User Guide

Table of Contents

Chapter 1 – Getting Started

Welcome to McAfee.com SpamKiller.

McAfee.com SpamKiller is a software service that helps stop spam from entering your e-mail inbox.

With it, you get the following features:

- Block spam using filters
- Monitor and filter multiple e-mail accounts
- Quarantine spam outside of your inbox
- Import friends' addresses into the Friends List
- Create custom filters
- Update filters automatically
- Fight back against spammers

New Features

This version of SpamKiller provides the following new features

- **MSN/Hotmail protocol support**
  SpamKiller now filters MSN/Hotmail e-mail accounts and imports MSN/Hotmail address books into the Friends List.
- **Improved look and feel**
  The new look makes SpamKiller easier to use.
- **Background filter updates**
  SpamKiller automatically checks for new filters once a day and downloads the new filters onto your computer.
- **Decoding of Base 64 encoded text**
  By decoding Base 64 text, SpamKiller expands its ability to block spam.
- **Enhanced Microsoft® Outlook address book support**
  You can now import into the Friends List all SMTP addresses in Contacts, Personal Address Book, and Global Address List. For Contract and Personal Address Book, addresses in distribution lists can be imported.
- **HTML e-mail viewing**
  SpamKiller can view HTML e-mail while blocking scripts and images.
- **Increased filtering speed**
  SpamKiller filters your e-mail accounts faster.

System Requirements

- A POP3, MAPI, or MSN/Hotmail account
- Microsoft® Windows 95, 98, Me, 2000, or XP
- 5 MB of free hard disk space (for installation)
- Microsoft® Internet Explorer 5.0 or higher

  Note: To upgrade to the latest version of Internet Explorer, visit the Microsoft Web site at http://www.microsoft.com/.

Downloading and Installing SpamKiller

Before you can download and install SpamKiller, you must purchase a license from the McAfee.com Web site. The following instructions describe how to purchase a license, as well as install and set up

SpamKiller. The basic set up includes adding an email account for SpamKiller to monitor and importing a list of friends' e-mail addresses. You can choose to perform the basic setup later.

Before installing SpamKiller:

- Save all of your work and close any open applications.
- Make sure your browser is configured correctly. For details, see "Configuring Microsoft® Internet Explorer" in Appendix A.

After you install SpamKiller, you will be prompted to restart your computer. You can restart your computer immediately, or you can restart it later. You must restart your computer before you can use SpamKiller.

To purchase, download, and install SpamKiller:

1. Purchase a license and download SpamKiller:
   a. Go to http://www.mcafee.com/.
   b. Click **Products & Services** on the top navigation bar.
   c. Click **SpamKiller Online** on the left navigation bar.
   d. Purchase a license of SpamKiller.
      After you purchase SpamKiller, you will be prompted to download the product.
   e. Download the product.

   The installation wizard appears. If it does not appear, click **Start**. The Welcome dialog box opens.
2. Click **Next**.
   The License Agreement dialog box opens.
3. Click **Yes**.
   The Readme dialog box opens. The Readme dialog box lists new features in SpamKiller, system requirements for installing SpamKiller, and contact information for online support.
4. Click **Next**.
   The Choose Directory dialog box opens. By default, SpamKiller will be installed to C:\Program Files\McAfee.com\SpamKiller.
5. Click **Next** to install SpamKiller in the default folder. Otherwise, click **Browse** to select another folder.
   If an older version of SpamKiller is already installed on your computer, the installation wizard asks you if you want to install the new version. Click **Yes**. The Start Copying Files page opens.
6. Click **Next** to copy SpamKiller files.
   The Setup Finished page opens when the SpamKiller files are completely copied.
7. To restart your computer now, click **Yes, I want to restart my computer now**, and then click **Finish**. Otherwise, click **No, I will restart my computer later**, and then click **Finish**. You must restart your computer before you can use SpamKiller. If you selected to restart your computer now, your computer will automatically restart. If you selected to restart your computer later, you must restart it manually.

   After restarting your computer, the Getting Started Wizard opens.

8. Click **Next** to continue with the basic setup, or click **Cancel** to perform the setup later.
   The basic setup lets you add an e-mail account for SpamKiller to monitor. Later, you can add more e-mail accounts. The basic setup also lets you import a list of e-mail addresses to your Friends List to prevent them from being blocked.

Setting Up SpamKiller for Initial Use

Select the e-mail program of the e-mail account you want to add:

1. Click **Yes, this is my e-mail program** if the e-mail account you want to add is for the program SpamKiller detected, and then click **Next**. Otherwise, click **No, I want to select another program**, and then click **Next**.
   If you clicked **No, I want to select another program**:
   a. Select an e-mail program in the list, or click **Browse** to select another e-mail program.
   b. Click **Next**.

You can import address books into SpamKiller from the following e-mail programs: Netscape Messenger, Qualcomm Eudora, Microsoft Outlook or Exchange, Microsoft Outlook Express, Pegasus Mail, MSN/Hotmail, and any program that can support its address book as a plain text file. If you do not have a list to import, you can import a list or add individual addresses later.

To import a list of friends' e-mail addresses:

1. Click **Yes, I want to import my address book now** to import a list now. Otherwise, click **No, I want to do this later**.
2. Click **Next**.
3. Select the type of address book you want to import, and then click **Next**.
   A confirmation page shows the number of new e-mail addresses SpamKiller added to the Friends List.
   If SpamKiller cannot find addresses in the address book, "The address book was not found" appears. Click **OK**, and then click **Back**. Select another address book, or add addresses to the book, and import the book again.
4. Click **Next**.

To add an e-mail account for SpamKiller to monitor:

1. Click **Yes, I want to enter information about my e-mail account** to add the account now. Otherwise, click **No, I want to do this later**.
2. Click **Next**.
   The New Account Wizard opens.

If SpamKiller detects more than one e-mail account, a list of the e-mail accounts appears. Follow the steps below:

1. Select an e-mail account you want to add, and then click **Next**.
   You can add more accounts later after SpamKiller is installed. If the e-mail account you want to add is not listed, click **My e-mail account is not listed above**, click **Next**, and then go to step 1 in the next section.
2. Enter the password you use for logging on to the account, and then click **Next**.
3. Click **Test Now** to verify that the account information you entered is correct. Otherwise, click **Next**.
4. Click **Finish**.

If SpamKiller does not detect multiple e-mail accounts, follow these steps:

1. Enter a description of the e-mail account, and then click **Next**.
2. Enter your name and e-mail address, and then click **Next**.
3. Select the type of account for the e-mail address, and then click **Next**.
   - **Standard e-mail account (POP3)**: Local dialup or broadband accounts, where your Internet service provider receives and holds your e-mail. Most home users have this type of account.
   - **MSN/Hotmail account**: MSN/Hotmail web-based accounts.
   - **MAPI e-mail account**: Local network e-mail accounts. Most corporate users have this type of account. Many corporate users have this type of account when their company is running Microsoft® Exchange Server.
4. Enter account information:
   - If you selected Standard e-mail (POP3 account):
     a. Enter the addresses of the incoming e-mail server and the outgoing e-mail server, and then click **Next**.
        In most cases, SpamKiller automatically detects your POP3 settings and pre-populates the incoming and outgoing server fields.

b. Enter your user name and password for the e-mail account.
Your user name is usually the first part of your e-mail address, before the @ sign.
Your password is the password you use to log on to the account.
c. Click **Next**.
If your computer is set to use dial-up connections, the connection type dialog box opens. Select the connection type for your account, and then click **Next**.

- If you selected MSN/Hotmail account:
  a. Enter your user name and password for the e-mail account.
  Your user name is always the first part of your e-mail address, before the @ sign. Your password is the password you use to log on to the account.
  b. Click **Next**.
  If your computer is set to use dial-up connections, the connection type dialog box opens. Select the connection type for your account, and then click **Next**.
- If you selected MAPI e-mail accounts:
  a. Select the profile type from the **Profile** list.
  b. Enter your password for the account, and then click **Next**.

5. Click **Test Now** to verify that the account information you entered is correct. Otherwise, click **Next**.
6. Click **Finish.**

You are finished with the basic setup of SpamKiller. At any time, you can add more e-mail accounts, add more e-mail addresses to the Friends List, or configure other SpamKiller settings.

Using McAfee.com SecurityCenter

The McAfee.com SecurityCenter is your one-stop security shop, accessible from its icon in your Windows system tray or from your Windows desktop. With it, you can perform these useful tasks:

- Get free security analysis for your PC.
- Launch, manage, and configure all your McAfee.com subscriptions from one icon.
- See continuously updated virus alerts and the latest product information.
- Receive free trial subscriptions to download and install trial versions directly from McAfee.com using our patented software delivery process.
- Get quick links to frequently asked questions and account details at the McAfee.com Web site.

Note: For more information about its features, please click **Help** in the SecurityCenter dialog box.

While the SecurityCenter is running and all of the McAfee.com features installed on your computer are enabled, a red M icon appears in the Windows system tray. This area is usually in the lower-right corner of the Windows desktop and contains the clock.

If one or more of the McAfee.com applications installed on your computer are disabled, the McAfee.com icon changes to black.

To open the McAfee.com SecurityCenter:

1. Right-click the McAfee.com icon.
2. Click Open SecurityCenter.

To access a SpamKiller feature:

1. Right-click the McAfee.com icon.
2. Click **SpamKiller**.
   The McAfee.com Security Center opens displaying SpamKiller options (see Figure 1).

Figure 1

3. Select an option to open the SpamKiller main window.

To accomplish additional tasks at the McAfee.com Web site via the McAfee.com icon, click the following menu items:

Members Only - Get special offers and discounts for valued members.

McAfee.com Store - Get news, product information, and promotional offers for our other security products.

Customer Support - Get help, send feedback, and report bugs or problems.

My Account Info - View your subscription status.

Clinic - Access additional McAfee.com services to enhance your computer's performance.

Chapter 2 – Quick Tour of SpamKiller

When you open SpamKiller, the SpamKiller main window opens. Take a quick tour of the tasks you can perform via the toolbar and icon bar (see Figure 2).

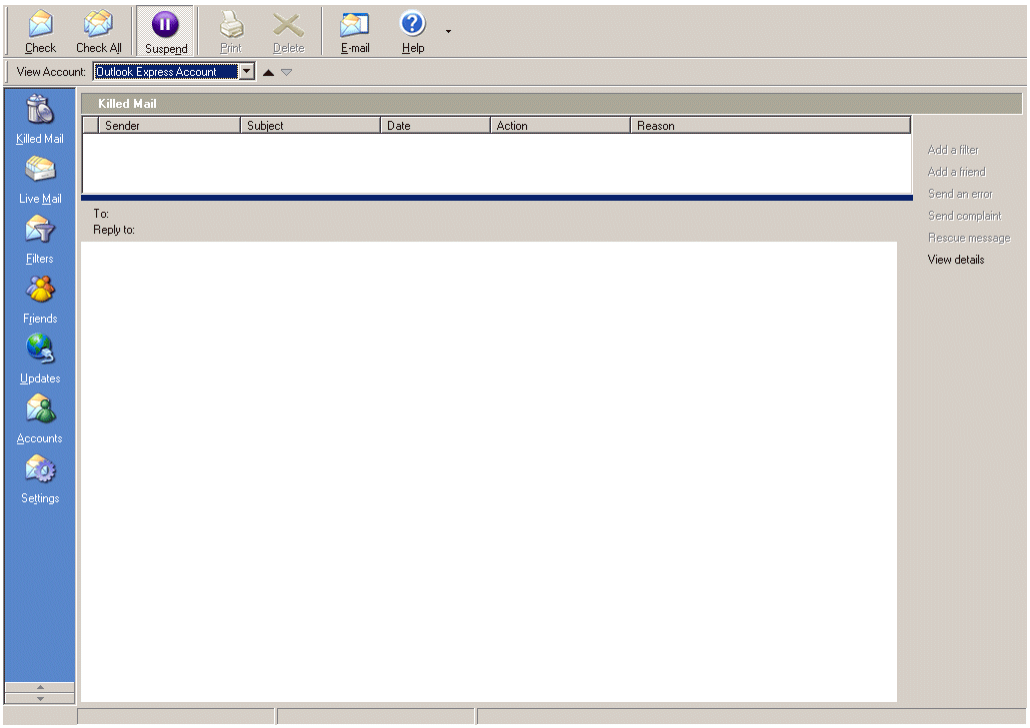


Figure 2

The Toolbar

See the toolbar to perform the most common tasks and display different e-mail accounts.

Select an account from the **View Accounts** list to view from e-mail accounts you added.

Click the **Check** button to check the selected e-mail account and filter all new messages in the account's inbox.

Click the **Check All** button to check all e-mail accounts that SpamKiller monitors.

Click the **Suspend** button to suspend automatic e-mail checking. To reactivate automatic checking, click the Suspend button again. When you open the SpamKiller main window, automatic checking is suspended.

Click the **Print** button to print a copy of one or more messages. Both headers and message text will be printed.

Click the **Delete** button to remove messages from the Killed Mail and Live Mail boxes, or delete filters.

Click the **E-mail** button to start your e-mail program. This button works only if you configured SpamKiller to start your e-mail program. To configure SpamKiller to start your e-mail program, see "Editing Connection Properties."

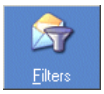
Click the **Help** button to open the online Help.

The Icon Bar

See the icon bar to navigate among the different pages in SpamKiller.

Click the **Killed Mail** icon to the view the messages that SpamKiller removed from your inbox and the reasons why they were filtered. A message pane shows the contents of the selected message. For MAPI accounts, internal mail does not appear in the Killed Mail box.

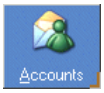
Click the **Live Mail** icon to view the messages currently in your inbox, as well as a message pane showing the contents of the selected message. For MAPI accounts, internal mail does not appear in the Live Mail box.



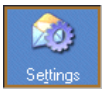
Click the **Filters** icon to view a list of available filters in SpamKiller. You can add, edit, or remove filters.

Click the **Friends** icon to view the Friends List. The Friends List contains senders that SpamKiller accepts all messages from.

Click the **Updates** icon to view a list of new filters for SpamKiller. You can remove any new filters that you do not need.



Click the **Accounts** icon to view information on e-mail accounts you added. You can add, edit, or remove accounts.



Click the **Settings** icon to edit various SpamKiller settings.

Chapter 3 – Adding E-mail Accounts

After you installed SpamKiller and restarted your computer, the Getting Started Wizard helped you to add an e-mail account. If you did not do so during installation, or if you want to edit account information, follow the steps in this chapter.

Adding E-mail Accounts

You can add multiple e-mail accounts, with default property settings, for SpamKiller to monitor. Once you add an e-mail account, you can edit its properties. SpamKiller lets you add three types of accounts:

- **Standard e-mail account (POP3)**: Local dialup or broadband accounts, where your Internet service provider receives and holds your e-mail. Most home users have this type of account.
- **MSN/Hotmail account**: MSN/Hotmail web-based accounts.
- **MAPI e-mail account**: Local network e-mail accounts. Many corporate users have this type of account when their company is running Microsoft® Exchange Server.

To add an e-mail account, click the **Accounts** icon, and then click **Add**. The New Account Wizard opens.

If SpamKiller detects more than one e-mail account, a list of the e-mail accounts appears. Follow the steps below:

1. Select an e-mail account you want to add, and then click **Next**.
   You can add more accounts later after SpamKiller is installed. If the e-mail account you want to add is not listed, click **My e-mail account is not listed above**, click **Next**, and then go to step 1 in the next section.
2. Enter the password you use for logging on to the account, and then click **Next**.
3. Click **Test Now** to verify that the account information you entered is correct. Otherwise, click **Next**.
4. Click **Finish**.

   If you added a MSN/Hotmail account, SpamKiller will search for a MSN/Hotmail address book to import into the Friends List. The benefit of adding addresses to the Friends List is that SpamKiller accepts all mail from those on the list. If SpamKiller finds your MSN/Hotmail address book, and you want to import it, follow the instructions in the dialog box that appears. Otherwise, click **Cancel**. You can add addresses later.

If SpamKiller does not detect multiple e-mail accounts, follow these steps:

1. Enter a description of the e-mail account, and then click **Next**.
2. Enter your name and the account's e-mail address, and then click **Next**.
3. Select the e-mail account type, and then click **Next**.
4. Enter account information:
   - If you selected Standard e-mail (POP3 account):
     a. Enter the addresses of the incoming and outgoing e-mail servers, and then click **Next**.
     b. Enter your user name and password for the e-mail account.
        Your user name is usually the first part of your e-mail address, before the @ sign.
        Your password is the password you use to log on to the account.
     c. Click **Next**.
        If your computer is set to use dial-up connections, the connection type dialog box opens. Select the connection type for your account, and then click **Next**.
   - If you selected MSN/Hotmail account:
     a. Enter your user name and password for the e-mail account.
        Your user name is usually the first part of your e-mail address, before the @ sign.
        Your password is the password you use to log on to the account.

b. Click **Next**.
   If your computer is set to use dial-up connections, the connection type dialog box opens. Select the connection type for your account, and then click **Next**.

- If you selected MAPI e-mail account:
  a. Select the profile from the **Profile** list.
  b. Enter the profile's password for the account, and then click **Next**.

5. Click **Test now** to verify that the account information you entered is correct. Otherwise, click **Next**.
6. Click **Finish.**

   If you added a MSN/Hotmail account, SpamKiller will search for a MSN/Hotmail address book to import into the Friends List. The benefit of adding addresses to the Friends List is that SpamKiller accepts all mail from those on the list. If SpamKiller finds your MSN/Hotmail address book, and you want to import it, follow the instructions in the dialog box that appears. Otherwise, click **Cancel**. You can add addresses later.

Editing E-mail Account Properties

All accounts have default settings that you can edit.

Editing General Properties

To edit an account's description and user information:

1. Click the **Accounts** icon.
2. Select an account from the **Accounts** list, click **Properties**, and then click the **General** tab. The General dialog box appears (see Figure 3).

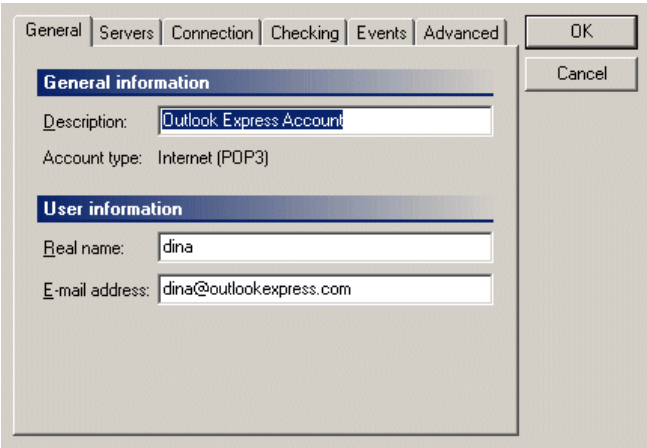


Figure 3

3. Edit **General information** and **User information**, and then click **OK**.

Editing Server Properties

Editing server properties is available for POP3 and MSN/Hotmail accounts only.

To edit an account's e-mail server, user name, and password:

1. Click the **Accounts** icon.
2. Select an account from the **Accounts** list, click **Properties**, and then click the **Servers** tab. The Servers dialog box appears (see Figure 4).

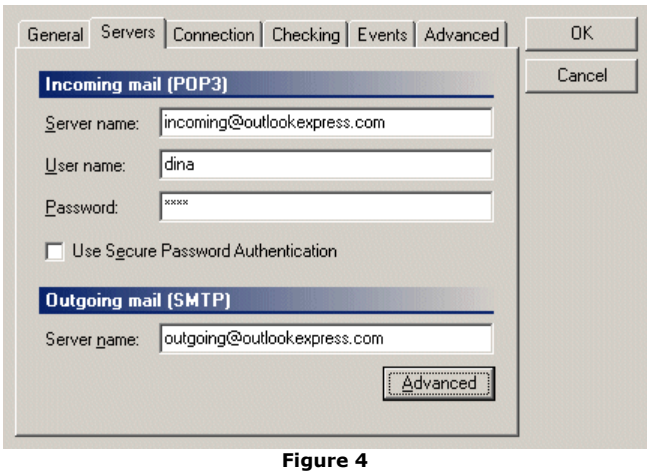


Figure 4

3. Enter server information for incoming and outgoing mail, and then click **OK**.

Editing Settings Properties

Editing settings properties is available for MAPI accounts only. You must configure a valid MAPI profile through the Windows Control Panel before you can add the account to the SpamKiller setup.

To edit settings for a MAPI account:

1. Click the **Accounts** icon.
2. Select an account from the **Accounts** list, click **Properties**, and then click the **Settings** tab.
   The Settings dialog box appears (see Figure 5).

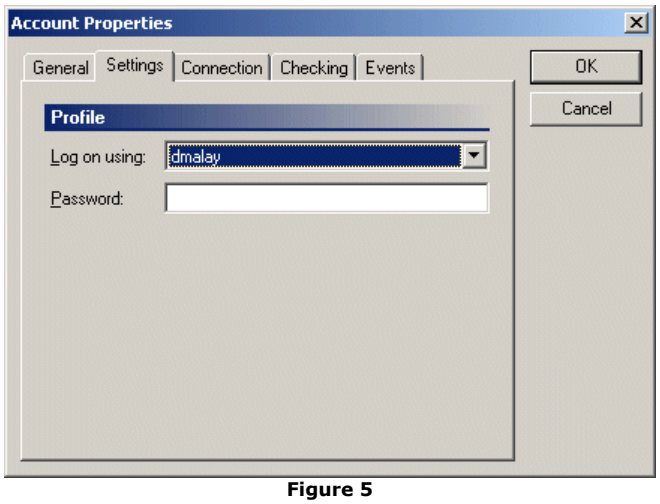


Figure 5

3. Select the appropriate MAPI profile from the **Log on using** list.
4. Enter the corresponding MAPI profile password in the **Password** field, and then click **OK**.

Editing Connection Properties

You can edit how your computer connects to an account's e-mail servers, and whether SpamKiller automatically connects to the account when needed.

To edit an account's connections:

1. Click the **Accounts** icon.
2. Select an account from the **Accounts** list, click **Properties**, and then click the **Connection** tab.
   The Connection dialog box appears (see Figure 6).

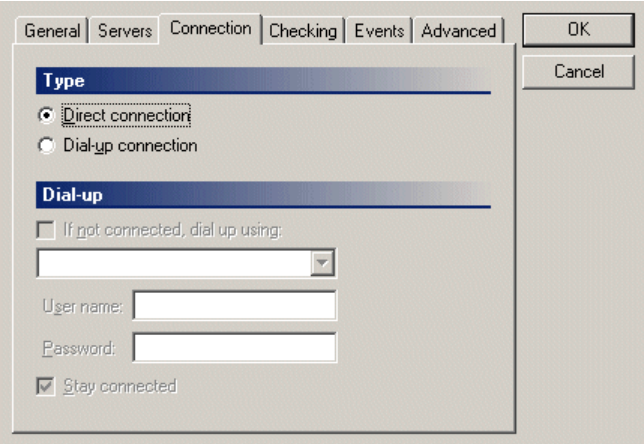


Figure 6

3. Select the appropriate connection type.
4. If you selected Dial-up connection, and your computer does not automatically connect to your account:
    a. Select **If not connected dial up using** for SpamKiller to automatically connect to the account when SpamKiller checks for spam.
    b. Enter the user name and password for accessing the connection.
    c. Select **Stay connected** for your computer to remain connected to the internet after SpamKiller has completed its operations.
5. Click **OK**.

Editing Filter Checking Properties

By default, SpamKiller scans your e-mail every ten minutes. You can change this setting for each e-mail account.

To edit filter checking properties:

1. Click the **Accounts** icon.
2. Select an account from the **Accounts** list, click **Properties**, and then click the **Checking** tab. The Checking dialog box appears. (See Figure 7.)

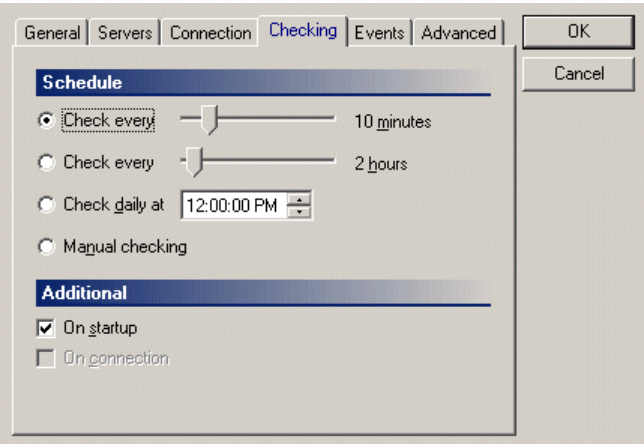


Figure 7

3. From the **Schedule** options, select the frequency at which you want SpamKiller to filter the account.

4. From the **Additional** options, specify additional times for SpamKiller to check the account:
    - Select **On startup** if you have a direct connection account, and you want SpamKiller to check the account every time SpamKiller starts.
    - Select **On connection** if you have a dial-up connection, and you want SpamKiller to check the account every time you connect to the Internet.
5. Click **OK**.

Editing Events Properties

SpamKiller plays a sound whenever an e-mail message arrives in your Killed Mail box or Live Mail box. You can disable the sound completely, or play a sound for specific types of e-mail you receive. For example, set SpamKiller to play a sound whenever you receive spam, but not when you receive mail from a friend. In addition, you can play a different sound for each type of mail you receive.

You can also run a program whenever an e-mail message arrives.

To edit Events properties:

1. Click the **Accounts** icon.
2. Select an account from the **Accounts** list, click **Properties**, and then click the **Events** tab. The Events dialog box appears (see Figure 8).

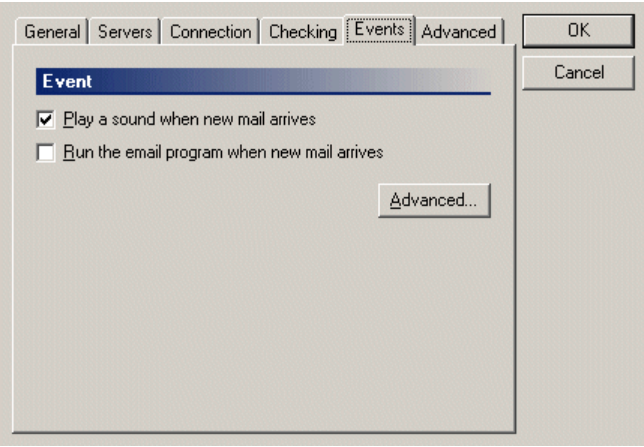


Figure 8

3. Clear the **Play a sound when new mail arrives** check box to disable sound for new e-mail.
4. Select **Run the e-mail program whenever new mail arrives** for SpamKiller to automatically open your default e-mail program when it detects new e-mail.
5. Click **Advanced** to set specific sounds and programs.
6. Click the **Sounds** tab to specify which events must play a sound:
   Select the events that must play a sound. You can listen to the sound by clicking **Listen**. To change the sound, click **Browse**, and then select a different sound.
7. Click the **Programs** tab to specify which events must run an e-mail program.
   Select events that must run an e-mail program. Select the e-mail program to run for each event.
8. Click **OK**.

Editing Advanced Properties

Editing advanced properties is available for POP3 accounts only. If SpamKiller is unable to access your e-mail account, you might need to change some of the account's Advanced properties. For example, if you are connecting through a proxy, you might need to change the port numbers.

To edit advanced properties:

1. Click the **Accounts** icon.
2. Select an account from the **Accounts** list, click **Properties**, and then click the **Advanced** tab. The Advanced dialog box appears (see Figure 9).

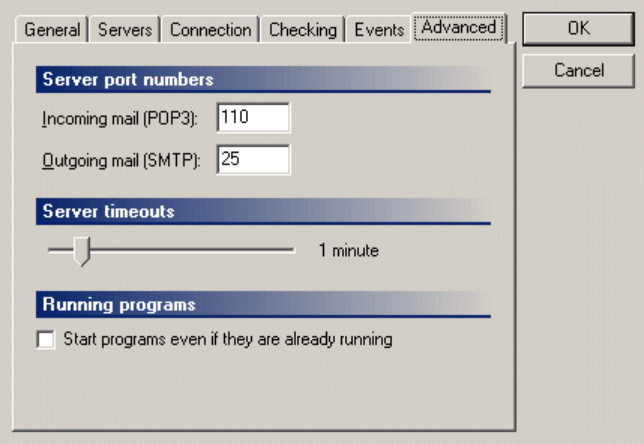


Figure 9

3. Enter the account's server port numbers.
   Change these values only if you are connecting through a proxy or e-mail server that does not use the standard port numbers.
4. Edit the **Server timeouts** value.
   You might want to increase the server timeout value if you receive many error messages. If you receive many error messages indicating that SpamKiller has timed out, your e-mail connection might be slow. Increase the server timeouts value so that SpamKiller will wait longer before timing out.
5. Select **Start programs even if they are already running** for SpamKiller to start your e-mail program even if it is already running.
6. Click **OK**.

Removing or Disabling E-mail Accounts

Remove e-mail accounts that you no longer want SpamKiller to monitor. Removing an account is permanent. You can disable an account instead.

To remove an e-mail account:

1. Click the **Accounts** icon.
2. Select the account you want to remove from the **Accounts** list.
3. Click **Remove**.
   A confirmation dialog box opens.
4. Click **Yes**.

To disable an e-mail account:

1. Click the **Accounts** icon.
2. Clear the check box next to the account you want to disable.
   The account is now disabled.

Chapter 4 – Adding Friends

SpamKiller accepts all e-mails from addresses and domains in the Friends List. Since SpamKiller bypasses these e-mails, the filtering process might be faster. Also, it helps prevent SpamKiller from accidentally blocking legitimate e-mail.

Add addresses one at a time, or add them all at once by importing an address book from an e-mail program. You can save the existing Friends List in SpamKiller and import it later. You can also add to the Friends List from the Killed Mail or Live Mail pages.

Adding an E-mail Address

You can add an email address from the Friends page, the Killed Mail page, or the Live Mail page. Adding addresses from the Killed Mail or Live Mail page lets you quickly add senders listed on those pages.

To add an e-mail address from the Friends page:

1. Click the **Friends** icon, and then click **Add**.
   The Friend Properties dialog box appears (see Figure 10).

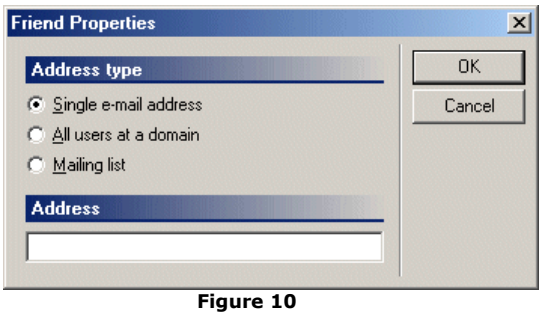


Figure 10

2. Select the address type you want to add:
   - **Single e-mail address**: The sender's e-mail address will be added to the Friends List.
   - **All users at domain**: The domain name will be added to the Friends List. SpamKiller will accept all e-mails coming from the domain.
   - **Mailing list**: The sender's mailing list will be added to the Friends List.
3. Enter an e-mail address in the **Address** field.
4. Click **OK**.

To add an email address from the Killed Mail or Live Mail page, see "Adding to the Friends List."

Importing an Address Book

You can import address books into SpamKiller from the following e-mail programs: Microsoft Outlook, Microsoft Outlook Express, Netscape Communicator, Qualcomm Eudora, Pegasus Mail, MSN/Hotmail, and any program that can support its address book as a plain text file.

To import an address book into the Friends List:

1. Click the **Friends** icon, and then click **Import Addresses**.
   The Address Book Wizard appears (see Figure 11).

Figure 11

2. Select the type of address book you want to import, and then click **Next**.
   A confirmation page shows the number of new e-mail addresses SpamKiller added.
   If SpamKiller did not find addresses in the address book, "The address book was not found" appears:
   a. Click **OK**.
   b. Click **Back**.
   c. Select another address book, or add addresses to the book, and import the book again.

Removing Addresses from the Friends List

To remove an address from the Friends List:

1. Click the **Friends** icon.
2. Select an address from the **Friends** list, and then click **Remove**.
   A confirmation dialog box opens.
3. Click **Yes**.

Saving a Copy of Your Friends List

You can save a backup copy of the Friends List in a file format used by SpamKiller. You can later import this file again to the Friends List.

To save a copy of the Friends List:

1. Click the **Friends** icon.
2. Click **Save Copy**.
   A confirmation dialog box appears.
3. Click **Yes**.

Chapter 5 – Using Killed Mail and Live Mail

The Killed Mail box contains spam messages that were removed from your inbox. The Live Mail box contains all messages currently in your inbox. The exception is with MAPI accounts where the Live Mail box does not contain internal email. The Killed Mail and Live Mail boxes have similar features.

Viewing Killed Mail

When SpamKiller finds spam, SpamKiller removes it from your inbox and places a copy in the Killed Mail box. You can view spam from the Killed Mail.

To view killed mail:

1. Click the **Killed Mail** icon.
   The Killed Mail page opens (see Figure 12).

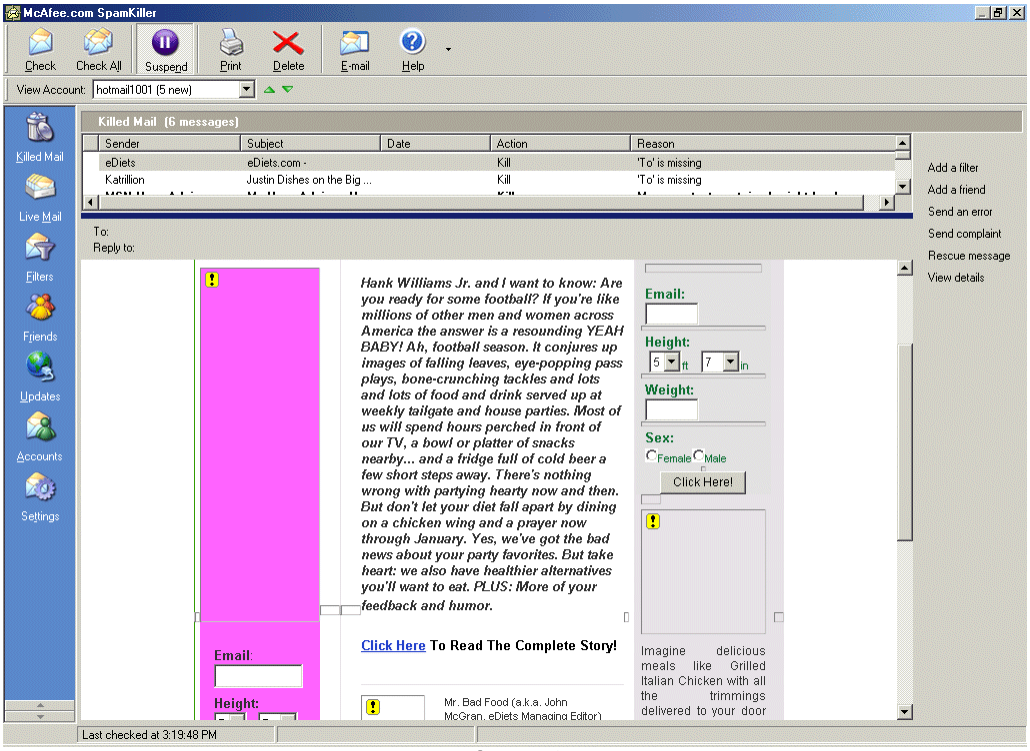


Figure 12

2. Select a message to view message details.

The top message pane lists spam messages. Each message shows the sender, the subject of the message, the date the message was received, the size of the message, and the reason why the message was removed. The leftmost column contains icons next to messages if complaints or error messages have been sent.

Complaint sent: This icon appears if you sent a manual complaint about a message.

Error message sent: This icon appears if you sent an error message.

The Reason column explains if a message was sent by someone on your Friends List, or if a message fit the criteria of a filter, but the filter action was set to Accept or Mark, But Do Not Kill.

The bottom message pane contains the actual message text for a selected message.

Handling Large Messages

By default, SpamKiller filters all e-mail, except for messages (including attachments) that are larger than 100 kilobytes. You can edit SpamKiller to check larger messages by increasing the maximum message size setting. However, if you increase the message size setting, SpamKiller might take longer to check your mail.

An example of spam that is often larger than 100 kilobytes is messages with viruses. Instead of modifying SpamKiller to check larger messages, you might want to install an anti-virus program on your computer. McAfee.com VirusScan Online is an anti-virus program that you can easily purchase and install from the McAfee.com Web site. For more information about VirusScan Online, go to http://www.mcafee.com/, click **Products & Services**, and then click **VirusScan Online**. For details on changing the maximum message size, see "Editing Message Options."

Viewing Live Mail

The Live Mail box displays all messages in your inbox. However, for MAPI accounts, the Live Mail box does not contain internal email.

To view live mail:

1. Click the **Live Mail** icon.
   The Live Mail page opens (see Figure 13).

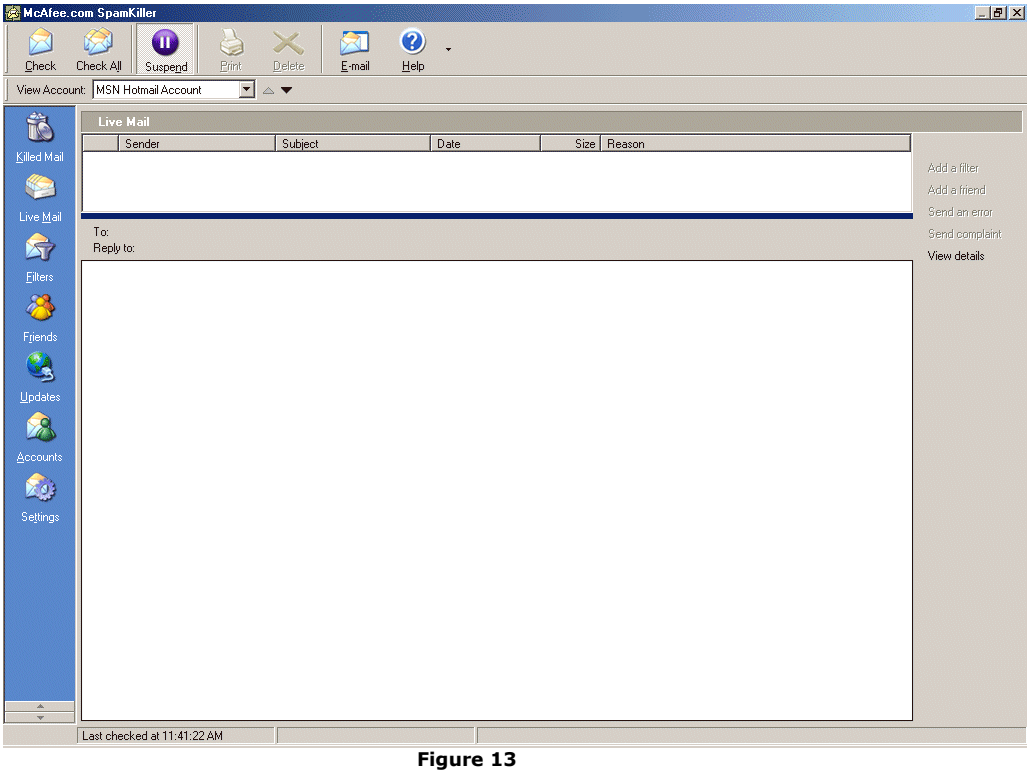


Figure 13

2. Select a message to view message details.

The top message pane of the Live Mail page lists messages. Each message shows the sender, the subject of the message, the date the message was received, and the size of the message. If an icon appears next to the message, an explanation of why SpamKiller flagged the message appears in the Reason column.

The following icons might appear next to messages:

Mail from a friend: When SpamKiller detects that the sender of a message is in the Friends List, the icon appears. This indicates the message is one you want to keep.

Possible spam: If a message matches a filter that has its action set to Mark, But Do Not Kill, the blue question mark appears.

Spam: Normally, spam messages do not appear in the inbox since they are automatically deleted. However, if you add or edit a filter so that the message now matches the filter, this icon indicates that the message is now classified as spam. The message will be deleted the next time you check e-mail.

Complaint sent: This icon appears if you sent a manual complaint about a message.

Error message sent: This icon appears if you sent an error message.

The Reason column explains if a message was sent by someone on the Friends List, or if a message fit the criteria of a filter, but the filter action was set to Accept or Mark, But Do Not Kill.

The bottom message pane contains the actual message text for a selected message. By default, SpamKiller retrieves the message text and places it in the box. The exception is message text that is larger than the maximum size that SpamKiller will automatically retrieve. If you do not want message text to automatically appear, turn it off. For details, see "Editing Message Options."

Performing Tasks for Killed Mail and Live Mail

Adding a Filter

To add a filter from the Killed Mail or Live Mail page, see "Adding Filters from the Killed Mail or Live Mail Pages."

Adding to the Friends List

SpamKiller accepts all messages from e-mail addresses and domains added to the Friends List. From the Killed Mail and Live Mail pages, you can easily add the sender of a message to the Friends List.

Note: If you find legitimate mail in your Killed Mail box, you can place the mail back in your inbox. For details, see "Rescuing Mail."

To add an e-mail address or domain to the Friends List:

1. Open the Killed Mail or Live Mail pages by clicking the **Killed Mail** or **Live Mail** icon.
2. Select a message from the **messages** list, and then click **Add friend**.
   The Friend Properties dialog box opens (see Figure 14).

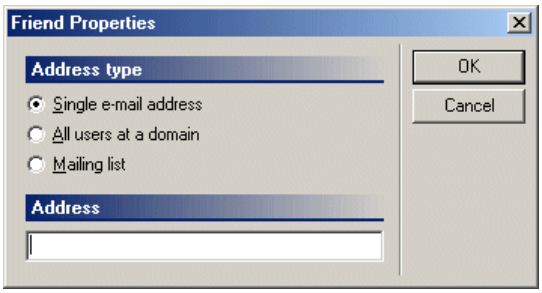


Figure 14

3. Select the address type that you want to add to the Friends List.
   - **Single e-mail address**: The sender's e-mail address will be added to the Friends List.
   - **All users at domain**: The domain name will be added to the Friends List. As a result, SpamKiller will accept all e-mails coming from the domain.
   - **Mailing list**: The sender's mailing list will be added to the Friends List.

   If the Killed Mail page is open, **Restore message automatically** is selected so that after you click OK, the killed message you selected will be added to your Friends List and placed back in your inbox. To place the address in the Friends List without restoring the message back to your inbox, clear this option.

4. Click **OK**.

Rescuing Mail

You might find that your Killed Mail box contains legitimate mail, and that you want to place those messages back in your inbox.

To rescue mail:

1. Click the **Killed Mail** icon.
   The Killed Mail page opens.
2. Select a message you want to rescue.
3. Click **Rescue**.
   If SpamKiller monitors more than one e-mail account, the Rescue message dialog box opens. Select the account in which to place the message.
4. Click **OK**.
   A copy of the message is placed back in your inbox, but still appears in the Killed Mail box. If you placed the message in a MAPI account, the rescued message appears immediately in the inbox. If you placed the message in a POP3 or MSN/Hotmail account, there is a slight delay before the rescued message appears in the inbox.

Sending Manual Complaints

You can send complaints to account-abuse addresses at the sender's domain. For details, see "Sending Manual Complaints."

Sending Error Messages

You can send an error message to try to prevent a sender from sending you more spam.

To send an error message:

1. Open your Killed Mail or Live Mail box by clicking the **Killed Mail** or **Live Mail** icon.
2. Select a message from the **messages** list.
3. Click **Send error**.
   An error message is sent to the reply address on the spam message you selected.

Viewing Header Details

By default, SpamKiller displays message text without the headers.

To view message headers:

1. Open your Killed Mail or Live Mail box by clicking the **Killed Mail** or **Live Mail** icon.
2. Select a message from the **messages** list.
3. Click **Details**.
   The message now shows both the message text and the headers in native format.

Removing Messages

SpamKiller automatically removes messages from the Killed Mail box 30 days after they SpamKiller removed them from your inbox. You can change the setting for automatic removal, or remove messages manually.

SpamKiller does not automatically remove messages from your Live Mail box. If you remove messages from your Live Mail box, you also remove them from your inbox.

To remove messages manually:

1. Open the Killed Mail or Live Mail box by clicking the **Killed Mail** or **Live Mail** icon.
2. Select a message to remove.
3. Click **Delete** on the top menu bar.

To change the setting for automatic removal, see "Editing Message Options."

Chapter 6 – Using Filters

Filters are the heart of SpamKiller. When SpamKiller checks for spam, filters examine each incoming e-mail. A filter specifies what to look for in an e-mail message, and the action to take against spam or possible spam. SpamKiller comes with many filters; however, you can edit the filters or create new ones to fine-tune which messages are removed from your inbox and which ones are accepted. You can also delete or disable filters.

SpamKiller automatically checks for new filters once a day and downloads the new filters onto your computer. You can view new filters and remove any you do not need. You can turn off automatic filter checking and check for new filters manually.

SpamKiller groups its filters into six types. Each type looks at a different part of an e-mail message.

- **Sender Filters**: Sender filters look for a specific sender's e-mail address or domain.
- **Subject Filters**: Subject filters look for the presence or absence of words or phrases, in the subject field of the header.
- **Message Text Filters**: Text filters look for the presence or absence of words or phrases in the body of the message.
- **Country Filters**: Country filters block messages from specified countries. Specifically, SpamKiller looks for country codes within e-mail addresses and message headers. Some spam e-mails are sent from servers in other countries.
- **Header Filters**: Header filters look for words or phrases in e-mail headers. All e-mail messages contain more information than you normally see in your e-mail program. This information is known as the message header. Message headers contain various required and optional fields, and can be very useful for detecting spam.
- **Other Filters**: Other filters are built into SpamKiller and therefore cannot be removed. SpamKiller contains only a few of these.

When a filter finds spam or possible spam, SpamKiller takes one of five actions against it.

- **Kill**: The message is deleted from your inbox, and a copy is placed in the Killed Mail box.
- **Kill After Complaining**: SpamKiller sends a complaint before deleting the message from your inbox and placing a copy in the Killed Mail box.
- **Kill After Error Message**: SpamKiller sends an error message before deleting the message from your inbox and placing a copy in the Killed Mail box.
- **Accept**: SpamKiller accepts the message. This action is useful if you want to accept certain types of e-mails, such as those from customer support. The message remains in your inbox.
- **Mark, But Do Not Kill**: SpamKiller does not delete the message, but marks it with a blue question mark, and places a copy of the message in the Live Mail box.

Adding or Editing Filters

When you create a new filter or edit an existing one, specify what you want SpamKiller to look for in an e-mail message, and the action to take against spam or possible spam.

SpamKiller gives you several ways to create new filters: from the Filters page, from your Killed Mail box, or from your Live Mail box. Creating filters from your Killed Mail and Live Mail boxes provides a fast and easy way to block future spam from senders currently in those boxes, or to block similar messages.

Adding Filters from the Killed Mail or Live Mail Pages

You can quickly create filters based on messages in the Killed Mail and Live Mail boxes. This helps prevent future spam from the same sender or with similar messages from entering your inbox.

After creating a filter, you have the option of editing advanced settings for the filter. All new filters have default settings that you can change.

To add a filter from Killed Mail or Live Mail page:

1. Click the **Killed Mail** or **Live Mail** icon.
   The Killed Mail or Live Mail page opens.
2. Select a message to base a new filter on.
3. Click **Add a filter**.
   The New Filter Wizard dialog box opens (see Figure 15).

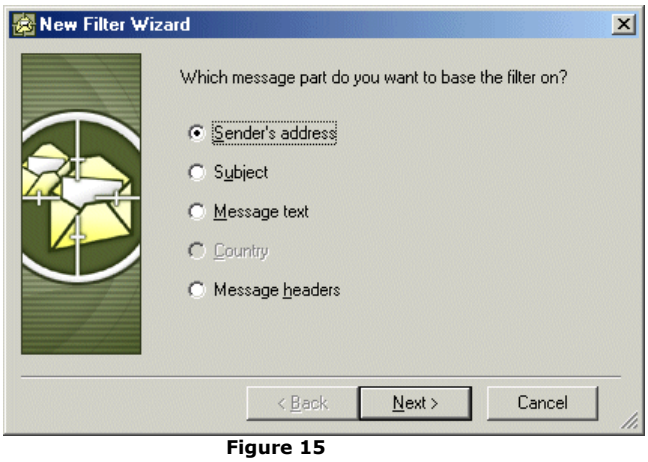


Figure 15

4. Select the part of the message to base the filter on, and then click **Next**.

If you selected Sender's address:

A dialog box opens displaying the address or addresses of the sender.

1. Select the address to filter on.
2. Select **Ignore the user name** to filter on the domain name only.
3. Click **Next**.
4. To edit advance filter settings, click **Advance**. Otherwise, click **Finish**.
   For details on editing advance settings, see "Adding or Editing Filters from the Filters Page."

If you selected Subject:

A dialog box opens displaying the text in the subject field of the spam (see Figure 16).

Figure 16

1. Select the part of the message to filter on, and then click **Next**.
2. To edit advance filter settings, click **Advance**. Otherwise, click **Finish**.
   For details on editing advance settings, see "Adding or Editing Filters from the Filters Page."

If you selected Message text:

A dialog box opens displaying the e-mail message.

1. Select up to 50 characters of the message text to filter on, and then click **Next**.
2. To edit advance filter settings, click **Advance**. Otherwise, click **Finish**.
   For details on editing advance settings, see "Adding or Editing Filters from the Filters Page."

If you selected Country:

A dialog box opens displaying a list of countries that the selected message has passed through.

1. Select one or more countries to filter on.
2. To edit advance filter settings, click **Advance**. Otherwise, click **Finish**.
   For details on editing advance settings, see "Adding or Editing Filters from the Filters Page."

If you selected Message headers:

A dialog box opens displaying the headers in the message.

1. Select the message header to filter on.
2. Select the part of the header to filter on.
3. Select **Look for address information** to search only for addresses in the headers.
4. Click **Next**.
5. To edit advance filter settings, click **Advance**. Otherwise, click **Finish**.

   For details on editing advance settings, see "Adding or Editing Filters from the Filters Page."

Adding or Editing Filters from the Filters Page

SpamKiller allows you to create or edit several types of filters.

Adding or Editing Sender Filters
Sender filters look for specific user names or domains in e-mail addresses. An e-mail address contains two parts, the user name and the domain: username@domain.com. You can create filters to look at an entire address, the user name, or just the domain.

To add or edit a Sender filter:

1. Click the **Filters** icon.
2. Click the **Sender** tab.
   The list of Sender filters appears in the Filters list.
3. Click **Add** to create a new filter, or to edit a filter, select a filter from the Filters list, and then click **Properties**.
   The Sender filter dialog box opens (see Figure 17).

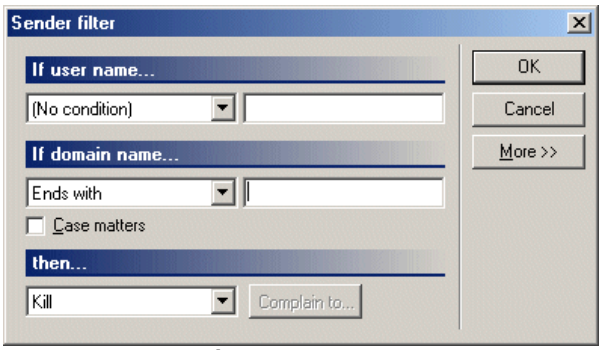


Figure 17

4. Define the user name condition, or select **[No condition]** if you do not want the filter to search on the user name portion of e-mail addresses. Conditions define what a filter should look for. To define a condition:
    a. Select a condition type from the list of available conditions.
    b. Enter the text that the filter should look for.
5. Define the condition for the domain name, or select **[No condition]** if you do not want the filter to search on the domain portion of e-mail addresses. To define a domain name condition:
    a. Select a condition type from the list of available conditions.
    b. Enter the text, number, or characters the filter should look for.
6. Select **Case matters** only if you want the filter to be case-sensitive.
   Case-sensitive means that the filter distinguishes between uppercase and lowercase letters.
7. Select the action you want SpamKiller to take against e-mail messages found by the filter.
   If you selected **Kill after complaining** or **Kill after error message**, specify the automatic message you want to send:
    a. Click **Send to** or **Complain to**.
    b. Select an address to send it to.
8. Click **OK**.

Adding or Editing Subject Filters
Subject filters look for words or phrases that are present or missing from the subject field of a message.

To add or edit a Subject filter:

1. Click the **Filters** icon.
2. Click the **Subject** tab.
   The list of Subject filters appears in the Filters list.
3. Click **Add** to create a new filter, or to edit a filter, select a filter from the Filters list, and then click **Properties**.
   The Subject filter dialog box opens (see Figure 18).

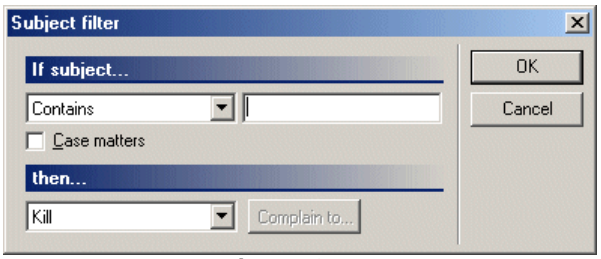


Figure 18

4. Define the condition for the filter:
    a. Select a condition type from the list of available conditions.
    b. Enter the text that the filter should look for.
       If you selected the condition type Is Missing or Is Blank, do not enter text, leave it blank.
5. Select **Case matters** only if you want the filter to be case-sensitive.
   Case-sensitive means that the filter distinguishes between uppercase and lowercase letters.
6. Select the action you want SpamKiller to take against e-mail messages found by the filter.
   If you selected **Kill after complaining** or **Kill after error message**, specify the automatic message you want to send:
    a. Click **Send to** or **Complain to**.
    b. Select an address to send it to.
7. Click **OK**.

Adding or Editing Message Text Filters

Message Text filters look for specific text in the body of a message.

To add or edit a Message Text filter:

1. Click the **Filters** icon.
2. Click the **Text** tab.
   The list of Text filters appears in the Filters list.
3. Click **Add** to create a new filter, or to edit a filter, select a filter from the Filters list, and then click **Properties**.
   The Message text filter dialog box opens (see Figure 19).

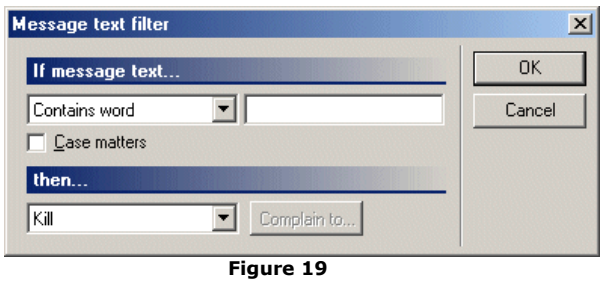


Figure 19

4. Define the condition for the filter:
   a. Select a condition type from the list of available conditions.
   b. Enter the text that the filter should look for.
5. Select **Case matters** only if you want the filter to be case-sensitive.
   Case-sensitive means that the filter distinguishes between uppercase and lowercase letters.
6. Select the action you want SpamKiller to take against e-mail messages found by the filter.
   If you selected **Kill after complaining** or **Kill after error message**, specify the automatic message you want to send:
   a. Click **Send to** or **Complain to**.
   b. Select an address to send it to.
7. Click **OK**.

Adding or Editing Header Filters

Header filters check for the presence or absence of specified fields in message headers as well as their contents. Header filters can look for specific values or restrict the filter's search to the address information parts of the headers.

To add or edit a Header filter:

1. Click the **Filters** icon.
2. Click the **Headers** tab.
   The list of Header filters appears in the Filters list.
3. Click **Add** to create a new filter, or to edit a filter, select a filter from the Filters list, and then click **Properties**.
   The Header filter dialog box opens (see Figure 20).

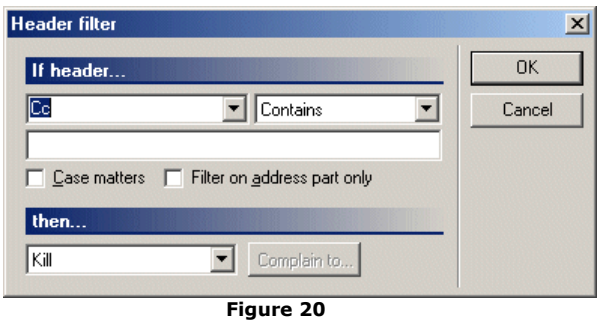


Figure 20

4. Define the condition for the filter:
    a. Select a header name that you want the filter to look for.
       If the list does not contain the header you need, type the header name.
    b. Select a condition type for the header from the list of available conditions.
    c. Enter the text that the filter should look for in the header.

   If you selected the condition type **Is Missing** or **Is Blank**, do not enter text, leave it blank.
5. Select **Case matters** only if you want the filter to be case-sensitive.
   Case-sensitive means that the filter distinguishes between uppercase and lowercase letters.
6. Select the action you want SpamKiller to take against e-mail messages found by the filter.
   If you selected **Kill after complaining** or **Kill after error message**, specify the automatic message you want to send:
    a. Click **Send to**.
    b. Select an address to send it to.
7. Click **OK**.

Enabling Country Filters

By default, all country filters are disabled. Country filters detect spam that originated in other countries.

To enable a Country filter:

1. Click the **Filters** icon.
2. Click the **Country** tab.
   The list of Country filters appears in the Filters list (see Figure 21).

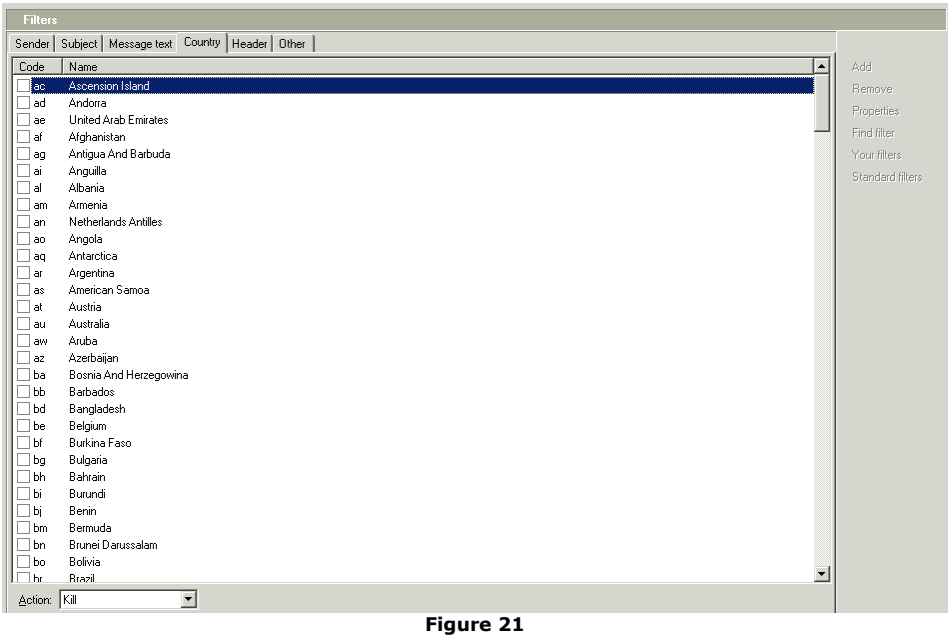


Figure 21

3. Select the country filter you want to enable.
   You can select or clear all countries by pressing CTRL+A.
4. Select the action you want SpamKiller to take against e-mail messages found by the filter.
   If you selected **Kill after complaining** or **Kill after error message**, specify the automatic message you want to send:
    a. Click **Send to** or **Complain to**.
    b. Select an address to send it to.

   The Country filter is now enabled.

Editing Other Filters

Other filters are built into SpamKiller. You cannot edit their properties, but you can edit their actions or disable them. To disable filters, see "Editing Filtering Options."

To edit Other filters:

1. Click the **Filters** icon.
2. Click the **Other** tab.
   The list of Other filters appears (see Figure 22).

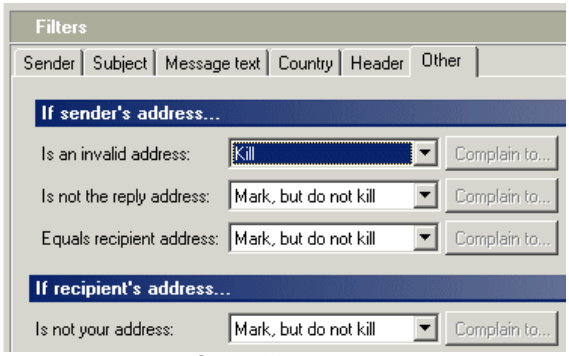


Figure 22

3. Change the filter actions if needed.
   If you selected **Kill after complaining** or **Kill after error message**, specify the automatic message you want to send:
   a. Click **Send to** or **Complain to**.
   b. Select an address to send it to.

Removing or Disabling Filters

You can remove any filter, except for Other filters. When you remove a filter, the filter is permanently removed from SpamKiller.

You can disable filter types instead of removing them. Disabled filter types can later be enabled. Disabling a filter type disables all filters associated with that filter type. In other words, SpamKiller does not use those filters when it scans your e-mail.

Note: You cannot disable an individual filter, only filter types.

Removing Filters

To remove a filter:

1. Click the **Filters** icon.
2. Click the filter type tab containing the filter, and then select the filter.
3. Click **Remove**.
   A confirmation dialog box opens.
4. Click **Yes** to remove the filter.

Disabling Filter Types

For details, see "Editing Filtering Options."

Finding Filters

Since the filters list can be long, SpamKiller provides a way to search for specific filters. You can also change the list of filters to display either filters you created or the standard filters. Standard filters are those that came with SpamKiller, or have been added through automatic filter updates.

Note: The search feature is not available for Country and Other filter types since they contain few filters.

To find a filter:

1. Click the **Filters** icon.
2. Click the filter type tab containing the filter, and then click **Find**.
   The Find filter dialog box opens (see Figure 23).

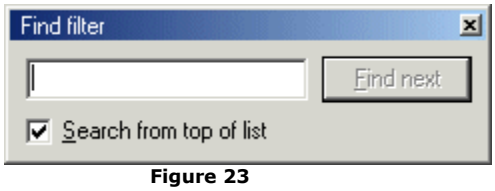


Figure 23

3. Enter any text that is included in the filter definition.
4. If you do not want the search to start from the beginning of the list, clear **Search from top of list**. The search starts at the selected filter.
5. Click **Search next**.
   If a filter fits the search criteria, the filter is highlighted in the **Filters** list. Click **Find Next** if you want to continue the search. If no filters fit the search criteria, the following message appears: "Could not find ……." Click **OK**.

To view filters you created:

1. Click the **Filters** icon.
2. Click the filter type tab.
   The list of all filters for the filter type appears.
3. Click **Standard filters**.
   The Filters list displays filters you created.

To view standard filters:

1. Click the **Filters** icon.
2. Click the filter type tab.
   The list of all filters for the filter type appears.
3. Click **Your filters**.
   The Filters list displays the standard filters.

Editing Filtering Options

You can change the default settings for filtering options, such as disable filter types, change the default action of filters you create, and turn off automatic filter updates.

If you disable filter types, SpamKiller might not be able to automatically delete failed complaints and failed error messages.

To edit filtering options:

1. Click the **Settings** icon.
2. Click the **Filtering** tab.
   The Filtering dialog box opens (see Figure 24).

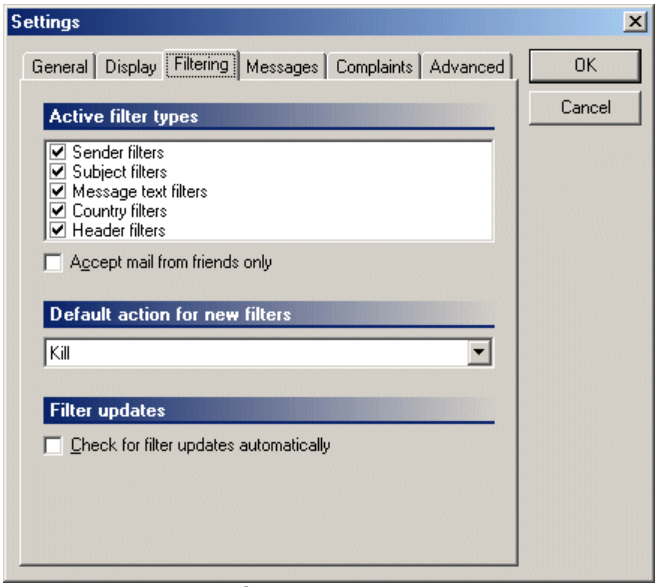


Figure 24

3. To disable filter types, clear the filter types located in the **Active filter types** list.
   You can enable the filter by selecting it.
4. Select **Accept mail from friends only** if you want to restrict incoming mail to people on your SpamKiller Friends List.
5. To change the default action of filters you create, select an action from the **Default filter action** list.
   Note: You can override the default action for new filters as you create new filters.
6. To turn of automatic filter updates, clear the **Check for updates automatically** check box. When this option is selected, SpamKiller will check for new filters once a day and download the filters onto your computer. You can view the list of updated filters in the Updates page. For more information on filter updates, see "Updating Filters."

Editing Filter Checking Options

SpamKiller scans your e-mail for spam every twenty minutes. You can change this setting for each of your e-mail accounts. For details, see "Editing Filter Checking Properties."

Disabling Filtering on an Account

You can prevent SpamKiller from filtering an e-mail account. For details, see "Removing or Disabling Filters."

Updating Filters

New filters for SpamKiller are available regularly. SpamKiller automatically checks for new filters once a day and downloads the new filters onto your computer. You can turn off auto-checking and check for filters manually. After each filter update, you can view the list of new filters and remove any you do not need.

If your computer is behind a firewall, you might need to access the filter updates server via a proxy. For details, see "Editing Advanced Options."

Updating Filters Manually

To update filters manually:

1. Click the **Updates** icon.
   The Updates page opens (see Figure 25).

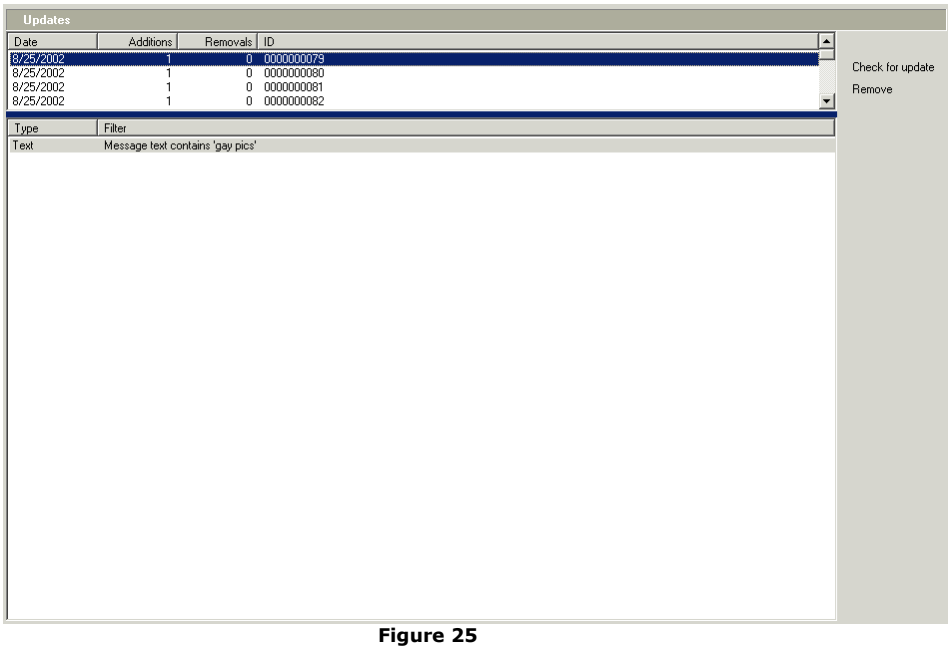


Figure 25

2. Click **Check for update**.
   A dialog box opens indicating the number of new filters added.
3. Click **OK**.
   The new filters appear in the list. The new filters also appear on the Filters page.

Removing Filter Updates

To remove filter updates:

1. Click the **Updates** icon.
   The Updates page opens.
2. Remove filters:
   - To remove all filters from an update, select an update at the top of the page.
   - To remove a single filter, select an update from the top portion of the page, and then select a filter at the bottom of the page.
3. Click **Remove**.
   A confirmation dialog box opens.
4. Click **Yes**.

Turning Off Automatic Filter Updates

To turn off automatic filter updates:

1. Click the **Settings** icon.
2. Click the **Filtering** tab.
3. Clear the **Check for updates automatically** check box.
4. Click **OK**.

Chapter 7 – Configuring Additional SpamKiller Options

SpamKiller has default settings that you can change.

Editing General Options

General settings specify which e-mail program you use, whether sound is turned off or on, and whether you want to use password protection. Password protection requires that you enter a password to access the SpamKiller main window. Using password protection helps prevent other users of your computer from viewing spam messages in the Killed Mail page or changing SpamKiller settings.

To edit general options:

1. Click the **Settings** icon, and the click the **General** tab.
   The General dialog box opens (see Figure 26).

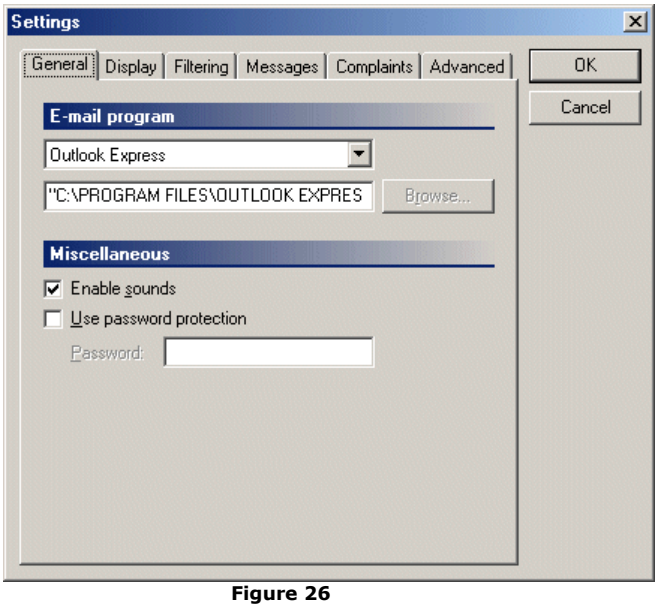


Figure 26

2. Select your e-mail program from the list.
   If your e-mail program is not on the list, click **Browse** to find the e-mail program.
   By selecting your e-mail program, you can launch your e-mail program whenever you click the e-mail button on the tool bar. Also, it is easier to set up your accounts and to run SpamKiller when new e-mail arrives.
3. Clear **Enable sounds** if you want to turn off all sounds associated with SpamKiller.
4. If you want to use password protection to access the SpamKiller main window:
   a. Select **Use password protection**.
   b. Enter the password in the **Password** box.
      Whenever you open SpamKiller, you must enter the password.
5. Click **OK**.

Editing Display Options

Display settings specify how SpamKiller looks on your screen and how it notifies you when new e-mail arrives and is processed.

To edit display options:

1. Click the **Settings** icon, and then click the **Display** tab.
   The Display dialog box opens (see Figure 27).

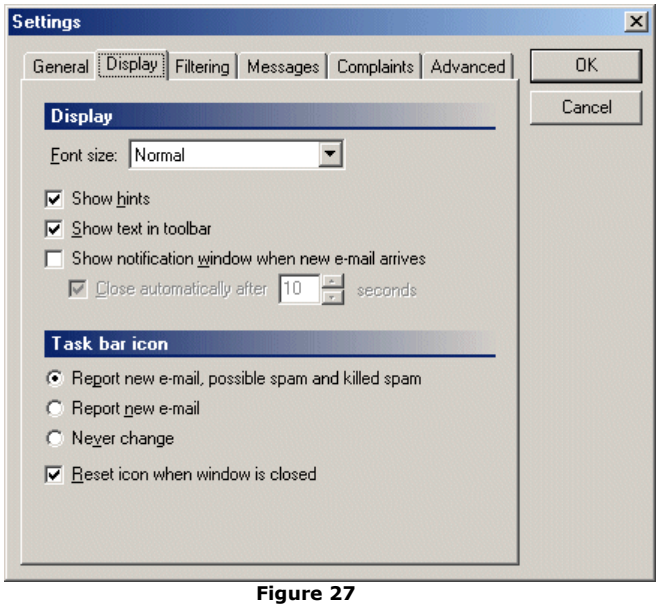


Figure 27

2. Select a font size from the **Font size** list.
   The Normal font size is the standard setting. The text on buttons and toolbars are not affected by the setting.
3. Clear or select other display options:
   - **Show hints**: When this option is selected, you see brief explanations of buttons and icons during mouse over.
   - **Show text in tool bar**: When this option is selected, buttons in the toolbar display explanatory text.
   - **Show notification window when new e-mail arrives**: When this option is selected, a small notification window tells you how many messages arrived and how SpamKiller processed them.
   - **Close automatically after**: When this option is selected, notification windows close automatically after a few seconds.
4. From the **Task bar icon** list, change the types of incoming e-mail that SpamKiller should report.
   If **Reset icon when window is closed** is selected, the envelope icon reverts to its empty state when the window is closed, even if there are messages in your inbox that your e-mail program has not received.
5. Click **OK**.

Editing Filtering Options

You can change the default settings for filtering options, such as, disable filter types, change the default action of filters you create, and turn off automatic filter updates. For details on all of these tasks, see "Editing Filtering Options."

Editing Message Options

Message settings indicate how SpamKiller handles large messages, deleted messages, and failed message replies. Failed message replies are messages in your inbox that notify you of a complaint or error message that cannot be sent.

Filtering Large Messages

By default, SpamKiller filters all e-mail, except for messages (including attachments) that are larger than 100 kilobytes. You can edit SpamKiller to check larger messages by increasing the maximum message size setting. However, if you increase the message size setting, SpamKiller might take longer to check your mail.

An example of spam that is often larger than 100 kilobytes is messages with viruses. Instead of modifying SpamKiller to check larger messages, you might want to install an anti-virus program on your computer. McAfee.com VirusScan Online is an anti-virus program that you can easily purchase and install from the McAfee.com Web site. For more information about VirusScan Online, go to http://www.mcafee.com/, click **Products & Services**, and then click **VirusScan Online**.

To edit message options:

1. Click the **Settings** icon, and then click the **Messages** tab.
   The Messages dialog box opens (see Figure 28).

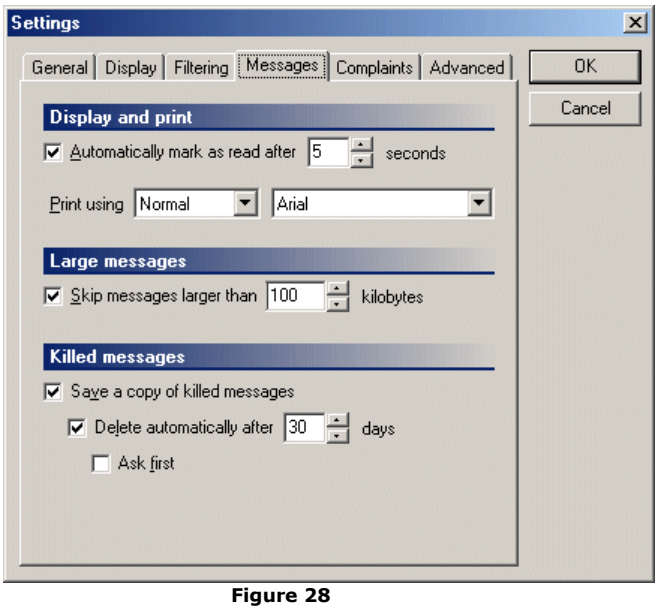


Figure 28

2. Define **Display and print options**:
   - **Automatically mark as read after**: When new messages are displayed in the Live Mail or Killed Mail list, they appear in bold type to indicate that they are unread. By default, the selected message is automatically marked as read after five seconds. You can adjust the time. To turn off the feature, clear the checkbox.
   - **Print using**: Use this option to specify the font and font size for printing messages.
3. Define how SpamKiller handles large messages.
   Most large messages are not spam. By default, SpamKiller skips messages larger than 100 kilobytes. This setting works well in most cases.
4. Define how SpamKiller handles killed messages:
   - **Save a copy of killed messages**: When this option is selected, SpamKiller will make a copy of all messages that are automatically deleted before removing them from your inbox. The copy is stored in each account's Killed Mail box so that you can view the mail. You can switch this option off to conserve disk space, but we do not recommend this. This option does not apply to messages you delete manually.
   - **Delete automatically after**: By default, SpamKiller removes messages from the Killed Mail box after 30 days. You can change the number of days.
   - **Ask first**: When this option is selected, SpamKiller will notify you before old messages are removed from the Killed Mail box.
5. Click **OK**.

Editing Complaint Options

You can define which automatic complaint messages SpamKiller will send. You can also write your own messages and send them out manually. For details, see "Creating, Editing, and Removing Messages."

Editing Advanced Options

You normally do not need to change Advanced settings. Advanced settings allow you to connect to the filter updates server through a proxy, change advanced options for automatic complaints and error messages, and turn on the communication log between SpamKiller and e-mail servers.

You might need to connect to the filter updates server using a proxy if your computer is behind a firewall. Updates are transmitted via the FTP protocol.

To edit advanced options:

1. Click the **Settings** icon.
   The Settings dialog box opens.
2. Click the **Advanced** tab.
   The Advanced dialog box opens (see Figure 29).

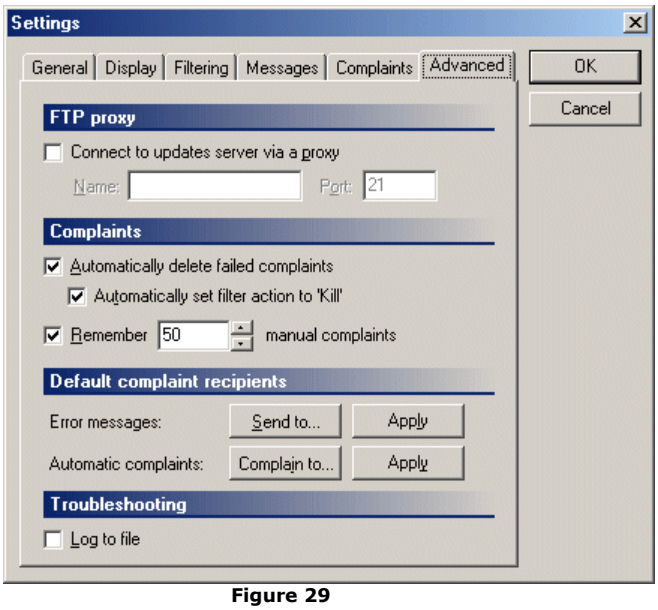


Figure 29

3. To connect to the filter updates server via a proxy:
   a. Select **Connect to updates server via a proxy**.
   b. Enter the name and number of your port address.
4. Edit **Complaints** options if necessary:
   A failed complaint is a complaint message that cannot be sent.
   - **Automatically delete failed complaints**: If this option is selected, SpamKiller will attempt not to notify you (via e-mail message) of failed complaints. If this option is not selected, SpamKiller will send you an e-mail whenever a complaint cannot be sent.
   - **Automatically set filter action to Kill**: A failed complaint usually means that the e-mail address that the complaint was sent to is invalid. SpamKiller will try to locate the filter that caused the complaint and set its action to Kill, so that no more complaints are sent out.
   - **Remember manual complaints**: By default, SpamKiller remembers the last 50 manual complaints that you sent. If you receive more spam from the same sender, you can retrieve and send the same complaints again without having to select addresses and complaint messages.
5. To edit **Default complaint recipients** for automatic complaints and error messages:
   a. Click **Send to** for error messages, or click **Complain to** for complaint messages.
   b. Select the address or account to send messages to.
   c. Click **Apply**.

6. Click **Log to File** to log the communication between SpamKiller and the e-mail server. The log is saved in the file SpamKiller.log on your computer. Reviewing the log file can often help solve configuration problems and other technical issues.
   Note: Selecting **Log to file** may cause SpamKiller to run slower.
7. Click **OK**.

Chapter 8 – Sending Complaints and Error Messages

When SpamKiller intercepts spam or possible spam, you can send complaints or error messages to try to prevent future spam from the same sender. SpamKiller includes standard complaints and error messages; however, you can edit them or create new ones to suit your needs. You can send messages automatically, manually, or both.

The difference between complaints and error messages is that complaints are sent to an abuse-reporting address (or somewhere similar) at the spam's domain. Error messages are sent to the reply address of the spam. The purpose of sending an error message is to trick the sender into believing that your e-mail address does not exist.

Sending Automatic Messages

SpamKiller can send complaint or error messages automatically as soon as you receive spam. Automatic messages are associated with filters. In other words, if you want SpamKiller to send an automatic message, you indicate it on the filter itself. When you specify a filter to send automatic messages, the filter will send a message when it detects spam or possible spam.

Sending Automatic Complaints and Error Messages

To send automatic complaints and error messages:

1. Select the filter that must send an automatic complaint or error message:
   a. Click the **Filters** icon.
   b. Select a filter-type tab that lists the filter.
   c. Select a filter from the **Filters** list.
2. Click **Properties**.
   A filter dialog box opens (see Figure 30).

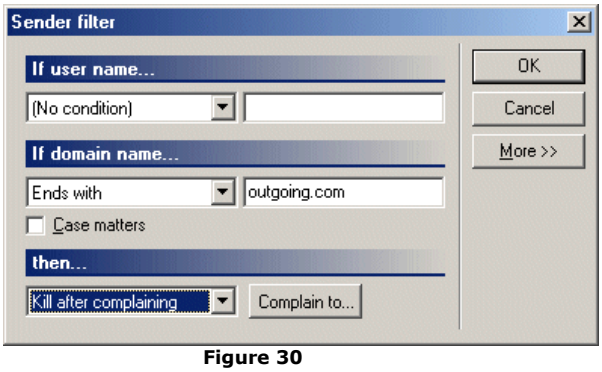


Figure 30

3. From the **then...** field, select **Kill after complaining** or **Kill after error message** (see Figure 31).

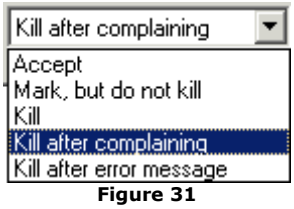


Figure 31

4. Click **Send to** or **Complain** to, and then select an address.
5. Click **OK**.

The filter will send the default complaint or error message to the selected address. To edit or view default messages, see "Changing or Viewing Default Automatic Messages."

Changing or Viewing Default Automatic Messages

To change or view default messages for automatic messages:

1. Click the **Settings** icon.
2. Click the **Complaints** tab.
   The Complaints dialog box opens (see Figure 32).

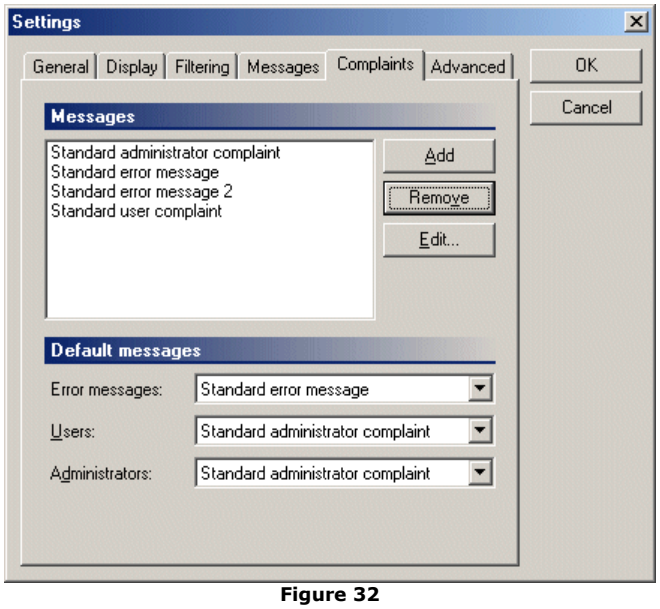


Figure 32

3. To change the default error message, select a message from the **Error messages** list.
   If sending "Standard error message" does not seem to prevent spam from entering your inbox, try sending "Standard error message 2."
4. To change the default user complaint message, select a message from the **Users** list.
5. To change the default administrator complaint message, select a message from the **Administrators** list.
6. Click **OK**.

Sending Manual Messages

If you want to target specific spam e-mail, you can send one or more manual messages. To view, add or edit message types, see "Creating, Editing, and Removing Messages."

Sending Manual Complaints

To send a manual message:

1. Click the **Killed Mail** or **Live Mail** icon to open your Killed Mail or Live Mail box.
2. Select a message to complain about.
3. Click **Send Complaint**.
   The Complain dialog box opens (see Figure 33).

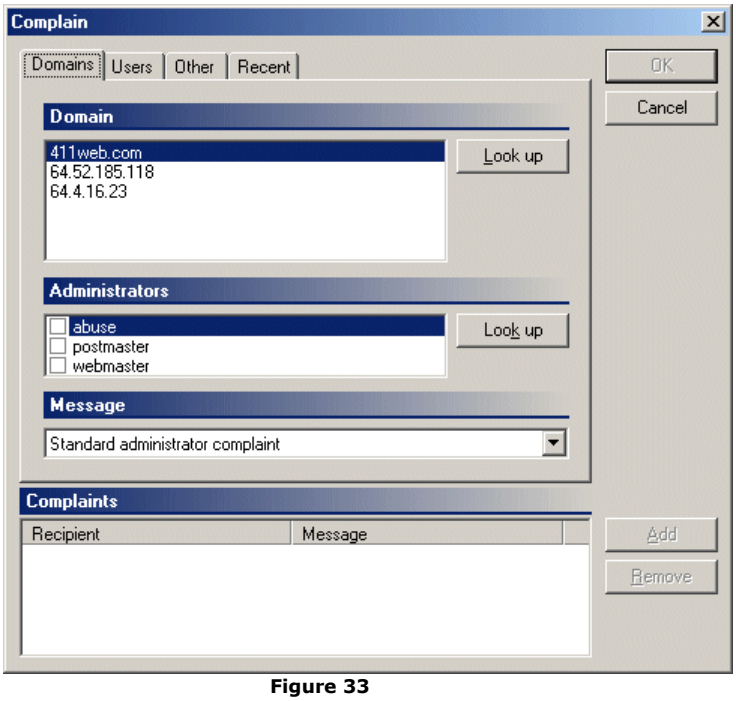


Figure 33

4. Define the complaints as described in the following instructions:

To send a domain-type complaint:

1. Click the **Domains** tab.
   The Domains dialog box opens (see Figure 34).

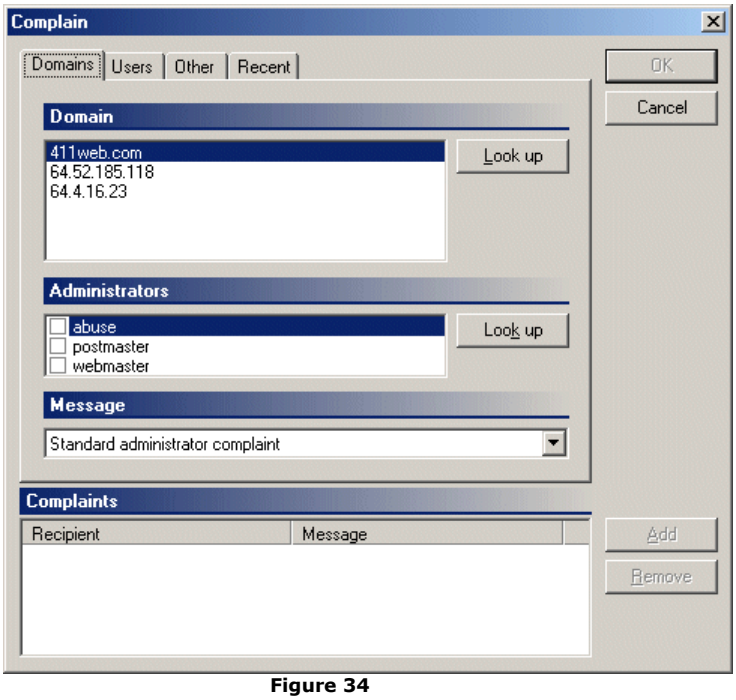


Figure 34

2. Select a domain to complain to from the **Domain** list.
   For more information on a domain, select the domain, and then click **Look up**.
3. From the **Administrators** list, select the accounts where you want to send the complaint.

For more information on an account, select the domain, and then click **Look up**. SpamKiller connects you to abuse.net. The information might help you determine where to send the complaint.

4. From the **Message** list, select the complaint message you want to send.
5. Click **Add**.
   The message or messages appears in the **Complaints** list.
   To remove a complaint from the **Complaints** list, select a complaint, and then click **Remove**.
6. To add to the list of messages before sending them, define another domain-type complaint, or click another tab to define another complaint type.
7. When you are finished, click **OK** to send all complaints in the **Complaints** list.

To send a user-type complaint:

1. Click the **Users** tab.
   The Users dialog box opens (see Figure 35).

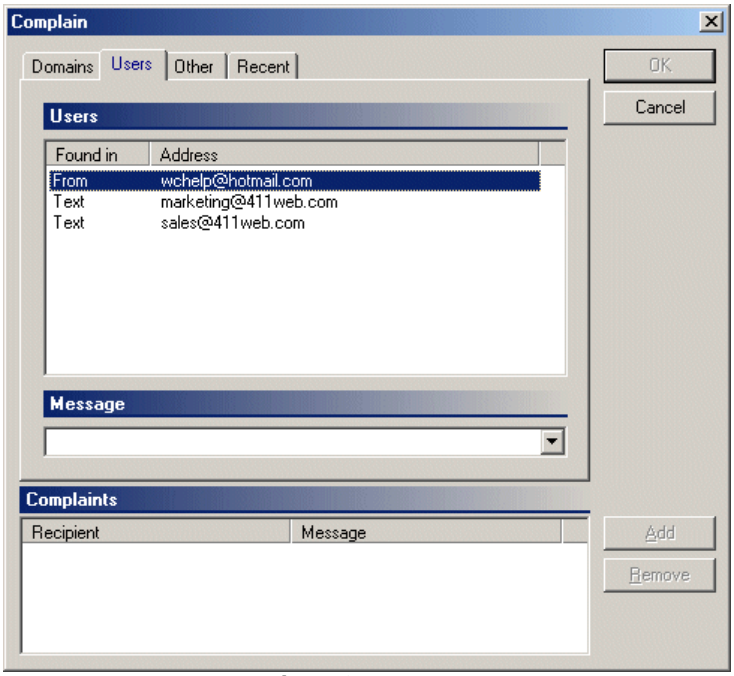


Figure 35

2. From the **Users** list, select an address where you want to send the complaint.
3. Select the message you want to send from the **Message** list.
4. Click **Add**.
   The complaint appears in the **Complaints** list.
5. To add to the list of messages before sending them, define another user-type complaint, or click another tab to define another complaint type.
6. When you are finished, click **OK** to send all complaints in the **Complaints** list.

To send an other-type complaint:

1. Click the **Other** tab.
   The Other dialog box opens (see Figure 36).

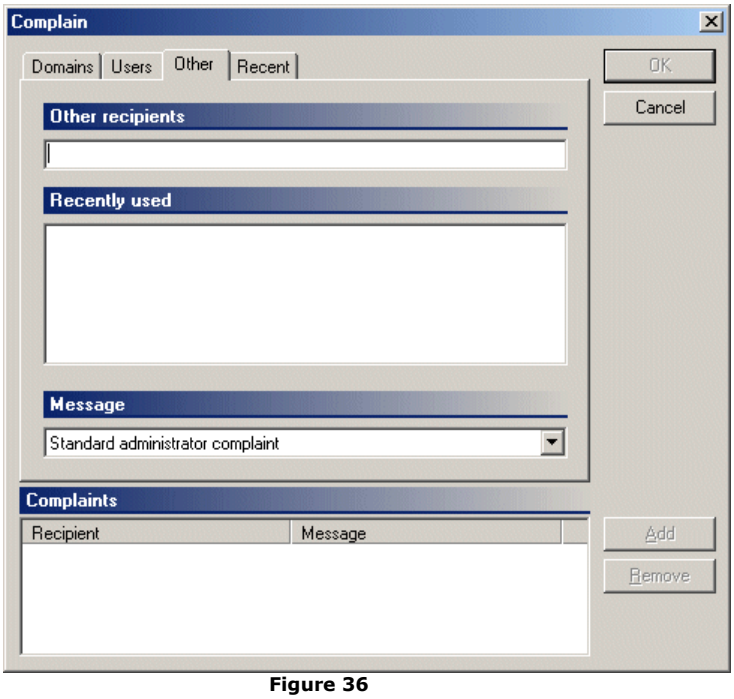


Figure 36

2. In the **Other recipients** field, enter the e-mail address where you want to send the complaint, or select an address from the **Recently used** list.
   The **Recently used** list contains address where you recently sent complaints.
3. Click **Add**.
   The complaint appears in the **Complaints** list.
4. To add to the list of messages before sending them, you can define another Other-type complaint, or click another tab to define another type of complaint.
5. When you are finished, click **OK** to send all complaints in the **Complaints** list.

To resend a recent complaint:

1. Click the **Recent** tab.
   The Recent Complaints dialog box opens (see Figure 37).

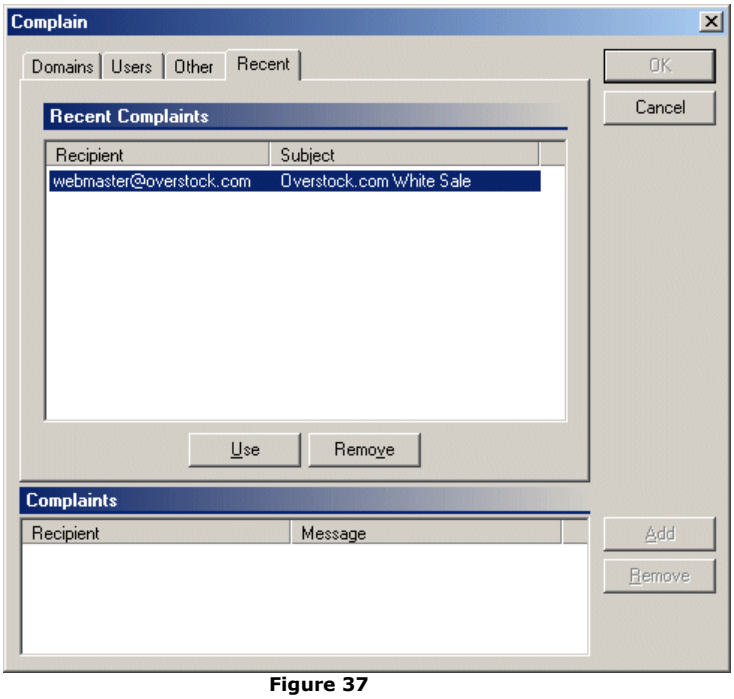


Figure 37

2. Select a complaint from the **Recent Complaints** list.
3. Click **Use**.
   The complaint appears in the **Complaints** list.
4. When you are finished, click **OK** to send all complaints in the **Complaints** list.

Sending Manual Error Messages

To send a manual error message:

1. Click the **Killed Mail** or **Live Mail** icon to open your Killed Mail or Live Mail box.
   A list of messages appears.
2. Select a message.
3. Click **Send error**.
   An error message is sent to the reply address on the spam message.

Creating, Editing, and Removing Messages

Before you create or send complaints and error messages, you might want to view the existing messages to see if you need to edit them, or create additional messages. You can also remove messages.

Adding, Editing, and Viewing Complaints and Error Messages

To add, edit, or view complaints and error messages:

1. Click the **Settings** icon, and then click the **Complaints** tab.
   The Complaints dialog box opens. The Messages list displays available messages (see Figure 38).

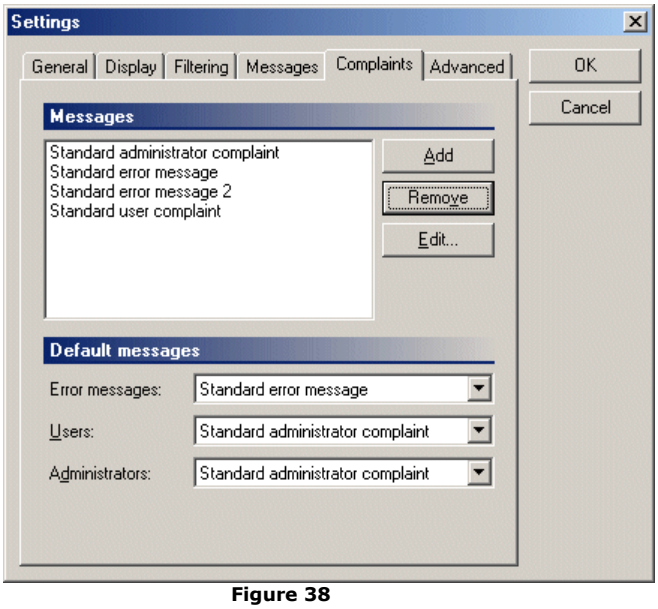


Figure 38

2. Click **Add** to create a new message, or to edit or view a message, select the message, and then click **Edit.**
   The Complaint Message dialog box opens (see Figure 39).

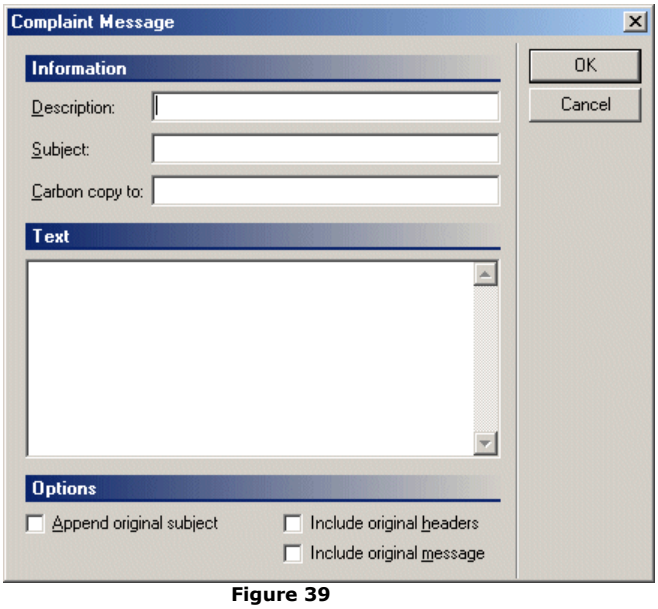


Figure 39

3. Enter information about the complaint or error message:
   - **Description**: Enter the description of the message. The description will appear in the list of available complaint messages.
   - **Subject**: The subject will appear as the subject on the message.
   - **Carbon copy to**: Enter any additional recipient e-mail addresses.
4. Enter the message text in the **Text** field.
5. Clear the following options if you want to disable the feature:
   - **Append original subject**: The subject of the original message is appended to the subject of the complaint message.
   - **Include original headers**: The headers on the spam e-mail are included in the complaint message. This option should be selected if complaints will be sent to system administrators, so administrators can use headers to track down the spam sender.

- **Include original message**: A copy of the spam message text is included in the complaint message.

6. Click **OK**.

Removing Complaints and Error Messages

To remove a complaint or error message:

1. Click the **Settings** icon, and then click the **Complaints** tab.
   The Complaints dialog box opens. The Messages list displays the available messages in the **Messages** list (see Figure 40).

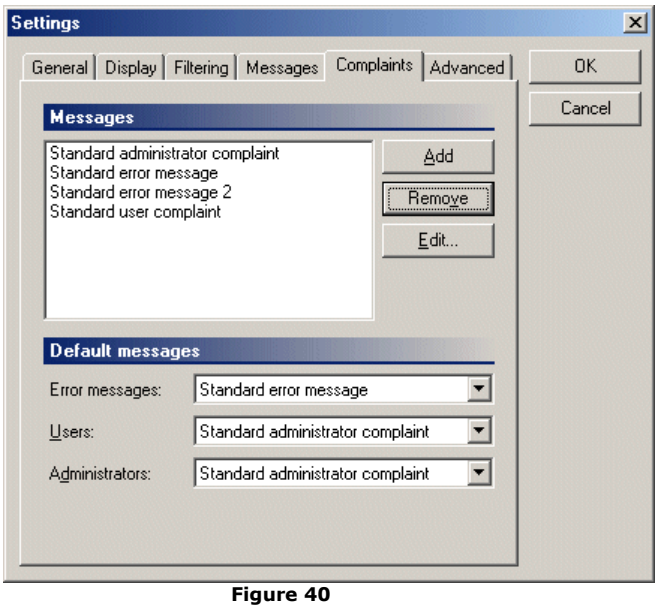


Figure 40

2. Select the message you want to remove, and then click **Remove**.

Editing Advanced Message Settings

Advanced message settings indicate how SpamKiller handles failed messages, the number of recent complaints SpamKiller must keep copies of, and default addresses for automatic complaints and error messages. You normally do not need to change these settings. For details see "Editing Advanced Options."

Appendix A – Tips and Troubleshooting

Using SpamKiller With Your E-mail Account

SpamKiller works with most Internet e-mail clients. In fact, since SpamKiller works directly with the email server, it does not matter which e-mail program you use. However, you might want to slightly modify the way you work with e-mail to optimize SpamKiller's ability to filter your e-mail. This does not apply to MAPI type e-mail accounts. For an explanation on the differences between MAPI and POP3 accounts, see "Mixed Protocol Environments."

To optimize SpamKiller's ability to filter your-email:

1. Switch off automatic e-mail checking in your e-mail program. This has two advantages:
   - First, SpamKiller must be able to filter your messages before they are retrieved by your e-mail program. If not, SpamKiller will not see the messages, since it works with your server, not your e-mail program.
   - Second, SpamKiller and the e-mail program will not be competing for access to your inbox.

     Internet e-mail servers (also known as POP3 servers) are designed to allow only one program at a time to access a inbox. For example, both your e-mail program and SpamKiller cannot check your e-mail simultaneously. The program that gets there first will succeed, while the other one will be refused access.
2. Set up SpamKiller to automatically run your e-mail program when you get new e-mail. Obviously, you still want to use the e-mail program to read your messages. You can configure SpamKiller to run any program when new e-mail arrives. The most common use for this feature is to automatically start the e-mail program. The added advantage is that you do not have to keep your e-mail program running at all times.

Changing How Lists Are Sorted

You can change how items are sorted in most of SpamKiller's lists. In most cases, the default sort order is the most useful.

For example, if you want to sort the message by size, you can click the Size column header. If you click the same column header again, it reverses the sort order (that is, it switches between ascending and descending sorting).

To reset the list to the original sorting (the order in which the messages were received), click the leftmost, unlabeled column header.

Adding the Right Filters

Knowing which filters to add can be difficult. A good filter blocks spam but lets ordinary messages through unscathed. Here are some useful recommendations.

Do not filter on individual e-mail addresses

Spammers frequently use so-called throwaway accounts, which are e-mail accounts that they use just a few times to send out their messages.

Most responsible Internet Service Providers close these accounts when they start receiving many complaints. Having 20,000 filters will not help you if most of them are obsolete.

Instead, filter on entire domains, and use the Friends List to ensure that the messages you want to read get through.

Be careful when you add a message text filter

The standard message text filters were created after careful analysis spam e-mail. Look carefully at the phrase that you plan on filtering on. If it is likely to appear in a normal e-mail message, use one of the other filter types instead.

Use the Friends List actively

The Friends List is one of the most useful features of SpamKiller. It ensures that your friends' messages are left untouched, and works very well in combination with other filters.

For example, if you have friends at a domain that also is the source of a lot of spam, first create a filter that blocks an entire domain, and then add your friends to the list. You will not see any more spam from that domain.

Use country filtering

Spammers sometimes route their messages via servers in other countries, as an attempt to avoid legal and other problems. SpamKiller's unique country filters let you counter this technique very easily. Simply add filtering on the involved countries, and if you have friends in these countries, add them to the Friends List.

Speeding Up Filtering

If you have a slow connection to the Internet, you might want to speed up the filtering process. While SpamKiller is highly optimized for speed, you can do a few things to reduce the amount of data that are transferred to your computer.

Adjust the 'large message' threshold

Spammers normally send short messages, usually just a kilobyte or two. If you receive a lot of e-mail with large attachments, you can improve performance by setting this number to a lower value (for example, 5 or 10). For other information about large messages, see "Handling Large Messages."

Don't send automatic complaints

Sending complaints takes time, just like receiving e-mail does. If you set your filter's action to Kill instead of Kill after complaining, you will improve performance.

Mixed Protocol Environments

SpamKiller is designed to work with three different types of e-mail accounts, POP3, MAPI, and MSN/Hotmail. There are some differences among them, which affect how SpamKiller performs filtering.

POP3

This is the most common account type, and is the standard for Internet e-mail. When you have a POP3 account, SpamKiller connects directly to the server and performs filtering there (that is, before the messages have been retrieved by your e-mail program).

Since most e-mail programs will delete the messages from the server when they are retrieved, SpamKiller will not be able to filter after you have loaded them into your e-mail program. This is why you should switch off automatic checking in your e-mail program.

MSN/Hotmail

MSN/Hotmail accounts are web-based e-mail accounts. Filtering on MSN/Hotmail accounts is similar to that on POP3 accounts.

MAPI

MAPI is a system designed by Microsoft that supports many types of messaging, including Internet mail, faxing, and Exchange Server messaging. For this reason, MAPI is often used in corporate environments when the company is running Microsoft® Exchange Server. However, many people use Microsoft's Outlook and Exchange programs for personal Internet e-mail.

SpamKiller can access MAPI accounts, but here are some issues that you should be aware of:

- Filtering is normally not performed until after you have retrieved the messages with your e-mail program.
- Filtering is much faster if you keep your e-mail programming running at all times.

- SpamKiller will filter only your default inbox, and only Internet e-mail messages.

Apart from these minor differences, MAPI, POP3, and MSN/Hotmail accounts are treated in the same way by SpamKiller.

To Complain or Not To Complain

Complaints can be a useful tool in the fight against spam, but use it sparingly. In some cases, complaining can increase the amount of spam that you get, rather than reduce it.

We recommend that you never complain directly to the spammer. Spammers often buy huge lists of e-mail addresses, many of which are no longer valid. Your response serves as a confirmation that your e-mail address is indeed valid, which means the spammer can keep you on the lists.

A better approach is to use the Send error feature. This will send an error message to the spammer that indicates your e-mail address is no longer valid. Most likely, the spammer will remove your address from the lists in order to save time and money.

You can also complain to the spammer's system administrator or to the upstream provider (explained below). Which one you choose depends on policies of the spammer's Internet Service Provider (ISP).

Most of the large ISPs have strict anti-spam policies, and will usually shut down the spammer's account when they receive complaints. If you recognize the spammer's domain as belonging to a responsible ISP, you can safely send your complaint to the postmaster or abuse accounts.

If, on the other hand, you have reason to suspect that the spammer's account is hosted by an ISP that endorses spamming, complaining to them is probably pointless. In this case, try to find out who is the next link in the chain (that is, who is providing the ISP with their Internet connection). This is known as the upstream provider. Sending a complaint to the administrators of this domain is sometimes effective, and sometimes not.

Tracking down upstream providers can be a complex subject. We suggest that you consult one of the many Web sites that provide information on spam tracking. A good place to start is http://www.cauce.org/.

What Does “(Not Retrieved)” Mean?

Sometimes, the message text pane on the Inbox pane displays this text instead of the message text.

This message was not retrieved automatically, either because it is too large or because you have disabled Message Text filtering.

Here are two possible reasons for this:

- The message is larger than the maximum size that SpamKiller can retrieve automatically. Since most spam messages are relatively small, you will save time by not filtering large messages. You can adjust the size limit in the program's settings.
- You have switched off Message Text filtering.

Command-Line Parameters

You can change the way SpamKiller behaves by adding command-line parameters to your shortcuts. Some parameters control what SpamKiller does on startup, while others are used for troubleshooting purposes.

These command-line parameters determine how SpamKiller starts up:

/ONCE
SpamKiller filters all accounts once and then terminates immediately.

/OPEN
The main window is opened automatically when SpamKiller starts.

/SUSPENDED
SpamKiller starts in suspended mode, i.e. no automatic filtering will be performed.

This option will compensate for this behavior, but it does incur a performance penalty.

Note that parameters must be added after the last quote, and that a space must be between the quote and the first parameter:

"C:\Program files\SpamKiller\SpamKiller.exe" /open

Remember to change all your shortcuts. By default, SpamKiller adds shortcuts both to the Programs menu and the StartUp folder.

If SpamKiller Is Unable To Autodial

On some Microsoft Windows 95 systems, automatic dial-up does not work correctly. This is caused by a bug in Windows, which damages the password lists on your computer.

The result is that the passwords associated with your dial-up connections are corrupted. Often, you must type in your password every time you log on. When an application tries to dial automatically, you might see an error message similar to this:

"The computer you have dialed in to has denied access because the username and/or password is invalid on the domain."

According to Microsoft, this problem can be solved by:

- Downloading and running the Mspwlupd2.exe program, available from the Microsoft Web sites.
- Deleting the file RNA.PWL, which is located in your Windows folder.
- Restarting your computer.

Additional assistance is available from Microsoft's support pages on the Web. You might find these technical support articles helpful:

Q135197

Q137361

Q148925

Q141858

Q148899

Sending Complaints Does Not Seem To Work

If you get an error message when SpamKiller tries to send an automatic or manual complaint, here are two possible reasons:

Your ISP does now allow "relaying"

Many ISPs will not let you send e-mail through their outgoing server unless you are connected to the Internet through them.

This is an anti-spam measure, and is intended to prevent abuse of mail servers for spamming purposes. It means that you must both have an account with the ISP and also connect to the Internet via them to be allowed to send e-mail.

If you check multiple e-mail accounts with SpamKiller, you might not be able to send complaints for accounts at other ISPs than the one you are currently connected to. The solution is to use the same e-mail server for all accounts (that is, the one that belongs to the ISP that you connect to).

Example:

Assume that you have two e-mail accounts, joe@smallisp.com and jane@bigisp.com. If you normally connect via smallisp.com, set the outgoing server for Jane's account to smallisp.com's server:

Incoming mail server: mail.bigisp.com

Outgoing mail server: mail.smallisp.com

Joe's account remains unchanged.

You might need to correct the name of your Outgoing mail server

When you set up a new e-mail account, SpamKiller automatically copies what you type in the Incoming mail server name to the Outgoing mail server name.

In many cases, these two names are the same. If your servers have different names, correct the name of the Outgoing mail (SMTP) server.

For details on editing server names, see Editing Server Properties.

If SpamKiller Killed Legitimate Mail

If you find legitimate mail in the Killed Mail box, you can place the message back in your inbox. For details, see "Rescuing Mail." From the Killed Mail box, you can also add sender information to the Friends List so that SpamKiller accepts all mail from that sender or the sender's domain. For details, see "Adding to the Friends List."

From the Friends page, you can add or import e-mail addresses into the Friends List. For details, see Chapter 4, "Adding Friends."

Handling Large Messages

By default, SpamKiller filters all e-mail, except for messages (including attachments) that are larger than 100 kilobytes. You can edit SpamKiller to check larger messages by increasing the maximum message size setting. However, if you increase the message size setting, SpamKiller might take longer to check your mail.

An example of spam that is often larger than 100 kilobytes is messages with viruses. Instead of modifying SpamKiller to check larger messages, you might want to install an anti-virus program on your computer. McAfee.com VirusScan Online is an anti-virus program that you can easily purchase and install from the McAfee.com Web site. For more information about VirusScan Online, go to http://www.mcafee.com/, click **Products & Services**, and then click **VirusScan Online**.

For details on changing the maximum message size, see "Editing Message Options."

Configuring Microsoft® Internet Explorer

McAfee.com uses ActiveX controls and cookies in its applications. These technologies require specific Internet browser configurations to ensure the applications are installed correctly and work properly on your computer.

Most Internet browsers already have the proper settings to install SpamKiller. To avoid any problems with the installation, we suggest that you verify that the Internet Explorer settings are correct before you try to install SpamKiller.

First, determine which version of Internet Explorer you are using:

1. Open Internet Explorer.
2. On the Internet Explorer menu bar, click **Help**, and then click **About Internet Explorer**.
3. Look at the version number next to **Version:**, and note the first three numbers.
   Example: in *Version: **5.50**.4807.2300*, the version of Internet Explorer is 5.50.
4. Follow the Configuration instructions for your version of Internet Explorer.

Configuring Internet Explorer 5.x

1. Open Internet Explorer. On the **Tools** menu, click **Internet Options** to open the Internet Options dialog box.
2. Click the **Security** tab (see Figure 41). Make sure that you are in the **Internet** Web content zone and that the security level for this zone is set to **Medium** (the default setting) or **Low**.
3. If you are not sure whether your security options are correct, click **Default Level** to set the zone to **Medium** (recommended).
4. If you are an advanced user who wants to customize your security settings, click **Custom Level** to open the Security Settings dialog box. McAfee.com requires that the following options must be enabled.

a. Select **Enable** for these ActiveX controls and plug-ins options:
   - **Download signed ActiveX controls**
   - **Run ActiveX controls and plug-ins**
   - **Script ActiveX controls marked safe for scripting**

b. Select **Enable** for the **Active scripting** option under the Scripting settings.

5. When you are done, click **OK**, and then click **Yes** to confirm the changes.
6. Click **OK** to close the Security Settings dialog box.
7. Click **OK** to close the Internet Options dialog box.
8. Exit Internet Explorer.

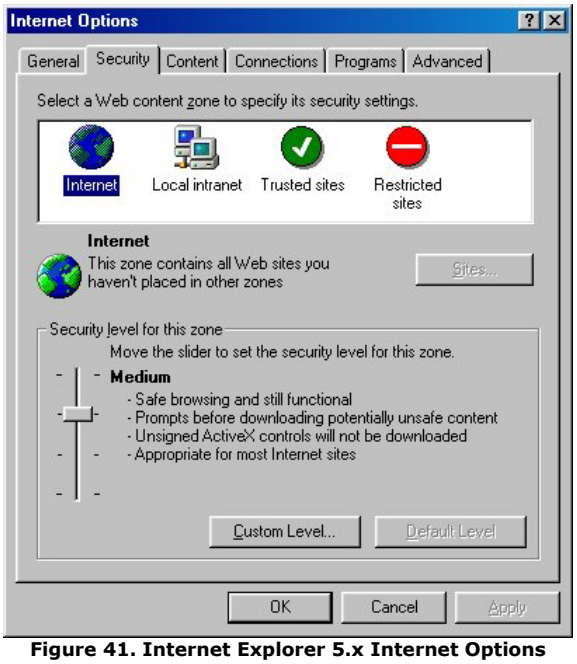


Figure 41. Internet Explorer 5.x Internet Options

Configuring Internet Explorer 6.x

1. Open Internet Explorer. On the **Tools** menu, click **Internet Options** to open the Internet Options dialog box.
2. Click the **Security** tab (see Figure 42). Make sure that you are in the **Internet** Web content zone and that the security level for this zone is set to **Medium** (the default setting) or **Low**.
3. If you are not sure whether your security options are correct, click **Default Level** to set the zone to **Medium** (recommended).
4. If you are an advanced user who wants to customize your security settings, click **Custom Level** to open the Security Settings dialog box. McAfee.com requires that the following options must be enabled.
   a. Select **Enable** for these ActiveX controls and plug-ins options:
      - **Download signed ActiveX controls**
      - **Run ActiveX controls and plug-ins**
      - **Script ActiveX controls marked safe for scripting**

   b. Select **Prompt** for these ActiveX controls and plug-ins options:
      - **Download unsigned ActiveX controls**
      - **Initialize and script ActiveX controls not marked as safe**

   c. Select **Enable** for the **Active scripting** option under the Scripting settings.
5. When you are done, click **OK**, and then click **Yes** to confirm the changes.
6. Click the **Privacy** tab on the Internet Options dialog box (see Figure 43), and then click **Advanced** to open the Advanced Privacy Settings dialog box.
7. Make sure that **Override automatic cookie handling** and **Always allow session cookies** are selected, and then click **OK** to close the Security Settings dialog box.
8. Click **OK** to close the Internet Options dialog box.

9. Exit Internet Explorer.

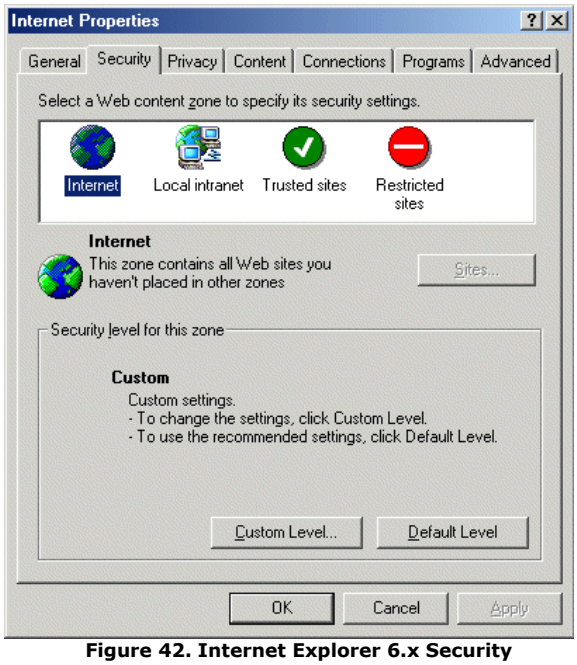


Figure 42. Internet Explorer 6.x Security

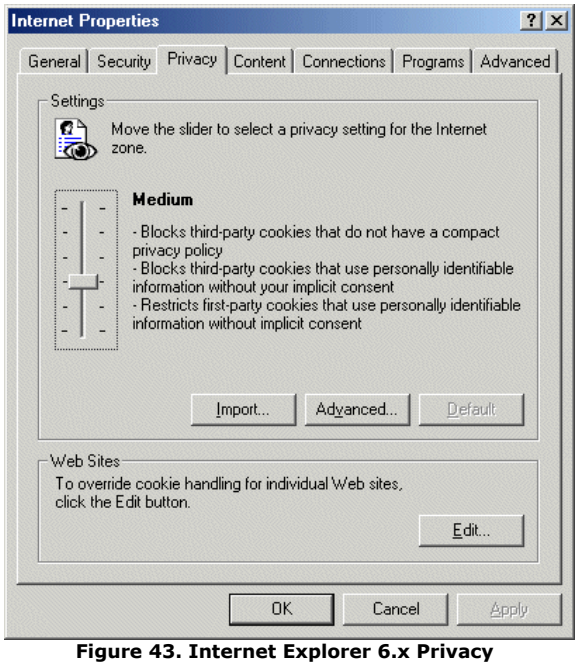


Figure 43. Internet Explorer 6.x Privacy

About ActiveX Controls

ActiveX controls are software modules based on Microsoft's Component Object Model (COM) architecture. They add functionality to software applications by seamlessly incorporating pre-made modules with the basic software package. Modules can be interchanged but still appear as parts of the original software.

On the Internet, ActiveX controls can be linked to Web pages and downloaded by an ActiveX-compliant browser, such as Internet Explorer 5.0 or later. ActiveX controls turn Web pages into software pages that perform as any other program launched from a server.

McAfee.com uses ActiveX controls in its applications, and you must download the specific ActiveX components required for each application. Once these components are loaded, you do not need to download them again unless upgrades or updates become available.

Appendix B - McAfee.com Privacy Policy

McAfee.com is committed to protecting your privacy as a consumer. As a data security company, we understand better than most the need for you to maintain control over your personal data when using the Internet. We maintain your privacy through the enforcement of strict internal polices that exceed industry standards. You can also find the Privacy Policy at http://www.mcafee.com/copyright/privacy.asp.

McAfee.com is a licensee of the TRUSTe Privacy Program. TRUSTe is an independent, non-profit organization whose mission is to build users' trust and confidence in the Internet by promoting the use of fair information practices. Because this Web site wants to demonstrate its commitment to your privacy, it has agreed to disclose its information practices and have its privacy practices reviewed for compliance by TRUSTe. By displaying the TRUSTe trustmark, this Web site agrees to notify you of:

1. What personally identifiable information of yours or a third-party is collected from you through the Web site
2. The organization collecting the information
3. How the information is used
4. With whom the information may be shared
5. What choices are available to you regarding collection, use, and distribution of the information
6. The kind of security procedures that are in place to prevent the loss, misuse, or alteration of information under McAfee.com's control
7. How you can correct any inaccuracies in the information.

If you have any questions or concerns regarding this statement, please send them to privacy@mcafee.com. For questions or concerns regarding non-privacy statement issues, please visit our Support Center. If you do not receive acknowledgment of your inquiry or your inquiry has not been satisfactorily addressed, you should then contact TRUSTe at http://www.truste.org/users/users_watchdog.html. TRUSTe will then serve as a liaison with the Web site to resolve your concerns. McAfee.com is committed to protecting your privacy!

McAfee.com is vigilant about protecting your privacy as a consumer. As a data security company, we understand better than most the need for you to maintain control over your personal data when using the Internet. We maintain your privacy through the enforcement of strict internal polices that exceed industry standards.

We Protect Your Right to Privacy
McAfee.com respects your privacy. Our guidelines for protecting the information you provide us during a visit to our Web site appear below. Furthermore, McAfee.com is a registered licensee of TRUSTe. TRUSTe is an independent, non-profit initiative whose mission is to build users' trust and confidence in the Internet by promoting the principles of full disclosure and informed consent. Because we want to demonstrate our commitment to your privacy, we have agreed to disclose our information practices and to have our privacy practices reviewed and audited for compliance by TRUSTe. These include:

- What information we gather/track
- How we use the information
- With whom we share the information
- Our opt-out policy
- Our policy on correcting and updating personally identifiable information
- Our policy on deleting or deactivating your name from our database
- Our policy regarding children who visit our site

Privacy Statement
This statement discloses the privacy practices for www.mcafee.com. We have designed McAfee.com so that no personal identifying information is displayed online or is accessible to the general public.

What Information We Gather/Track
We collect and store some or all of the following information about our users: name; email address; and billing information, such as address, phone number and credit card number. If you do not wish to have your credit card number stored, please contact Customer Service. We also receive and may store certain types of information whenever you interact with us. For example, like many Web sites, we use "cookies", and we obtain certain types of information when your Web browser accesses McAfee.com.

In order to tailor our subsequent communications to you and continuously improve our products and services (including registration), we may also ask you to provide us with information regarding your personal or professional interests, demographics, experience with our products, and more detailed contact preferences. You will have the option of choosing not to provide us with this information.

Use of Data
McAfee.com uses your information to better understand your needs and provide you with better service. Specifically, we use your information to help you complete a transaction, including fulfillment of promotional offers, to communicate back to you, to update you on service and benefits, to personalize our web sites for you, and to manage and renew your subscription(s). Credit card numbers are used only for payment processing and fraud protection, and are not used for other purposes without your permission.

Web Applications
Certain online applications, such as the various elements of the McAfee.com Clinic, store some components on your hard drive. The software employs proprietary technology to scan your computer system and retrieve information regarding your installed software and hardware. The information that is retrieved is used to provide the services you have chosen to subscribe to or use. In addition, unless you indicate you do not want this service, the information will be used to generate advertising that is appropriate for you. The information gathered by these applications is used only to generate output directed to you and is not aggregated or used for any other purpose. It is not stored along with any identifying information about you, nor is it sold, rented, or shared with any outside parties in any form whatever. TRUSTe is currently developing a program to address the collection of data through downloadable consumer software. However, as this program is not yet ready for implementation, TRUSTe does not yet cover data collected in this manner. As soon this program is put in place, McAfee.com looks forward to working with TRUSTe to address this data practice.

Use of Your Email Address
If you provide us with your email address when you register as a customer or make a purchase from us, we will occasionally send you email with recommendations or notices of new products, prices, and services. This email may include paid advertisements from third parties. You may block future email of this type, simply by following the instructions at the bottom of the update messages.

Separately, we send service notifications via email to keep you informed about the status of your service orders or accounts and to provide updates and technical notices. These messages are essential to the maintenance of your subscription and the functionality of our services. Therefore no opt-out is available for service notifications, and these messages cannot be blocked.

Who We Share It With
McAfee.com will not sell, rent, or lease your personally identifiable information to others. Unless we have your permission or are required by law, we will only share the personal data you provide online with other McAfee.com entities and/or business partners who are acting on our behalf for the uses described in "Use of Data". By contract, third parties such as CyberSource and Digital River must comply with their own privacy policies with regard to the renting, selling, or sharing of information. As partners of McAfee.com, they must also offer McAfee.com customers the chance to opt out of information sharing. For advertising purposes, visitor and customer information is statistically aggregated and reported to advertisers. However, we do not disclose to these entities any information that could be used to personally identify you, such as your name, email address, account, password, or transaction history.

Special Relationships
McAfee.com has a number of relationships with business partners. These business partners provide a number of different services.

CyberSource and Telecheck are intermediaries in the purchasing process for McAfee.com. CyberSource provides credit card transaction services for McAfee.com. Telecheck provides electronic check processing services for McAfee.com. Both CyberSource and Telecheck verify your purchase information, such as credit card number or checking account number, and authorize your transaction. In doing so, CyberSource and Telecheck have access to sensitive data about users. They do not use this information for any other purpose. Read CyberSource's privacy policy.
Read Telecheck's privacy policy.

Digital River powers the McAfee Store, and in doing so collects information about users, including credit card information. When a user purchases a product from the McAfee Store, information about the customer and the purchase are shared with McAfee.com. Digital River may occasionally notify you of special offers, new products, services, promotions, and other similar information. McAfee.com users can opt out of receiving such mail from Digital River by calling 1-800-656-5426 and asking to be removed from future emails.
Read Digital River's privacy policy.

Affiliates
When a user or a company signs up to be a McAfee.com affiliate, they do so through LinkShare. LinkShare does share personally identifiable information about affiliates with McAfee.com. This information is not sold, shared, or rented to any third-party, and is used internally only to manage and maintain relationships with affiliates.

Links
McAfee.com contains links to other Web sites. Please note that when you click one of these links, you are 'clicking' to another Web site. We encourage you to read the privacy statements of these linked sites, as their privacy policies may differ from ours.

Cookies
McAfee.com uses software tags called "cookies" to identify customers when they visit our site. Cookies are used to remember user preferences and maximize performance of our services. Additionally, cookies help us to identify returning users so that we don't ask them to enter their email and McAfee.com password with every visit. The information we collect with cookies is not sold, rented, or shared with any outside parties. We also ask that you fill in your first name and last name in a box so that our customer support services can identify and assist you in case of login problems. We cannot provide subscription services to users whose browsers are set to reject all cookies.

We may use third-party advertising companies to serve ads on our site. These companies may employ cookies and action tags (also known as single pixel gifs or web beacons) to measure advertising effectiveness. Any information that these third parties collect via cookies and action tags is non-personal and anonymous. DoubleClick.net sets cookies in McAfee.com visitors' browsers. McAfee.com does not require that users accept cookies from DoubleClick.net in order to access our services. McAfee.com does not have access to the information contained in advertisers' cookies. If you would like more information about this practice and your choices, click here http://www.networkadvertising.org/optout_nonppii.asp.

McAfee.com uses the services of Engage for the serving and/or targeting of ads, promotions and other marketing messages. To do this, Engage collects anonymous data through the use of cookies. To learn more about Engage, including your ability to opt out of the Engage system, go to http://www.engage.com/privacy.

McAfee.com also uses the services of DoubleClick for the serving and/or targeting of ads, promotions, and other marketing messages. To do this, DoubleClick collects non-personal data through the use of cookies about the types of sites you visit and other non-personally identifiable information about you

in order to deliver advertisements about goods and services that may be of interest to you. In the course of serving advertisements or providing other marketing services, DoubleClick may place or recognize a unique, non-personally identifiable cookie in your browser. In providing these services, DoubleClick does not link personally identifiable information (such as your name, land address or telephone number) to your Web site visits. If you would like more information about DoubleClick, its business practices, and its privacy policies, please click here. To opt out of this anonymous online preference marketing service, please click here.

Log Files
McAfee.com maintains log files of the traffic that visits the McAfee.com site. We do not link any information gathered in these log files to personally identifying information. Log files are used to manage traffic loads and information technology requirements for providing reliable service. Information collected includes IP addresses and browser types.

Feedback
We collect user feedback. We do not typically respond to user feedback in the form of email. We do cull testimonials that appear on the site from our feedback form, but only after we have obtained permission from the senders. Users who want a response to specific questions concerning the service or their subscriptions are directed to the customer service area. These questions will be respond to as quickly as possible. We read all of our customer service queries and use the information contained therein only to resolve the question at hand. We also post surveys on our site, ranging from one to ten questions. These surveys are optional and all information is collected anonymously. The information is collected to better understand our user population. It is not sold or transferred to any third-party.

Correct/Update/Delete User Information
Users can update, correct, or delete their personal information on McAfee.com by clicking on the "My Account Info" link. Users may cancel their accounts by accessing the "How to Update your Automatic Renewal and Subscription Status" page at http://clinic.mcafee.com/clinic/membership/cancel.asp.

Our Privacy Policy Regarding Children who Visit our Site

What Information Is Collected?
It's our policy to create website content that requires minimum collection of information from children visiting our site. From time to time, however, we may request limited personally identifiable information (e.g. a child's email address and/or email address of parent or guardian), as explained below, in order to conduct online contests or sweepstakes or offer other online activities. McAfee.com does not condition a child's participation in any of our online activities on the disclosure of more information than is reasonably necessary to participate in the activity.

McAfee.com will not sell, rent, or lease this information to others. Unless required by law, we will only share the personal data provided online with other McAfee.com entities and/or business partners who are acting on our behalf for the uses described in "Use of Data" or for purposes of conducting a contest or sweepstakes.

- **Contests and Sweepstakes**
  McAfee.com occasionally offers contests and sweepstakes, which may be entered online. To participate in a contest or sweepstakes, a **child is asked to provide his or her first name, last name, email address and age. If the child is 13 years old or younger, the last name and the email address are deleted immediately**. He or she is also required to enter the name of a parent and the email address of a parent. We then send the child's parent an email within two business days informing him or her of the child's entry. **The parent must respond and approve the child's entry into the contest or the child's information will be deleted from our records**. All the information collected by McAfee.com is securely maintained and used only for the purpose of conducting the contest or sweepstakes and notifying the winner(s). The parent will be notified if their child wins the contest if the child is

under 13, otherwise the child will be contacted. Once the contest or sweepstakes is finished, we then delete any personal information collected.

Information for Parents

- **How to Update Your Child's Information**
  Please use the link provided in the email that we send you following your child's enrollment in our contest OR send an email to kidsinfo@mcafee.com. The email should contain your child's name and email address, as well as which information you would like updated.
- **How to Prevent Use of Your Child's Information (Request Deletion of Record)**
  Please send an email to kidsinfo@mcafee.com with your child's name and email address, along with the request that your child's name should be deleted from our records.
- **How to Contact Us**
  Privacy Coordinator
  McAfee.com Corp
  535 Oakmead Parkway
  Sunnyvale, CA 94085
  USA
  Tel: (408) 992-8100
  Email: privacy@mcafee.com

Information Security
All information gathered on the McAfee.com site is stored and maintained in secure facilities that limit access to authorized personnel only. This personnel can only access the information through a series of access-control procedures. All McAfee.com employees are briefed about the company's privacy and security policies on a regular basis. The McAfee.com Web site is regularly tested for security breaches to ensure that all information collected is secure from unauthorized viewing.

Notification of Changes
If we change our privacy policy, we will post a notice on our site so our users are aware of the change in what information we collect, how we use it, and/or under what circumstances, if any, we disclose it. If at any point we decide to use personally identifiable information in a manner different from that stated at the time it was collected, we will notify users by email. Users will have a choice as to whether or not we use their previously submitted information in this different manner. Users may choose to have their information used in accordance with the privacy policy under which the information was collected.

Appendix C - General Privacy and Security Guidelines

The following guidelines provide good information about security and privacy issues on the Internet. They are provided as general information. For specific information regarding McAfee.com and its Web site, please see the McAfee.com Privacy Policy appendix of this user guide, or the McAfee.com privacy policy at http://www.mcafee.com/copyright/privacy.asp.

Privacy Statements
Thoroughly read the posted privacy statements of Web sites. A privacy statement is a legally binding document that describes what personal information Web sites gather, how it is collected, and with whom it will be shared. Make sure you understand how businesses will use your information before you do business with a Web site.

Third-Party Approval Seals
These seals indicate an outside agency, such as TRUSTe, monitors the privacy policies of a Web site. In other words, a neutral agency ensures the Web site's owners adhere to their online privacy statement. They also act as a third-party that you can contact if you feel that your privacy has been violated.

Third-party seals usually link to the Web site's privacy statement and to the outside agency's Web site. If you cannot find a Web site's privacy policies, contact the site directly and ask for a copy of its privacy collection and dissemination practices.

Passwords

- Don't create passwords similar to your real name, commonly used nickname, or online screen name.
- Always protect your online passwords. Never offer it to anyone who asks for it, even to someone who says that he or she is calling on behalf of your Internet service provider.
- Change your passwords often.
- Don't store your passwords near your computer or in your desk.

Aggregate Information
Aggregate information might be collected by a Web site but is not "personally identifiable" to you. Aggregate information includes demographic data, domain names, Internet provider addresses, and Web site traffic. As long as companies do not link this information to a user's personal information, the data is considered aggregate.

Security and Credit Cards
Only place credit card orders through secure servers. Most online merchants alert you when you are entering their secure servers. In addition, see if the URL (Web address) begins with "https" rather than "http"; this indicates that you have entered the secure area. Some browsers represent secure areas by either a closed lock or a solid key symbol in the status bar at the bottom of the browser.

The same consumer protection laws that apply in stores apply on the Internet. Using credit cards allows you to contest any charges if the merchandise does not live up to the promotion. In addition, federal law limits your liability to $50 for purchases made with stolen credit card information.

Common Sense
Don't disclose information you wouldn't disclose over the phone or in person.

You can always contact the Web site for more information about its privacy and security practices before you make a purchase.

Index