Legal Notice

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from an authorized representative of Norman Safeground AS. The inclusion of brief quotations in reviews may be possible only with the mention of the quoted source. The content can not be modified in any way.

Warning and Disclaimer. This product and its documentation are protected by copyright. The information in this document is provided on an “as is” basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party Websites that are not under the control of Norman Safeground AS, therefore Norman Safeground AS is not responsible for the content of any linked site. If you access a third-party website listed in this document, you will do so at your own risk. Norman Safeground AS provides these links only as a convenience, and the inclusion of the link does not imply that Norman Safeground AS endorses or accepts any responsibility for the content of the third-party site.

Trademarks. Trademark names may appear in this book. All registered and unregistered trademarks in this document are the sole property of their respective owners, and are respectfully acknowledged.
# Table of Contents

Using This Guide ................................................................. v
  1. Purpose and Intended Audience .......................................... v
  2. How to Use This Guide .................................................... v
  3. Conventions Used in This Guide ......................................... vi
    3.1. Typographical Conventions .......................................... vi
    3.2. Admonitions ........................................................... vi

1. Installation and Removal .................................................. 1
  1.1. System Requirements ................................................... 1
  1.2. Installing Norman Antivirus for Mac .................................. 1
    1.2.1. Step 1 - Welcome Window ......................................... 3
    1.2.2. Step 2 - View the Readme File .................................... 4
    1.2.3. Step 3 - Read the License Agreement ............................... 5
    1.2.4. Step 4 - Start Installation .......................................... 6
    1.2.5. Step 5 - Installing Norman Antivirus for Mac .................. 7
    1.2.6. Step 6 - Finish ...................................................... 8
  1.3. Removing Norman Antivirus for Mac ................................... 8

2. Getting Started .............................................................. 10
  2.1. About Norman Antivirus for Mac ....................................... 10
  2.2. Opening Norman Antivirus for Mac ..................................... 10
  2.3. Application Main Window ................................................. 11
  2.4. Application Dock Icon .................................................. 12

3. Protecting against Malicious Software ................................. 14
  3.1. Best Practices .......................................................... 14
  3.2. Scanning Your Mac ...................................................... 15
  3.3. Scan Wizard .............................................................. 16
  3.4. Fixing Issues ............................................................. 17
  3.5. Quarantine ................................................................. 20
  3.6. Web protection .......................................................... 21
  3.7. Updates ................................................................. 22
    3.7.1. Requesting an Update .............................................. 23
    3.7.2. Getting Updates through a Proxy Server ....................... 23
    3.7.3. Upgrade to a new version ......................................... 24
4. Configuring Preferences .................................................. 25
   4.1. Accessing Preferences .............................................. 25
   4.2. General Preferences ................................................ 25
   4.3. Scanner Preferences ............................................... 26
   4.4. Scan Exclusions .................................................... 28

5. Registering Norman Antivirus for Mac ............................. 30
   5.1. About Registration ................................................ 30
   5.2. Registering Norman Antivirus for Mac ....................... 30
   5.3. Purchasing a License Key ........................................ 31

6. Support and Contact Information ................................... 32
Types of Malicious Software ............................................. 33
Using This Guide

1. Purpose and Intended Audience

This guide is intended to all Macintosh users who have chosen Norman Antivirus for Mac as a security solution for their computers. The information presented in this book is suitable not only for computer literates, it is accessible to everyone who is able to work under Macintosh.

You will find out how to configure and use Norman Antivirus for Mac to protect yourself against viruses and other malicious software. You will learn how to get best from Norman Safeguard AS.

We wish you a pleasant and useful lecture.

2. How to Use This Guide

This guide is organized around several major topics:

*Getting Started (p. 10)*
Get started with Norman Antivirus for Mac and its user interface.

*Protecting against Malicious Software (p. 14)*
Learn how to use Norman Antivirus for Mac to protect yourself against malicious software.

*Configuring Preferences (p. 25)*
Learn more about the Norman Antivirus for Mac preferences.

*Support and Contact Information (p. 32)*
Where to look and where to ask for help if something unexpected appears.
3. Conventions Used in This Guide

3.1. Typographical Conventions

Several text styles are used in this guide for an improved readability. Their aspect and meaning are presented in the table below.

<table>
<thead>
<tr>
<th>Appearance</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sample syntax</td>
<td>Syntax samples are printed with monospaced characters.</td>
</tr>
<tr>
<td>Using This Guide (p. v)</td>
<td>This is an internal link, towards some location inside the document.</td>
</tr>
<tr>
<td>filename</td>
<td>File and directories are printed using monospaced font.</td>
</tr>
<tr>
<td>option</td>
<td>All the product options are printed using bold characters.</td>
</tr>
<tr>
<td>keyword</td>
<td>Important keywords or phrases are highlighted using bold characters.</td>
</tr>
</tbody>
</table>

3.2. Admonitions

The admonitions are in-text notes, graphically marked, bringing to your attention additional information related to the current paragraph.

**Note**

The note is just a short observation. Although you can omit it, the notes can provide valuable information, such as specific feature or a link to some related topic.

**Important**

This requires your attention and is not recommended to skip over it. Usually, it provides non-critical but significant information.
Warning
This is critical information you should treat with increased caution. Nothing bad will happen if you follow the indications. You should read and understand it, because it describes something extremely risky.
1. Installation and Removal

This chapter includes the following topics:

- System Requirements (p. 1)
- Installing Norman Antivirus for Mac (p. 1)
- Removing Norman Antivirus for Mac (p. 8)

1.1. System Requirements

You may install Norman Antivirus for Mac on computers with OS X Lion (10.7.x), OS X Mountain Lion (10.8.x), or OS X Mavericks (10.9.x).

Your Mac must also meet all of these additional requirements:

- Minimum 1 GB of RAM Memory
- Minimum 400 MB available hard disk space

An Internet connection is required to register and update Norman Antivirus for Mac.

How to find out your Mac OS X version and hardware information about your Mac

Click the Apple icon in the upper-left corner of the screen and choose About This Mac. In the window that appears you can see the version of your operating system and other useful information. Click More Info for detailed hardware information.

1.2. Installing Norman Antivirus for Mac

To install Norman Antivirus for Mac:

1. Log in to your Mac as an administrator.
2. Do either of the following:
Insert the installation CD/DVD into the drive. Normally, a window with the installer and uninstaller packages will appear in a few moments. If it does not appear, search for the disk image on your Desktop and open it.

Download or copy the installation image (a .dmg or .iso file) to your Desktop, then open it. A window with the installer and uninstaller packages will appear immediately.

3. Click Norman Antivirus for Mac.pkg. This will launch the installer, which will guide you through the installation process.

4. Follow the installation wizard.
1.2.1. Step 1 - Welcome Window

Click **Continue**.
1.2.2. Step 2 - View the Readme File

The readme file provides useful information about Norman Antivirus for Mac. You can print or save the readme file so that you can review it at a later time. Click **Continue**.
1.2.3. Step 3 - Read the License Agreement

The License Agreement is a legal agreement between you and Norman Safeground AS for the use of Norman Antivirus for Mac. You can print or save the License Agreement so that you can review it at a later time.

Please read the License Agreement carefully. To continue installing the software you must agree to the terms of the software license agreement. Click Continue and then Agree.

Important
If you do not agree to these terms, click Continue and then Disagree to cancel the installation and quit the installer.
1.2.4. Step 4 - Start Installation

Norman Antivirus for Mac will be installed in Macintosh HD/Library/Norman. You cannot change the installation path.

Click **Install** to start the installation.
1.2.5. Step 5 - Installing Norman Antivirus for Mac

Wait until the installation is completed and then click **Continue**.
1.2.6. Step 6 - Finish

Click **Close** to close the installer window.

1.3. Removing Norman Antivirus for Mac

Being a complex application, Norman Antivirus for Mac cannot be removed in the normal way, by dragging the application icon from the Applications folder to the Trash.

To remove Norman Antivirus for Mac, you need the installation disc or the installation image (either the original or a new one). The installation image is a .dmg or .iso file.

Follow these steps:
1. Log in to your Mac as an administrator.

2. Insert the installation CD/DVD into the drive or locate the installation image and double-click it. The following window will appear.

3. Click *Norman Antivirus for Mac Uninstaller.pkg*. The installer will help you run the uninstall script of Norman Antivirus for Mac.

4. Click **Continue**.

5. Click **Install** to run the uninstall script.

6. You can see if the uninstall script was run successfully. Click **Close** to close the installer window.
2. Getting Started

This chapter includes the following topics:

- *About Norman Antivirus for Mac* (p. 10)
- *Opening Norman Antivirus for Mac* (p. 10)
- *Application Main Window* (p. 11)
- *Application Dock Icon* (p. 12)

2.1. About Norman Antivirus for Mac

Norman Antivirus for Mac is a powerful antivirus scanner, which can detect and remove all kinds of malicious software ("malware"), including:

- viruses
- spyware
- Trojan horses
- keyloggers
- worms
- adware

This app detects and removes not only Mac malware, but also Windows malware, thus preventing you from accidentally sending infected files to your family, friends and colleagues using PCs.

2.2. Opening Norman Antivirus for Mac

You have several ways to open Norman Antivirus for Mac.

- Click the Norman Antivirus for Mac icon in the Launchpad.
- Open a Finder window, go to Applications and double-click the Norman Antivirus for Mac icon.
  
  Alternatively, you can use Spotlight to find and open the application.
2.3. Application Main Window

In the application's main window you can take important actions to improve your system protection. You can check your computer's security status, secure your web browsing experience and register the product.

![Application Main Window](image)

The status bar at the top of the window informs you about the system's security status using explicit messages and suggestive colors. If Norman Antivirus for Mac has no warnings, the status bar has shades of green. When a security issue has been detected, the status bar green shades are replaced with yellow shades. It may also include an action button to help you quickly fix the issue. For detailed information on issues and how to fix them, refer to *Fixing Issues (p. 17)*.

Under the status bar, four scan buttons are available to help you scan your Mac:
Scan Critical Locations - checks for malware the most vulnerable locations on your system (for example, the folders that contain the documents, downloads, mail downloads and temporary files of each user).

Full System Scan - performs a comprehensive check for malware of the entire system. All connected mounts will be scanned too.

Scan a Custom Location - helps you check specific files, folders or volumes for malware.

Continuous Scan - continuously monitors the applications running on the computer, looking for malware-like actions and prevents new malware threats from entering your system.

For more information, refer to Scanning Your Mac (p. 15).

Besides the scan buttons, additional options are available:

Web protection - filters all web traffic and blocks any malicious content to secure your web browsing experience. For more information, refer to Web protection (p. 21).

Number of days left - displays the time remaining before your current license expires. Click the link to open a screen where you can see more information about your license key or register your product with a new key.

Feedback - opens a new window in your default e-mail client from where you can contact us.

2.4. Application Dock Icon

The Norman Antivirus for Mac icon can be noticed in the Dock as soon as you open the application. The icon in the Dock provides you with an easy way to scan files and folders for malware. Just drag and drop the file or folder over the Dock icon and the scan will start immediately.
Dock Icon
3. Protecting against Malicious Software

This chapter includes the following topics:

- *Best Practices* (p. 14)
- *Scanning Your Mac* (p. 15)
- *Scan Wizard* (p. 16)
- *Fixing Issues* (p. 17)
- *Quarantine* (p. 20)
- *Web protection* (p. 21)
- *Updates* (p. 22)

3.1. Best Practices

To keep your system malware-free and to prevent accidental infection of other systems, follow these best practices:

- Keep *Continuous Scan* enabled, as to allow system files to be scanned by Norman Antivirus for Mac.

- Maintain your Norman Antivirus for Mac product up to date with the latest malware signatures and product updates, while having *Continuous Scan* activated.

- Check and fix the issues reported by Norman Antivirus for Mac regularly. For detailed information, refer to *Fixing Issues* (p. 17).

- Check the detailed log of events concerning the Norman Antivirus for Mac activity on your computer. Whenever something relevant to the security of your system or data happens, a new message is added to the Norman Safeguard AS history.

To access the History logs, follow these steps:
1. Open Norman Antivirus for Mac.

2. Do any of the following:
   ▶ Click Norman Antivirus for Mac in the menu bar and choose **Show History**.
   ▶ Press Command-Comma(i).

   Details about the product activity are displayed.

You should also adhere to these best practices:

▶ Make a habit of scanning files that you download from an external storage memory (such as an USB stick or a CD), especially when you do not know the source.

▶ If you have a DMG file, mount it and then scan its contents (the files within the mounted volume/image).

The easiest way to scan a file, a folder or a volume is to drag&drop it over the Norman Antivirus for Mac window or Dock icon.

No other configuration or action is required. However, if you want to, you can adjust the application settings and preferences to better suit your needs. For more information, refer to *Configuring Preferences* (p. 25).

### 3.2. Scanning Your Mac

You can scan your Mac or specific files anytime you want.

The easiest way to scan a file, a folder or a volume is to drag&drop it over the Norman Antivirus for Mac window or Dock icon. The scan wizard will appear and guide you through the scanning process.

You can also start a scan as follows:

1. Open Norman Antivirus for Mac.
2. Click one of the four scan buttons to start the desired scan.
● **Scan Critical Locations** - checks for malware the most vulnerable locations on your system (for example, the folders that contain the documents, downloads, mail downloads and temporary files of each user).

● **Full System Scan** - performs a comprehensive check for malware of the entire system. All connected mounts will be scanned too.

**Note**

Depending on the size of your hard disk, scanning the entire system may take a while (up to an hour or even more). For improved performance, it is recommended not to run this task while performing other resource-intensive tasks (such as video editing).

If you prefer, you can choose not to scan specific mounted volumes by adding them to the **Exclusions** list from the Preferences window.

● **Scan a Custom Location** - helps you check specific files, folders or volumes for malware.

● **Continuous Scan** - continuously monitors the applications running on the computer, looking for malware-like actions and prevents new malware threats from entering your system.

### 3.3. Scan Wizard

Whenever you initiate a scan, the Norman Antivirus for Mac scan wizard will appear.
You can see real-time information about the scan. Detected threats and the action taken on them are displayed in the Scan results section.

Wait for Norman Antivirus for Mac to finish scanning.

Note
The scanning process may take a while, depending on the complexity of the scan.

3.4. Fixing Issues

Norman Antivirus for Mac automatically detects and informs you about a series of issues that can affect the security of your system and data. In this way, you can fix security risks easily and in a timely manner.

Fixing the issues indicated by Norman Antivirus for Mac is a quick and easy way to ensure optimal protection of your system and data.

Detected issues include:
The new malware signatures and product updates have not been downloaded from our servers, because **Continuous Scan** is disabled.

Unresolved threats have been detected on your system. **Continuous Scan** is turned off.

To check and fix detected issues:

1. Open Norman Antivirus for Mac.
2. If Norman Antivirus for Mac has no warnings, the status bar has shades of green. When a security issue has been detected, the status bar green shades are replaced with yellow shades.
3. Check the description for more information.
4. Depending on the detected issue, a button may be available on the status bar to help you quickly fix it. Click the button to remove the security risk.

Usually, this happens when there are unresolved threats. You can view them and decide what to do with them.

**Note**

Norman Antivirus for Mac can take actions on current user's files only. Infected files owned by other users cannot be cleaned or quarantined by this app. Such files will be reported as unresolved issues.
Unresolved Threats Window

The list of unresolved threats is updated after each system scan.

You can choose to take the following actions on unresolved threats:

- Reveal in Finder. Take this action to remove the infections manually.
- Add to Exclusions. This action is not available for malware found inside archives.
- Ignore for now. The issue will be removed from the status bar until the next scan.
3.5. Quarantine

Norman Antivirus for Mac allows isolating the infected or suspicious files in a secure area, named quarantine. When a virus is in quarantine it cannot do any harm because it cannot be executed or read.

To view and manage the quarantined files, open the Quarantine window:

1. Open Norman Antivirus for Mac.
2. Click **Actions** in the menu bar.
3. Choose **View Quarantine**.

The Quarantine section displays all the files currently isolated in the Quarantine folder.
To delete a file from quarantine, select it and click **Delete**. If you want to restore a quarantined file to its original location, select it and click **Restore**.

### 3.6. Web protection

Norman Antivirus for Mac uses the Web Advisor extensions to completely secure your web browsing experience. The Web Advisor extensions intercept, process and filter all web traffic, blocking any malicious content.

The extensions work and integrate with the following web browsers: Mozilla Firefox, Google Chrome and Safari.

An array of features is available to protect you from all kinds of threats you may encounter while web browsing:

- **Advanced Phishing Filter** - prevents you from accessing websites used for phishing attacks.
- **Malware Filter** - blocks any malware you come in contact with while browsing the Internet.
- **Search Results Analyzer** - provides advance warning of risky websites within your search results.
- **Antifraud Filter** - provides protection against fraudulent websites while browsing the Internet.
- **Tracker Notification** - detects trackers on the visited web pages protecting your online privacy.

#### Enabling Web Advisor extensions

To enable the Web Advisor extensions, follow these steps:

1. Open Norman Antivirus for Mac.
2. Click **Activate** to activate the Web protection.
3. To install the Web Advisor extension on your browser, click **Get extension**.
4. You will be redirected to this online location:
   http://www.norman.com/Norman_Web_Advisor

5. Select Free Download.
6. Follow the steps to install the Web Advisor extension corresponding to your web browser.

Page rating and alerts

Depending on how Web Advisor classifies the web page you are currently viewing, one of the following icons is displayed in its area:

- This is a safe page to visit. You can continue your work.
- This web page may contain dangerous content. Exercise caution if you decide to visit it.
- You should leave the web page immediately. Alternatively, you can choose one of the available options:
  - Navigate away from the website by clicking Take me back to safety.
  - Proceed to the website, despite the warning, by clicking I understand the risks, take me there anyway.

3.7. Updates

New malware is found and identified every day. This is why it is very important to keep Norman Antivirus for Mac up to date with the latest malware signatures.

Keep the Continuous Scan turned on to allow the malware signatures and product updates to be automatically downloaded on your system. If an update is detected, it is automatically downloaded and installed on your computer.
The malware signatures update is performed on the fly, meaning that the files to be updated are replaced progressively. In this way, the update will not affect the product operation and, at the same time, any vulnerability will be excluded.

- If Norman Antivirus for Mac is up-to-date, it can detect the latest threats discovered and clean the infected files.
- If Norman Antivirus for Mac is not up-to-date, it will not be able to detect and remove the latest malware discovered by Norman Safeground AS Labs.

3.7.1. Requesting an Update

You can request an update manually anytime you want. Update by user request is recommended before you start a comprehensive scan.

An active Internet connection is required in order to check for available updates and download them.

To request an update manually:

1. Open Norman Antivirus for Mac.
2. Click the Actions in the menu bar.
3. Choose Update Virus Database.

You can see the update progress and downloaded files.

3.7.2. Getting Updates through a Proxy Server

Norman Antivirus for Mac can update only through proxy servers that do not require authentication. You do not have to configure any program settings.

If you connect to the Internet through a proxy server that requires authentication, you must switch to a direct Internet connection regularly in order to obtain malware signature updates.
3.7.3. Upgrade to a new version

Occasionally, we launch product updates to fix product issues. These updates may require a system restart in order to initiate the installation of new files. By default, if an update requires a computer restart, Norman Antivirus for Mac will keep working with the previous files until you reboot the system. In this case, the update process will not interfere with the user's work.

When a product update is completed, a pop-up window will inform you to restart the system. If you miss this notification, you can either click **Restart to upgrade** from the menu bar or manually restart the system.
4. Configuring Preferences

This chapter includes the following topics:

- Accessing Preferences (p. 25)
- General Preferences (p. 25)
- Scanner Preferences (p. 26)
- Scan Exclusions (p. 28)

4.1. Accessing Preferences

To open the Norman Antivirus for Mac Preferences window:

1. Open Norman Antivirus for Mac.
2. Do any of the following:
   - Click Norman Antivirus for Mac in the menu bar and choose Preferences.
   - Press Command-Comma(,).

4.2. General Preferences

The general preferences allow you to configure the general behavior of the application.

![General Preferences](image.png)
Enable notifications. Allows you to receive notifications regarding Norman Antivirus for Mac events and activities. On systems 10.8 and up, you will automatically be notified through Notification Center. On systems 10.7, you will be notified in Growl, if the application is installed. If you do not have Growl installed, you will still receive notifications through Norman Antivirus for Mac notification mechanism. Integration with Growl is an extra feature and it does not affect in any way your Norman Antivirus for Mac product.

Note
Growl is a third-party application developed by The Growl Project. It is not installed by default on Mac OS X. You can find out more information and download Growl from http://growl.info/.

4.3. Scanner Preferences
The scanner preferences allow you to configure the overall scanning approach. You can configure the actions taken on the infected and suspicious files detected and other general settings.
● **Action for infected items.** When it detects a virus or other malware, Norman Antivirus for Mac will automatically attempt to remove the malware code from the infected file and reconstruct the original file. This operation is referred to as disinfection. Files that cannot be disinfected are moved to **quarantine** in order to contain the infection.

Though not recommended, you can set the application to take no action on infected files. Detected files are only logged.

Continuous Scan ensures good protection against malware, with minor impact on system performance. If there are unresolved threats, you can view them and decide what to do with them.

![Malware warning](image)

● **Action for suspect items.** Files are detected as suspicious by the heuristic analysis. Suspicious files cannot be disinfected, because no disinfection routine is available.

By default, suspicious files are moved to quarantine. When a virus is in quarantine it cannot do any harm because it cannot be executed or read.

If you prefer, you can choose to ignore suspicious files. Detected files are only logged.
● **Scan only new and changed files.** Select this check box to set Norman Antivirus for Mac to scan only files that have not been scanned before or that have been modified since their last scan.

You can choose not to apply this setting for drag&drop scanning by selecting the corresponding check box.

● **Only scan archives less than {0} MB.** Use this option to optimize the scanning process by excluding larger archives from scanning.

**Note**

Scanning archived files increases the overall scanning time and requires more system resources.

Specify the maximum size of the archives to be scanned (in megabytes) in the corresponding field. Archives exceeding the specified size limit will not be scanned. If you want to scan all archives, regardless of their size, type 0.

### 4.4. Scan Exclusions

If you want to, you can set Norman Antivirus for Mac not to scan specific files, folders, or even an entire volume. For example, you might want to exclude from scanning:

● Files that are mistakenly identified as infected (known as false positives)
● Files that cause scanning errors
● Backup volumes
Scan Exclusions

The exclusions list contains the paths that have been excluded from scanning. There are two ways to set a scan exclusion:

- Drag&drop a file, folder or volume over the exclusions list.
- Click the button labeled with the plus sign (+), located under the exclusions list. Then, choose the file, folder or volume to be excluded from scanning.

To remove a scan exclusion, select it from the list and click the button labeled with the minus sign (-), located under the exclusions list.
5. Registering Norman Antivirus for Mac

This chapter includes the following topics:

- About Registration (p. 30)
- Registering Norman Antivirus for Mac (p. 30)
- Purchasing a License Key (p. 31)

5.1. About Registration

Norman Antivirus for Mac comes with 30-day trial period. During the trial period, the product is fully functional and you can test it to see if it meets your expectations.

You must register the product with a license key before the trial period ends. The license key specifies how long you are entitled to use the product. As soon as the license key expires, Norman Antivirus for Mac stops performing its functions and protecting your computer.

You should purchase a license key or renew your license a few days before the current license key expires.

5.2. Registering Norman Antivirus for Mac

An active Internet connection is required in order to register Norman Antivirus for Mac.

To register Norman Antivirus for Mac:

1. Open Norman Antivirus for Mac. If you do not know how to do this, refer to Opening Norman Antivirus for Mac (p. 10).

2. A link that indicates the number of days left on your license appears at the bottom of the Norman Antivirus for Mac window. Click this link to open the registration window. The registration window will appear.
3. Click **New serial** and enter your license key.

4. Click **Continue** to register your new license.

   After the registration is completed, you can see the new registration information in the registration window.

### 5.3. Purchasing a License Key

When your trial or licensing period comes close to end, purchase a license key to register Norman Antivirus for Mac and extend protection.

To purchase a license key:

1. Open Norman Antivirus for Mac.

2. A link that indicates the number of days left on your license appears at the bottom of the Norman Antivirus for Mac window.

   Click this link to open the registration window.

3. Click **Buy** in the bottom of the window.

4. Follow the instructions provided in the web page to purchase a license key.
6. Support and Contact Information

If you need help or additional information on Norman Antivirus for Mac, use the contact information provided below.

Norman Safeground AS
Product web page:
http://www.norman.com/home_and_small_office/products/norman_antivirus_for_mac
Technical support:
http://safeground.norman.com/home_and_small_office/help_support/
FAQ web page:
http://www.norman.com/home_and_small_office/products/norman_antivirus_for_mac/faqs
Types of Malicious Software

Adware
Adware is often combined with a host application that is provided at no charge as long as the user agrees to accept the adware. Because adware applications are usually installed after the user has agreed to a licensing agreement that states the purpose of the application, no offense is committed.

However, pop-up advertisements can become an annoyance, and in some cases degrade system performance. Also, the information that some of these applications collect may cause privacy concerns for users who were not fully aware of the terms in the license agreement.

Keylogger
A keylogger is an application that logs anything you type.
Keyloggers are not malicious in nature. They can be used for legitimate purposes, such as monitoring employees or children activity. However, they are increasingly being used by cyber-criminals for malicious purposes (for example, to collect private data, such as login credentials and social security numbers).

Polymorphic virus
A virus that changes its form with each file it infects. Since they have no consistent binary pattern, such viruses are hard to identify.

Rootkit
A rootkit is a set of software tools which offer administrator-level access to a system. The term was first used for the UNIX operating systems and it referred to recompiled tools which provided intruders administrative rights, allowing them to conceal their presence so as not to be seen by the system administrators.
The main role of rootkits is to hide processes, files, logins and logs. They may also intercept data from terminals, network connections or peripherals, if they incorporate the appropriate software.

Rootkits are not malicious in nature. For example, systems and even some applications hide critical files using rootkits. However, they are mostly used to hide malware or to conceal the presence of an intruder into the system. When combined with malware, rootkits pose a great threat to the integrity and the security of a system. They can monitor traffic, create backdoors into the system, alter files and logs and avoid detection.

Spyware
Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

Spyware's similarity to a Trojan horse is the fact that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.
**Trojan**

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

**Virus**

A program or piece of code that is loaded onto your computer without your knowledge and runs against your will. Most viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

**Worm**

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.