FREE PRODUCT DEMO | DOWNLOADS | FORTICLOUD LOGIN

FORTINET Products Solutions Support Partners Company Contact Us FORTIGUARD LABS THREAT INTELLIGENCE

Spam Filtering

Learn about spam filters, how they work, why they exist, and how to avoid being filtered.

EMAIL SECURITY RECOMMENDATIONS 2025 THREAT LANDSCAPE REPORT

What Is Spam Filtering?

What is a spam filter? Spam filters are designed to identify incoming dangerous emails from attackers or marketers. Attackers often use emails that claim to offer a beneficial service or protect you from imminent danger, but they are really just clickbait, designed to get you to click on a link that downloads malicious software onto your computer or sends you to a dangerous site.

Spam can also contain relatively harmless content but can clutter up your inbox, consuming valuable space and making it more difficult to identify important, useful emails. Spam filters can detect spam emails. These helpful tools can recognize patterns that spam emails tend to follow.

What is spam protection? When you get spam, in many cases, your email address was purchased by a person or company as part of a list. It also could have been stolen by a hacker who had gained access to lists of client email addresses. The person sending the spam sends the same email to many people at the same time, knowing that if the email works on only one in many thousand people, the attack or marketing scheme will be successful.

Because an email spam filtering can recognize these kinds of emails, it can be a valuable solution for protecting users from unwanted messages. To enhance the protection, some spam filters use insights gained from machine learning to more accurately target junk mail.

Often, an internet service provider (ISP) will use spam detection to reduce the amount of spam delivered to users. Companies can do the same to lessen the burden of spam on their employees. However, spam filtering can also flag legitimate emails from companies users actually want to get messages from. In this case, users often have the option to determine the kinds of emails they want and adjust their settings to allow them to pass through the filter.

Email Security Resources

- Cybersecurity
- Types of Cyber Attacks
- IT vs OT Cybersecurity
- AI Cybersecurity
- Cyber Threat Intelligence
- Cybersecurity Management
- Network Security
- Data Security
- Email Security
- Endpoint Security
- Web Security
- Enterprise Security
- Cybersecurity Mesh

Quick Links

- Fortinet Products
- Fortinet Demos
- Analyst Reports
- Contact Us

Spam refers to any type of unwanted bulk communication. It is sent via email, text messages, social media, or phone calls.

It is unclear exactly where the term “spam” came from, but one theory says it is derived from a Monty Python skit where people were told to eat the canned meat Spam, regardless of whether they wanted to or not. Similarly, many inboxes get “force-fed” spam emails on a constant basis.

Why Email Security Is Valuable for Protecting Against Ransomware

Download the eBook to get actionable recommendations to enhance your email security against ransomware.

Download Now

How Does A Spam Filter Work?

Spam filters all have the same basic objective: to keep unwanted emails out of users’ inboxes. However, there are several different types of spam filters, and they each use different filtering methods to hone in on spam.

Content filters

Content filters analyze the text inside an email and use that information to decide whether or not to mark it as spam. The content of spam emails is often predictable, particularly because they tend to have the same basic objectives: offer deals, promote explicit material, or otherwise tap into human emotions, feelings, and desires, such as greed or fear.

Content filters may search for words connected to money, such as “discount,” “limited time,” or “offer.” To trigger the filter, there typically would have to be multiple uses of the target word.

Content filters may also examine an email for inappropriate language of a sexual nature that could indicate explicit content. In some campaigns, an attacker may use sexually explicit emails to lure users into opening the email and then clicking on malicious links.

Blacklist email spam filters work by blocking emails from senders that have been put on a list of spammers. Blacklist filters are updated on a regular basis because spammers can change their email addresses relatively easily. If a spammer switches from one email domain to another, the email may still be able to penetrate the filter until it is updated and the sender's emails once again get labeled as spam.

A company can also use its own blacklist spam filtering to protect its interests. For example, they can use them to target headhunters seeking to attract their employees to other companies. They could also use a blacklist filter to block emails that could waste employees' time with sales offers and promotions that could distract them from getting their work done.

Header filters

Header filters examine the header of an email to see if it may be coming from an illegitimate source. This could include Internet Protocol (IP) addresses that spammers tend to use. It may also include information that indicates the email is just one copy of many emails sent at the same time to pre-organized groups of recipients.

Language filters

Sometimes spammers target people from other countries, and the email is therefore in a different language than that of the recipient. In most cases, a user will only want to receive emails in languages in which they are fluent.

However, if a business connection or customer from another country reaches out, there exists the chance that the language filter could categorize that legitimate email as spam, so users may have to be instructed to check their spam folders when expecting these kinds of messages.

Rule-based filters

You can use a filter to set up specific rules that can be applied to all emails coming into your system. If the email's content or origin matches one of the rules, it can be automatically sent to a spam folder. For example, you can set the filter to look for specific words or phrases in the body of an email. If these words are present, the message gets sent to the spam folder.

You can also set the filter so it looks for particular words or phrases in the header. This can be useful for emails associated with memberships that, while still useful, result in unwanted messages from time to time.

Rule-based spam filtering is also useful for targeting specific senders. You can set them up to look for information in the domain the email is coming from or the name of the person sending it.

A Bayesian filter can learn your preferences by examining the emails that you send to spam. It observes the content of the emails you mark as spam and then sets up rules accordingly. These rules are then applied to future emails trying to get into your inbox.

For example, if you constantly mark all emails from a specific sender as spam, a Bayesian filter can recognize this pattern. It will then look for emails from that sender and move them to your spam folder automatically.

Why Do Spam Filters Exist?

Even though a lot of spam is relatively harmless, email providers use spam filtering to ensure the experiences of their users are as annoyance-free as possible. Spam emails can fill up your inbox to the point where the amount of available storage approaches its limit and inbox management becomes a pain. In this case, users may have to choose between upgrading their storage or getting another free email account. When a user migrates from one provider to another, the initial provider stands to lose money, so keeping them around by trying to eliminate spam will improve their bottom line.

Spam can also contain malicious content that can infect users' computers with viruses or other **malware**. If an email provider, including a private company, cannot prevent these kinds of emails from getting through, the service may gain a reputation as a liability more than an asset. Filtering out spam therefore improves both the user experience and the reputation of the provider.

For companies, a spam filter can protect valuable assets, including workstations, servers, and other elements of its network. Filtering out malicious emails can stop malware from penetrating the system and then moving east to west, infecting the computers of other users.

How Can Spam Filters Help You?

Spam filters can help you by preventing unwanted emails from entering your inbox. While this may sound like a straightforward task, it can be a challenge for filters that are not constantly updated according to the most recent spam techniques and senders.

Spammers may change the address from which emails come or the wording inside the header or body to bypass out-of-date spam filters. This can be effective if the spam filter is not updated with the correct information on a regular basis. Therefore, it is important to make sure your spam filter has adequate spam intelligence. If it does, it can block hundreds or thousands of spam emails every month.

Spam filters are also helpful because they provide an extra layer of security for your network. Email is a popular **attack vector** for hackers and other malicious actors seeking to infect computers with malware. An attacker may send an email with an attachment that looks like an innocent image. However, hidden within

In other situations, the body of the email itself may have a link in it. When the recipient clicks on that word or phrase, they are brought to a malicious website. With the right kind of spam filter, you can keep dangerous emails out of the inboxes of your employees.

With an adaptable spam filter, administrators can adjust the settings to target particularly harmful emails. They can also filter out emails that could distract employees or waste their time. Further, because spam folders can be set to automatically delete the emails inside after a certain amount of time, an administrator can conserve space on an email server by targeting space-devouring spam. As spam is periodically deleted, the server is alleviated of wasteful email content.

What Is A Spam Folder And How Can You Avoid It?

If you have ever searched for the answer to the question, “What is spam in Gmail?” you may have come across a spam folder. This is a feature of many email services that automatically puts spammy communications in a specific folder. In this way, the recipient does not have to see or deal with these emails at all.

The problem with spam folders is that legitimate emails can get sent there, too. If you do not want your email to end up in the spam folder, it is best to send them one at a time to a single addressee. Also, avoid spammy terms, such as “free” or “special offer,” which often get flagged by spam filters.

Spam Filter FAQs

What is a spam filter and how does it work?

Spam filters are designed to identify emails that attackers or marketers use to send unwanted or dangerous content. They use specific filtering methods to identify the content of emails or their senders and then flag the email as spam. The email can then be automatically deleted instantly or after a period of time.

What is the best spam filter?

The best spam filter for your needs will depend on the challenges and goals of your business. However, for some, a Bayesian filter may offer convenience because it can automatically learn what you think is spam by studying which emails you flag.