SpamStopsHere™
Email Security in the Cloud since 2002

800-458-3348 / 734-426-7500 | www.SpamStopsHere.com | sales@SpamStopsHere.com

Whitelist Dangers and Cyber-Security

Email Security
By SteveG 02/12/2014

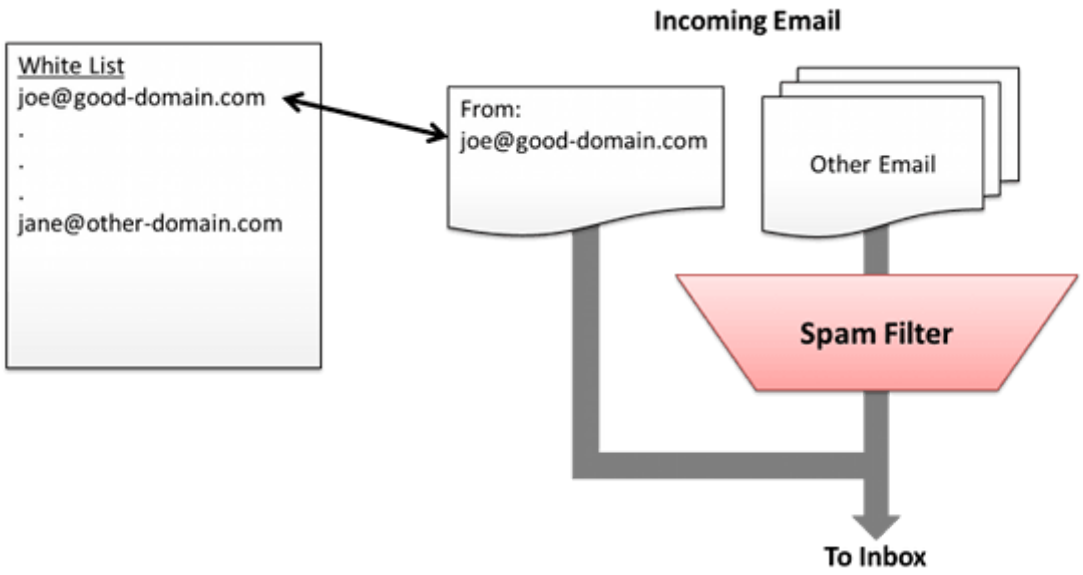
Many anti-spam programs block a lot of spam, but they also mistakenly block a lot of legitimate email and send it to your spam box. Good emails blocked as spam are known as "false positives". You want an antispam program that blocks a lot of spam with as few false positives as possible, so you don't waste a lot of time looking for your email.

One method that's used to prevent false positives is called "whitelisting". You tell the antispam program what email addresses are trusted sources, so email from those addresses is not blocked as spam. If your antispam program encourages you to use whitelists, it probably has to rely on that to compensate for a high false positive rate. That's a bad thing, because whitelisting introduces new security risks.

Whitelist Definition

A whitelist (or "white list") is a list of email addresses that your antispam program treats as trusted sources. You get to manage it, so you can add and delete whatever email addresses you want. Many programs also let you whitelist entire domains in addition to specific email addresses.

Emails from addresses matching those on your white list are not scanned for spam, phishing scams or other threats. They are sent directly to your Inbox. Note: Some anti-spam programs might not even scan attachments. We do, just to be safe.



How Whitelisting Works

Sounds great, right? Read on...

A Cyber-Security Issue

Spammers take advantage of typical whitelisting practices. They try to fool your antispam program (and you) into thinking malicious emails are from trusted sources by making them look like they are coming from an address on your whitelist. So, anti-spam programs that rely on whitelisting can make you more susceptible to spam, phishing scams and viruses by creating a false sense of security that all your email is safe. It's not.

Each whitelist entry that you add is a potential source of danger. For one, it's easy for the sender to make an email (especially a phishing scam) look like it's coming from any address. That's called "spoofing". Spammers often spoof the emails they send out with addresses of popular banks, stores, credit card companies, etc. (like "support@<bank name>.com")

The dangers should be obvious by now. Someone at your company gets an email that looks like it's from a trusted source because you've whitelisted it, and they feel safe clicking on a link in the email. But it's a spoofed email and the link takes them to the spammer's site; where a virus is downloaded or they enter their username and password, provide their corporate credit card number, etc. You know the rest.

Other Spammer Tricks

Spammers know that many people whitelist their own domains. So, another common trick is to spoof the email to look like it's from your own organization (sales@mydomain.com) or even from yourself (bob@mydomain.com). If you whitelist your own domain, emails that look like they come from you or someone else in your company, but are really sent by spammers, get delivered to your Inbox ready to do harm.

When Friends Become Zombies

White listing can also lead to problems from otherwise innocent sources that have been infected and start send out spam to all of the source's contacts. According to Ted Green, a co-creator of SpamStopsHere: "If any person or company that you've whitelisted gets infected with a virus, it can easily spread to your company and even your entire organization."

How to Avoid Whitelisting Dangers

There are some ways to make whitelisting safer (but not completely safe):

- Don't Whitelist Entire Domains: Many anti-spam programs let you specify that any email from a domain (the part after the "@" sign) is safe. Don't ever do that, because the spammer won't even need an exact email address to get through. If you're unable to get a better antispam program, only whitelist specific email addresses that you trust.
- Don't Whitelist Popular Companies: Don't whitelist any email address from merchants, banks, credit card companies, etc. (like "support@bigcitybank.com") Those are the addresses used in phishing scams and they'll all get through unscanned.
- Never Whitelist Your Own Domain. PERIOD: It's usually unnecessary anyway. Unless you're a larger company with more than one mail server, intra-domain emails never go out on the Internet.

Or, Get Better Anti-Spam Protection

Managing whitelists is a lot of work, especially if you're a business. The best way to avoid problems is to use a better anti-spam service that doesn't rely on white listing to reduce false positives.

SpamStopsHere has such a low false positive rate (blocks almost no legitimate emails) that we actually discourage our customers from using white listing. A majority of our customers don't do any white listing at all! (Even more don't do any blacklisting, but that's a topic for some other time.)

Health Care Providers

If you're a health care provider, whitelisting is a big problem because patients and vendors often send email asking about prescription drugs. Other antispam programs automatically block emails with individual trigger words like Rx names, forcing you to either manage long whitelists with patient email addresses (an additional HIPAA concern), or constantly check your spam box for missing emails. Either way, you end up wasting time and money.

SpamStopsHere is different. Among other techniques, it blocks emails with long phrases that appear only in spam. It never blocks based on individual trigger words. Emails from patients and your sales reps go to your Inbox, as they should. But pharmaceutical spam is blocked.

Try SpamStopsHere Free for 30 days (https://www.spamstopshere.com/) to see how much better it works.

For More Info

SpamStopsHere does not rely on whitelisting to prevent false positives. It works differently from other anti-spam programs blocking 99.5% of spam while delivering over 99.999% of legitimate emails. That means we block fewer that 1 out of 100,000 good emails, which is why businesses and professionals love our service.

Our spam review team, along with our proprietary Spamalyzer 3.0, analyzes and blocks email threats for our customers 24/7/365. That's a claim almost no other antispam provider can make. Click here for more about SpamStopsHere and our 24/7/365 live support (https://www.spamstopshere.com/)