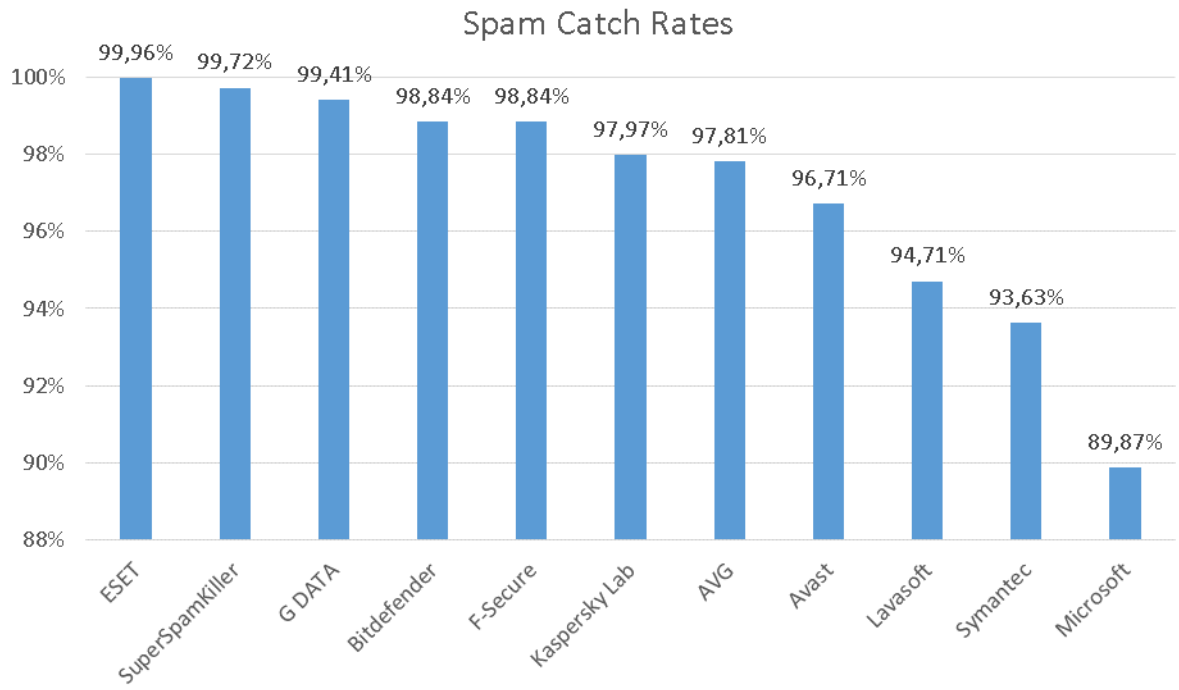
Results

This test provides a guide to the anti-spam capabilities included in popular Internet security products.

Below are the spam catch rates observed during the test. Microsoft Outlook provides its own spam filter, the score for which is included in the table below. We have not included the scores for products which scored below it, i.e. which were lower than the baseline[8].

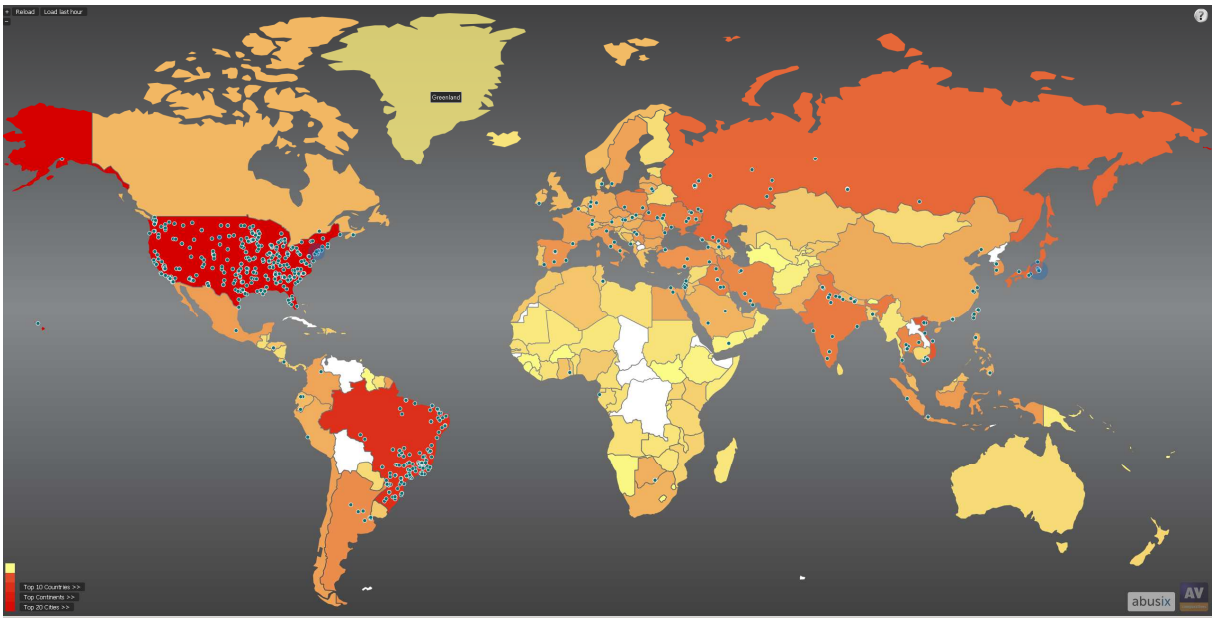
1.	ESET	99.96%
2.	SuperSpamKiller	99.72%
3.	G DATA	99.41%
4.	Bitdefender, F-Secure	98.84%
5.	Kaspersky Lab	97.97%
6.	AVG	97.81%
7.	Avast	96.71%
8.	Lavasoft	94.71%
9.	Symantec	93.63%
10.	Microsoft Outlook	89.87%

Graphic



[8] McAfee and BullGuard scored below Microsoft Outlook.

AV-Comparatives Spam Map



This map shows the origin of spam attacks captured by the spam traps. The background colour of each country represents the total number of spam mails sent, with the scale in the bottom left-hand corner showing the range from yellow (least spam mails) to dark red (most spam mails). The blue markers on the map represents the latest incoming spam sources (above example map shows the last one hour).

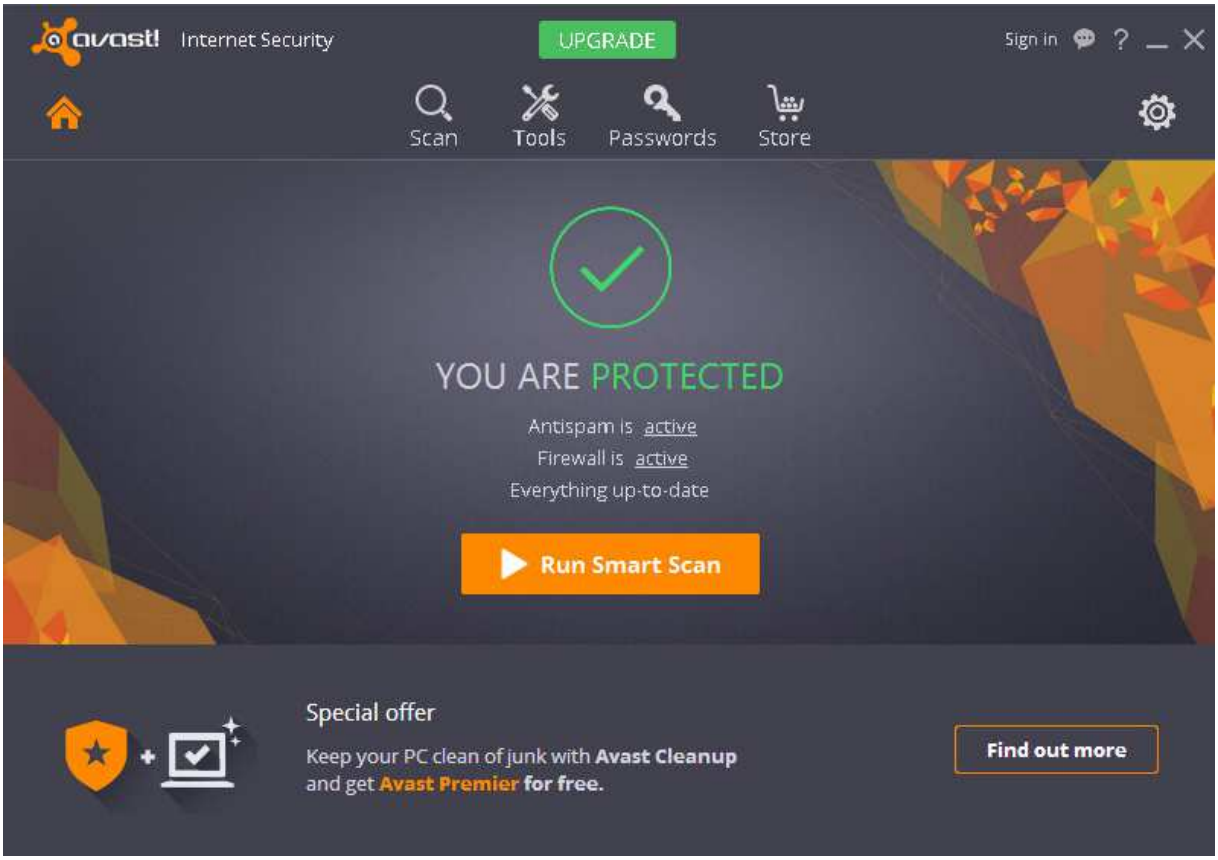
There is an interactive version of the Spam Map on our website: http://spammap.av-comparatives.org. In this version, the text links in the bottom left-hand corner (which are not related to the colour scale) provide additional information; click on a link to display details of the topic.

According to the above map[9], the **Top 10 Spam Countries** are:

1.	USA	40.3%
2.	Brazil	15.6%
3.	Vietnam	5.4%
4.	Russia	3.8%
5.	Japan	3.3%
6.	China	3.2%
7.	Hong Kong	3.0%
8.	India	2.0%
9.	Ukraine	2.0%
10.	Taiwan	1.5%

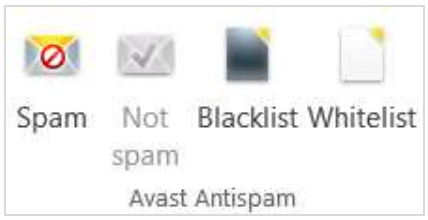
[9] As of March 2016 (based on a sample set of over 500,000 spam mails).

Avast Internet Security



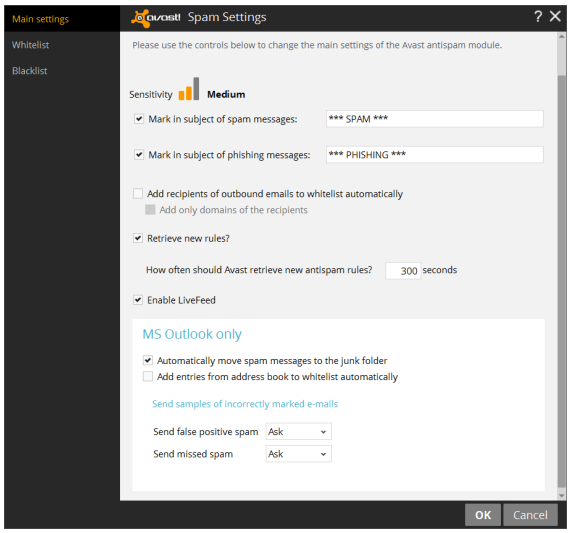
User interface

Avast Internet Security adds a group to the Home tab of the Outlook Ribbon:



Configuration

The antispam component is activated by default. Under Settings/Active Protection/Antispam in the main window, whitelists and blacklists can be managed and options set:



In our test, the *automatically move spam messages to the junk folder* option worked as expected – mails from blacklisted addresses were moved to the spam folder.

Cleaning the Inbox

We could not find a means of cleaning up mails that have already been downloaded. Blacklisting a mail from a particular address only deletes this particular mail. Other mails from that sender stay in the inbox.

Help

The *?* symbol in the top right-hand corner of the main program window opens a context-sensitive help page, which just refers to the screen visible at the time. There is an FAQ on the manufacturer's website, although we could not find any articles relating to the Antispam component.

Conclusion

Avast Internet Security's Antispam component requires no initial configuration. However, we were not able to retrospectively clean up spam mails already received, and the option to move spam mails to the Outlook Junk E-mail folder appears not to work. The program blocked 96.71% of unwanted messages in our spam-filtering test.

AVG Internet Security

User interface

AVG Internet Security adds a group to the Home Tab of the Outlook Ribbon:

This allows individual mails to be registered as Spam or Wanted, and the AVG main program window or Anti-Spam configuration page to be opened. We could not find a means of blocking a sender or domain from within Outlook, only by going to the Anti-Spam configuration page and manually entering addresses to be blocked.

Configuration

AVG's Anti-Spam module does not require configuration before it can be used.

Cleaning the Inbox

We could not find a means of retrospectively cleaning the Inbox.

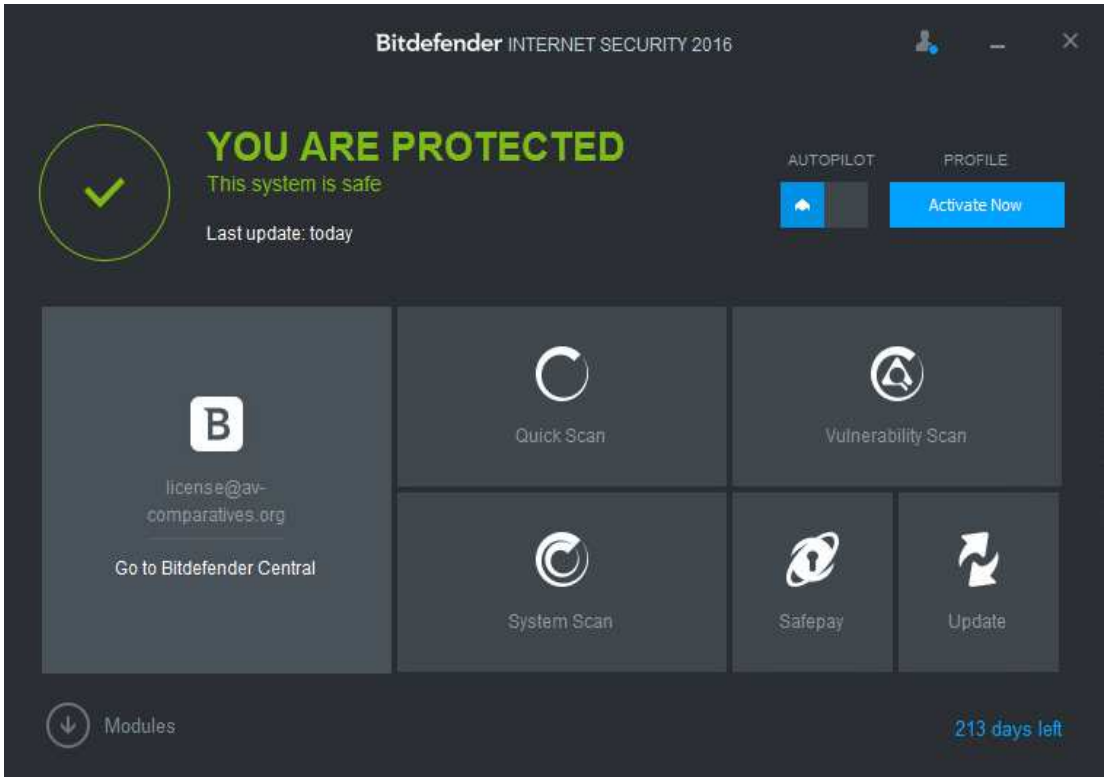
Help

Clicking the *?* symbol on the main window or configuration page provides context-sensitive help as a Windows Help file. This explains the features available on the current page, but does not easily let the user find a particular page in the first place. There is also an online FAQ page; searching this page for "blacklist" turns up results for using the suite's blacklisting functions.

Conclusion

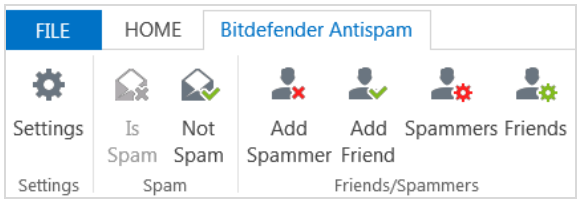
AVG Internet Security is very easy to install and no configuration of the email account is required. However, it is not possible to retrospectively clean up spam mails already received. The program blocked 97.81% of unwanted messages in our spam-filtering test.

Bitdefender Internet Security



User interface

Bitdefender Internet Security adds its own tab to the Outlook Ribbon:



The *Is Spam* button allows individual mails to be marked as spam, which moves them to a Spam subfolder of Outlook's Deleted Items folder. When the Deleted Items folder is emptied, all the mails in the Spam subfolder are permanently deleted. The *Add Spammer* button marks an address as a spam sender, meaning further mails from this address are all treated as spam. *Spammers* and *Friends* allow blacklists and whitelists, respectively, to be managed.

Configuration

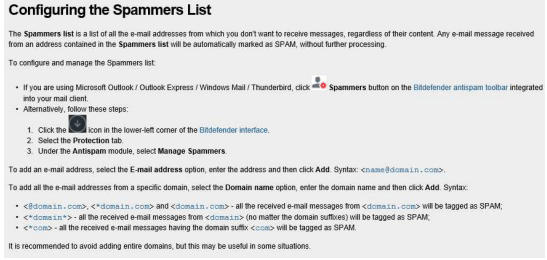
No initial configuration is required. Blacklist and whitelist management, as well as the possibility to turn on/off Asian and Cyrillic charset filters, are the only significant configuration options available.

Cleaning the Inbox

We could not find a means of cleaning spam mails already in the Inbox.

Help

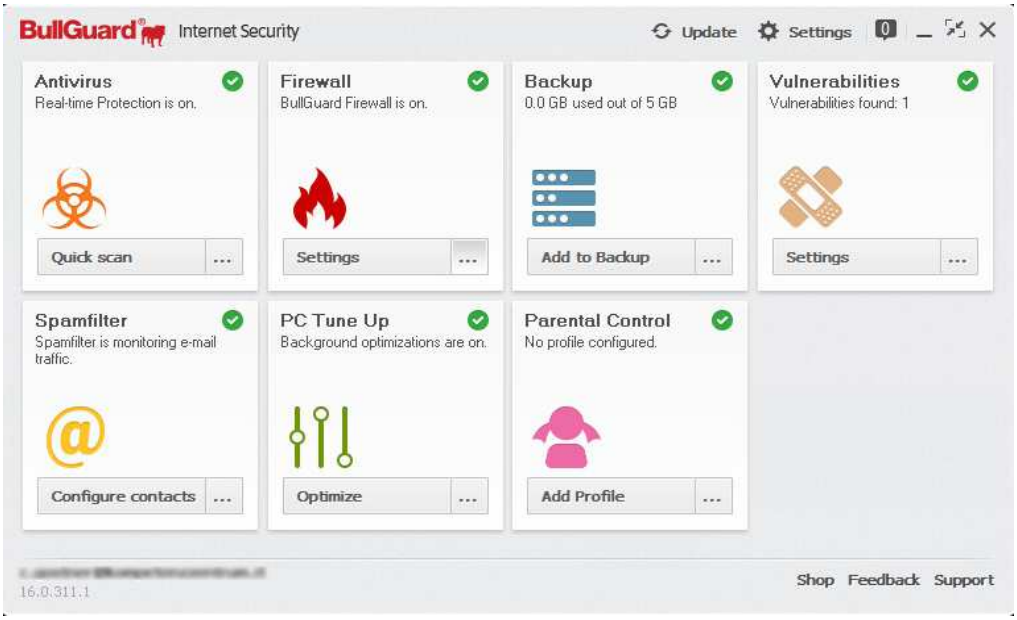
Clicking *Help and Support* in the menu of the main program window provides access to the online knowledge base in HTML format. This provides simple but effective instructions for configuring the product:



Conclusion

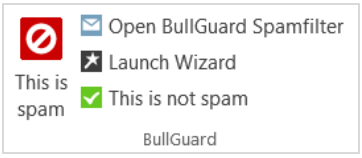
Setting up Bitdefender Internet Security is very simple. Whilst configuration options are not extensive, we found that defining spam and blacklisting addresses was made easy. The program blocked 98.84% of unwanted messages in our spam-filtering test.

BullGuard Internet Security



User interface

BullGuard adds a group to the Outlook Ribbon:



The *Launch Wizard* button starts a spam-training wizard, which asks the user to point to folders known to be spam-free, and a folder containing only spam mails. *Open BullGuard Spamfilter* opens the main program window at the configuration page for the spam filter. The other two buttons allow mails to be marked as spam or non-spam. Although there is no explicit way of blacklisting addresses from within Outlook, we found that having marked a few mails from one address as spam, further emails to this address were automatically treated as spam.

Configuration

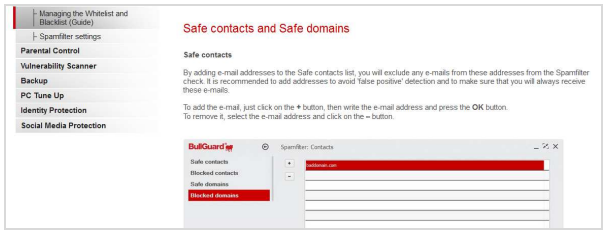
No initial configuration is necessary; the feature is activated by default. Minor options, such as which folder to send spam mails to, can be configured in the main program window's configuration page. Addresses to be blacklisted or whitelisted can be entered by clicking *Configure contacts* in the *Spamfilter* tile of the main program window. In this window it is also possible to add safe and blocked domains to the *Spamfilter*.

Cleaning the Inbox

We could not find a means of removing spam mails that had already been received.

Help

Clicking the *Support* button in the bottom right-hand corner of the main program window opens the program's online support pages. These provide illustrated instructions for configuring the various features:



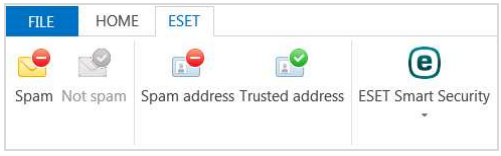
Conclusion

BullGuard is very simple to set up, and spam mails can easily be marked in the Outlook Inbox. The program identified (in its default settings) fewer unwanted messages than Microsoft Outlook in our spam-filtering test.

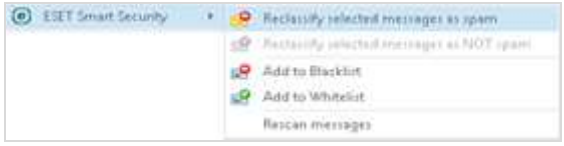
ESET Smart Security

User interface

ESET adds its own tab to the Outlook ribbon. This allows individual mails to be designated as spam or not, and addresses to be designated as spam or trusted:



The ESET Smart Security menu provides additional options, including rescanning messages and Antispam setup. Additionally, ESET adds its own sub-menu to Outlook's email context menu (shown when a mail is right-clicked):



Configuration

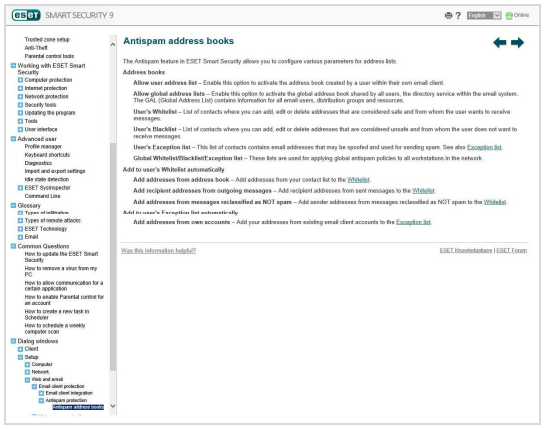
Whilst some options are available for the anti-spam component, such as changing the subject line and moving spam mails to a different folder, no configuration is necessary to make the service work.

Cleaning the Inbox

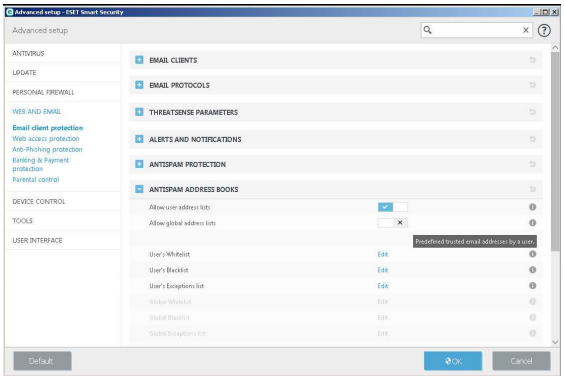
This can be done by selecting *Rescan messages* from the ESET Smart Security menu, with the option *Rescan already scanned messages*. Messages from blacklisted addresses will then be moved to Outlook's Junk E-mail folder.

Help

The online help service, which can be opened from the *Help and Support* page of the main program window, provides simple text instructions for marking mails as spam, or blacklisting and address, along with an overview of the component's configuration page:



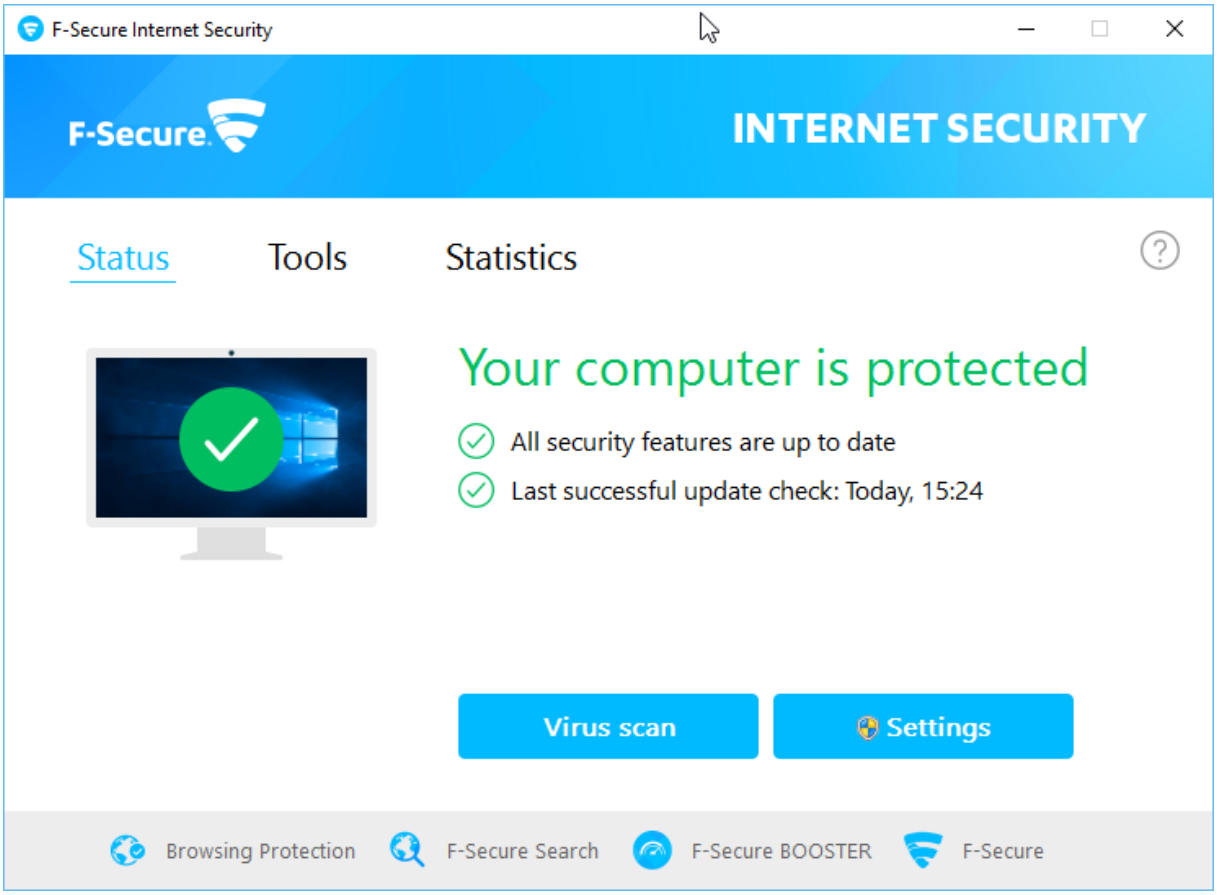
The program has some local help features in form of small „i“ icons as well:



Conclusion

We found the integration of ESET Smart Security into Outlook to be very simple but effective, allowing easy marking of mails or addresses as spam. The program blocked 99.96% of unwanted messages in our spam-filtering test, the highest score of any product tested.

F-Secure Internet Security

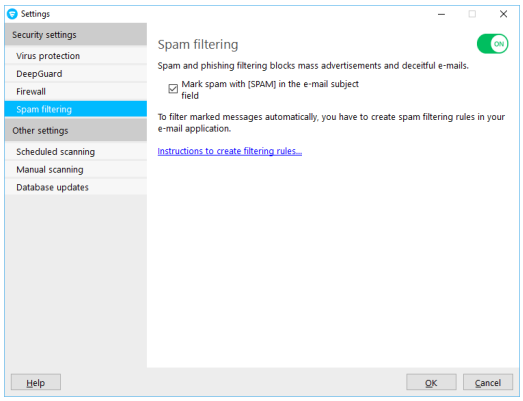


User interface

The antispam component is not configurable. The program has no Outlook integration or blacklist/whitelist.

Configuration

The Spam Filtering component is not activated by default. It has to be enabled in the settings of the main application. Mails which are declared to be spam are marked with *[SPAM]* on the beginning of the subject line but remain in the Inbox. The user has to create a rule in Outlook itself that moves the marked mails to a different Folder.

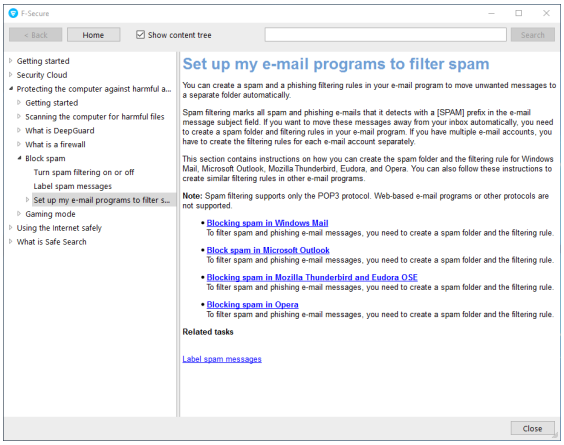


Cleaning the Inbox

We could not find a means of retrospectively cleaning the Inbox of spam that had already been delivered.

Help

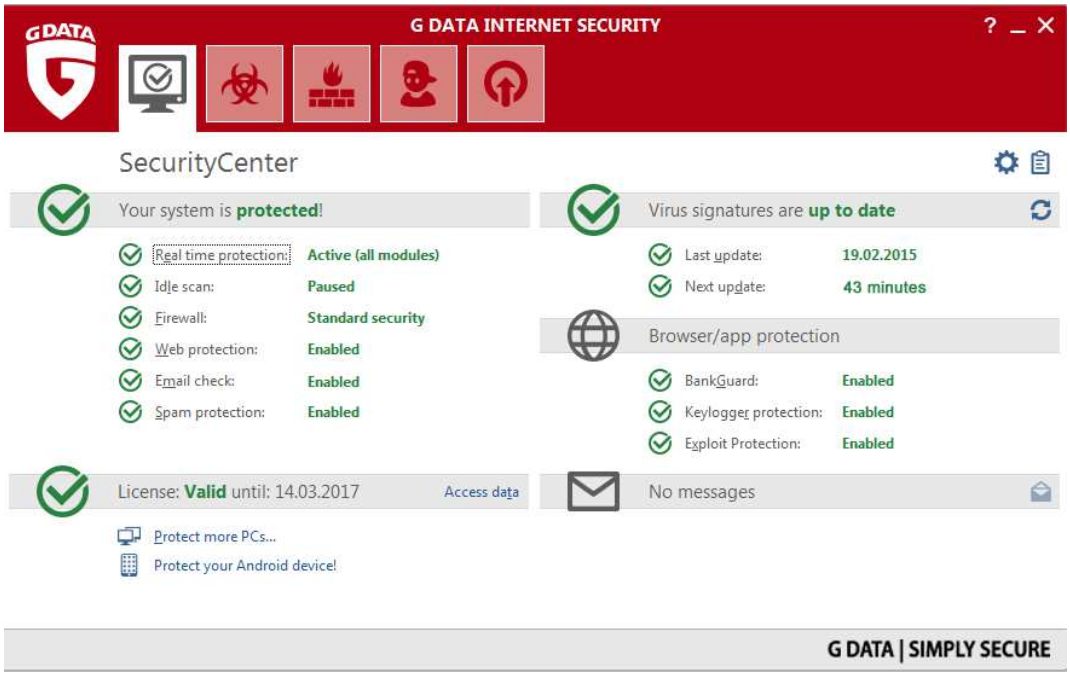
Clicking *Help* in the *Spam Filtering* tab opens the program's context sensitive knowledge base. This is a local, detailed guide to each available setting.



Conclusion

The Antispam Component of F-Secure is easy to set up, but has no configuration options. The program blocked 98.84% of unwanted messages in our spam-filtering test.

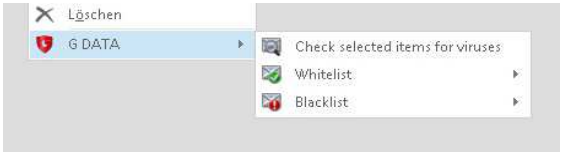
G DATA Internet Security



User interface

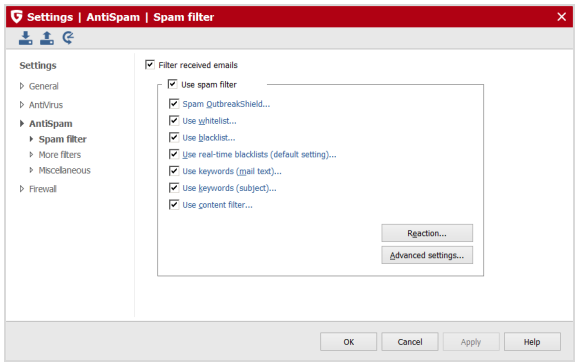
G DATA adds its own context-sensitive tab to the Outlook Ribbon. When an email is selected in the Inbox or other folder, the following buttons are displayed:

The Blacklist and Whitelist menus both have options to apply the action to the sender's address or the entire domain. The same commands are also available in an add-on to Outlook's context menu, accessed by right-clicking an email:



Configuration

No configuration is required to start using the spam-protection component. Details can be tweaked by clicking *Spam Protection* | *More Settings* in the program's main window:

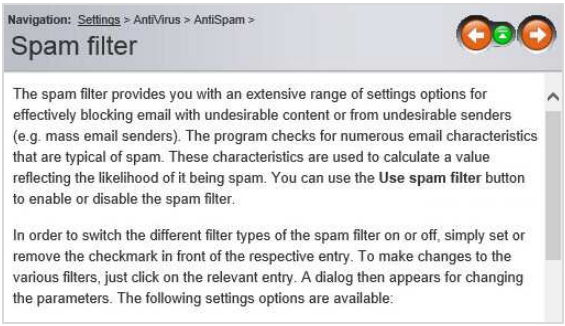


Cleaning the Inbox

We could not find a means of retrospectively cleaning the Inbox of spam that had already been delivered.

Help

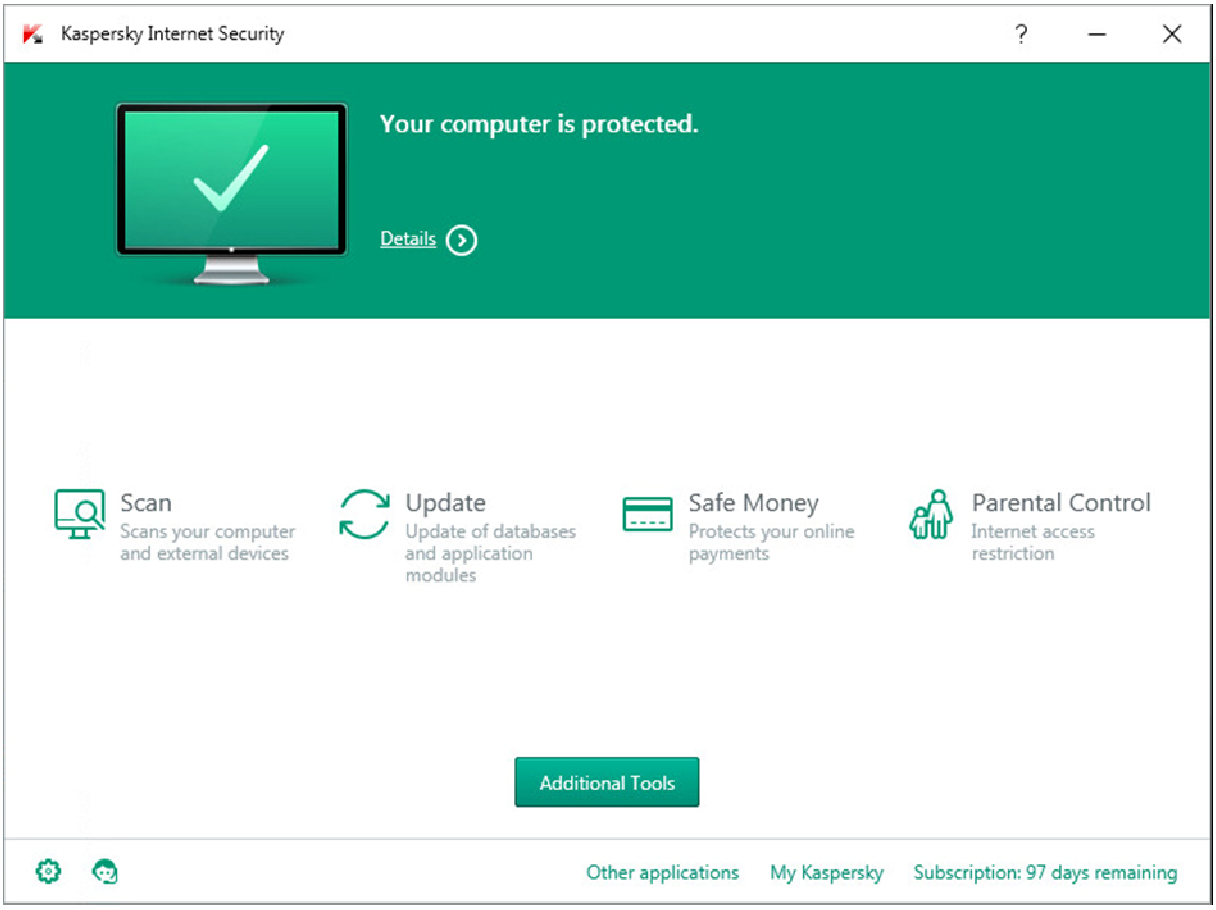
Clicking *Help* in the bottom right-hand corner of the Spam Filter Settings dialog opens the program's online knowledge base at the relevant page. This provides simple text explanations of the options available:



Conclusion

G DATA Internet Security is easy to set up, and its most important anti-spam controls are easily accessible from the Outlook Ribbon or context menu. The program blocked 99.41% of unwanted messages in our spam-filtering test, the third-best result out of all the products tested.

Kaspersky Internet Security



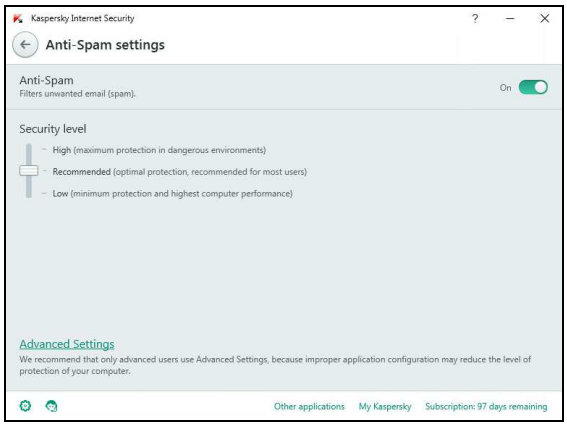
User interface

Kaspersky integrates a context-sensitive Anti-Spam component into the Home tab of the Outlook Ribbon. It is possible to mark individual emails as spam or not spam.

Selecting a mail in the Inbox and clicking *Mark as Spam* sends the message to Outlook's Junk E-mail folder, but does not add the sender's address to the blacklist.

Configuration

The anti-spam component is not enabled by default. It can be activated by going into the settings of Kaspersky Internet Security, *Protection*, and switching the slider switch for *Anti-Spam* to on. The user can choose from three protection levels:

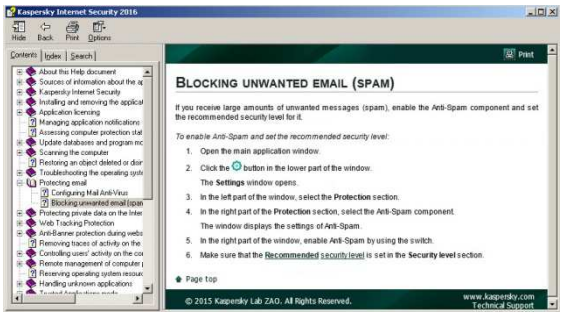


Cleaning the Inbox

There is no means of cleaning spam mails that have already been downloaded.

Help

Clicking the *?* symbol in the top right-hand corner of the KIS window opens the local help file. This contains simple instructions for activating the anti-spam component:

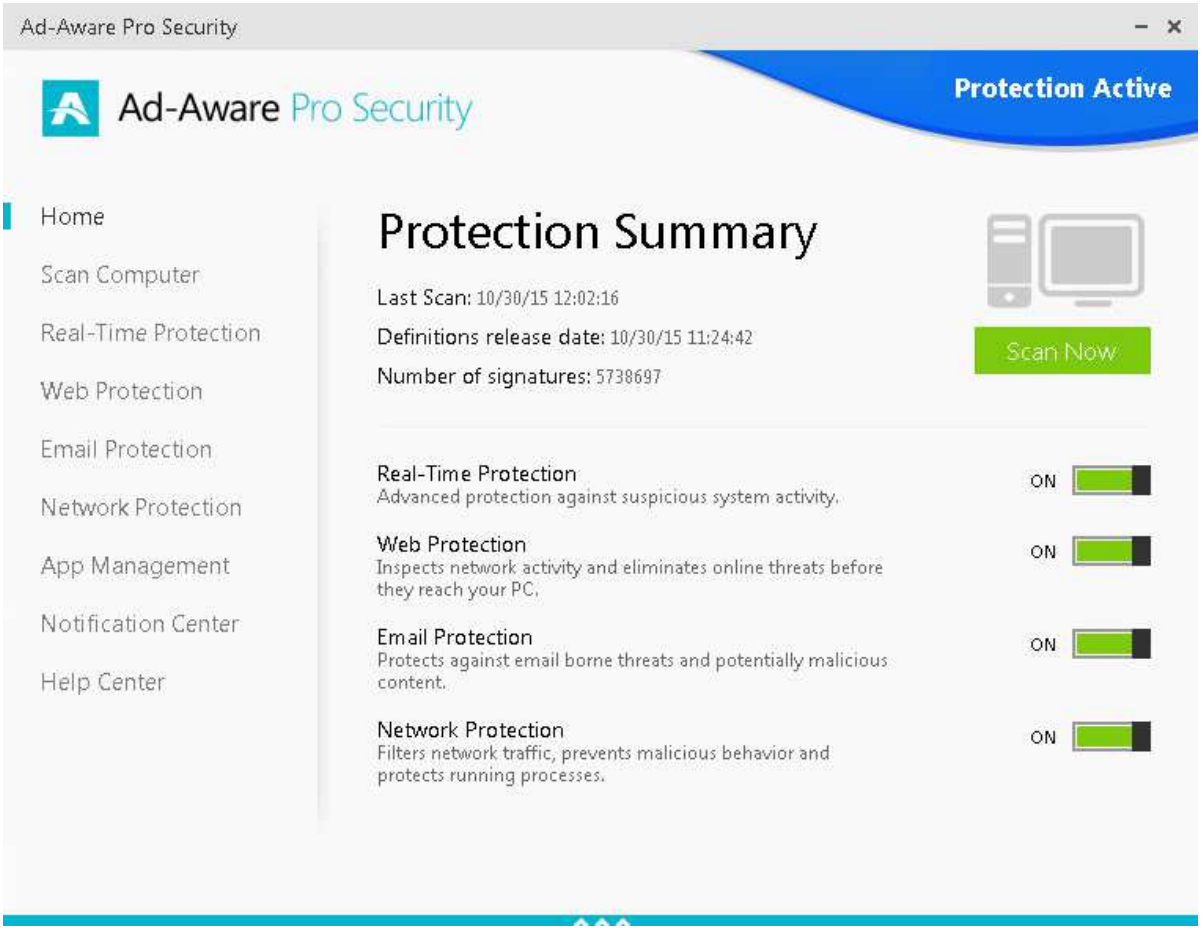


Conclusion

Kaspersky Internet Security's anti-spam component is not activated by default, although the help file explains how to do this. The integration with the Outlook window provides an easy way to mark mails as spam. The program blocked 97.97% of unwanted messages in our spam-filtering test.

Kaspersky Lab inform us that according to their statistics, Internet users today extremely rarely use desktop mail clients and Anti-Spam feature correspondently. This feature was switched off by default in consumer products, and was turned on and used in combination with mail client by only one percent of users. So, Kaspersky Lab's efforts required to develop and maintain plugins for mail clients will be focused on other more demanded protection features.

Lavasoft Ad-Aware Pro Security



User interface

The program does not integrate with Outlook.

Configuration

No configuration is required; the component is activated by default. The only possible changes the user can make are to add or remove email addresses from the safe senders list, and choose *Normal, Aggressive* or *Permissive* as the level of email protection.

Cleaning the Inbox

This is not possible, due to the lack of Outlook integration.

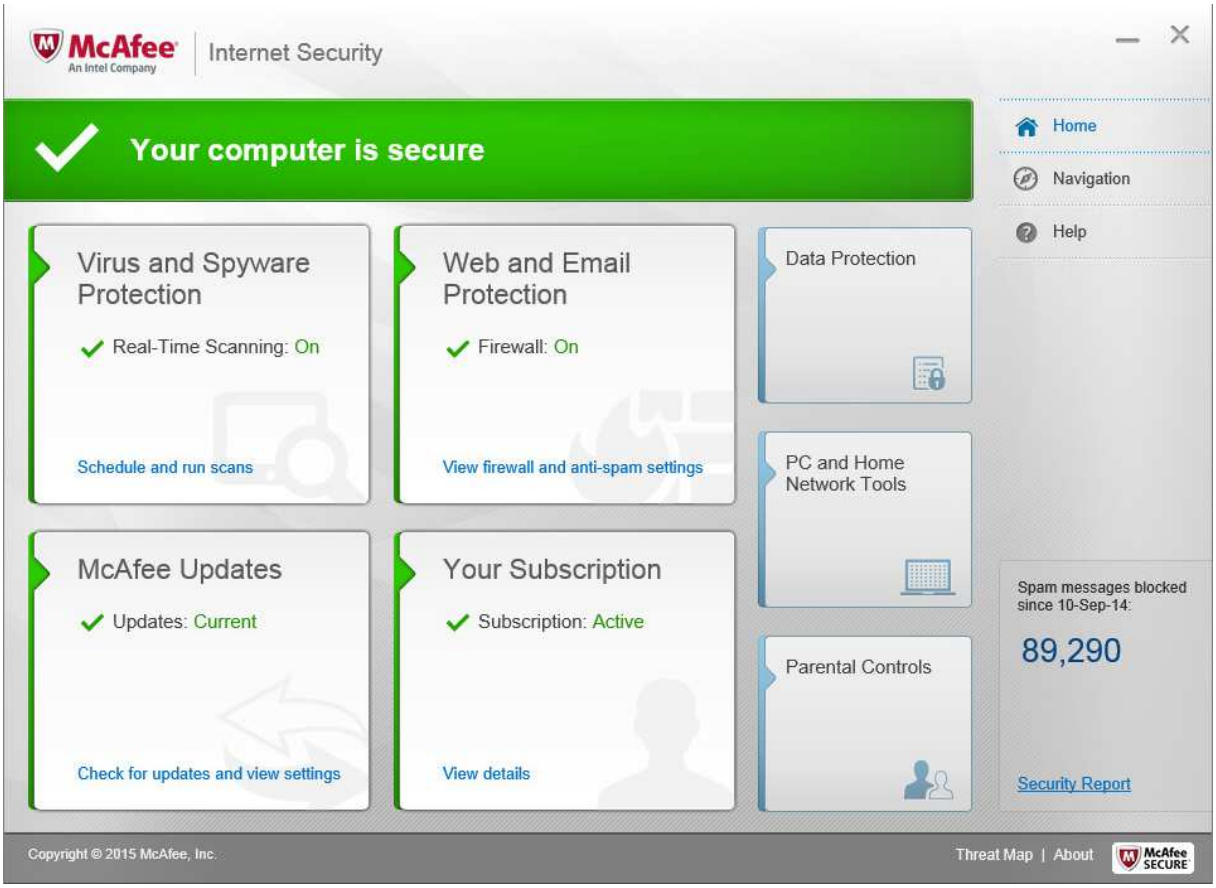
Help

Clicking the *Help Center* entry in the menu panel on the left opens the help and support page, which includes a link to the download page for Lavasoft product manuals. The product manual for Pro Security notes and explains the (minimal) configuration options described above.

Conclusion

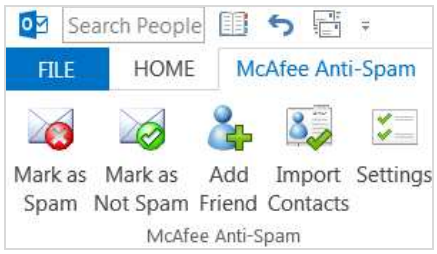
Ad-Aware Pro Security does not provide Outlook integration, and has only minimal configuration options in the program itself. The program blocked 94.71% of unwanted messages in our spam-filtering test.

McAfee Internet Security

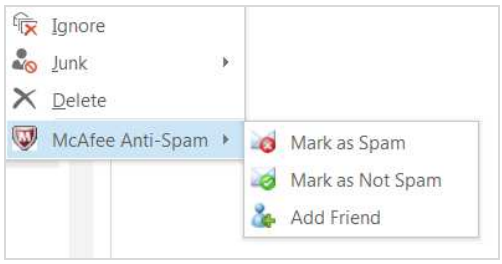


User interface

McAfee makes two additions to the Outlook Ribbon, a Group on the Home tab and an entire tab:



An addition is also made to Outlook's context menu:



All three components of the interface allow mails to be marked as spam or not spam, and the email address to be added to the whitelist. However, it is not possible to blacklist an address here.

Configuration

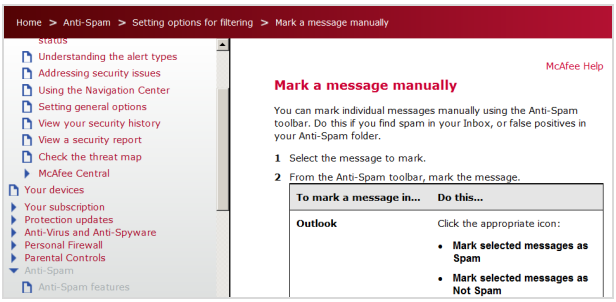
No configuration is necessary; the product starts working after installation. Settings can be customised by clicking the Settings button on the McAfee Anti-Spam tab on the Outlook Ribbon.

Cleaning the Inbox

We could not find a means of cleaning up spam messages that have already been downloaded.

Help

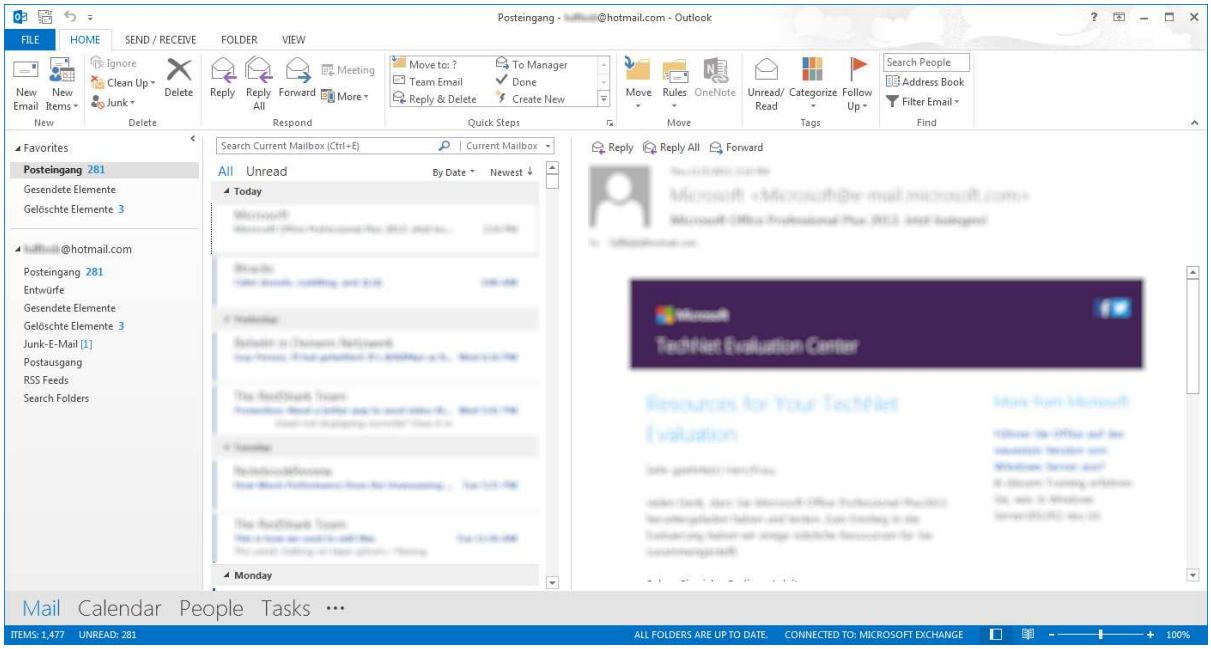
Clicking the *Help* link in the main program window allows the user to open the online help pages. These provide simple text instructions for a wide range of topics:



Conclusion

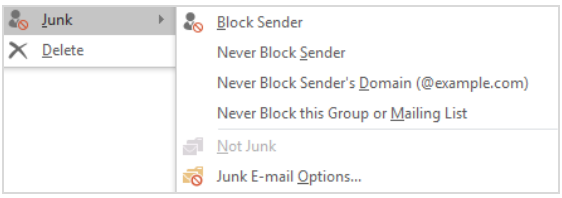
McAfee Internet Security is easy to install, and no additional configuration is required. Abundant add-ins make it easy to access the important features from within Outlook. The program identified (in its default settings) fewer unwanted messages than Microsoft Outlook in our spam-filtering test.

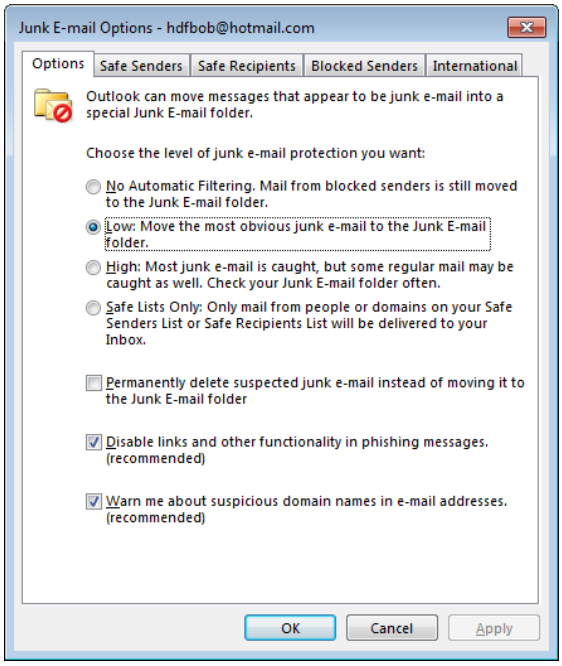
Microsoft Outlook 2013



User interface

The antispam features of MS Outlook 2013 can be accessed by using the *Delete* section in the *Home* tab in the Ribbon, or from the context menu shown when a mail is right-clicked:





Configuration

No initial configuration is necessary; the feature is activated by default. Options like blocking the sender of the mail or whitelisting the sender's domain are possible via the context menu. The Settings can be accessed from *Junk-E-Mail -> Junk-E-Mail -Options*. There are four levels of spam filtering: *No Automatic Filtering*, *Low* (default), *High* and *Safe Lists Only*. At first start Outlook adds all senders in the Sent Items folder to the Safe Senders list. There are some settings for automatic handling of spam messages as well:

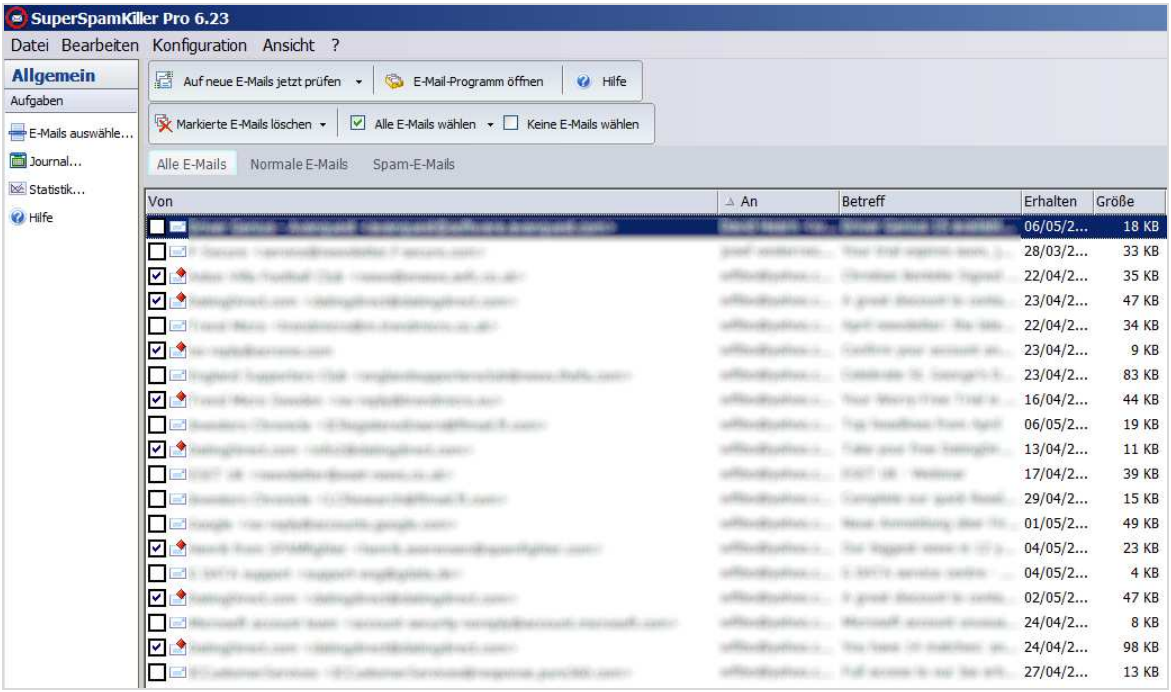
Help

Clicking the question mark button next to the window control on the main page opens the online or local help, depending on the network status of the computer. It includes a search box, making it easy to find the required information.

Conclusion

The integrated Antispam component of Outlook 2013 is very compact but provides most of the features needed. There is no initial set up needed and spam mails can easily be marked in the Outlook Inbox. The program blocked 89.87% of unwanted messages in our spam-filtering test. Microsoft inform us that their spam-filtering work is concentrated on their own mail services (Office 365 and outlook.com) rather than developing antispam features in individual mail client. We included spam-filtering results for Microsoft Outlook as a baseline, i.e. the level of protection a user would have without an additional anti-spam product.

SuperSpamKiller Pro

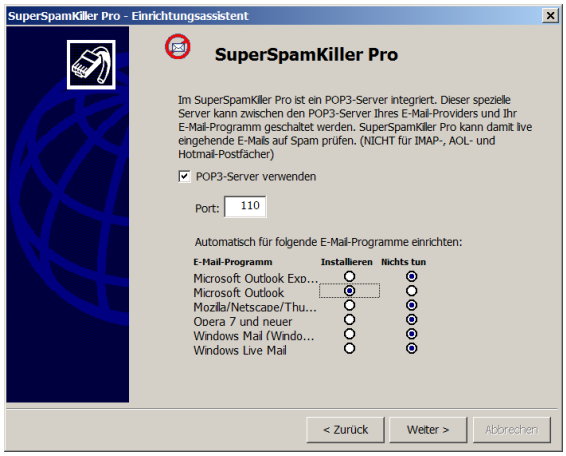


User interface

SuperSpamKiller Pro is only available in German. It is a stand-alone program that allows the user to manage spam before downloading it to Outlook (or other mail client). It is effectively a simple email client in itself, and can even be used to answer or forward mails. The main pane of the program window shows the emails on the mail server waiting to be downloaded; it pre-selects mails it has defined as spam, but lets the user change the selection before deleting.

Configuration

When the actual installation has finished, a configuration wizard starts. This warns that mails deleted by the program are permanently deleted and cannot be recovered. The wizard then asks for the Internet connection type (e.g. direct ADSL connection or via LAN/WLAN), and the email client being used:



The configuration wizard then attempts to import existing email accounts. In our test, this did not work, but we were able to configure the account manually. This requires exactly the same information as setting up an account in Outlook, namely email address, username, password, incoming and outgoing servers etc.

Cleaning the Inbox

As SuperSpamKiller Pro works by deleting spam before it is picked up by Outlook, it is not possible to clean up mails that have already been downloaded.

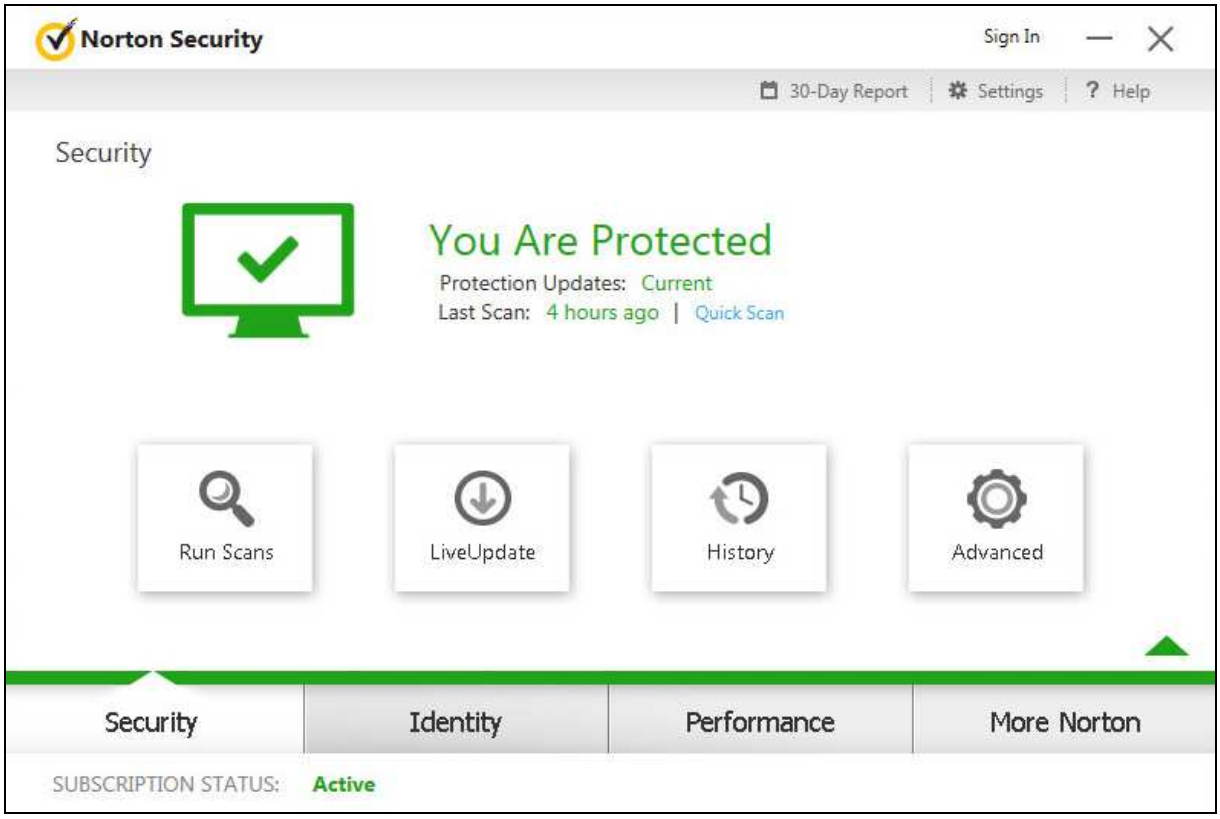
Help

Clicking "*? Hilfe*" (Help) opens a standard Windows Help window, with topics listed in the left-hand pane.

Conclusion

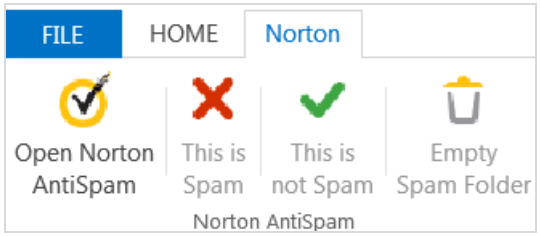
SuperSpamKiller Pro is an independent program that is installed and configured much like an email client, and indeed allows users to answer and forward mails. Some users may find it inconvenient to have to use a separate program window for spam filtering, in addition to the email client. We wonder whether the manufacturers might not try adding some more email-client functionality, such as the ability to compose new mails, meaning that it could be used without a separate email client. The program blocked 99.72% of unwanted messages in our spam-filtering test, putting it into second place.

Symantec Norton Security

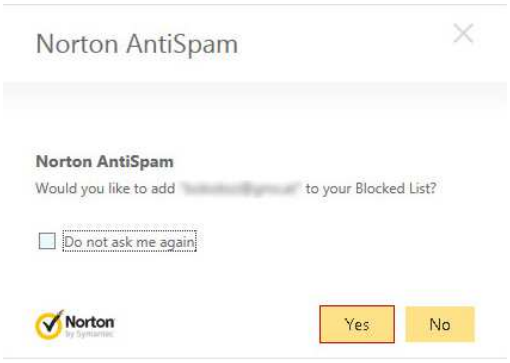


User interface

Norton adds a new tab to the Outlook Ribbon:



Selecting a mail in the Inbox and clicking *This is Spam* sends the message to Outlook's Junk E-mail folder. It also opens a dialog box which lets the user easily add the sender to the *Blocked List*:



Configuration

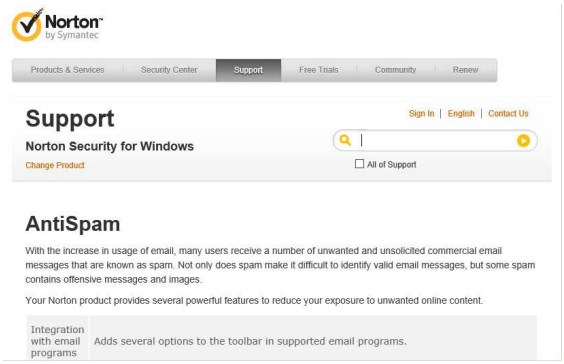
No initial configuration is necessary. Blacklists and whitelists can be managed from the program's configuration page (this can be opened by clicking *Open Norton AntiSpam* on the Outlook Ribbon).

Cleaning the Inbox

We could not find a means of cleaning spam already in the Inbox.

Help

Clicking the *?* icon on the AntiSpam Settings page of the program opens the online support page for the AntiSpam component, which explains the features and settings of the anti-spam component:



Conclusion

We found Norton Security to be simple to install and use. The program blocked 93.63% of unwanted messages in our spam-filtering test.

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives (April 2016)