



---

# Frequently Asked Questions (FAQs)

---

## Boundary Defense for Email

---

MailStreet Live Support: [866-461-0851](tel:866-461-0851)

---

## Boundary Defense for Email – Anti-Spam FAQs

### What is Spam?

Spam is unsolicited e-mail sent to a large number of addresses, usually for a commercial purpose. Most spam is commercial advertising, usually for dubious products, get-rich-quick schemes, or quasi-legal services. Often the products advertised are worthless, deceptive, and partly or entirely fraudulent. Other times, it is simply advertising for something that you may not be interested in.

### What is Phishing?

Phishing is the process of luring unsuspecting Internet users to a fake website by using authentic-looking email with the real organization's logo, in an attempt to steal passwords, financial or personal information, or introduce a virus.

### What is Open Relay?

An open relay, also known as 'third party relay' or 'insecure relay', is where a mail server will route email for anybody in the world. Any machine that will accept email for any domain and forward it on regardless of who the sender is or what IP address the email is sent from is generally called an 'open relay'. Spammers hunt for and abuse these servers to try to cover their tracks. When spammers locate such a machine, they can use it as a free distribution service for their junk email.

### What is a Whitelist and a Blacklist?

A whitelist is a list of emails, domains or IP addresses from which you will always accept email, even if it would otherwise be considered spam. For example, newsletters you subscribe to.

A blacklist is a list of emails, domains or IP addresses from which you will never accept email even if it is otherwise legitimate.

### What is a Denial of Service Attack (DOS) ?

DOS is an attack designed to bring the network down by flooding it with requests and traffic. A mail or web server can only handle a finite amount of requests and will crash once that limit is reached.

A variation on DOS is Distributed DOS, where a few to thousands of computers at various locations are part of a coordinated attack on a network.

### What is a false-positive?

It is a negative instance that is erroneously reported as being positive — that is, a non-spam email which is erroneously reported as being spam.

### What is a blocked senders list?

This is a list of email addresses from which email is blocked from being received into the recipient's inbox. A user may have been enabled to manage a personal blocked senders list. There may also be public and company block lists in place. Quarantine Administrators can view and manage a user's personal blocked list.

### What is a public block list?

They are recognized public block lists of IP addresses of globally known sources of spam.

### **What is an approved senders list?**

The list can contain email addresses, domains, or IP addresses. The list enables email from a sender on list to pass through the spam service without interruption.

### **What are signaturing systems?**

They are proprietary and commercially available signature-building engines that create a vast knowledge base of signatures of spam messages currently in email circulation.

## **Boundary Defense for Email – Anti-Virus FAQs**

### **What is an email virus?**

A virus is a software program designed to spread itself by infecting files and system areas of a storage device, such as a hard drive. You can't get a virus just by reading a plain-text e-mail message or Usenet post. Be careful of encoded messages containing embedded executable code (i.e., JavaScript in an HTML message) or messages that include an executable file attachment (i.e., an encoded program file or a Word document containing macros).

### **How does a virus filter work?**

There are two types of anti-virus filters, one that blocks known viruses based on their signature and another that blocks new or unknown viruses based on behavior. Many Anti-Virus companies use a combination of commercial engines to increase their chances of stopping a virus.

### **What are Spoofed mail viruses?**

Many of the latest viruses forge the sender's email address. The technique, commonly known as spoofing, is used in order to cause confusion and attempt to hide the identity of the true virus sender. The Sobig and Klez family are examples of viruses that employ spoofing techniques. The difficult part is stopping new and unknown viruses. A heuristic algorithm that checks the structure and behavior of the email attachment is a popular approach, although it takes years of data-acquired experience and expertise to create one that works well.

### **What is malware?**

Short for malicious software, it is software designed to infiltrate or damage a computer system without the owner's informed consent. Malware includes computer viruses, worms, Trojan horses, most rootkits, spyware, dishonest adware, crime ware and other malicious and unwanted software.

### **What is spyware?**

It is a type of malware that is installed on computers and collects information about users without their knowledge. The presence of spyware is typically hidden from the user. Spyware programs can collect various types of personal information, such as Internet surfing habits and sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software and redirecting Web browser activity. Spyware is known to change computer settings, resulting in slow connection speeds, different home pages, and/or loss of Internet or functionality of other programs.

### **What is Adware?**

It is any software package which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used.

### **What is a Trojan Horse?**

It is a type of program that is often confused with viruses. Trojan Horse is not a virus, but simply a program (often harmful) that pretends to be something else. For example, you might download what you think is a new game; but when you run it, it deletes files on your hard drive. Or the third time you start the game, the program e-mails your saved passwords to another person.

### **What is a targeted attack?**

This is a class of malware destined for one specific organization or industry. These threats are of particular concern because they are designed to capture sensitive information. Targeted attacks may include threats delivered via SMTP e-mail, port attacks, zero day attack vulnerability exploits or phishing messages. The home user is the most targeted sector. Financial industries are the second most targeted sector, most likely because cybercriminals desire to profit from the confidential, sensitive information the financial industry IT infrastructure houses.

### **What is a worm?**

A self-replicating computer program. It uses a network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or devour files on a targeted computer.

### **What is a zero-day (or zero-hour) attack?**

A computer threat that tries to exploit computer application vulnerabilities that are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the vulnerability

## Boundary Defense for Email – Content Control FAQs

### **How can I add email addresses to Boundary Defense for Email Content Control?**

When a user sends an outbound email, Email Content Control automatically harvests their email address for future use. Addresses can also be added manually to a user group or added for a specific rule.

### **Can I differentiate between the parts of the email to look in?**

Yes. You can define whether to scan within the header, subject line, body, and the attachment of emails.

### **Does Boundary Defense for Email Content Control scan within MS Office documents as well as email?**

Yes. The Boundary Defense for Email Content Control Service scans within MS Office documents for words and phrases or regular expressions.

### **Does Boundary Defense for Email Content Control automatically scan within archive files such as ZIP and RAR for file types?**

Yes, if you set up a rule to detect specific file types or content, Boundary Defense for Email Content Control will look inside the archive files to see if the file type or content are hidden in there.

### **If I am sent a spoofed file, for example, an XLS file renamed with a DOC extension, is the Boundary Defense for Email Content Control service able to pick this up?**

Yes. If the spoofed file is malicious, it will already have been detected by the Boundary Defense for Email Anti-Virus service. However if the file is simply spoofed, then the Email Content Control service can be configured to detect this within the Attachment tab.

### **How do wildcards work?**

Wildcards are used when you do not want to state exactly the numbers or characters to trigger a rule, but when there are specific alphanumeric characters that must be present. An example of this may be something like patient numbers, which, in a certain scenario, may always have the first five characters as HGTYU, but after those characters could be any combination of letters or numbers. So you could use HGTYU\* to monitor emails leaving an organization that include this arrangement of characters.

---