



Computer Associates®

## eTrust™ Anti-Spam Frequently Asked Questions

### **Q: What is Spam?**

**A:** Spam is the common term for electronic 'junk mail' or unwanted messages sent to a person's e-mail account.

### **Q: Why is spam a problem; can't I just delete spam from my Inbox by hitting delete?**

**A:** Today, 40% of all e-mail is unsolicited, unwanted spam. The billions of spam messages circulating across the Internet can disrupt e-mail delivery, degrade system performance, and reduce overall productivity. Deleting spam e-mails seems like the simple solution, but if you add up the time spent deleting every spam e-mail 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 e-mail messages. Spammers are using home computers to send bulk e-mails 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?**

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

- Harvesting from Websites – Most companies list e-mail addresses and contact information on their websites. Spammers use web-crawlers to search for these e-mail 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 e-mail addresses.
- Usenet Posting – Spammers can also use bots to cruise newsgroups on Usenet in order to collect e-mail addresses.
- Coincidental – Your e-mail 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 e-mail addresses and change the ISP name to create a list of several e-mail addresses.
- Dictionary Attacks – Spammers make educated guesses on e-mail addresses by stringing together common names and words.

### **Q: What is 'Phishing'?**

**A:** Phishing generally refers to e-mail 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 e-mails, 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



Computer Associates®

## eTrust™ Anti-Spam Frequently Asked Questions

rather places certain restrictions on what bulk mail senders can do. If spammers comply, they can send their unsolicited e-mails. The CAN-SPAM Act also does not apply to e-mail 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 e-mails by 'unsubscribing'?**

**A:** No. Any response to spam e-mails confirms the accuracy of your e-mail 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** – eTrust Anti-Spam only allows mail from your personalized 'white list' of approved senders to reach your Inbox, thereby protecting you from any unwanted e-mails.
- **Automatically Manages White List** – eTrust Anti-Spam quickly learns who you communicate with and updates your white list of approved senders as you work.
- **Easy to Use and Understand** – There is no complex configuration or setup of content filters with eTrust Anti-Spam.
- **Suppression of New Mail Notification for Spam** – You are only notified when new mail is received from approved senders. Mail notification is suppressed when inbound messages are diverted to the quarantine folder.
- **Optional Challenge/Response** – Optionally allows eTrust Anti-Spam to confirm that senders of quarantined messages are real people and not automated spam robots.
- **Supports Bonded Sender** – Allows mail from legitimate senders of commercial e-mail (e.g. order confirmations from Amazon) to be delivered to your Inbox.
- **Protects Multiple E-mail Accounts** – Monitors inbound messages for all of your Microsoft Exchange and any POP3 mail accounts you have configured in Outlook.
- **Spoof-Proof Fraud Protection** – Automatically verifies the authenticity of messages from people and companies using industry-standard digital signatures.
- **International Language Support** – eTrust Anti-Spam properly filters spam sent in any language and automatically works in English, German, French, Italian, Spanish, Brazilian Portuguese, Chinese, Japanese, and Korean.