

Cloudmark Desktop

for Microsoft Outlook

User's Guide



© 2001-2006 Cloudmark, Inc. All rights reserved. Cloudmark, the Cloudmark logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of Cloudmark Inc. and its subsidiaries in the United States and in foreign countries. Other brands and products are trademarks of their respective holders. All product information is subject to change without notice.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine readable form without prior consent in writing from:

All examples with names, company names or companies that appear in this guide are fictitious and do not refer to, or portray, in name or substance, any actual names, organizations, entities or institutions. Any resemblance to any real person, organization, entity or institution is purely coincidental.

While every effort has been made to ensure technical accuracy, information in this document is subject to change without notice and does not represent a commitment on the part of Cloudmark, Inc. Cloudmark makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Cloudmark shall not be liable for any errors or for incidental or consequential damages in connection with the furnishing, performance or use of this manual or examples herein.

Cloudmark, Inc. 128 King Street, 2nd Floor, San Francisco, CA 94107 USA

Cloudmark Europe, Ltd. Carmelite, 50 Victoria Embankment, Blackfriars, London EC4Y 0DX UK

Cloudmark Desktop version 5.0 for Outlook

Last modified: December 12, 2006



Contents

CHAPTER 1	Overview	.1
	What is spam?	.2
	What is email fraud or “phishing”?	.3
	What are email-borne viruses?	.4
	What is <i>not</i> spam or phishing?	.4
	What is Cloudmark Desktop?	.4
	What is My Cloudmark?	.5
CHAPTER 2	Getting started	.7
	System requirements	.7
	Installing Cloudmark Desktop	.8
	Your subscription to Cloudmark	.9
CHAPTER 3	Using Cloudmark Desktop	11
	Blocking spam and phishing	11
	<i>Automatically scanning folders for spam and phishing</i>	12
	<i>Manually scanning a folder for spam and phishing</i>	12
	<i>Blocking a single spam message</i>	13
	<i>Blocking a single phishing message</i>	14
	Unblocking legitimate messages	15
	<i>Unblocking a single legitimate message</i>	15
	<i>Using the smartlist</i>	16
	<i>Adding a sender to the smartlist</i>	17
	<i>Changing an entry in the smartlist</i>	18
	<i>Removing a sender from the smartlist</i>	19
	Configuring your preferences	20

- Selecting folders for automatic scanning 20
 - Adding a folder for automatic scanning 20
 - Removing a folder from automatic scanning 22
 - Selecting the spam detection action 23
 - Showing or hiding statistics and your rating in the toolbar 25
 - Configuring general spam options 25
 - Configuring your firewall settings 27
- Turning off spam blocking 28
- Updating Cloudmark Desktop 29
- Using Cloudmark Desktop on another computer 30
- Uninstalling Cloudmark Desktop 30

- CHAPTER 4 *Using My Cloudmark* 39**
- Logging in to My Cloudmark 39
- Subscribing to Cloudmark 41
 - Purchasing a new subscription. 42
 - Subscribing with an activation code. 44
 - Renewing a subscription 45
 - Switching from a monthly to annual subscription 46
 - Cancelling your subscription 46
- Viewing your referral information. 46
- Changing your email address or password 47
- Retrieving a lost password 48
- Changing your billing information 50

- CHAPTER 5 *Statistics and your rating* 51**
- How statistics work 51
- How your rating works. 52
- Viewing statistics and your rating. 53
- How to influence your rating 54

CHAPTER 6 *Troubleshooting* **55**

CHAPTER 7 *Spreading the word about Cloudmark Desktop* . . **59**

 Telling a friend about Cloudmark Desktop **59**

 Adding a Cloudmark Desktop signature to your email **60**

CHAPTER 8 *Finding more information* **63**

APPENDIX A *Glossary* **65**

Index **69**

Overview

Welcome to the *Cloudmark Desktop User's Guide*. In addition to this introductory chapter, the guide includes chapters that explain how to use Cloudmark Desktop and My Cloudmark:

- Chapter 2, “Getting started”, tells you how to install Cloudmark Desktop and, when you're ready, purchase a subscription.
- Chapter 3, “Using Cloudmark Desktop”, explains how to blocking spam and using the other features of Cloudmark Desktop.
- Chapter 4, “Using My Cloudmark”, provides instructions for managing your Cloudmark subscription, changing your account information, or unsubscribing.
- Chapter 5, “Statistics and your rating”, explains what the statistics mean, how your rating is calculated, and how to achieve the highest ratings.
- Chapter 6, “Troubleshooting”, provides solutions to common problems.
- Chapter 7, “Spreading the word about Cloudmark Desktop”, shows you how to help others block spam and fraudulent email in their own mailboxes.
- Chapter 8, “Finding more information”, provides a list of additional resources that are available to you as a Cloudmark Desktop user.

This chapter explains how Cloudmark Desktop works:

- “What is spam?” below
- “What is email fraud or “phishing?”” on page 3
- “What are email-borne viruses?” on page 4
- “What is not spam or phishing?” on page 4
- “What is Cloudmark Desktop?” on page 4
- “What is My Cloudmark?” on page 5

What is spam?

Spam is unsolicited bulk email, usually for a commercial purpose. A spam message may have some or all of these characteristics:

- the sender is someone you do not know
Spammers make up fake names and email addresses to avoid getting caught. This is called “spoofing”.

- the message contains an advertisement
Usually, the advertisement comes from a merchant from whom you have never purchased products or services.

- the message or its Subject contains jibberish

The following is an example of jibberish that appeared in a spam message:

```
Subject: Re: Zdenko Cushing Check this Offr  
Hi  
Do  
AVE UP  
% on  
ons?  
CIAXanAmbLevVALVIA  
LIS Now $axienitraIUM Now $GRA Now $
```

- the message asks you to click on a Web address
Spam usually points to a commercial Web site where the advertised products or services are sold.
- the message was sent to an email address that does not appear to be yours
Spammers sometimes send messages to an “alias”, that is, an email address that actually points to a list of many email addresses.

Not all messages with these characteristics are spam. For example, a message that you receive from one of your favorite merchants may contain advertising and a Web address, sent from an email account that you may not immediately recognize. Because there is no rigid definition for spam, email users decide what is spam and what is not.

The Cloudmark network consists of many users like you, sending feedback to Cloudmark about which messages are spam and which ones are legitimate. Using your own judgment, you can contribute information about spam that will help everyone in the network.

! *Not all unwanted messages are spam. For example, a message from someone you dislike may be unpleasant, but it is not spam. Reporting such a message may lower your rating in the Cloudmark network.*

What is email fraud or “phishing”?

Fraudulent email, also known as “phishing”, is email that pretends to come from a legitimate commercial source and solicits personal information from the recipient. Whereas the purpose of spam is to sell a product or service, the purpose of phishing is to get information from you that can be used for identity theft.

! *Inspect all commercial email messages carefully before responding. Identity theft is a common and expensive form of crime.*

For example, a message may appear to come from an online merchant of which you are a regular customer. The message may ask you to update your account information, including your credit card, social security number, and other important information. If this message is not really from a legitimate merchant, this information could be used for identity theft.

A phishing message may have some or all of these characteristics:

- the message claims to originate from a merchant
- the message asks you to provide personal information
- the message includes a Web link to a domain that does not match the name of the merchant

For example, imagine the message claims to be from eBay, but the link points to <http://ebay423.detaliesbbl.com/>. The domain is “detaliesbbl”, not ebay.com. This message is probably phishing.

- the message promises financial rewards if you provide the requested information
- the message threatens action against you if you do not provide the requested information

Not all messages with these characteristics are phishing. Use your best judgment when deciding what is phishing and what is not.

What are email-borne viruses?

Email-borne viruses are malicious programs that are carried to your computer by email. They may arrive inside a spam or phishing message, or in messages from friends who do not realize that their own computers are infected. Viruses can inflict serious damage to your computer.

Cloudmark Desktop detects email-borne viruses. Infected email messages are treated just like spam and phishing messages.

What is *not* spam or phishing?

Not all unwanted messages are spam or phishing. Below are some examples of messages which, while undesirable, are neither spam nor phishing:

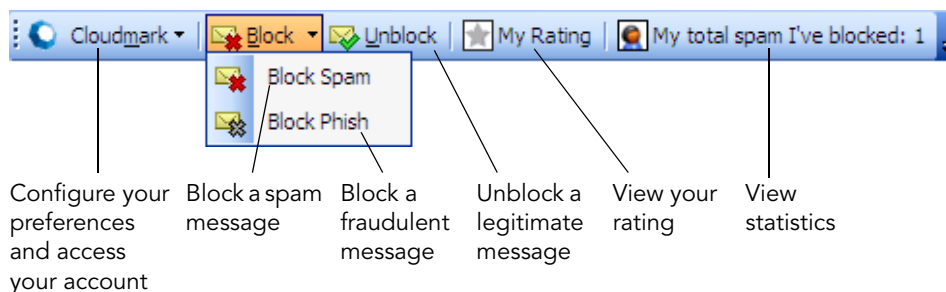
- messages from someone you dislike
- a newsletter you subscribed to but no longer wish to receive

If you report such messages as spam or phishing, your rating in the Cloudmark network may fall. In the case of the unwanted newsletter, consider unsubscribing instead; newsletters typically include instructions for doing this.

What is Cloudmark Desktop?

Cloudmark Desktop is a simple add-on module for Microsoft Outlook and Outlook Express. It adds spam- and phishing-blocking features to your regular email, giving you the power to filter your email so that only legitimate messages arrive in your Inbox. It also filters email-borne viruses.

When you install Cloudmark Desktop, this toolbar is added to your Outlook window:



You can learn how to use this toolbar in Chapter 3, “Using Cloudmark Desktop”.

If, after trying Cloudmark Desktop, you decide to keep it, then you can subscribe to Cloudmark’s network. The network consists of other users like yourself, all filtering their email to reduce spam and phishing. Whenever a spam message is detected on its way to your mailbox, information about the message is sent to the Cloudmark network, where it is used to block similar messages. By participating in this network, you help prevent spam and phishing throughout the network.

For more information about subscribing, see “Your subscription to Cloudmark” on page 9 and “Subscribing to Cloudmark” on page 41.

What is My Cloudmark?

My Cloudmark is your interface to your Cloudmark account. Here you can view your statistics, modify your account information, or update your subscription. My Cloudmark is secure; your account information is received only by Cloudmark. For instructions, see Chapter 4, “Using My Cloudmark”.

Getting started

Once you have installed Cloudmark Desktop, it automatically blocks most spam and phishing without any special action by you. If you would like to learn to use Cloudmark Desktop's additional features, see Chapter 3, "Using Cloudmark Desktop" to learn how.

This chapter shows you how to get started using Cloudmark Desktop.

- "System requirements", below, tells you what you need to have before you begin installing Cloudmark Desktop.
- "Installing Cloudmark Desktop" on page 8 gives you instructions for downloading and installing the software.
- "Your subscription to Cloudmark" on page 9 explains how subscriptions work and which features are available with the different subscription levels.

System requirements

Your computer must have the following components in order to run Cloudmark Desktop:

Operating System Microsoft Windows 2000/XP (2002)

Email Software Microsoft Outlook 2000/XP (2002)/2003

Email Account Cloudmark Desktop works with any type of email account supported by Microsoft Outlook :

- IMAP
- POP3
- SSL POP3
- Microsoft Exchange

- Gmail using SSL POP3
- MSN/Hotmail using HTTP, or Hotmail Plus using POP3 or HTTP
- Yahoo! using HTTP, or Yahoo! Mail Plus using POP3 or HTTP

Cloudmark is currently developing Cloudmark Desktop for Windows Vista for general availability in early 2007.

Installing Cloudmark Desktop

TO INSTALL CLOUDMARK DESKTOP

- 1** If Microsoft Outlook Express is running, close it.
- 2** Use your Web browser to open this page:
<http://www.cloudmark.com/desktop/download/>
- 3** Click the Download Desktop button for Microsoft Outlook Express.
This downloads the program that installs Cloudmark Desktop. Your download will begin automatically. Your browser may ask you to choose a location in which to save the downloaded installer program.
- 4** When the download is complete, double-click the installer file.
The installer file is usually in your My Downloads folder, with this filename:

CloudmarkDesktopOL5.0Eng.exe

The Setup Wizard appears:



5 Click Next.

The License Agreement appears.

6 Select “I accept the terms in the License Agreement”.

7 Click Next.

8 Click Install.

The Setup Wizard installs Cloudmark Desktop.

9 Click Finish.

Desktop is now ready to use. See Chapter 3, “Using Cloudmark Desktop”. Initially, you have a free 15-day trial. See “Your subscription to Cloudmark” below.

Your subscription to Cloudmark

When you first install Cloudmark Desktop, you get a free 15-day trial. All features are fully functional during this trial period.

When the trial period ends, the software no longer automatically filters spam. However, phishing filtering and My Cloudmark remain available.

If you want the complete set of features, you must purchase a subscription to Cloudmark. When you activate your subscription, the complete feature set becomes available. You can find instructions for purchasing, renewing, or cancelling a subscription in “Subscribing to Cloudmark” on page 41.

Using Cloudmark Desktop

This chapter includes topics that explain how to use the features of Cloudmark Desktop:

- “Blocking spam and phishing” below
- “Unblocking legitimate messages” on page 15
- “Configuring your preferences” on page 20
- “Turning off spam blocking” on page 28
- “Updating Cloudmark Desktop” on page 29
- “Using Cloudmark Desktop on another computer” on page 30
- “Uninstalling Cloudmark Desktop” on page 30

Blocking spam and phishing

Cloudmark Desktop provides several ways to block spam and phishing:

- automatically scanning messages before they are delivered
See “Automatically scanning folders for spam and phishing” on page 12.
- manually scanning a folder full of messages that have already been delivered
See “Manually scanning a folder for spam and phishing” on page 12.
- blocking a single message that appears in your mailbox
See “Blocking a single spam message” on page 13 and “Blocking a single phishing message” on page 14.

Whenever you block a message, or a message is automatically caught on its way to your Inbox, the message is moved to the Spam Folder in your mailbox. Cloudmark Desktop creates this folder automatically.

! *Look inside your Spam Folder periodically to check for any legitimate messages that may have been mistaken for spam or phishing.*

If a legitimate message is mistaken for spam or phishing, you can unblock that message to ensure that you receive similar messages in the future. See “Unblocking legitimate messages” on page 15.

Automatically scanning folders for spam and phishing

Cloudmark Desktop can automatically scan incoming email before it appears in your email folders. When it finds spam or phishing on its way to your mailbox, it sends those messages to your Spam Folder. Spam and phishing messages that are caught during automatic scanning will not appear in your regular email folders.

When you install Cloudmark Desktop, it is already configured to scan your Inbox folder automatically. If you have additional email folders, you can also select them for automatic scanning. You may also turn off automatic scanning by selecting no folders. See “Selecting folders for automatic scanning” on page 20.

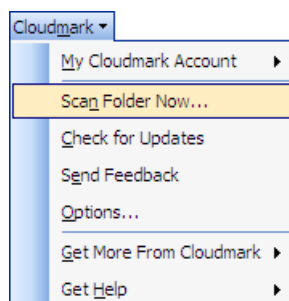
The list of folders to scan is in your Cloudmark Desktop preferences. See “Selecting folders for automatic scanning” on page 20.

Manually scanning a folder for spam and phishing

If you have an email folder that you prefer not to scan automatically (as explained in “Automatically scanning folders for spam and phishing” above), you can scan it manually whenever you like.

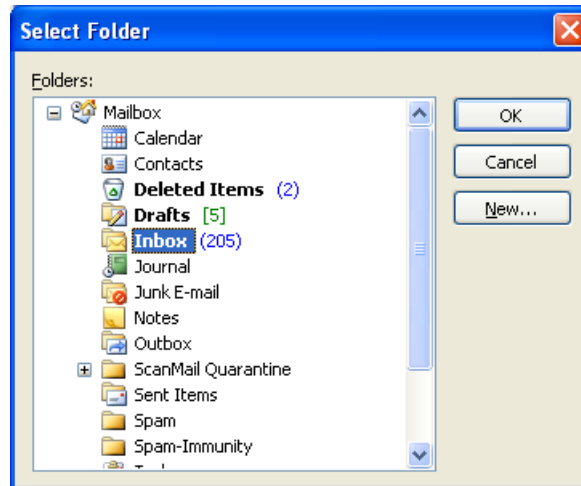
TO SCAN A FOLDER MANUALLY

- 1 Open the Cloudmark menu:



2 Select Scan Folder Now.

The Select Folder window appears, displaying the list of your email folders:



3 Select the email folder you want to scan.

4 Click OK.

Cloudmark Desktop scans the folder, searching for spam and phishing and moving those messages to your Spam Folder.

This may take some time, depending on the number of messages in the folder. A folder with only a few messages may take just a few seconds, while a folder with thousands of messages may require several minutes. When scanning is complete, the progress window closes automatically.

Blocking a single spam message

If a spam or phishing message appears in your mailbox, you can block it. Blocking a message sends it to your Spam Folder and reports it to the Cloudmark network, where it is used to prevent similar messages from appearing in the future, for all users in the network.

! *The messages that you block are sent to the Spam Folder regardless of the Detection Action that you've selected. See "Selecting the spam detection action" on page 23.*

Before blocking a message, check it carefully to be sure that it really is spam. See "What is spam?" on page 2 and "What is email fraud or "phishing"?" on page 3. If

you think the message may be phishing instead of spam, see “Blocking a single phishing message” on page 14.

TO BLOCK A SINGLE SPAM MESSAGE

- 1 In your message list, select the spam message.
- 2 In the Cloudmark Desktop toolbar, click the Block button.



You can click the Block button alone, or you can click the arrow and select Block Spam. Alternatively, you can drag the message into your Spam Folder.

The message disappears from the message list. If you want to look at it again, you can find it in the Spam Folder. If you change your mind and want to unblock the message, see “Unblocking legitimate messages” on page 15.

Blocking a single phishing message

If a fraudulent message appears in your mailbox, you can block it. Blocking a message sends it to your Spam Folder and reports it to the Cloudmark network, where it is used to prevent similar messages from appearing in the future, for all users in the network.

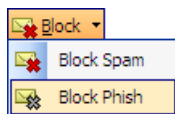
! *The messages that you block are sent to the Spam Folder regardless of the Detection Action that you've selected. See “Selecting the spam detection action” on page 23.*

Before blocking a message, check it carefully to be sure that it really is phishing. See “What is email fraud or “phishing?”” on page 3. If you think the message may be spam instead of phishing, see “Blocking a single spam message” on page 13.

TO BLOCK A SINGLE PHISHING MESSAGE

- 1 In your message list, select the fraudulent message.
- 2 In the Cloudmark Desktop toolbar, click the arrow next to the Block button.

3 Select Block Phish:



Alternatively, you can drag the message into your Spam Folder.

The message disappears from the message list. If you want to look at it again, you can find it in the Spam Folder. If you change your mind and want to unblock the message, see “Unblocking legitimate messages” on page 15.

Unblocking legitimate messages

Occasionally, a legitimate message may be mistaken for spam or phishing. This can happen for different reasons:

- the message may resemble a known form of spam or phishing
For explanations of some of the characteristics of spam and phishing, see “What is spam?” on page 2 and “What is email fraud or “phishing?”” on page 3.
- the message may have been blocked by you or other users in the network
Be sure to categorize your messages accurately. This affects your rating in the Cloudmark network. See “How your rating works” on page 52.

Look inside your Spam Folder periodically to check for any legitimate messages that may have been mistaken for spam or phishing. There are two ways to correct this:

- unblock a single message in your Spam Folder
Use this option for the occasional message that is mistakenly sent to your Spam Folder. See “Unblocking a single legitimate message” below.
- add a legitimate sender to your smartlist
Use this option if multiple messages from one sender are consistently mistaken for spam. See “Using the smartlist” on page 16.

Unblocking a single legitimate message

If you find a legitimate message in your Spam Folder, you can unblock it to ensure that you continue to receive similar messages in the future. Like blocking,

unblocking is reported to the Cloudmark network, where it is used to correctly identify legitimate messages in the future, for all users in the network.

TO UNBLOCK A LEGITIMATE MESSAGE

- 1 Open your Spam email folder.
- 2 In the message list, select the message you want to unblock.
- 3 Click the Unblock button:



The message returns to your Inbox.

If message from certain legitimate senders are consistently mistaken for spam, you can exclude them from filtering by adding them to your smartlist. See “Using the smartlist” below.

Using the smartlist

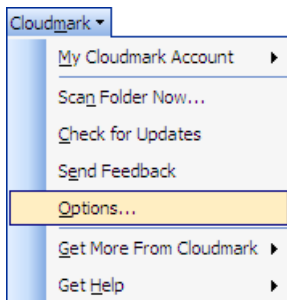
The smartlist is a list of senders whose messages to you are never filtered. All messages from these senders go straight to your regular email folders and will never be diverted to your Spam Folder. This option is useful for serial messages that could be mistaken for spam, such as electronic newsletters, or offers from merchants of whom you are a regular customer.

Keep in mind that spam messages can be “spoofed”, that is, they can be made to appear as if they originate from a different email address than the spammer’s true email address. The smartlist does not prevent spam, because a spammer may pretend to be sending messages from an address in your smartlist. Use the smartlist sparingly.

Adding a sender to the smartlist

TO ADD A SENDER TO YOUR SMARTLIST

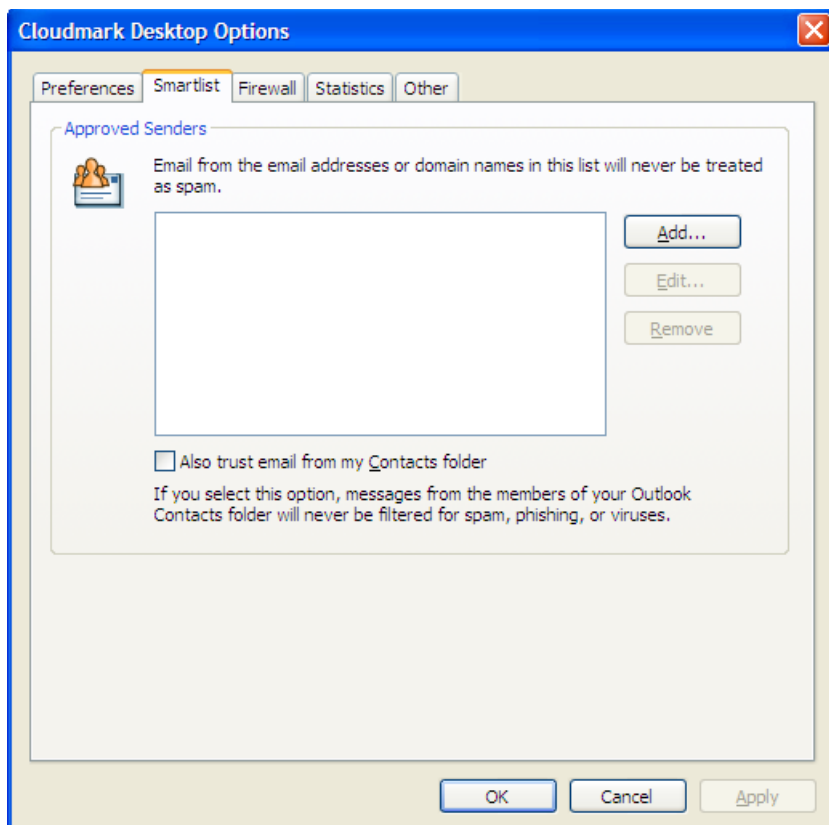
- 1 Click the Cloudmark button to open the menu:



- 2 Select Options....

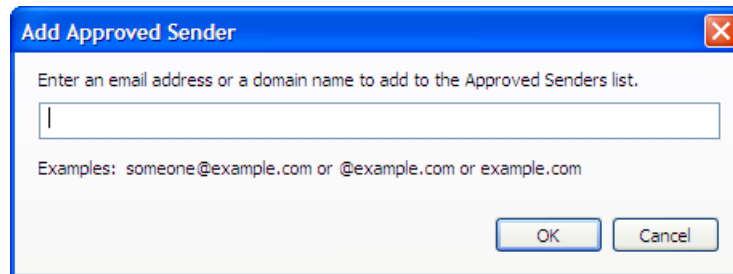
The Cloudmark Desktop Options window appears.

- 3 Click the Smartlist tab:



4 Click the Add button.

The Add Approved Sender window appears:

**5** Enter one of the following:

- an email address, like this:

jane@domain.com

All email from this sender will be whitelisted.

- a domain, like this:

@domain.com

All email from all senders in this domain will be whitelisted.

- a domain and its subdomains, like this:

domain.com

All email from all senders in this domain and its subdomains (such as host1.domain.com, host2.domain.com, and so on) will be whitelisted.

6 Click OK.

The email address now appears in the smartlist window.

7 Click OK.

Changing an entry in the smartlist

If you enter an email address incorrectly in your smartlist, or if a sender's email address changes, you can change the smartlist entry.

TO CHANGE A SMARTLIST ENTRY

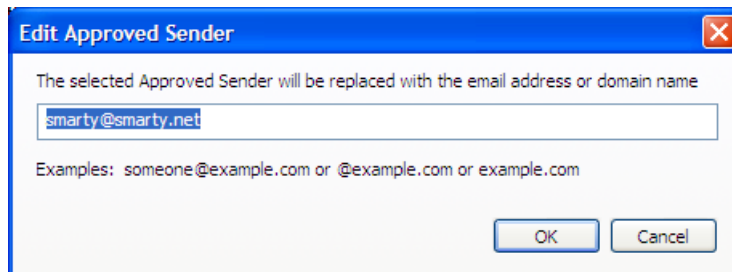
1 Click the Cloudmark button to open the menu.**2** Select Options....

The Cloudmark Desktop Options window appears.

3 Click the Smartlist tab.**4** In the Approved Senders list, select the email address you want to change.

- 5 Click the Edit button.

The Edit Approved Sender window appears:



- 6 Edit the email address as desired.
- 7 Click OK.
The modified email address now appears in the smartlist window.
- 8 Click OK.

Removing a sender from the smartlist

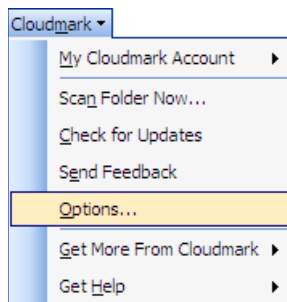
You can remove one sender from your smartlist, or you can empty your entire smartlist.

TO REMOVE AN ENTRY FROM THE SMARTLIST

- 1 Click the Cloudmark button to open the menu.
- 2 Select Options....
The Cloudmark Desktop Options window appears.
- 3 Click the Smartlist tab.
- 4 In the Approved Senders list, select the email address you want to remove.
- 5 Click the Remove button.
A prompt appears, asking you to confirm that you want to remove this entry.
- 6 Click Yes.
The email address disappears from the smartlist.

Configuring your preferences

For most users, the default settings that come with Cloudmark Desktop are sufficient. You can change these settings to suit your preferences. You access your preferences by selecting Options... from the Cloudmark menu in your toolbar:



Preferences are explained in the following topics:

- “Selecting folders for automatic scanning” below
- “Selecting the spam detection action” on page 23
- “Showing or hiding statistics and your rating in the toolbar” on page 25
- “Configuring general spam options” on page 25
- “Configuring your firewall settings” on page 27

Selecting folders for automatic scanning

Cloudmark Desktop can automatically scan incoming messages before they appear in your email folders, as explained in “Automatically scanning folders for spam and phishing” on page 12. You can control the list of folders for automatic scanning, as explained in these topics:

- “Adding a folder for automatic scanning” below
- “Removing a folder from automatic scanning” on page 22

Adding a folder for automatic scanning

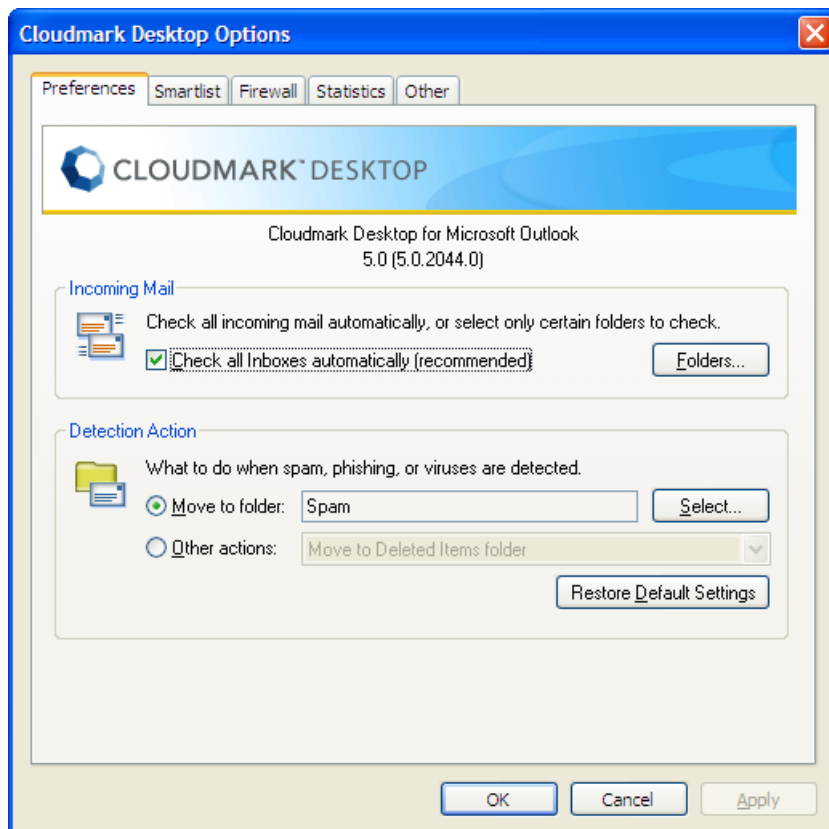
By default, your Inbox folder is scanned for spam and fraud automatically. You can select additional folders for automatic scanning

TO SELECT FOLDERS FOR AUTOMATIC SCANNING

- 1 Click the Cloudmark button to open the menu.

2 Select Options....

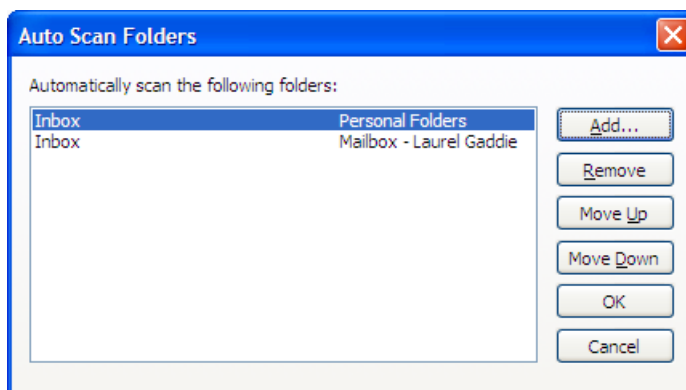
The Cloudmark Desktop Options window appears:



3 Make sure that Check All Inboxes Automatically is selected.

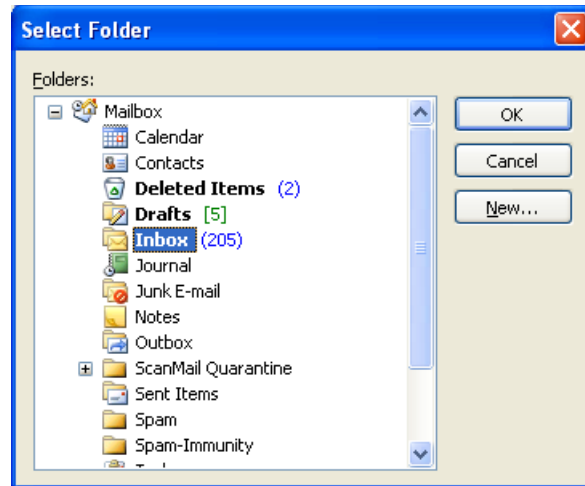
4 Click the Folders... button.

The Auto Scan Folders window appears:



- 5 Click the Add... button.

The Select Folder window appears:



- 6 In the Folders list, select the folder you want to add to the folders that are scanned automatically.
- 7 Click OK.
The selected folder now appears in the Auto Scan Folders window.
- 8 Click OK to close the Auto Scan Folders window.
- 9 Click OK to close the Cloudmark Desktop Options window.

Removing a folder from automatic scanning

If you do not want a folder to be scanned automatically, you can remove it from the list of folders to scan.

TO REMOVE A FOLDER FROM AUTOMATIC SCANNING

- 1 Click the Cloudmark button to open the menu.
- 2 Select Options....
The Cloudmark Desktop Options window appears.
- 3 Click the Folders... button.
The Auto Scan Folders window appears.
- 4 In the folders list, select the folder you want to exclude from automatic scanning.
- 5 Click the Remove button.
The folder disappears from the list of folders to scan.

- 6 Click OK to close the Auto Scan Folders window.
- 7 Click OK to close the Cloudmark Desktop Options window.

Selecting the spam detection action

You can choose the action that Cloudmark Desktop takes when it detects spam or phishing. The following actions are available:

- move to folder

The default option moves messages to the Spam Folder. If you prefer, you can select a different folder.

- move to Deleted Items folder

This option moves spam and phishing messages to the Deleted Items folder. Messages in this folder are deleted whenever your trash is emptied.

- delete instantly

This option deletes spam and phishing messages instantly upon detection, without first moving them to the Deleted Items folder.

! *This option deletes messages permanently. Use it with care.*

- move to Spam Folder and delete after one week

Spam and phishing are moves to the Spam Folder upon detection, then permanently deleted after one week.

- move to Spam Folder and delete after one month

Spam and phishing are moves to the Spam Folder upon detection, then permanently deleted after one month.

- tag as Spam

If you select this option, messages are not moved to another folder. Instead, Cloudmark Desktop clearly marks them as spam. If you want to perform further actions on these messages, such as deleting or moving them, you must do so manually.

TO SELECT THE SPAM DETECTION ACTION

- 1 Click the Cloudmark button to open the menu.

2 Select Options....

The Cloudmark Desktop Options window appears:



3 In the Detection Action area, select the action you want Cloudmark Desktop to take when it finds a spam or fraudulent message.

If you select Move to Folder and you want to use an email folder other than the Spam Folder, then click Select... to choose a different folder.

4 Click OK.

Cloudmark Desktop will apply the selected action to all spam and phishing that detects upon arrival.

! *The selected action does not apply to messages that you block with the Block Spam or Block Phish buttons. Those messages are always moved to your Spam Folder in case you change your mind.*

Showing or hiding statistics and your rating in the toolbar

Statistics tell you how much spam and fraud has been processed by Cloudmark Desktop. You can view statistics at a glance in the toolbar. For more information about statistics, see Chapter 5, “Statistics and your rating”.

TO SHOW OR HIDE STATISTICS IN THE TOOLBAR

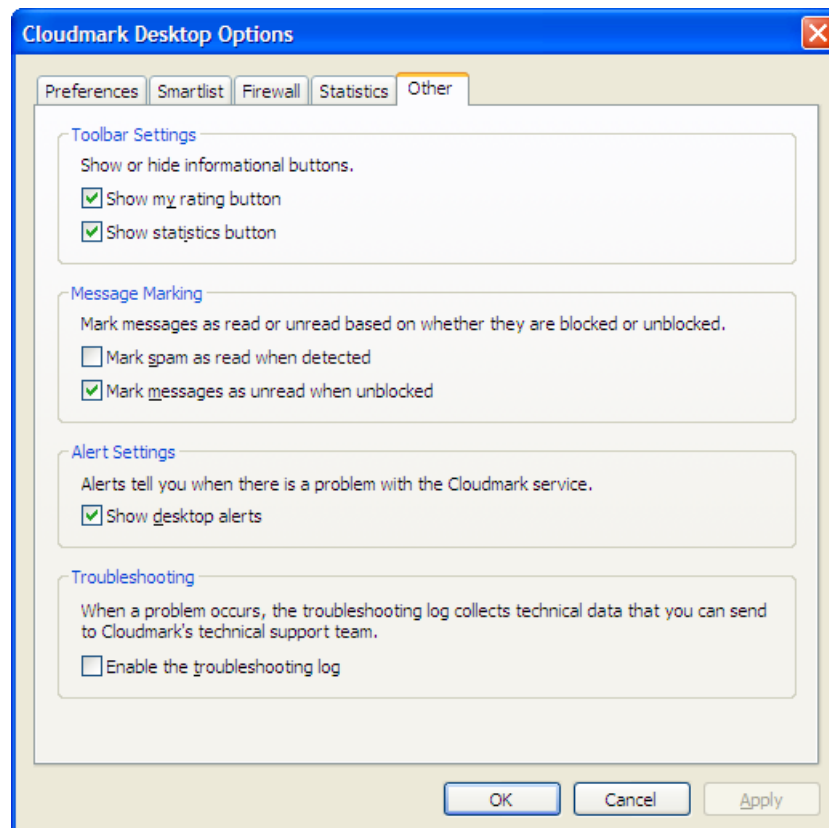
- 1** Click the Cloudmark button to open the menu.
- 2** Select Options....
The Cloudmark Desktop Options window appears.
- 3** Click the Other tab.
- 4** Select or deselect “Show statistics and My Rating on toolbar”.
- 5** Click OK.

Configuring general spam options

TO CONFIGURE GENERAL SPAM OPTIONS

- 1** Click the Cloudmark button to open the menu.
- 2** Select Options....
The Cloudmark Desktop Options window appears.

3 Click the Other tab.



4 Select or deselect the options as desired:

- Mark Spam As Read When Detected

When this option is selected, spam and phishing messages are marked as read even if you haven't view them. This prevents them from contributing to your count of unread messages.

- Mark Messages As Unread When Unblocked

When this option is selected, any message to which you apply the Unblock button is automatically marked as unread, regardless of whether you've previously viewed it.

- Show Desktop alerts

When this option is selected, Cloudmark Desktop displays an alert message when there is a problem connecting to the network.

5 Click OK.

Configuring your firewall settings

If your computer is behind a firewall, you must enter your firewall settings in order to use Cloudmark Desktop. Your network administrator or internet service provider can give you the appropriate settings to enter.

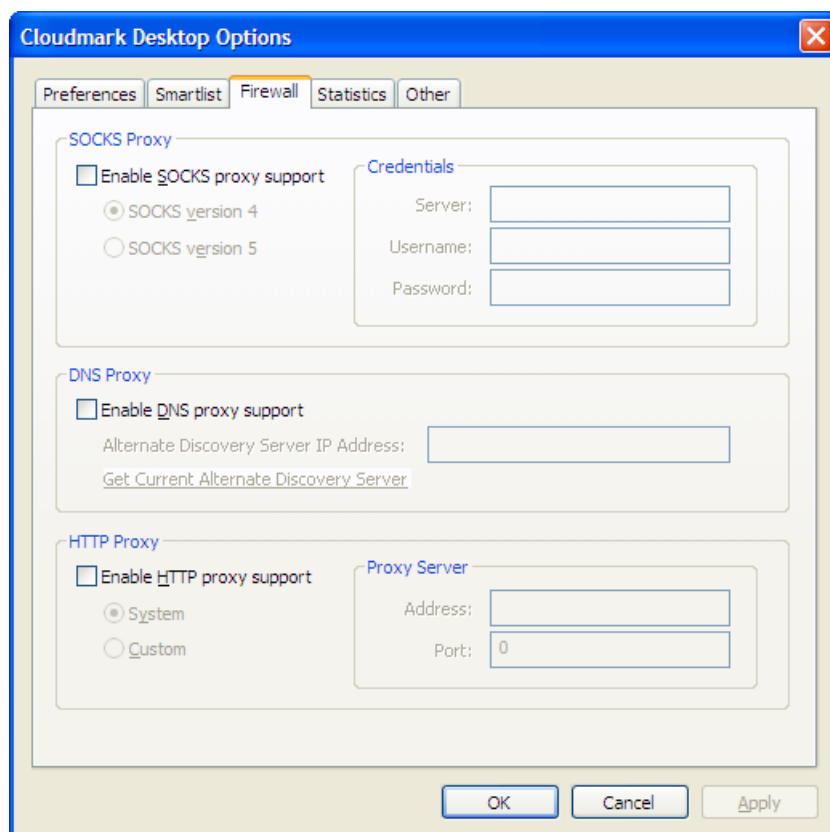
TO ENTER YOUR FIREWALL SETTINGS

1 Click the Cloudmark button to open the menu.

2 Select Options....

The Cloudmark Desktop Options window appears.

3 Click the Firewall tab:



4 If you are accessing the network through a SOCKS proxy, select Enable SOCKS Proxy Support.

If you select this option, enter your SOCKS settings in the Configuration area:

- Select the SOCKS version, either Version 1 or Version 5.
- Enter the hostname or IP address of the SOCKS server.

- Enter your SOCKS username.
 - Enter your SOCKS password.
- 5 If you are using a DNS proxy, select Enable DNS Proxy Support.
If you select this option, enter the IP address of the alternate discovery server. You can locate an alternate discovery server by clicking Get Current Alternate Discovery Server.
 - 6 If you are using an HTTP proxy, select Enable HTTP Proxy Support.
 - To use your default web browser's HTTP proxy settings, select System.
 - To enter settings that differ from those of your browser, select Custom.
 - 7 Click OK.

Turning off spam blocking

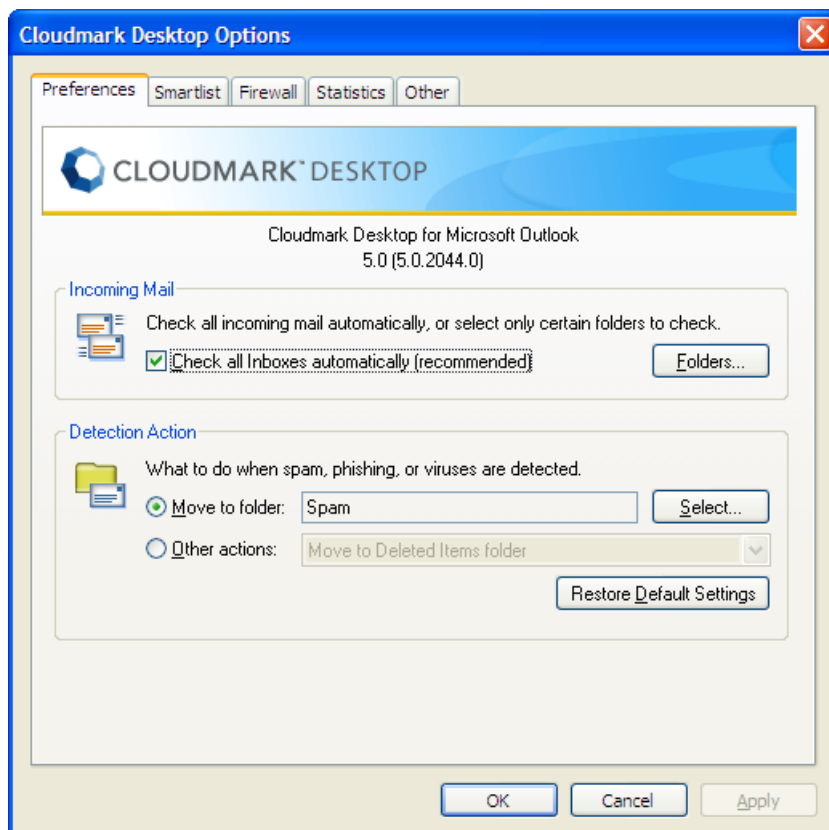
You can turn off spam blocking altogether.

TO TURN OFF SPAM BLOCKING

- 1 Click the Cloudmark button to open the menu.

2 Select Options....

The Cloudmark Desktop Options window appears:



3 Remove the check mark next to Check All Inboxes Automatically.

4 Click OK.

Cloudmark Desktop will no longer check your email for spam and phishing automatically. You can still scan messages manually whenever you like; see “Manually scanning a folder for spam and phishing” on page 12.

To re-enable automatic spam checking, return to the Properties window and select Check All Inboxes Automatically.

Updating Cloudmark Desktop

You can check for new versions of Cloudmark Desktop to download and install.

TO CHECK FOR A NEW VERSION OF CLOUDMARK DESKTOP

- 1 Click the Cloudmark button to open the menu.
- 2 Select Check For Updates.

The InstallShield Wizard appears, checking for updates. When it finishes checking, the wizard tells you whether an update is available.

- If the wizard does not find updates, click Finish to exit.
- If the wizard finds updates, it guides you through the installation process.

Using Cloudmark Desktop on another computer

With any one subscription, you can install Cloudmark Desktop on as many computers as you like, though it will only run on two computers simultaneously. To use Cloudmark Desktop this way, install it on each computer and log in to My Cloudmark, or enter your activation code if you have one. Your login or activation code works with both Outlook and Outlook Express. For instructions, see “Logging in to My Cloudmark” on page 39 or, if you have an activation code, see “Subscribing with an activation code” on page 44.

If you want to permanently stop using Cloudmark Desktop on one of your computers, you can uninstall it. For instructions on uninstalling, see “Uninstalling Cloudmark Desktop” below.

There is no limit to the number of email addresses that you can filter. Cloudmark Desktop filters all of your open mailboxes.

Uninstalling Cloudmark Desktop

If you wish, you can completely remove Cloudmark Desktop from your computer.

TO UNINSTALL CLOUDMARK DESKTOP

- 1 If Microsoft Outlook is running, close it.
- 2 Open the Start menu in Windows.
- 3 Select Control Panel.

The Control Panel window appears.

4 Double-click Add or Remove Programs.

The Add or Remove Programs window appears, displaying a list of programs that are currently installed on your computer.

5 In the program list, select Cloudmark Desktop for Microsoft Outlook.**6** Click the Remove button.

A prompt appears, asking you to confirm that you want to remove the program.

7 Click Yes.

The uninstaller appears, removing Cloudmark Desktop and related files from your computer.

Using My Cloudmark

My Cloudmark is a simple, self-service account management interface for Cloudmark subscribers. This chapter includes topics that explain how to use My Cloudmark:

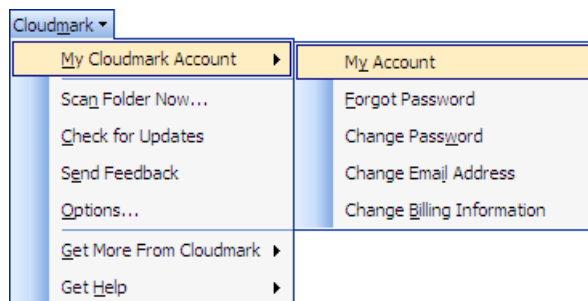
- “Logging in to My Cloudmark” below
- “Subscribing to Cloudmark” on page 41
- “Viewing your referral information” on page 46
- “Changing your email address or password” on page 47
- “Retrieving a lost password” on page 48
- “Changing your billing information” on page 50

Logging in to My Cloudmark

You access My Cloudmark through the Cloudmark menu in Cloudmark Desktop.

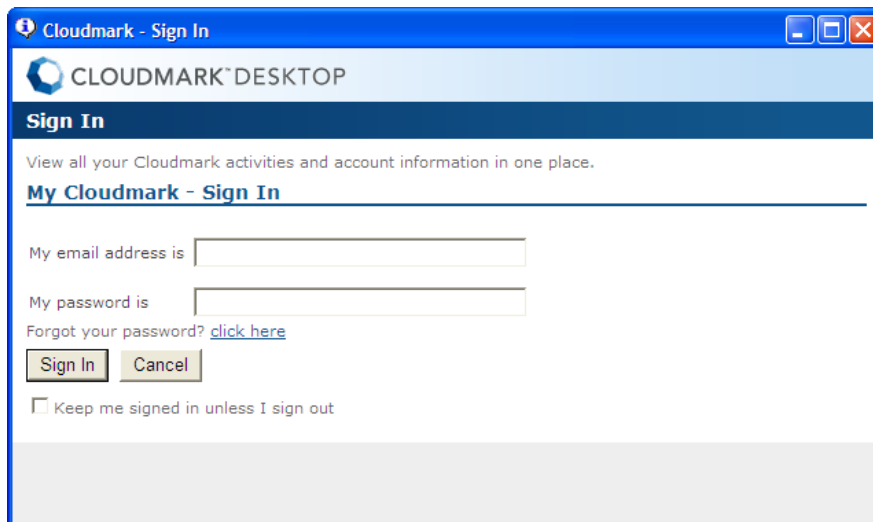
TO LOG IN TO MY CLOUDMARK

- 1 Open the Cloudmark menu:



- 2 Select My Cloudmark Account > My Account.

The My Cloudmark login window appears:

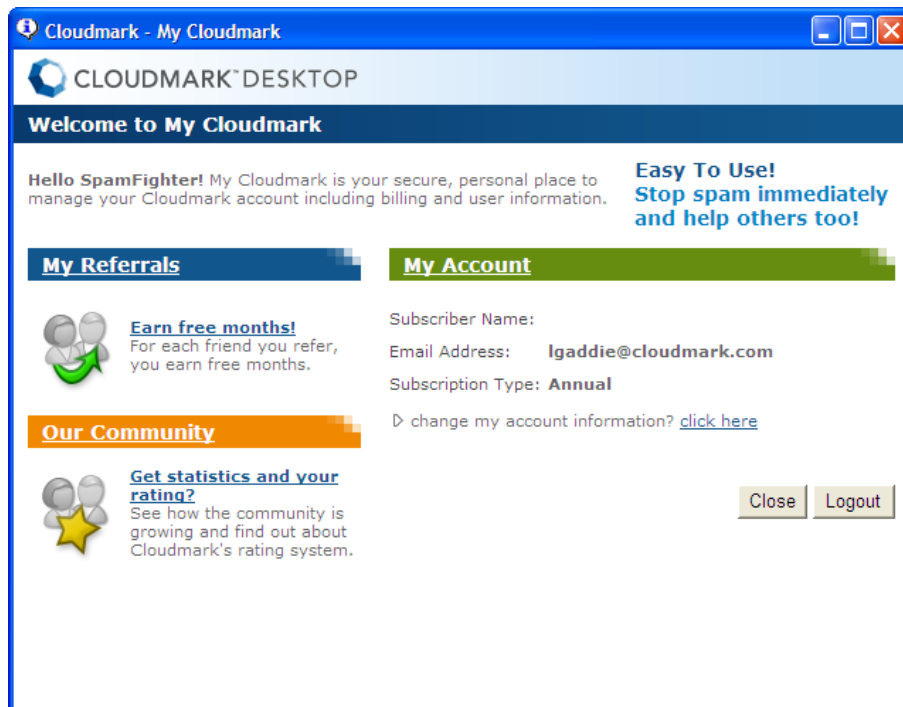


The screenshot shows a window titled "Cloudmark - Sign In". The window has a blue header bar with the Cloudmark logo and the text "CLOUDMARK™ DESKTOP". Below the header, there is a "Sign In" section. The text "View all your Cloudmark activities and account information in one place." is displayed. The "My Cloudmark - Sign In" section contains two input fields: "My email address is" and "My password is". Below the password field, there is a link "Forgot your password? [click here](#)". At the bottom of the form, there are two buttons: "Sign In" and "Cancel". Below the buttons, there is a checkbox labeled "Keep me signed in unless I sign out".

- 3 Enter your email address.
- 4 Enter your password.
If you have forgotten your password, click the "click here" link to retrieve it.

5 Click the Sign In button.

The My Cloudmark page appears:



From here, you can perform the following tasks:

- “Viewing your referral information” on page 46
- “Changing your email address or password” on page 47
- “Retrieving a lost password” on page 48
- “Changing your billing information” on page 50
- You can view statistics and your rating by clicking the Our Community link. See Chapter 5, “Statistics and your rating”

Subscribing to Cloudmark

Cloudmark Desktop runs in Trial Mode when you first install it. When the trial period ends, the software runs in a more limited Basic Mode. To restore the full set of features, you must purchase a subscription. See also “Your subscription to Cloudmark” on page 9.

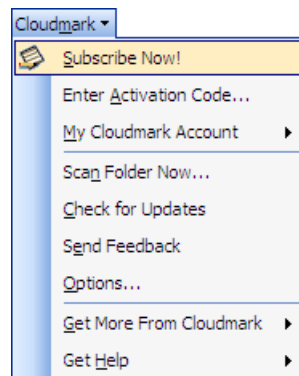
These topics explain how to buy, renew, or cancel your subscription:

- “Purchasing a new subscription” below
- “Subscribing with an activation code” on page 44
- “Renewing a subscription” on page 45
- “Cancelling your subscription” on page 46

Purchasing a new subscription

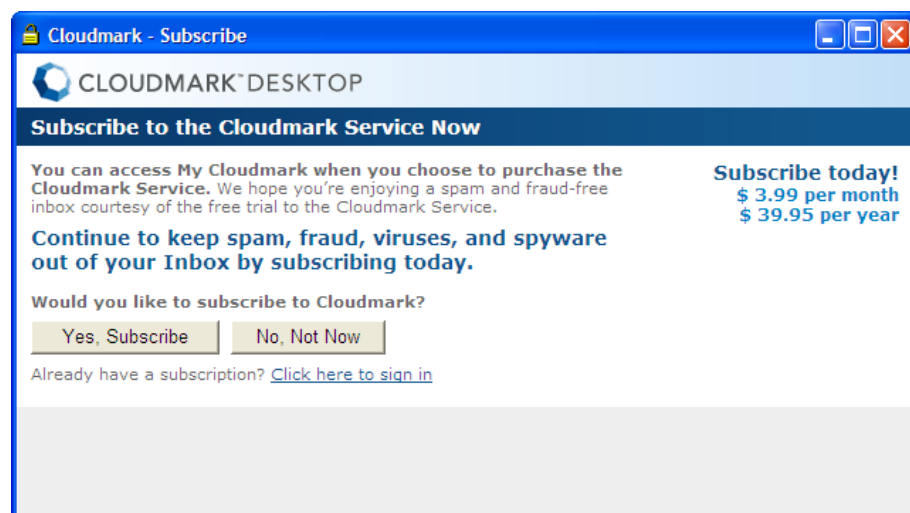
TO PURCHASE A SUBSCRIPTION

- 1 Open the Cloudmark menu:



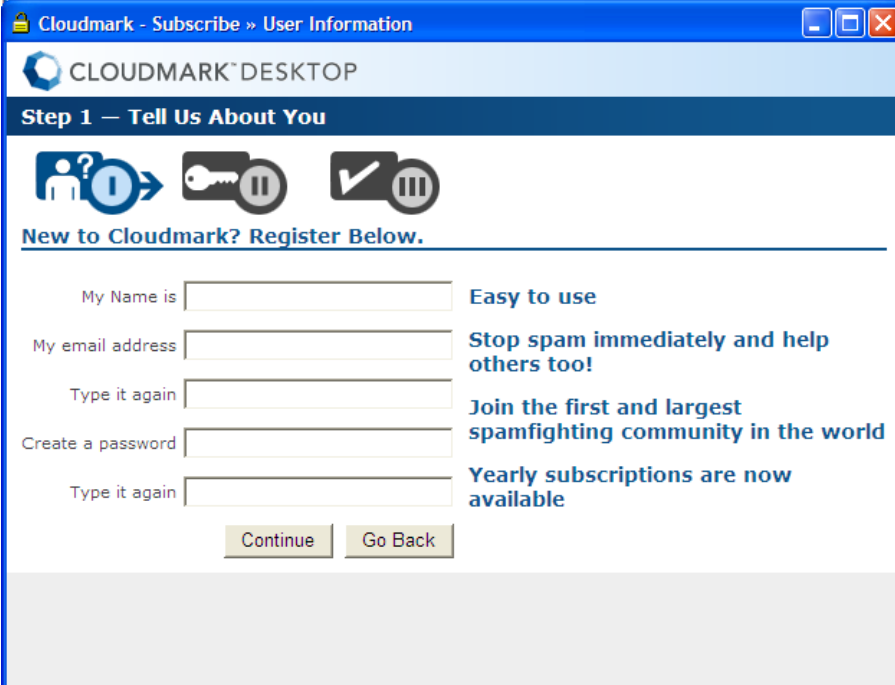
- 2 Select Subscribe Now.

The Subscribe window appears:



- 3 Click the Yes, Subscribe! button.

The User Information window appears:



The screenshot shows a web browser window titled "Cloudmark - Subscribe » User Information". The page header includes the Cloudmark logo and "CLOUDMARK™ DESKTOP". The main heading is "Step 1 — Tell Us About You". Below this, there are three icons: a person with a question mark, a key, and a checkmark. A sub-heading reads "New to Cloudmark? Register Below." The registration form consists of five input fields: "My Name is", "My email address", "Type it again", "Create a password", and "Type it again". To the right of the form, there are four lines of promotional text: "Easy to use", "Stop spam immediately and help others too!", "Join the first and largest spamfighting community in the world", and "Yearly subscriptions are now available". At the bottom of the form are two buttons: "Continue" and "Go Back".

- 4 Enter your name.
- 5 Enter your email address (twice).
- 6 Choose a password and enter it (twice).

Entering your email address twice ensures that you've entered it correctly.

Create a password that is at least five characters long. For the best security, use a password that combines upper- and lower-case letters with numbers or symbols. Do not use a password that is easily guessed by others, such as your birthday or a pet's name.

7 Click Continue.

The Billing Information window appears:

8 Select the Credit Card payment method.**9** Click Purchase.

An order confirmation appears.

Subscribing with an activation code

If the vendor from whom you purchased Cloudmark Desktop provided an activation code, you must enter it in order to activate your subscription. You only need to do this once.

TO ACTIVATE CLOUDMARK DESKTOP

1 Open the Cloudmark menu.

2 Select Enter Activation Code.

The Cloudmark Desktop Activation window appears:



Cloudmark Desktop Activation

CLOUDMARK™ DESKTOP

Thank you for purchasing Cloudmark Desktop.
To finish installation, please enter the following.

Activation Code

Enter the activation code you received at the time of purchase.

Activation Code:

(Code format is xxxxx-xxxxx-xxxxx-xxxxx-xxxxx)

Create Account

Email Address:

Password:

Confirm Password:

Password length should be at least 6 characters.

Click "Activate Now" to complete your subscription to Cloudmark

3 Paste your activation code into the Activation Code field.**4** Enter your email address in the Email Address field.**5** Enter your password, twice.**6** Click Activate Now.

Renewing a subscription

Your subscription is renewed automatically, and a receipt is sent to your email address. If your billing information changes, be sure to update it so that automatic renewal can continue; see “Changing your billing information” on page 50. If you wish to stop automatic renewal by cancelling your subscription, see “Cancelling your subscription” on page 46.

Switching from a monthly to annual subscription

If you have purchased a monthly subscription, you can convert to an annual subscription at any time.

TO CONVERT FROM A MONTHLY TO ANNUAL SUBSCRIPTION

- 1 Log in to My Cloudmark.
See “Logging in to My Cloudmark” on page 39.
- 2 Click My Account.
- 3 Click the “Change my payment plan” link.
- 4 Follow the online instructions.

Canceling your subscription

TO CANCEL YOUR CLOUDMARK SUBSCRIPTION

- 1 Log in to My Cloudmark.
See “Logging in to My Cloudmark” on page 39.
- 2 Click My Account.
The Change Information window appears.
- 3 Click the link next to “cancel your subscription”.
The Cancel Subscription window appears.
- 4 Enter a brief description of the reason for cancelling your subscription.
Your feedback helps Cloudmark improve its service.
- 5 If you are sure you want to cancel your subscription, click Yes.

Viewing your referral information

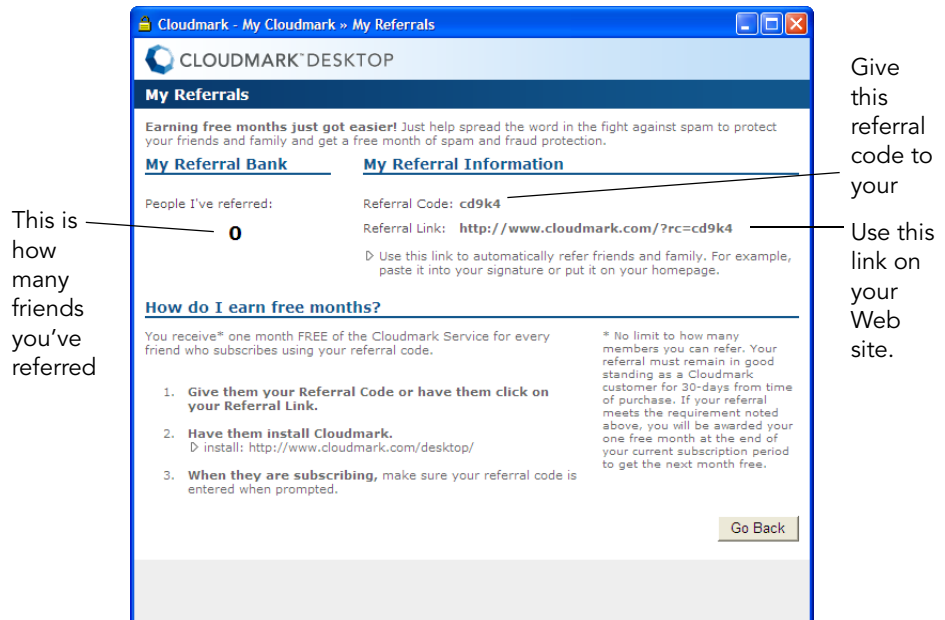
The My Referrals area of My Cloudmark shows you how many people you've referred to Cloudmark, along with information about how to refer people.

TO VIEW YOUR REFERRAL INFORMATION

- 1 Log in to My Cloudmark.
See “Logging in to My Cloudmark” on page 39.

2 Click the My Referrals link.

The My Referrals page appears.



For more information about referring your friends to Cloudmark, see Chapter 7, “Spreading the word about Cloudmark Desktop”.

Changing your email address or password

Each subscription is tied to exactly one email address. Your email address is also your login to My Cloudmark. If your email address changes, you must update it in My Cloudmark in order to use it with Cloudmark Desktop. When you do this, your subscription no longer applies to your previous email address.

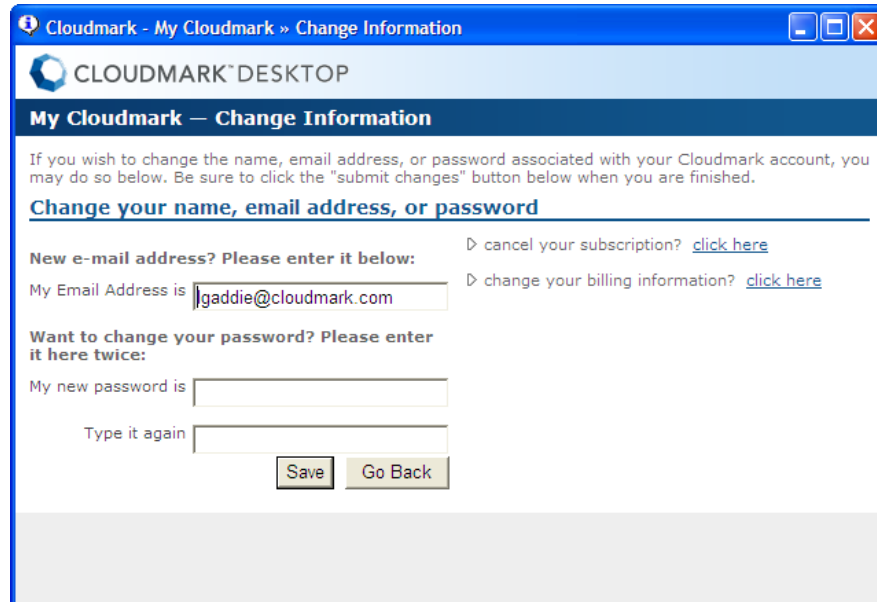
You can also change your password at any time. For example, you may wish to change it to a more memorable password, or change it periodically for security reasons.

TO CHANGE YOUR EMAIL ADDRESS OR PASSWORD

1 Open the Cloudmark menu:

- 2 Select My Cloudmark Account > Change Password.

The Change Information window appears.



- 3 If your email address has changed, enter the new one.
- 4 Enter your new password, twice.
- 5 Click the Save button.

Retrieving a lost password

It is common to forget a password. If this happens, you can select a new password.

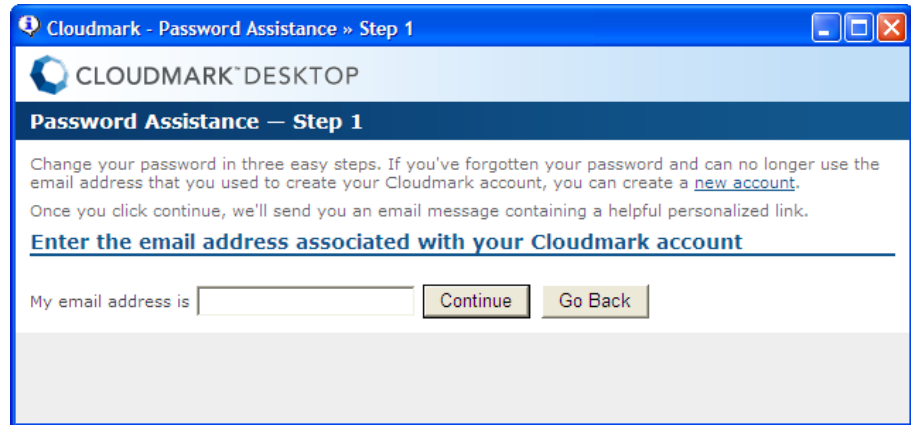
TO RETRIEVE A LOST PASSWORD

- 1 Open the Cloudmark menu.
- 2 Select My Cloudmark.

The My Cloudmark login window appears.

- 3 Click the link next to “Forgot your password”.

The Password Assistance window appears:



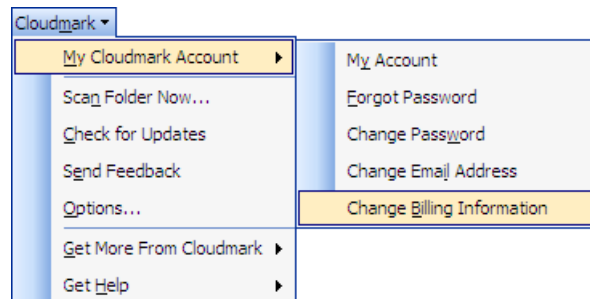
- 4 Enter your email address.
This is the address with which you normally log in to My Cloudmark.
- 5 Click Continue.
The next Password Assistance window informs you that a message is being sent to your email address.
- 6 Close the Password Assistance window.
- 7 Check your Inbox for a message from Cloudmark Service.
- 8 Click the link that is provided in the message.
The Password Assistance window appears in your Web browser.
- 9 Choose a new password and enter it (twice).
When you lose your old password, a new password is necessary for security reasons.
- 10 Click Submit Changes.
A final page appears, informing you that your password has been changed.

You may now log in to My Cloudmark with your new password.

Changing your billing information

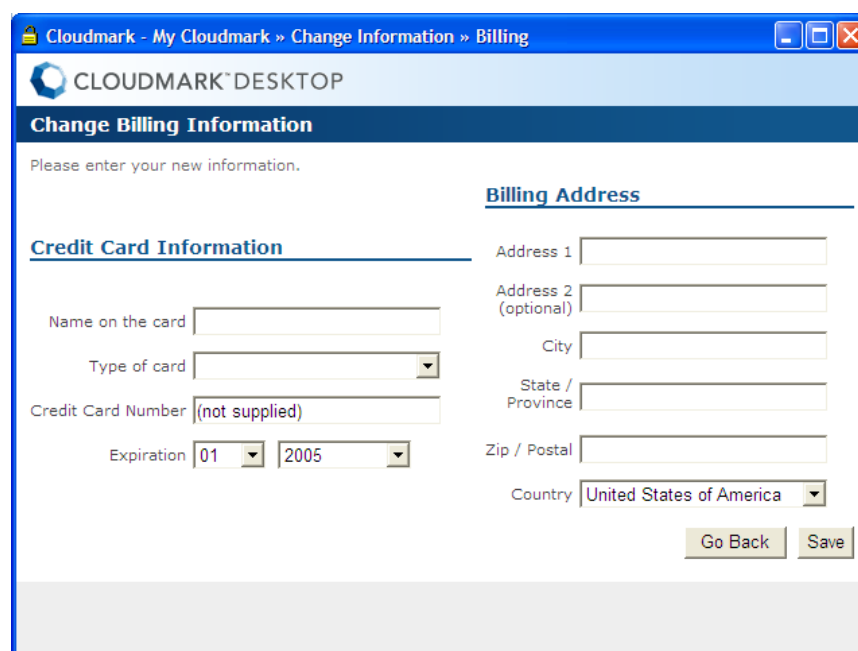
TO CHANGE YOUR BILLING INFORMATION

- 1 Open the Cloudmark menu:



- 2 Select My Cloudmark Account > Change Billing Information. You may be asked to log in.

The Billing page appears:

A screenshot of the 'Change Billing Information' page in the Cloudmark Desktop application. The window title is 'Cloudmark - My Cloudmark » Change Information » Billing'. The page has a blue header with the Cloudmark logo and the text 'CLOUDMARK™ DESKTOP'. Below the header, the title 'Change Billing Information' is displayed. A message says 'Please enter your new information.' The page is divided into two main sections: 'Credit Card Information' and 'Billing Address'. The 'Credit Card Information' section includes fields for 'Name on the card', 'Type of card' (a dropdown menu), 'Credit Card Number' (with '(not supplied)' text), and 'Expiration' (two dropdown menus showing '01' and '2005'). The 'Billing Address' section includes fields for 'Address 1', 'Address 2 (optional)', 'City', 'State / Province', 'Zip / Postal', and 'Country' (a dropdown menu showing 'United States of America'). At the bottom right of the form, there are two buttons: 'Go Back' and 'Save'.

- 3 Enter your new credit card information.
- 4 Enter your new billing address.
- 5 Click Save.

Statistics and your rating

Statistics tell you about anti-spam and anti-phishing activity through the Cloudmark network. Your rating tells you how effective you have been at preventing spam and phishing. This chapter explains these numbers and provides instructions for influencing them:

- “How statistics work” below
- “How your rating works” on page 52
- “Viewing statistics and your rating” on page 53
- “How to influence your rating” on page 54

How statistics work

Statistics summarize activity throughout the Cloudmark network. They show you how much spam and phishing activity is occurring, as well as how much of this activity is being blocked by Cloudmark. You can view this information graphically or in tables. Viewing statistics helps you visualize how much spam and phishing is being blocked.

You can display these statistics about the Cloudmark community:

- total number of spam fighters
- time saved today
- money saved today
- total messages processed today
- total spam caught today

You can display these statistics through Cloudmark Desktop. See “Viewing statistics and your rating” on page 53.

How your rating works

Your rating reflects your effectiveness within the Cloudmark network. This called the Trust Evaluation System (TES). Whenever you click the Block Spam, Block Phish, or Unblock buttons, your rating affects and is affected by your vote, as follows:

- The more users agree with your vote, the more your rating rises.
Consensus with other Cloudmark users suggests that your vote is accurate. This increases your credibility within the network.
- The higher your rating, the more weight your votes carries.
Highly credible users have more influence over which messages get automatically blocked. Likewise, users who consistently vote incorrectly have less influence.

Ratings help keep users honest and ensure the effectiveness of Cloudmark's service.

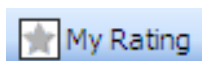
For example, imagine that spammers sign up for the Cloudmark service, then use the Unblock button to unblock their own spam, reporting to Cloudmark that these messages are actually legitimate. Potentially, this could contaminate the network with false information.

However, their votes will not concur with those of the majority of users, who will apply the Block Spam button to the same messages. Consequently, those spammers will quickly develop negative ratings. Their votes therefore become weaker when compared with those of highly-rated users, and Cloudmark will continue to regard their messages as spam. This is why your votes are so important.

Viewing statistics and your rating

TO VIEW STATISTICS AND YOUR RATING

- 1 In the Cloudmark toolbar, click the My Rating button:



The Our Community page appears:

 A screenshot of a web browser window titled "Cloudmark - Cloudmark Desktop". The page content is as follows:

Cloudmark - Cloudmark Desktop

CLOUDMARK® DESKTOP

Your rating

Thank you for participating in the Cloudmark Collaborative Security Network. Each time you use the Block or Unblock buttons, you contribute valuable data that helps everyone in the network avoid spam and phishing. Your rating is based on the timeliness and accuracy of your feedback.

Your rating began at the Normal Trust rating. It can go up or down, including negative trust. Here are some tips for increasing your rating:

- **Block only the messages that are really spam or phishing.** For example, don't block newsletters to which you have subscribed.
- **Unblock only legitimate messages.** Don't unblock spam or phishing messages, even if you are interested in their content.
- **Block or unblock messages soon after you receive them.** Your feedback is most valuable immediately after a spam or phishing attack.

Rating System

★ Most Trusted
 ★
 ★
 ★
 ★ YOU HAVE ACHIEVED NORMAL TRUST
 ★
 ★
 ★ Least Trusted

Community Statistics

Total SpamFighter	2,274,016
Time saved today (days)	37,321
Money saved today	\$17,914,167
Emails processed today	940,932,896
Spam caught today	322,455,009

[Go Back](#)

On this page, you can view the following:

- your rating
- total number of spamfighters in the Cloudmark Collaborative Security Network
- estimated time saved, in days, throughout the network
- estimated money saved throughout the network
- email messages processed today
- spam and phishing messages caught today

How to influence your rating

Your rating is influenced by the way you use Cloudmark Desktop. The following are some tips for improving your rating:

- Be sure to use the Block Spam button only for messages that really are spam.
See “What is spam?” on page 2.
- Be sure to use the Block Phish button only for messages that really are phishing.
See “What is email fraud or “phishing?”” on page 3.
- Be sure to use the Unblock button only for messages that are neither spam nor phishing.
Use this button only for messages from your friends, family, colleagues, or companies with whom you have a business relationship.
- Timeliness is important. If a message requires action, don't wait.
That is, click the Block Spam button as soon as you find spam, the Block Phish button as soon as you find phishing, and the Unblock button as soon as you find a misclassified message in your Spam Folder. This keeps the network's data current.

Troubleshooting

In the event that you encounter a problem while using Cloudmark Desktop or My Cloudmark, this chapter provides solutions and tips. If the solution to your problem cannot be found here, consult the additional resources listed in Chapter 8, “Finding more information”.

“Error reading setup initialization file” This occurs when the installer file was not downloaded completely or has become corrupt.

1. Locate the installer file on your hard drive.
2. Drag the installer file to your Recycling Bin.
3. Right-click the Recycle Bin to open its menu.
4. Select Empty Recycle Bin.

A prompt appears, asking you to confirm that you want to permanently delete the items in the Recycle Bin.

5. Click Yes.
6. Restart your computer.
7. Download a fresh copy of the installer and run it.
See “Installing Cloudmark Desktop” on page 8.

“Unable to connect” This can occur for any of several different reasons:

- temporary network outage

This may be the case if the error begins to occur well after Cloudmark Desktop was installed. Your network service provider may be experiencing temporary issues. This does not inhibit Cloudmark’s ability to block spam. If the issue continues for 24 hours or more, contact Cloudmark’s technical support team.

- corporate firewall or proxy

Cloudmark Desktop connects to the Cloudmark service on port 2703. Your corporate firewall may not allow outbound connections to that port on all IP addresses. Ask your network administrator to configure the firewall to allow outbound connections to port 2703 in this IP range:

66.151.150.11 - 66.151.150.60

If IP restriction is not the issue, you may be required to connect through a corporate proxy server. Ask your network administrator for the correct settings, then follow the instructions in “Configuring your firewall settings” on page 27.

- personal firewall software

Blank messages don't get filtered as spam Blank messages are usually not spam. Sometimes, a sender may put the entire (brief) message in the Subject field and leave the body of the message blank. This is why Cloudmark does not interpret blank messages as spam.

I keep blocking messages that appear identical Some spam and phishing messages that appear identical contain subtle differences that occasionally prevent Cloudmark from recognizing all the variants. Please continue to apply the Block Spam or Block Phish button to such messages; this helps improve Cloudmark's accuracy.

The Cloudmark Desktop toolbar disappears You may need to reinstall the program:

1. Uninstall Cloudmark Desktop.
See “Uninstalling Cloudmark Desktop” on page 30.
2. Restart your computer.
3. Reinstall Cloudmark Desktop.
See “Installing Cloudmark Desktop” on page 8.

Cloudmark Desktop freezes or crashes If the program repeatedly freezes or crashes, you may need to remove it and then replace it:

1. Uninstall Cloudmark Desktop.
See “Uninstalling Cloudmark Desktop” on page 30.
2. Restart your computer.
3. Re-install Cloudmark Desktop.
See “Installing Cloudmark Desktop” on page 8.

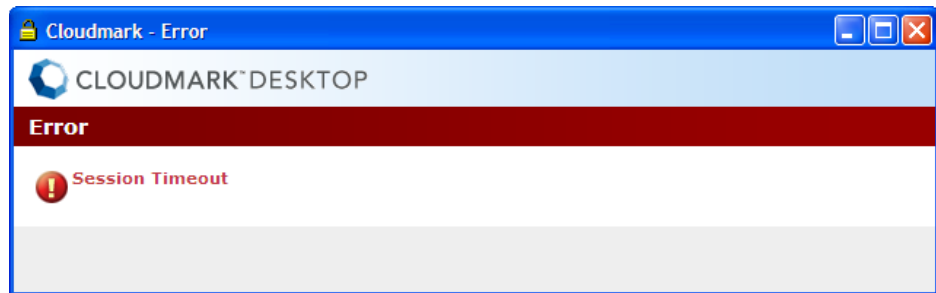
The Check For Updates command doesn't work You may receive one of the following errors when using the Check For Updates command:

- 13003 - Version not registered with the Update Service
This error indicates a temporary interruption of the update service. Wait 24 hours, then try the command again.
- 13004 - Version not registered with the local Agent

In either case, you can update the software by visiting this download page:

<http://www.cloudmark.com/desktop/download/>

My Cloudmark gives me a “Session Timeout” error When you click a link in My Cloudmark after a period of inactivity, this error message appears:



TO RETURN TO MY CLOUDMARK

- 1 Close the error message window.
- 2 Log in to My Cloudmark again.
See “Logging in to My Cloudmark” on page 39.

Spreading the word about Cloudmark Desktop

Email users worldwide struggle with spam and fraud. If you find Cloudmark Desktop helpful, you can help other email users by telling them about it.

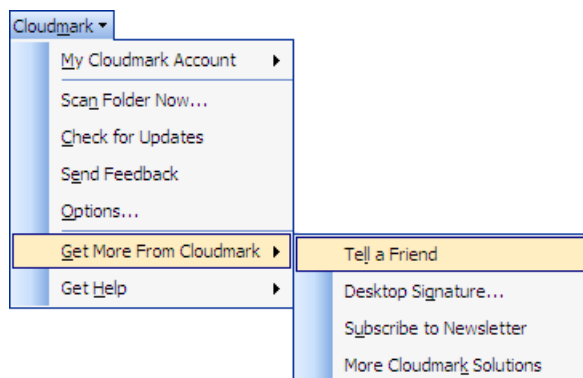
- “Telling a friend about Cloudmark Desktop” below
- “Adding a Cloudmark Desktop signature to your email” on page 60

Telling a friend about Cloudmark Desktop

If you have one specific friend, family member, or colleague whom you would like to tell about Cloudmark Desktop, you can use the Tell A Friend command to send a pre-formatted email message.

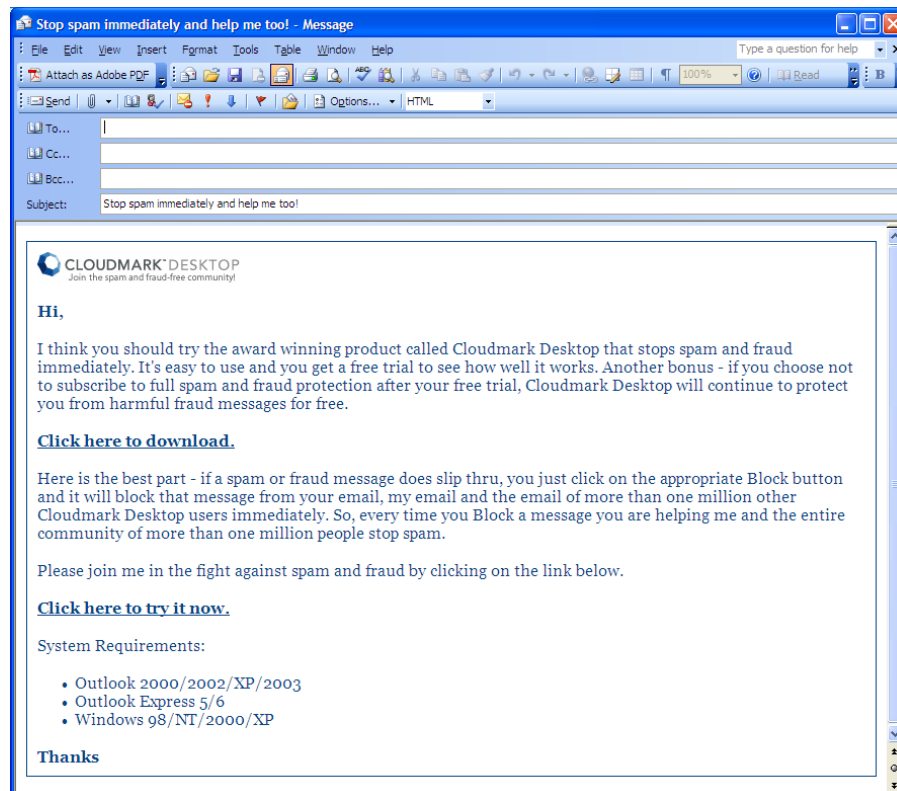
TO TELL A FRIEND

- 1 Open the Cloudmark menu:



2 Select Get More From Cloudmark > Tell a Friend.

A preformatted email message appears:



3 In the To field, enter the email address or addresses to which you want to send the message.

4 Click Send.

The message is delivered to the specified address or addresses. The recipients can click the links in the message to download Cloudmark Desktop and try it.

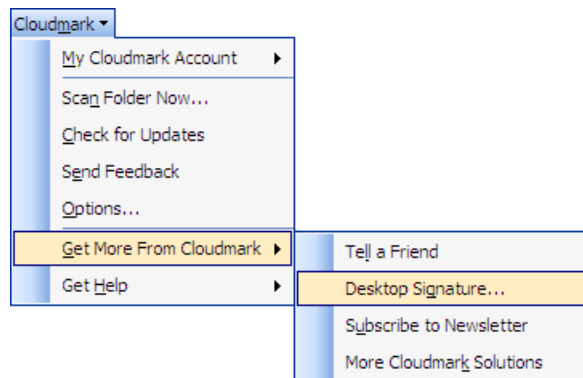
Adding a Cloudmark Desktop signature to your email

A signature is a bit of text or images that appears at the bottom of every email message you send. When you set up a signature, Outlook automatically appends it to each message without any special action on your part.

A Cloudmark Desktop signature is a way to automatically spread the word about spam-fighting technology. Cloudmark Desktop can help you create one.

TO CREATE A CLOUDMARK DESKTOP SIGNATURE

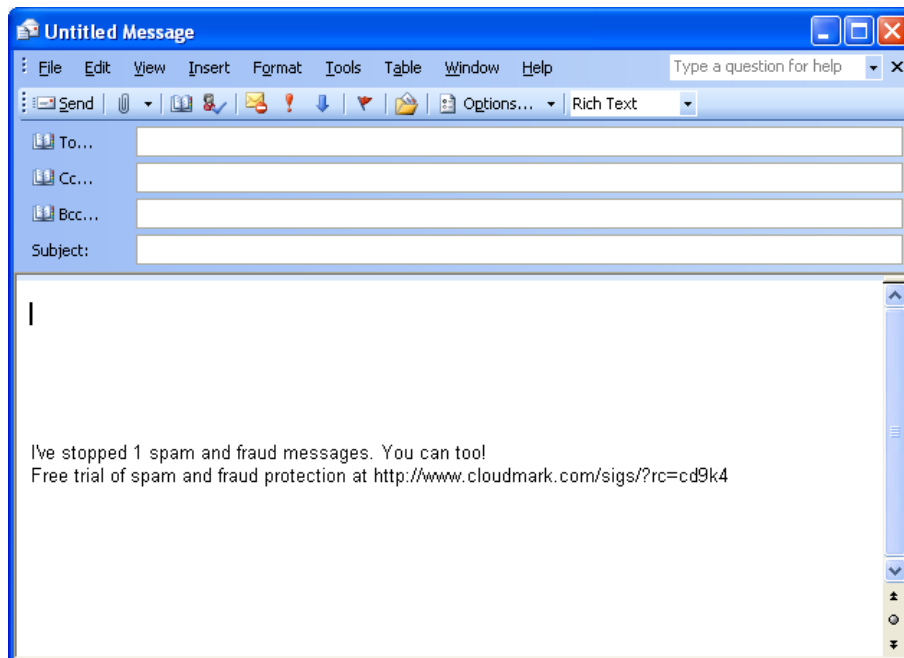
- 1 Open the Cloudmark menu:



- 2 Select Get More From Cloudmark > Desktop Signature.
The Add Cloudmark Desktop Signature window appears.
- 3 Click Yes.
A dialog box appears, informing you that you may need to restart Windows after creating the signature.
- 4 Click OK.
Cloudmark Desktop automatically configures the new signature.
- 5 From Outlook's Tools menu, select Options.
The Options window appears.
- 6 Click the Mail Format tab.
- 7 In the "Signature for new messages" field, select "Cloudmark SpamNet - Join The Fight! - New".
- 8 In the "Signature for replies and forwards" field, select "Cloudmark SpamNet - Join The Fight! - Reply".

9 Click OK.

Whenever you compose a message, the signature will appear at the bottom, like this:



The link in the signature includes your referral code. When someone follows the link and installs Cloudmark Desktop, you get credit for a referral. For each referral, you receive one free month with Cloudmark.

Finding more information

This guide is one of many resources available to you. If you need more information about Cloudmark Desktop or My Cloudmark, consult these resources:

- online help

From the Cloudmark Desktop menu, select “Get Help > Cloudmark Desktop Help”.

- Knowledge Base

The knowledge base contains information compiled by the technical support team. You can use your web browser to access the Knowledge Base here:

<http://www.cloudmark.com/desktop/kb/>

- release notes

Release notes contain a list of changes and new features for each new version of Cloudmark Desktop. You can find the latest release notes here:

<http://www.cloudmark.com/desktop/ol/releasenotes/>

- user forum

In the user forum, you can ask questions and discuss Cloudmark Desktop with other users and Cloudmark’s team of technical experts.

<http://www.cloudmark.com/desktop/forum/>

- Technical support

If you do not find the solutions you’re looking for in the resources listed above, you can contact Cloudmark’s team of technical support experts for personal assistance. Use your web browser to create a request for assistance here:

<http://www.cloudmark.com/desktop/contact/>

Glossary

activate You activate Cloudmark Desktop by first purchasing a subscription, then entering the activation code that you receive. This gives you access to the complete feature set, until your subscription expires.

See also: “Subscribing with an activation code” on page 44.

activation code You receive an activation code if you purchase Cloudmark Desktop from a Cloudmark partner. Your activation code unlocks all of Cloudmark Desktop’s features. You receive your activation code when you purchase a subscription.

See also: “Subscribing with an activation code” on page 44.

block When you block a message by clicking the Block Spam or Block Phish button, you report it to Cloudmark as spam or phishing. Your vote against that message is compiled with the votes of other users and may result in permanently classifying that message as spam or phishing for all users throughout the network.

See also: “Blocking a single spam message” on page 13, “Blocking a single phishing message” on page 14.

Cloudmark Collaborative Security Network The Cloudmark Collaborative Network consists of users like you, all providing feedback about which messages are spam or phishing and which ones are legitimate. When users reach consensus about a message, they influence how that message is classified for all users throughout the network.

email-borne virus Email-borne viruses are malicious programs that are carried to your computer by email. They may arrive inside a spam or phishing message, or in messages from friends who do not realize that their own computers are infected. Viruses can inflict serious damage to your computer.

firewall A firewall is an internet gateway that provides security for the computers and users inside the network. You may need to enter special

configuration information to allow Cloudmark Desktop to operate through your firewall.

See also: “Configuring your firewall settings” on page 27.

fraud Email fraud, or phishing, is email designed for identity theft. It typically pretends to come from a legitimate commercial source and solicits personal information from the recipient. Cloudmark Desktop automatically sends new fraud to your Spam Folder. If you find a fraudulent message in your Inbox, you can block it by clicking the Block Phish button.

See also: “What is email fraud or “phishing”?” on page 3, “Blocking spam and phishing” on page 11.

phishing Phishing, also known as email fraud, is email designed for identity theft. It typically pretends to come from a legitimate commercial source and solicits personal information from the recipient. Cloudmark Desktop automatically sends new phishing to your Spam Folder. If you find a fraudulent message in your Inbox, you can block it by clicking the Block Phish button.

See also: “What is email fraud or “phishing”?” on page 3, “Blocking spam and phishing” on page 11.

proxy A proxy is a trusted server that acts as an intermediary between your computer and the internet, providing a barrier against security threats. You may need to enter special configuration information to allow Cloudmark Desktop to operate through your proxy. A proxy often runs on a firewall.

See also: “Configuring your firewall settings” on page 27.

rating Cloudmark users are rated on their effectiveness as spam fighters. When you block spam and phishing in a timely and accurate manner, your rating increases, as does the weight of your vote.

See also: “How your rating works” on page 52, “Viewing statistics and your rating” on page 53, “How to influence your rating” on page 54.

referral You provide a referral by recommending Cloudmark Desktop to others. When someone installs and purchases Cloudmark Desktop based on your referral, you earn free months for your monthly subscription.

See also: Chapter 7, "Spreading the word about Cloudmark Desktop".

signature A signature is a short message that appears at the bottom of each email message you send. You can configure Outlook Express to insert your

signature automatically in every message you send. A signature is a simple way to spread the word about Cloudmark Desktop's spam-fighting benefits.

See also: "Adding a Cloudmark Desktop signature to your email" on page 60.

smartlist A smartlist is an intelligent whitelist. Cloudmark Desktop's smartlist can automatically incorporate your personal address book, in addition to the whitelist entries that you create.

spam Spam is unsolicited, bulk email, usually for a commercial purpose. Cloudmark Desktop automatically sends most spam to your Spam Folder. If you find a spam message in your Inbox, you can block it by clicking the Block Spam button.

See also: "What is spam?" on page 2, "Blocking spam and phishing" on page 11.

statistics Statistics tell you how much spam has been blocked by you and by the Cloudmark Collaborative Security Network. You can use statistics to find out how effective Cloudmark Desktop is.

See also: "How statistics work" on page 51, "Viewing statistics and your rating" on page 53.

subscription Your subscription is your ongoing membership in the Cloudmark Collaborative Security Network. When you purchase a monthly or yearly subscription, you receive a login or an activation code that unlocks all of Cloudmark Desktop's features.

See also: "Subscribing to Cloudmark" on page 41.

unblock When you unblock a message by clicking the Unblock button, you indicate to Cloudmark that the message is neither spam nor phishing. Your vote is compared with the votes of other users and may result in reclassifying that message as legitimate.

See also: "Unblocking a single legitimate message" on page 15.

virus See "email-borne virus" on page 65.

whitelist A whitelist contains email address or domains from which you always want to receive messages. By adding an email address or domain to your whitelist, you prevent messages from those sources from being sent to your Spam Folder.

See also: "Using the smartlist" on page 16.

Index

A

activation code 30, 44, 65

B

billing 50

Block button 14

Block Fraud button 5, 15, 52

Block Phish button 65, 66

Block Spam button 5, 14, 52, 65, 67

buttons

Block 14

Block Fraud 5, 15, 52

Block Phish 65, 66

Block Spam 5, 14, 52, 65, 67

Unblock 5, 16, 52, 67

C

Cloudmark Collaborative Security
Network 65

Cloudmark Desktop 4, 11

installing 8

moving to another computer 30

system requirements 7

uninstalling 30

updating 29, 56

D

disabling spam blocking 28

DNS proxy 28

E

email

signature 60

unblocking 15

email address

changing 47

errors 55

F

firewall 55, 65

settings 27

folders

automatically scanning 12, 20

manually scanning 12

Spam 11, 13, 23

fraud 3, 66

blocking 14

G

Gmail 8

H

Hotmail 8

HTTP proxy 28

I

installation 8

L

logging in to My Cloudmark 39

M

messages

blank 56

marking as read 26

marking as unread 26

unblocking 15

Microsoft Exchange 7

MSN 8

My Cloudmark 5, 39

logging in 39

O

options 20

P

password
 changing 47
 lost 48
phishing 3, 66
 blocking 14
preferences 5, 20
problems 55
proxy 66
proxy servers 55
 DNS 28
 HTTP 28
 SOCKS 27

R

rating 51, 52
 influencing 54
 viewing 53
ratings 66
referrals 59, 66
 viewing 46

S

scanning folders 12, 20
signature 60, 66
smartlist 16
SOCKS proxy 27
spam 2, 67
 action against 23
 blocking 11, 13
 deleting 23
 options 25

spam blocking
 disabling 28
Spam Folder 11, 13, 23
spoofing 2, 16
statistics 51, 67
 hiding 25
 in the toolbar 25
 showing 25
 viewing 53
subscription 5, 9, 41, 67
 billing 50
 cancelling 46
 new 42
 renewing 45
system requirements 7

T

timeout 57
toolbar 5, 56
troubleshooting 55
Trust Evaluation System (TES) 52

U

Unblock button 5, 16, 52, 67

W

whitelist 16, 67
Windows Vista 8

Y

Yahoo! 8