Email service provider adjusts sending policy to not be disclosed

Email service provider, Thexyz have updated the anti-abuse policies in order to better protect customers and infrastructure. This change has been made to decrease the number of false positives and curb outgoing spam from our system. For the security

Toronto, Feb 13, 2019 (Issuewire.com) - Toronto, ON - Independent email hosting provider Thexyz Inc has recently updated the sending policy for its enterprise and private business email hosting.

The change came without advanced warning to an existing user base of 30,000 users. The new policy is also being kept evasive and not being disclosed. This is part of the strategy to not let spammers and people who are looking to abuse the system know what the limits are.

Thexyz has implemented 4 layers of advanced in bound mail filtering to protect users from inbound spam. "We've been blocking spam and viruses through our spam filtering technology for the past 12 years and we have become quite good at it." Explains Thexyz Webmail product manager Perry Toone.

This new policy update is not related to inbound spam as over the last few months a new form abuse is increasing. Spammers are setting up accounts and working within the acceptable limits of Thexyz. These were previously set at a maximum of 250 recipients and a maximum of 10,000 outbound messages per day.

"Slightly staying within these limits is now no longer an option," adds Ryan Woods from the anti-abuse team. "Not knowing what these limits are makes it even harder for a spammer to bypass our anti-abuse limits."

"The reason spammers are targeting our mail services is because our domains and IP addresses are generally well trusted amongst email providers," proclaims Perry. "Our system is reliable and it works, it is, therefore, a target." Perry also plays down the secrecy of the rate limits, “it's not so much a secret as it adjusts based on user behavior, so we don't have a concrete limit at any given time beyond our hard 10k limit assuming perfect trust and reputation, and saying more than best practices gives away too much and would allow gaming of the system beyond what is clear and obvious.”

The negative repercussions from having spam be sent from an IP or domain in your environment can impact every user of the service and not just those on the same domain name. This is because spam blacklists collect reports from users who report spam. These spam lists look at the headers of the sent email and will mark the IP address as spam. Many email service providers subscribe to these services to help control the flow of inbound spam.

Once listed in a spam blacklist, it can take anywhere from hours to days to be removed. IP is usually removed automatically from the larger blacklists, once they have started to see reports of spam diminish.

Having an IP blacklisted is disruptive for the end users, who find an increase in bounced messages if their recipients' email service has subscribed to a blacklist that has listed an IP address. It also means an increased workload for the email service provider who will likely deal with an increase in support requests, as more users deal with the repercussions of having an IP address blacklisted.

The majority of users will not experience any trouble when an IP is blacklisted. Unless they are heavy users of email and sending to a lot of service providers that rely on these blacklists to help reduce the amount of inbound spam. These new rules are now in effect and are introduced to help further protect Thexyz IPs from systematic abuse.

To take your organizations digital sovereignty into your own hands or to learn more about our extensive multi-layer spam filtering, check out our business email hosting and spam protection.

Media Contact

Thexyz Inc

ryan@thexyz.com

18003149082

1 Yonge St, 1801

Source : Thexyz Inc

See on IssueWire : https://www.issuewire.com/email-service-provider-adjusts-sending-policy-to-not-be-disclosed-1625368394807397