

Stop illegitimate mails - save money and increase productivity

When the web was in its infancy, spam was a minor annoyance and not much more. However, as with all other aspects of the web, spam has evolved into something far more dangerous that is costing business enormously, in terms of bandwidth, productivity and down time.



Image: www.freedigitalphotos.net

"To get a handle on the size of the spam problem, we need to look at the tidal wave of unsolicited emails that is drowning the enterprise," said John McLoughlin, MD of J2 Software. "Reports estimate that as much as 80% of the billions of emails sent on a daily basis are spam. These illegitimate mails clog up and waste expensive bandwidth, put a strain on servers, and waste time and money delivering the emails to the intended mailboxes, and even more in sifting through them."

He said that J2 did an investigation across its email user base to see if the research was correct in an African context. "When we looked at J2 Software's customers using Mimecast, we saw that email rejections of spam, dangerous attachments and other illegitimate emails blocked in the cloud totalled an average of 1,905,459 a week, adding up to some 7.6 million emails being rejected monthly just on the J2 Software customer base. These emails were rejected and never filtered down to our clients, saving them enormously in terms of both bandwidth, and time spent sorting the wheat from the chaff."

Mc Loughlin cited research done by the Radicati Group as showing the average size of an email without an attachment to be 26 KB. "This translates into savings in excess of 47GB for our client base."

Malicious websites and dangerous applications

He said that over and above losses of bandwidth and productivity, spam can be dangerous in other ways. "Spam emails will also often try to trick the recipient into following links to malicious websites or to download dangerous applications that can then be used to target the business or individual by stealing sensitive information. By blocking and, therefore, preventing these mails from reaching our clients we have helped ensure that there is no chance of human error in infecting the corporate network."

He added that email is also still the most common vector for spreading malware and that, in addition to distributing dangerous applications, this sort of spam could crash your system and, in turn, the systems of people you email, or log your keystrokes to steal your financial login details."

Phishing is another tactic that spammers use. "The cyber-criminal will send out an email that is so close in appearance to the genuine article that it would fool all but the closest scrutiny. Phishing mails attempt to trick the recipient into clicking on a link and filling in their private financial information. Not only are bank accounts cleaned out in this way, but the cost of identity theft resulting from phishing can also run into the millions."

The risks associated with spam and other illegitimate mail is growing daily - spammers are continually adapting to try to bypass new methods of detection. This can cost not only money, but customers and reputation. "Spam isn't going anywhere, but with a leading solution like Mimecast, backed by the certified support and recommendations of J2 Software's experienced staff, we will continue to fight this battle on our clients' behalf. We aim to provide our clients with ongoing spam-free inboxes so they can save vast amounts of time, bandwidth and frustration.

For more, visit: <https://www.bizcommunity.com>