



eTrust[®] EZ Antivirus

Q: What is a virus?

A: A computer virus is a form of malicious software – also referred to as malware. Malware is a word derived from the combination of the words malicious, and software.

The forms of malware that antivirus solutions protect against include the following. All of these forms are commonly referred to simply as “viruses”.

- Viruses – a small program that attaches itself to another program or document and replicates with the potential to cause damage.
- Worms – specifically engineered to make extensive use of email to spread them rapidly.
- Trojans – programs that pretend to be something harmless but have a damaging or otherwise malicious intent.
- Zombies – programs that install themselves on machines, and remain dormant until an external event triggers them into action. This could do damage to your PC, steal your personal information and send it to an unauthorized email account, or even open up remote control access to your machine.

Q: How do antivirus solutions work?

A: Antivirus solutions provide protection by detecting viruses and disabling or removing them from your system. Detecting viruses is the job of the antivirus “engine”, which scans your systems, looking for the tell tale signatures of these malicious programs. Once detected, the software will take the appropriate action such as remove, rename, or disable.

Q: How do viruses spread?

A: Viruses today are typically spread via email, but can also be spread by sharing diskettes; network drives, or Internet downloads. Viruses cannot spread on their own and must be run (or executed) by someone to cause damage. Boot sector viruses spread when a user inadvertently boots his or her workstation from an infected floppy disk. Macro viruses can spread by simply opening an infected document.

Q: What damage can viruses cause?

A: The type of damage viruses can do varies dramatically. Some of them do a great deal of damage to files, or even destroy the contents of a hard drive, while others install programs intended to corrupt or steal information from your machine.

Q: What makes eTrust EZ Antivirus different from the rest?

A: eTrust EZ Antivirus leverages our expertise in providing security solutions to large businesses and government agencies worldwide. With over 27 years experience as a leading provider to Fortune[®] 500 companies, CA has developed the top technology for the defense against viruses. CA’s world-wide Security Advisor team provides continuous research and daily updates. eTrust EZ Antivirus leverages this expertise, yet provides a simple to use, extremely low-cost alternative for home and small office users.

Q: Why does antivirus software need continually updated signature files?

A: Since new viruses are released on a daily basis, it is critical that the antivirus software you use is updated with new virus signatures to provide protection against the most current threats.



eTrust[®] Internet Security Suite Frequently Asked Questions

Q: How does eTrust EZ Antivirus provide automated updates?

A: eTrust EZ Antivirus is configured to automatically check and update virus signatures via a standard Internet connection. This process is completely automated and does not require user intervention.

Q: How can eTrust EZ Antivirus protect me from tomorrow's viruses today?

A: Heuristic scanning engines enable eTrust EZ Antivirus to detect even unknown viruses by analyzing file characteristics to prevent potential infection.

Q: Who tests and certifies antivirus software?

A: There are several independent third parties that test and certify antivirus software. The most widely recognized is the International Computer Security Association (ICSA). To be ICSA-certified, the software must detect 100% of viruses "in-the-wild" (in general distribution) and 90% of over 6,000 test viruses. All versions of eTrust EZ Antivirus are ICSA-certified and the test results can be seen at <http://www.icsa.net>.

Q: What is included with the eTrust EZ Antivirus product?

A: A 1-year subscription of eTrust EZ Antivirus includes the software application along with:

- FREE daily virus signature file updates
- FREE product upgrades for up-to-date features and platform support
- FREE 24 X 7 web-based support and access to online tools

eTrust[®] Personal Firewall

Q: What is a firewall?

A: A firewall is an important first line of defense for computer security. A firewall is software or hardware that acts as a barrier between your PC and the Internet. It prevents unauthorized access (unauthorized programs or unauthorized Internet users) to your PC and hides your Internet-connected PC from view. All information leaving and entering your PC must pass through the firewall. It ultimately helps keep hackers away from your personal and confidential data.

Q: Why do I need a firewall?

A: In today's world of computing, several layers of protection are needed in order to defend your confidential data from hackers. Every PC connected to the Internet is a potential target. Computers are under constant attack from cyber vandals. Whether your connection is dial-up, DSL, or always-on, a firewall is necessary to stop intruders from getting into your PC.

Q: What kinds of threats do firewalls protect against?

A: Firewalls protect against hackers and online intruders who steal personal and confidential data that could lead to identity theft. Firewalls inspect each "packet" of data as it arrives on either side of the firewall – inbound from the Internet or outbound from your computer. The firewall determines whether or not it should be allowed to pass or if it should be blocked.

Q: If I already have antivirus and anti-spyware software, do I need a firewall?

A: Yes. eTrust Personal Firewall stops unauthorized access and hides your PC from possible hacker attacks. Firewalls protect you from things that antivirus software and anti-spyware software are not designed to find.

Antivirus software detects and removes viruses, while anti-spyware software detects and removes spyware, adware, Trojans, and other non-viral malicious code. Accordingly, eTrust Personal Firewall is the perfect complement to antivirus and anti-spyware software, providing a key component of a multilayered security strategy.



eTrust[®] Internet Security Suite Frequently Asked Questions

Q: What are the features of eTrust Personal Firewall?

A: eTrust Personal Firewall offers simple-to-use yet powerful features such as:

- **Automatic Program Control** that reduces necessary user interaction
- **ID Lock** that prevents confidential and personal data from being sent through the Internet without your knowledge
- **Cache Cleaner** that provides a convenient way to remove cookies and temporary files from your PC
- **Cookie Control, Ad Blocking, and Mobile Code Control** to reduce interruptions while protecting your privacy
- **Stealth Mode** that hides your PC on the Internet so that hackers cannot see it
- **MailSafe** that identifies and quarantines potentially harmful email attachments
- **Password Protected Program Options** that protect your security settings from modification by unauthorized users

Q: What is included with the eTrust Personal Firewall product?

A: A 1-year subscription includes:

- FREE product upgrades
- FREE 24 x 7 web support
- FREE access to our rich knowledge base and online tools

Q: Is eTrust Personal Firewall a certified product?

A: Yes, eTrust Personal Firewall is ICSA Certified. There are several different independent third parties that test and certify PC firewall software; the most widely recognized being the International Computer Security Association (ICSA). ICSA Labs tests firewall products against a standard yet evolving set of criteria. The firewall certification criteria is composed of both functional and assurance requirements. The criteria requirements define an industry-accepted standard that all products claiming to have firewalling capabilities must have networking and logging capabilities, and the ability to defend against attacks.

eTrust[®] PestPatrol[®] Anti-Spyware

Q. What is eTrust PestPatrol Anti-Spyware?

A. eTrust PestPatrol Anti-Spyware detects and removes a wide variety of spyware to protect your PC from unauthorized access, information theft and diminished system performance.

Q. What is spyware?

A. Spyware and adware are non-viral applications (surveillance tools) that are loaded without the user's knowledge and can monitor computer activity including keystroke tracking and capture, email logging, instant message usage and snapshots. Spyware comes in many shapes and sizes: some are simply an annoyance while others threaten security. Here are some common types of spyware:

- **Spyware** – tracks information about you, your computer, and your surfing habits
- **Adware** – displays unwanted advertising that can slow your computer to a crawl
- **Keyloggers** – can record every keystroke you make, then steal your passwords and other personal data
- **Browser Hijackers** – can change your homepage and search results
- **Remote Access Trojans (RATS)** – allows attackers to remotely control your computer

Q. How do I get infected with spyware?

A. Spyware and adware can enter a system in several ways, such as through everyday web browsing, unauthorized software downloads, peer-to-peer file swapping, email attachments,



eTrust[®] Internet Security Suite Frequently Asked Questions

instant messaging and chat sessions, bundles with legitimate software, hacker website downloads, and “drive-by” installs from websites.

Q. Why do I need anti-spyware software?

A. Spyware can lead to anything from PC crashes to increased spam to identity theft. These threats are rapidly proliferating and represent a major security and privacy risk, therefore requiring a solution.

Q. If I already have antivirus software, do I need anti-spyware software?

A. Your antivirus protection is important — it detects and removes viral threats. But your PC can be infected with other dangers such as spyware. Anti-spyware software is designed to stop these threats, which have unique properties that can remain hidden on your PC and cause havoc. eTrust PestPatrol Anti-Spyware detects and removes a wide range of spyware threats, making it a powerful complement to your antivirus defense.

Q. Why not use free anti-spyware software?

A. Free anti-spyware typically does not offer all of the functionality that is available in eTrust PestPatrol Anti-Spyware, such as real-time protection, a pest information database, logging, support and automatic updates. Also, ‘freeware’ products typically cannot afford to invest heavily in research and development, meaning their solutions may not be as effective in detecting and removing a wide range of threats. In addition, freeware products usually do not offer the same level of customer service and technical support.

Q. What are the key features of eTrust PestPatrol Anti-Spyware?

A. eTrust PestPatrol Anti-Spyware detects and removes spyware, adware, Trojan horses, browser hijackers, keyloggers and other web-based threats in real-time. It provides an easy-to-use interface with automatic pest definition updates, on-demand or scheduled scanning, automated alerts and logs, and is supported by one of the largest spyware research facilities in the world, the CA Security Advisory Team. eTrust PestPatrol Anti-Spyware proactively protects your PC against new spyware threats and generally improves PC performance.

eTrust[®] Anti-Spam

Q: What is Spam?

A: Spam is the common term for electronic ‘junk mail’ or unwanted messages sent to a person’s email account.

Q: Why is spam a problem; can’t I just delete spam from my Inbox by hitting Delete?

A: Today, 40% of all email is unsolicited, unwanted spam. The billions of spam messages circulating across the Internet can disrupt email delivery, degrade system performance, and reduce overall productivity. Deleting spam emails seems like the simple solution, but if you add up the time spent deleting every spam email you receive, you lose a significant amount of productivity.

Additionally, spam messages may contain offensive or fraudulent material and can even be used to spread viruses. Spammers may also be using your computer to send these unsolicited and possibly offensive email messages. Spammers are using home computers to send bulk emails by the millions. According to the FTC, as much as 30% of all spam is relayed by compromised home and home office PCs, but controlled from afar. Therefore, not only is spam a nuisance that affects PC and user productivity, but it can also be a serious threat to security and privacy.

Q: How do I get spam?



eTrust[®] Internet Security Suite Frequently Asked Questions

A: Spammers often use bulk email programs to send out their unsolicited messages to lists of email addresses that are often collected without the recipient's knowledge. There are several ways spammers obtain these email addresses.

- **Harvesting from Websites** – Most companies list email addresses and contact information on their websites. Spammers use web-crawlers to search for these email addresses located on web pages.
- **Mailing Lists** – Many people sign up for mailing lists for newsletters, news alerts, coupons, special offers, and other interests. However, spammers can also sign up for these mailing lists and obtain the email addresses.
- **Usenet Posting** – Spammers can also use bots to cruise newsgroups on Usenet in order to collect email addresses.
- **Coincidental** – Your email address may be unique to your Internet Service Provider (ISP), but it may also be used by several other people using different ISPs. Spammers use the front part of email addresses and change the ISP name to create a list of several email addresses.
- **Dictionary Attacks** – Spammers make educated guesses on email addresses by stringing together common names and words.

Q: What is 'Phishing'?

A: Phishing generally refers to email messages that appear to come from trusted companies, but then attempt to send people to fake websites where they are asked to give out sensitive personal information. This information can then be used by the creators of the website to commit identity fraud. Phishing emails may appear to come from banks, credit card companies, and other businesses and the websites look identical to the legitimate company's website.

According to ZDNet, "Phishing is one of the fastest growing forms of personal fraud in the world." Phishing attacks have reached 57 million US adults and compromised at least 122 well-known brands so far. In a recent survey, seven out of ten people who go online have received phishing emails, while 15% have actually given out personal information.

Q: Are there laws to stop spam?

A: The 'Controlling the Assault of Non-Solicited Pornography and Marketing' (CAN-SPAM) Act took effect in the United States in January, 2004. However, it does not make spam illegal, but rather places certain restrictions on what bulk mail senders can do. If spammers comply, they can send their unsolicited emails. The CAN-SPAM Act also does not apply to email sent from outside of the United States, even though other countries around the world have some measures in place.

Q: Can't I get rid of spam emails by 'unsubscribing'?

A: No. Any response to spam emails confirms the accuracy of your email address and may result in even more spam messages.

Q: How can I solve my spam problem?

A: eTrust[®] Anti-Spam is the easiest and most effective anti-spam solution available to block 100% of your unwanted spam. eTrust Anti-Spam allows you to see important messages from people you know while blocking questionable messages from people you don't.

Q: What are some of the features of eTrust Anti-Spam?

A: eTrust Anti-Spam offers simple-to-use yet powerful features like:

- **Blocks 100% of Spam** - Allows only messages from your approved senders list to reach your Inbox - all other mail is quarantined for you to review later, eliminating time wasted sorting and deleting unwanted email.
- **Protects Multiple Email Accounts** – Monitors inbound messages for all of your Microsoft Exchange and any POP3 mail accounts you have configured in Outlook.



eTrust[®] Internet Security Suite Frequently Asked Questions

- **Anti-Phishing and Fraud Protection** — Uses industry-standard authentication methods to determine if an email is actually from the sender indicated on the message, and displays a clear visual warning on suspicious emails.
- **Supports Bonded Sender** – Allows mail from legitimate senders of commercial email (e.g. confirmations from Amazon) to be delivered to your Inbox.
- **International Language Support** – Automatically displays German, French, Italian, Spanish, Brazilian Portuguese, Chinese, Japanese and Korean based on your Windows language settings, and properly filters spam sent in any language.
- **Email Search*** - Creates a comprehensive search index of the information stored in Outlook, so you can quickly and easily find messages, attachments, appointments, contacts, journal entries and notes.
- **Spam Score** - Automatically 'scores' the spam in your Quarantine folder, allowing you to sort your quarantined mail based on its likelihood of being spam. This helps you easily determine which messages are most likely to be spam, and allows you to take the appropriate action.
- **Automatic Updates** - Notifies you when product updates are available for download, providing you with the latest features to defend against spam.

** For English-language Outlook and Outlook Express only*