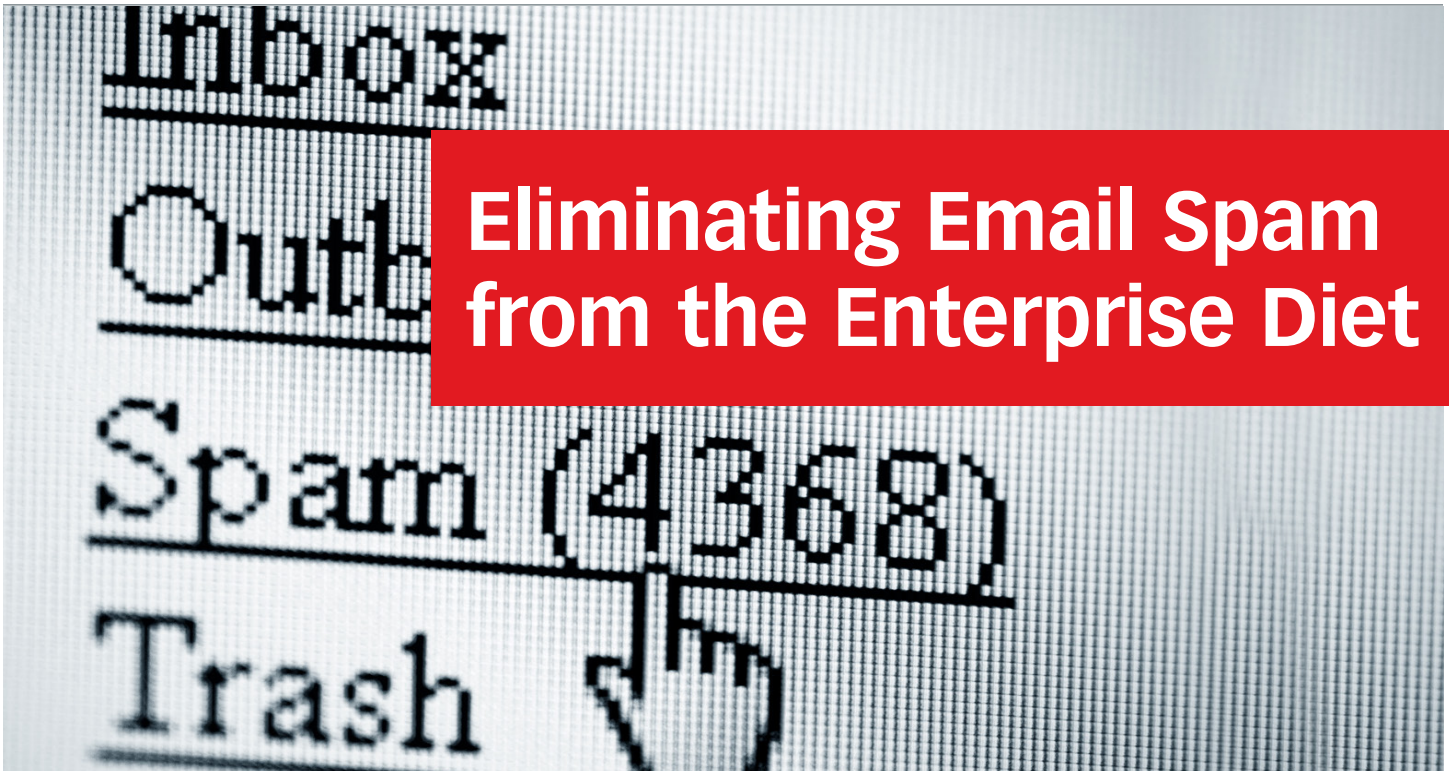

Eliminating Email Spam from the Enterprise Diet

HOW ORGANIZATIONS CAN COMBAT THE SUDDEN RISE IN SPAM AND SAFEGUARD AGAINST NEW TACTICS

EXECUTIVE SUMMARY

Just when you thought unsolicited email "spam" couldn't get any worse, it has. Several organizations have reported increases in volume during 2013, following almost three years of stagnation. More perilously, spammers are spoofing domain names of legitimate, trusted enterprise suppliers to generate email that many unsuspecting workers might be inclined to open. It's time to reignite the battle against spam and ensure that workers engage in safe email practices.

InfoWorld
Custom Solutions Group

DocuSign®
The Global Standard for eSignature®

MORE SPAM ON THE MENU

Electronic "spam" is the computer-age equivalent of junk mail on steroids. Using electronic messaging systems, spammers are able to send unsolicited bulk messages indiscriminately and for little cost. Familiar to just about anyone with an active email account, spam jams in-boxes with huge volumes of unwanted advertising, but can also mask malicious efforts aimed at infecting user computing devices for nefarious purposes.

Increasingly, perpetrators of malicious spam are spoofing the domain addresses of organizations from which enterprise users would expect to receive legitimate messages. For example, somebody might attach a compressed file, such as a .zip archive file or a file using Adobe's Portable Document File (PDF) .pdf format, to an email that misleadingly appears to have been sent from the legitimate docusign.net or docusign.com domains, even though DocuSign's service never includes attachments for e-signing purposes.

Users who attempt to open attachments or click on links in malicious spam may inadvertently have their systems infected with malware. There are many types of malware designed with different purposes, such as gaining access to enterprise servers, "phishing" for passwords or a user's banking information, and linking a user's system into a "bot net" network of infected machines to create more spam or participate in a Distributed Denial of Service (DDoS) attack.

Aside from management of their mailing lists, spammers incur little if any operating costs, and holding them accountable for mass mailings is difficult and in many cases impossible. The barriers to entry are so low that the practice attracts numerous participants. One Internet security company that tracks spam traffic reported that in the first quarter of 2013, "an average of 97.4 billion spam emails and 973 million malware emails were sent worldwide each day," and in the month of March daily volume of spam emails exceeded one billion.

Enterprise email solutions and cloud-based email services such as Google Gmail and Yahoo! Mail are well aware of the perils of spam and implement filtering techniques aimed at diverting such traffic into user or server spam folders. Such filtering may inadvertently lower a user's awareness of the spam issue, though. Because nothing can guarantee 100 percent protection, it is crucial that enterprises reaffirm email policy and continually re-educate employees on email best practices.

SPAMMER TACTICS CONSTANTLY EVOLVING

Since the cost to send spam is minimal, spammers can constantly revise their tactics to skirt spam filters and catch users unaware. The popularity of social media sites such as Facebook and Twitter has created another entrée for perpetrators. According to security solutions provider Trend Micro, users of these services "may encounter the malicious posts while browsing people's profiles or while visiting social media sites. These posts typically include malicious URLs that can lead to malware download pages and/or phishing sites or can trigger spamming routines."

Still, for many enterprises, a growing danger is from emails that have been "spoofed" to make it appear that they come from legitimate enterprise software or service providers so that the user often is not suspicious of embedded links or attached files. Kaspersky, another security solutions provider, reported that in July 2013, "malicious

"In July 2013, malicious attachments were detected in 2.2% of emails, an increase of 0.4 percentage points from June."

— KASPERSKY REPORT

attachments were detected in 2.2% of emails, an increase of 0.4 percentage points from June."

DocuSign has alerted its customers to effort that attempt to entice users to click on attachments by sending email "spoofing" the DocuSign domain, which makes it appear that the email comes from DocuSign. One example of a recent malicious campaign used emails with the subject line: *"Please DocuSign this document: Important Changes – Employers Only.pdf."*

However, emails requesting somebody "DocuSign" a document never contain attachments of any kind and users should be alerted to NEVER open or click on attachments within an email requesting a signature. Legitimate DocuSign emails only contain PDF attachments of completed documents after all parties have signed the document—and that's only when the sender has configured DocuSign to provide a completed PDF. DocuSign NEVER attaches zip files or executable files.

KEEPING IT CLEAN

The computer industry is constantly monitoring the latest spam assaults and working to improve defenses. A key element in the anti-spam battle is the effort to ensure authentication of emails and make it increasingly difficult for spam perpetrators to spoof legitimate domain addresses.

One of the earliest endeavors was the Sender Policy Framework (SPF), which grew out of efforts initiated from participants in the Internet Engineering Task Force (IETF), an open standards organization that develops and promotes Internet standards. SPF essentially provides a way for administrators of a particular domain name to indicate that a certain host is a legitimate distributor of their emails. Administrators create SPF records in the Domain Name System (DNS) that are used by mail exchangers to authenticate that mail from a given domain is being sent by a host that the domain administrator has sanctioned.

"DMARC standardizes how email receivers perform email authentication using the well-known SPF and DKIM mechanisms. This means that senders will experience consistent authentication results for their messages at AOL, Gmail, Hotmail, and Yahoo! and any other email receiver implementing DMARC."

— DMARC ORGANIZATION

A related and complementary specification is DomainKeys Identified Mail (DKIM), which was developed by an informal industry consortium and subsequently submitted to the IETF for enhancement and formal standardization. DKIM essentially applies a digital signature to an email message and "allows an organization to take responsibility for transmitting a message in a way that can be verified by a recipient."

While DKIM and SPF provide a means for domain name owners to vouch for mail sent in their name, there are limits to their usefulness. One issue is that the specifications don't detail what to do with messages that fail the validation test. Another is that DKIM and SPF may not be applied consistently due to the complexity of email environments. If a domain owner sends some messages that can be validated and others that can't, "email receivers are forced to discern between the legitimate messages that don't authenticate and the fraudulent messages that also don't authenticate."

To resolve those issues, a group of technology providers promulgated Domain-based Message Authentication, Reporting & Conformance (DMARC). According to the DMARC organization, "DMARC standardizes how email receivers perform email authentication using the well-known SPF and DKIM mechanisms. This means that senders will experience consistent authentication results for their messages at AOL, Gmail, Hotmail, and Yahoo! and any other email receiver implementing DMARC."

The DMARC policies are publicly available to anyone via the DNS. By implementing a DMARC policy, the sender system indicates that emails are protected by SPF and/or DKIM. Email receivers use the policy to guide what they do if the emails don't pass either authentication message and to report back to the sender about messages that pass or fail.

"DMARC removes guesswork from the receiver's handling of these failed messages, limiting or eliminating the user's exposure to potentially fraudulent and harmful messages," according to the DMARC organization.

By sharing information about the email they send to each other, enterprises are able to improve email authentication and also to direct that illegitimate messages either go directly into a spam folder or be rejected. Organizations update their DNS records for each legitimate server with a DMARC TXT entry.

According to the DMARC organization, senders or domain owners can use DMARC policies to collect statistics about messages using their domain from DMARC receivers and see how much of their traffic is passing or failing authentication checks.

DocuSign has implemented both SPF lookup functionality and DMARC on its mail servers. The combination of these technologies helps to protect from malware spam attacks, and email administrators who configure their email servers to use SPF lookup functionality can use DMARC to instruct recipient email servers how to treat malicious spam.

VIGILANCE IS KEY

DMARC along with SPF and DKIM are increasingly moving the industry toward more efficient management of unwanted spam. But until they're universally adopted they won't provide foolproof protection. So organizations must continue to take steps to filter email attachments and educate their users about staying vigilant to the dangers of malicious spam.

Learning to properly detect and avoid online and email scams is the ultimate protection against fraud. Educating end users to spot fraudulent emails and websites is a key factor in a defense strategy. In the case of emails purporting to be from DocuSign, users can check for the following signs, advises Tom Pageler, Chief Information Security Officer for DocuSign:

ATTACHMENTS

As mentioned earlier, emails requesting someone to legitimately DocuSign a document never contain attachments of any kind. Remember that DocuSign emails contain PDF attachments of completed documents after all parties have signed the document—and that's only when the sender has configured DocuSign to provide a completed PDF.

FAKE EMAIL ADDRESSES

If the sender of a DocuSign envelope or an email is not recognized, the user should contact the sender to verify the authenticity of the email. However, it is not uncommon for fake emails to include a forged email address in the "From" field to make it look legitimate. When spam filters catch these emails they typically put "SPAM" at the beginning of the subject line to alert the user.

Organizations must continue to take steps to filter email attachments and educate their users about staying vigilant to the dangers of malicious spam.

DECEPTIVE URLS AND FAKE LINKS

Only enter DocuSign user names and passwords on DocuSign pages, which begin with http://www.docusign.com or https://www.docusign.net. If users see an "@" sign in the middle of a URL, there's a good chance it is fake. Even if a URL contains the word "DocuSign," it may not be a DocuSign site. Users should always log in to a DocuSign account by opening a new Web browser and typing in http://www.docusign.com or https://www.docusign.net.

GENERIC GREETINGS

Many fake emails begin with a generic greeting like "Dear [Company Name] Customer." If users do not see their names in the salutation, they should be suspicious and not click on any links or attachments.

A FALSE SENSE OF URGENCY

Many fake emails try to deceive users with the threat that their accounts are in jeopardy if they don't provide immediate updates. Emails may also state that unauthorized transactions have occurred on an account or that the sender needs to update his or her account information immediately.

EMAILS THAT APPEAR TO BE WEBSITES

Some fake emails are made to look like a website in order to get users to enter personal information. DocuSign never asks users for personal information, such as login, ID, or password in email. Be cautious of other emails or websites that do.

MISSPELLINGS AND BAD GRAMMAR

While no one is perfect, fake emails often contain misspellings, incorrect grammar, missing words, and gaps in logic. Mistakes like this help fraudsters avoid spam filters.

UNSAFE SITES

The term "https" should always precede any website address where users enter personal information. The "s" stands for secure. If they don't see "https," they are not in a secure Web session, and shouldn't enter data.

POP-UP BOXES

DocuSign does not use pop-up boxes in emails. Users should be cautious of emails that do.

GETTING SPAM OFF THE MENU

Many companies use the Internet to deliver legitimate marketing messages and other information. Those that do should join the effort to implement SPF and DKIM and utilize the DMARC best practices.

At the same time, users should be alert to what they allow to reach their mailboxes and be knowledgeable of the potential harm that malicious spam can cause. They can work with the filtering tools on their devices and with their administrators to blacklist undesired emails. Enterprises need to keep their security software patched with the latest updates and ensure that safe email practices are constantly reinforced.

There is no doubt that malicious email spam continues to be a major security concern for organizations of all sizes. IT must diligently educate employees on email best practices on an on-going basis. This is especially critical to keep up with spammers' constantly evolving tactics.

Organizations that follow the guidelines in this white paper will help protect themselves from the dangers of malicious spam until the industry universally adopts anti-spam standards. ■

To learn more about DocuSign's eSignature solution, please go to:
www.docusign.com/demo

For further information, please visit:
www.docusign.com

InfoWorld
Custom Solutions Group

DocuSign®
The Global Standard for eSignature®