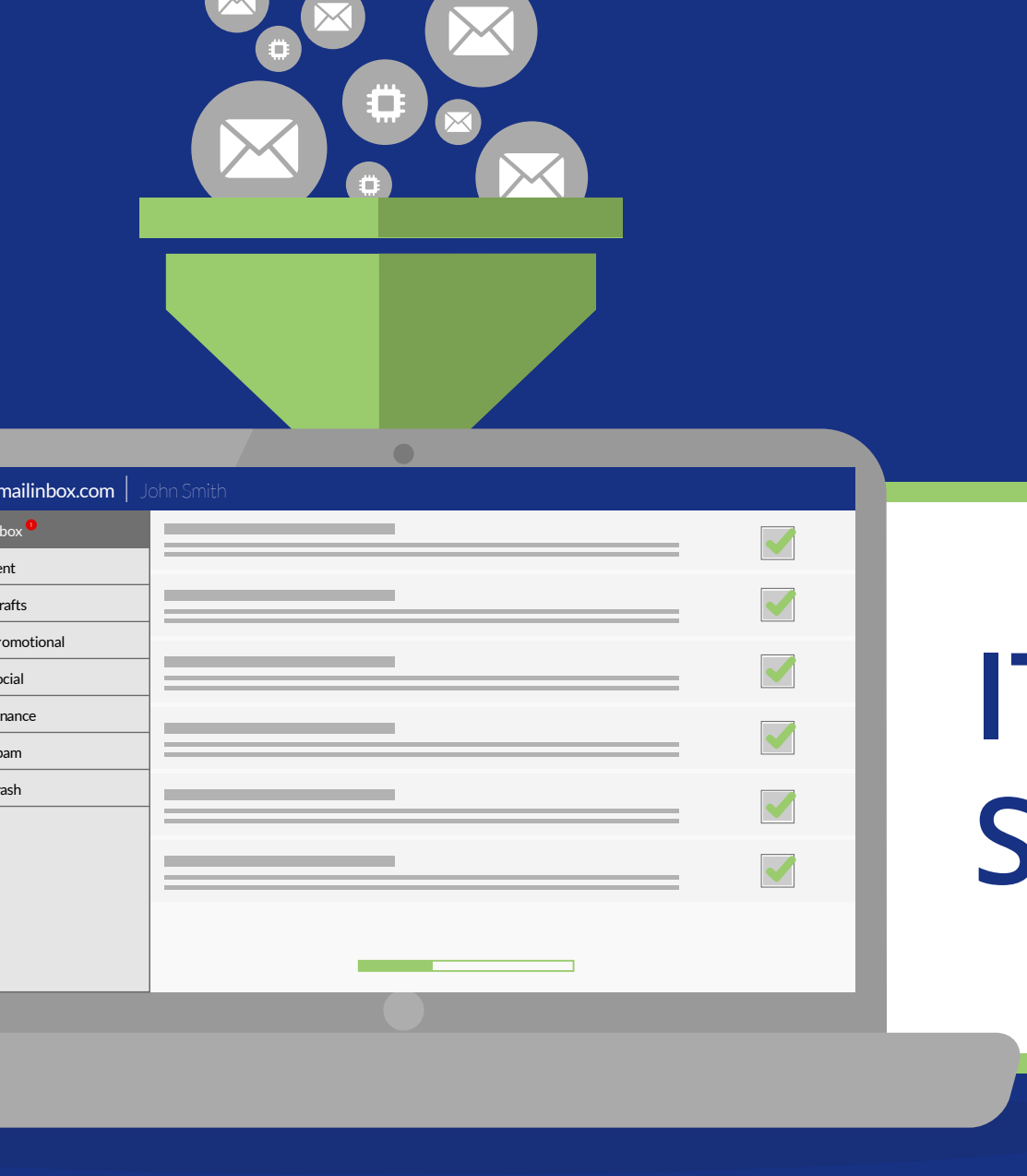


IT Checklist for Spam Filtering

sendio®

Spam filtering solutions have become an integral part of the business email landscape. Businesses, no matter the size, have come to rely on spam filters to help keep both malicious and junk email messages out of user's inboxes: messages that made up 59.2 percent of all email traffic in the first quarter of 2015, according to Securelist's quarterly spam report.[1] Although the percentage of illegitimate emails is 6 percent lower than the previous quarter, spam continues to make up a majority of all emails sent on a daily basis.

To manage illicit emails, businesses turn to email security solutions that use a variety of filtering techniques, such as Bayesian, keyword, heuristic, and list-based, combined with other technologies such as challenge/response, DNS lookup, Sender Policy Framework (SPF), and DomainKeys Identified Mail (DKIM) to block spam and other malicious email messages before they are delivered.

In order for these email-filtering services to work effectively, someone needs to configure them properly so that legitimate emails pass through with ease while those that intend to do harm are kept at bay. This, however, has proved to be a challenge for email security professionals in both small- and medium-sized organizations and larger enterprises alike because fine-tuning even the most easy-to-manage email filters requires data from your logs, feedback from your end-users, and a bit of practice.

Out of the box, your email filtering solution must be configured to block spam and other threats using techniques such as:

Filtering lists to include blacklisting, whitelisting and silverlisting

Blocking attachments that contain file types known to cause harm

Scanning for viruses and malware

Scanning for links to known malicious URLs

The combination of these techniques will provide you with a foundation for effective email security.

Set up Filtering Lists

Filtering lists are used to indicate how an email security solution should handle each and every incoming message that your email server receives. Based on these lists, your email filtering service will either:

- Deny the email message if the sender's IP address is on any of the blacklists
- Deliver the message if the sender is part of your whitelist
- Put things into a holding pattern using a technique known as silverlisting (or an enhanced version, Silverlisting)

CREATE A BLACKLIST

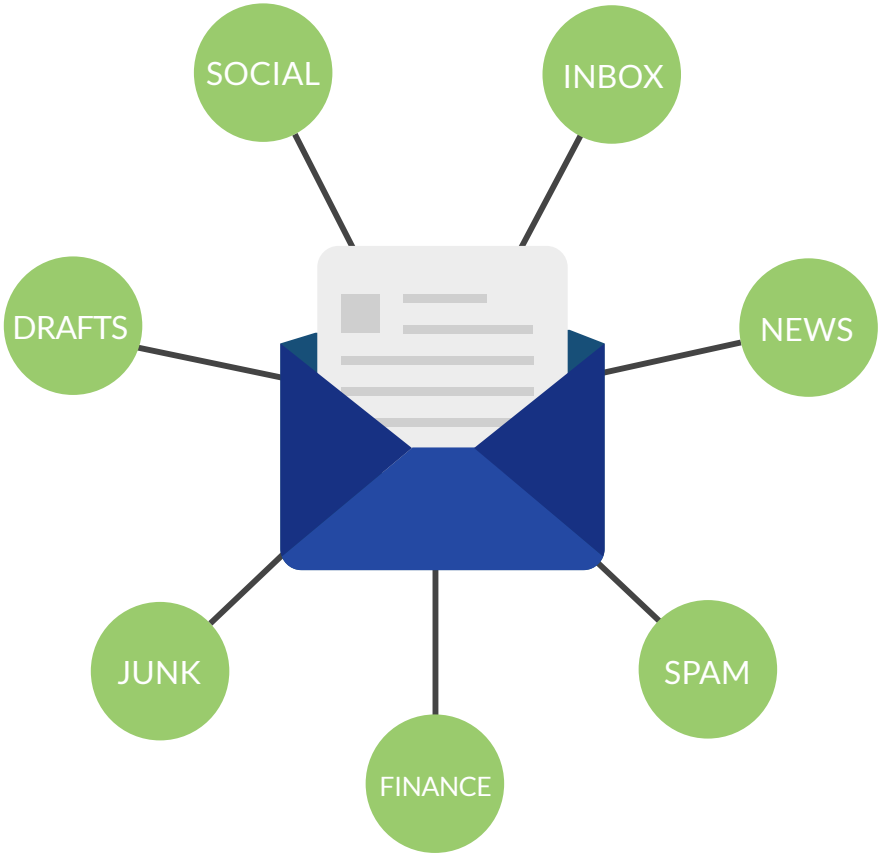
Email security relies heavily on two things: effective technical solutions and a collaborative community. Choosing the right solutions provider is an essential part to stopping spam; however, relying on the community of professionals is equally as important because this is where the shared intelligence that so many blacklists come from. Also known as DNS Black Lists (DNSBL) or Realtime Black Lists (RBL), these lists contain the IP addresses of mail servers that are known to send spam.

One way addresses find their way onto this list is by security professionals who identify servers that are known to send spam or are known open relays. Another way an IP address could wind up on this list is if enough recipients, or end-users, identify an email sender's message as spam. This happens frequently when unsolicited marketing emails are sent out en masse. This is why effective blacklisting is so reliant on the community of email users for success.

If you employ blacklists as part of your filtering, then any email from a IP address on the blacklist will not be delivered to anyone in your organization. So even if a legitimate business partner is identified as a spammer, perhaps because of a poorly planned email marketing campaign, important messages from them may wind up blocked by your filtering service. To see some of the major blacklists, or to check to see if your company or any partners are on these lists, visit MXToolbox.com or DNSBL.info. Both provide access to more than 100 well-known lists to check against.

DECIDE BETWEEN WHITELISTING AND SILVERLISTING

Although blacklists tell your email filters which messages to block, whitelists and silverlists work in the opposite manner by telling your email filter which messages to let in. Unlike blacklists, these options are not a shared resource that can be polluted with illegitimate IP addresses or domain names. As an IT professional, whitelists and silverlists give you the ability to more granularly define which IP addresses and domain name users you will automatically receive emails from. But as an IT professional, you must also decide which method is best for your organization's email security needs.



When activated, a whitelist becomes the first checkpoint for email filtering services. If the sender matches with an entry on the whitelist, the message is delivered to the recipient's inbox without undergoing any further checks. If it does not, it goes through the other processes to determine if the message is safe to deliver or if it should be rejected.

This poses some problems, as one common method attackers use to bypass email filtering is to spoof legitimate email addresses. They can easily find out who an organization is doing business with and forge email accounts that appear to come from a trusted source. Any filtering tools that automatically deliver messages from whitelisted senders may not catch this, so malicious emails would wind up in the recipient's inbox instead of undergoing additional checks that could identify them as spam.

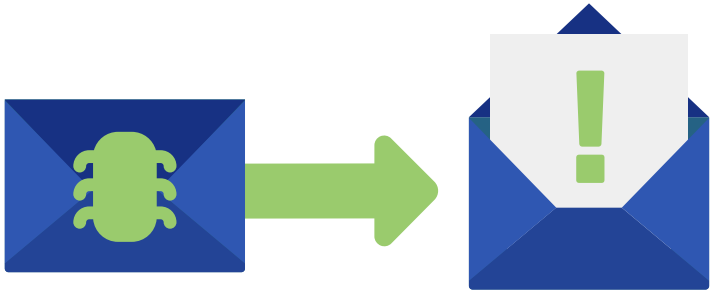
The same can be said for emails that come from compromised accounts.

With Silverlisting, messages from unknown senders are temporarily rejected. When this happens, Simple Mail Transfer Protocol (SMTP) dictates that a legitimate email server will assume that the message it sent had a problem and it needs to be resent. When an email filtering service that uses silverlisting receives that second message from the original email server, it allows the message to pass through because most servers used by spammers and phishers do not resend rejected messages because it would clog up precious computing resources needed to send massive amounts of emails.

Instead, these servers simply continue sending messages rather than fix any perceived problems. In this case, silverlisting does what whitelisting cannot: It keeps out malicious messages that appear to come from known sources.

If the sender matches with an entry on the whitelist, the message is delivered to the recipient's inbox without undergoing any further checks.

Address Attachments



The easiest way for an attacker to infect a computer system is to simply send an email with malware attached to it and ask recipients to download and install it. The message content may use curiosity to entice victims into opening a malicious file by telling them it contains funny pictures or maybe confidential information that they should not be seeing. Attackers may also try to scare recipients into downloading an attachment by telling them that the file contains critical security software or even essential information that they must read.

No matter the method used to get someone to download the file, once a person opens the file, it has the potential to infect that computer with malware that can be used to steal usernames, passwords, documents, and other confidential information. If the malware is recognized by the email security system's anti-virus tool, infection can be prevented. However, if the attacker uses a zero-day exploit in which there are no signature patterns or known behaviors that will identify it as malware, there is a chance that the file will pass through for delivery. That is why it is so important that file types known to deliver malware are stopped by your email filtering solution.

Essentially, you will want to block any type of file that can execute or run a program from being delivered as an email attachment. Files with extensions such as .exe, .bat, and .cmd are some of the more commonly known ones. Even .zip files are often blocked because they can be used to contain harmful files. Blocking files by their Multipurpose Internet Mail Extension (MIME) type in addition to the file extension is also important because an attacker can easily change the extension to something that is commonly allowed to pass through for delivery. For more information about file types that are commonly blocked,[2] review this referenced list of file types that Microsoft Outlook blocks by default.

Scan for Viruses and Malware

Attackers have long used email as a means to infect systems with malicious software such as viruses, Trojan horses, keyloggers, and ransomware. Most of the criminals who rely on spam to send emails loaded with malware find that they can purchase malware online to use in these campaigns. All they need to do is rent out a botnet, upload their list of recipients, craft their email, attach the file, and hit send. Odds are, they will successfully infect enough computers for their ventures to remain profitable.

“Most of the criminals who rely on spam to send emails loaded with malware find that they can purchase malware online to use in these campaigns”

Anti-virus protection at the email gateway helps put a stop to this. By checking the files for all incoming email attachments, known threats can be stopped before the file makes its way to the intended victim.

However, in order for this to work effectively, the signature database for the anti-virus solution must be updated frequently.

Make sure to set your anti-virus engine to automatically update, and also make sure that your solution updates every day at a minimum; updating every hour is preferable.

To further protect against emails that contain malware, you should also set your email security solution to check for possible zero-day threats using Recurrent Pattern Detection™ (RPD) technology.

Filter Malicious URLs

Attackers have long figured out that effective email security solutions will stop messages that contain malware. So, they have expanded the threat landscape and started taking advantages of weaknesses in the victim's Internet browser software. By creating a webpage that hosts malicious files, they can infect the computer of anyone who visits the infected site.

Instead of sending emails with attachments, the spammer includes a link to a malicious website in the body of the email message. Using the rest of the message content to entice the user to click on that link, the attacker is able to direct intended victims to the site without relying on the chance that someone may visit it unsolicited. This method has been so successful for attackers that the Anti-Phishing Working Group identified 46,824 unique malicious domains in the fourth quarter of 2014 alone.[3]

> Instead of sending emails with attachments, the spammer includes a link to a malicious website in the body of the email message.

These domains may look like legitimate sites or may employ a technique known as typosquatting, in which letters or numbers may be substituted or transposed so that the domain looks just like that of a well-known address. For example acmecrop.com may take the place of acmecorp.com. At first glance, the differences may be difficult to spot, but on closer examination, they have been altered.

To combat this method of attack, you must ensure that your email security solution is checking URLs against lists such as URIBL and SURBL that help identify websites that are known to be malicious in nature. If an email contains a link to a site that may be harmful, your email security will be able to stop it from causing harm to your company and users.

Communicate with users

As with any security initiative, your users can serve as a valuable resource or as the weakest link. If your users are trained on how the solution works to protect them, and how to spot spam and other dangerous email threats, they will feel comfortable with your email security plans. They may also help you fine-tune your filtering system and will be able to set personal whitelists and blacklists as well as identify false positives and false negatives. Armed with this information, you will be able to adjust systemwide filters to better protect the organization as a whole and keep legitimate emails from being wrongly directed to the spam folder. The communication steps you should take include:

- ☑ **Create Training Materials for a New Solution**
- ☑ **Use a Survey to Judge How Effective the New Solution Is**
- ☑ **Encourage Users to Give You Ongoing Feedback**

Regularly collecting feedback from your users about your email filtering services is also important. This feedback allows you to take proactive steps to help assist those who may:

Have trouble dealing with spam that is still being delivered to their inbox

Lose messages due to false positives

Not understand how to build personal filtering lists

Need assistance working with their email

Need additional training on email security best practices

Fine-Tune the Filters

WATCH FOR FALSE POSITIVES

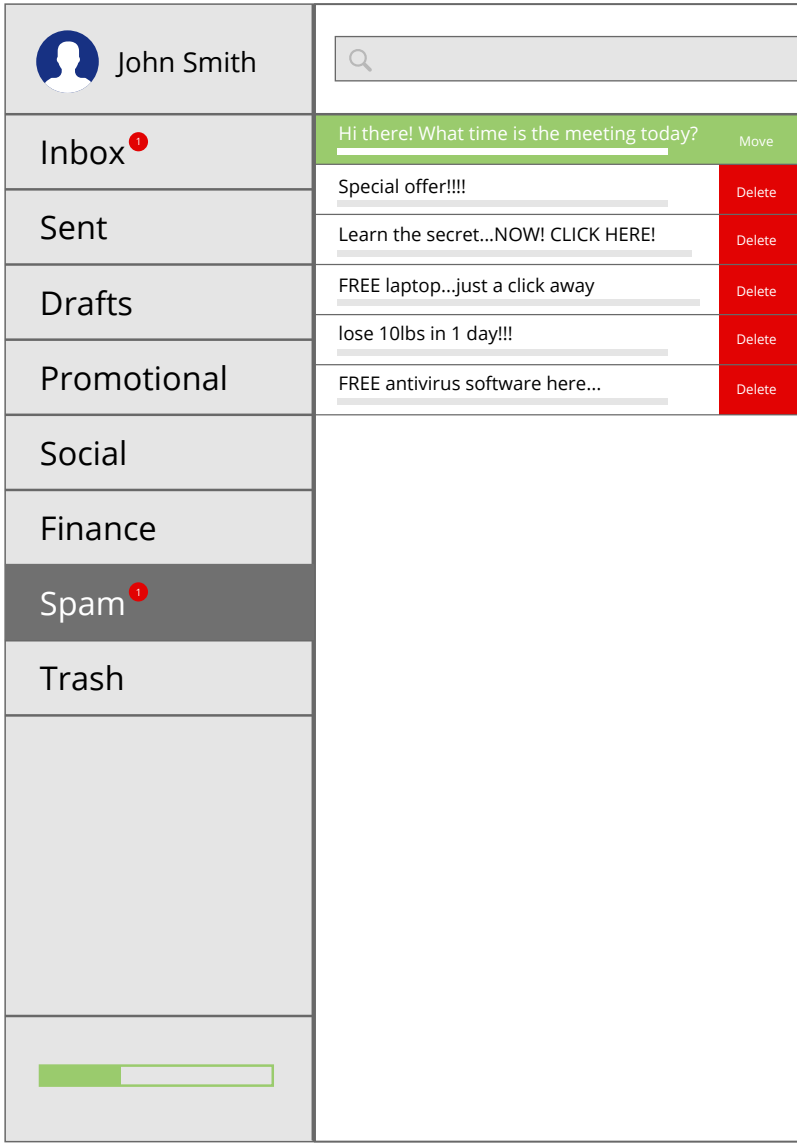
Once you have gone through the initial steps to setting up your email filtering, you must continue watching to see if illicit emails are still making their way through to your users, known as false negatives, and to see if legitimate emails are being blocked from delivery or sent to the spam folder, known as false positives. Though you may be able to identify some occurrences early on, continue to watch for these events. Some time is necessary to really get things set to where you want them by fine-tuning your email filter so that it learns what emails are allowed and which ones should to be sent to the spam folder. Take the time to review your email security settings and consider what might be causing false positives, and then make the appropriate changes.

> Take the time to review your email security settings and consider what might be causing false positives

CONTROL FALSE NEGATIVES

False negatives have the potential to be more damaging than false positives. Imagine if a deal was lost or if your company failed to respond to legal requests in time because an email was incorrectly caught in someone's spam filter? These scenarios can occur when email security controls are set too tightly. Most organizations will see false negatives occur after making adjustments to deal with an excess of false positives. However, any time you, or anyone in your company, see legitimate emails in the spam folder, this should be addressed. Take the time to review why the message was tagged as spam, and if this same rule affects other emails, it may need to be changed.

As you, and your users, identify messages as spam, you will be able to use this information to create filtering lists on your email gateway that are unique to your company.



Quick Reference Checklist

- [ ] Apply a filter to address email servers that are known senders of spam/phishing emails
- [ ] Apply a filter to address domains and IP addresses that are used by spammers/phishers
- [ ] Create an effective whitelisting policy that includes contacts from various lists within your organization
- [ ] Ensure that whitelisted email messages do not bypass additional checks
- [ ] Enable silverlisting to address unknown senders
- [ ] Create, and apply, a list of file types that you will not accept as email attachments
- [ ] Turn on anti-virus scanning for all incoming emails
- [ ] Set your anti-virus signature database to update as frequently as possible
- [ ] Apply a filter to address emails that contain domains that are known to be used by spammers/phishers
- [ ] Train your users on how to apply personal filtering lists
- [ ] Train your users on what to do if they experience false positives and false negatives
- [ ] Collect user feedback
- [ ] Collect data from your filtering logs
- [ ] Fine-tune your filters to eliminate false positives and false negatives

ABOUT SENDIO

Sendio's Email Security Gateway provides you with the technical controls you need to take command over spam and other harmful email threats. Whitelisted emails undergo the same security processes as any other message that comes into your organization because it is the last check in the process. When messages come from an unknown user, Sendio's silverlisting technology holds that email until a challenge/response check takes place to ensure that the sending server is legitimate. When a sender's email passes the required checks, users have the ability to add the to their personal whitelist known as a trusted community. Trusted communities in the Sendio Opt-Inbox™ queue effectively eliminate false positives and false negatives for your users. By making the installation and administration of their email filtering services comprehensive and simple, both smaller businesses and enterprise users are able to harness world-class email protection without complication.

Request a demo to learn more about how Sendio's Email Security Gateway can help your company protect against email threats.

1. Shcherbakova, Tatyana, Maria Vergelis, and Nadezhda Demidova. "Spam and Phishing in the First Quarter of 2015." Securelist Information about Viruses Hackers and Spam. Securelist, 13 May 2015. Web. 3 Sept. 2015. <https://secure-list.com/analysis/quarterly-spam-reports/69932/spam-and-phishing-in-the-first-quarter-of-2015/>.

2. "Blocked Attachments in Outlook." Blocked Attachments in Outlook. Microsoft. Web. 3 Sept. 2015. <https://sup-port.office.com/en-US/Article/Blocked-attachments-in-Outlook-ac9af004-eb9f-45e2-9164-65b1b95b206d#bm3>.

3. Aaron, Greg. "Phishing Activity Trends Report." AWPG. Ed. Ronnie Manning. AWPG, 29 Apr. 2015. Web. 3 Sept. 2015. <http://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf>.

GLOSSARY

Blacklisting

Email security relies heavily on two things: effective technical solutions and a collaborative community. Choosing the right solutions provider is an essential part to stopping spam; however relying on the community of professionals is equally as important because this is where the shared intelligence that so many blacklists come from. Also known as DNS Black Lists (DNSBL) or Realtime Black Lists (RBL), these lists contain the IP addresses of mail servers that are known to send spam. One way addresses find their way on to this list is by security professionals who identify servers that are known to send spam or are known open relays. Another way an IP address could wind up on this list is if enough recipients, or end-users, identify an email sender's message as spam. This happens frequently when unsolicited marketing emails are sent out en masse. This is why effective blacklisting is so reliant on the community of email users for success.

False Negative

When a spam or malicious email makes it into a user's inbox, even after an email security solution is added.

False Positive

When an email security or filtering solution marks a legitimate email as spam.

Silverlisting

Though the name may imply that silverlisting is a middle ground between blacklisting and whitelisting, it actually is not. Rather, silverlisting is a technique that temporarily rejects a message that comes from an unknown sender. When this happens, Simple Mail Transfer Protocol (SMTP) dictates that a legitimate email server will assume that the message it sent had a problem and must be resent. When an email filtering service that uses silverlisting receives that second message from the original email server, it allows the message to pass through since most servers used by spammers and phishers do not resend rejected messages because it would clog up precious computing resources needed to send massive amounts of emails. Instead, these servers simply continue sending messages rather than fix any perceived problems.

Typosquatting

A method for tricking users into clicking malicious URLs by including typos in seemingly legitimate Web addresses. Letters may be substituted or transposed so that the domain looks just like that of a well-known address. For example securl-ty-site.com may be used in place of security-site.com or acmecrop.com may take the place of acmecorp.com. At first glance, the differences may be difficult to spot but on closer examination, you can see where they have been altered.

Whitelisting

While blacklists tell your email filters which messages to block, whitelists work in the opposite manner by telling your email filter which messages to always deliver. Unlike blacklists, whitelists are not a shared resource because anyone could pollute a list with illegitimate IP addresses or domain names. Instead, whitelists are maintained by those responsible for email security in your organization. When put into place, email-filtering services check the message against the whitelist before anything else. Often, if the sender matches with against an entry on the whitelist, the message is delivered to the recipient's inbox without undergoing any further checks. If it does not, it goes through the other processes to determine if the message is safe to deliver or if it should be rejected.