



Can the spam

It has been 10 years since spam surfaced. While there is still no surefire way to eliminate spam, the best way to contain the menace is through a combination of technology, people, and policies.

BY LEONG KHAY MUN

Sspam is a four-letter word that evokes emotions of disgust and dread among CEOs and CIOs, rather similar to how a housewife would take to cockroaches in her kitchen.

Spam can carry malicious code, network worms, viruses, similar to how cockroaches can spread diseases.

And just like cockroaches that have survived the ice ages, droughts and famines, spam has come a long way.

On Apr 12, spam celebrated its 10-year anniversary, demonstrating its resilience to technologically-constructed "spamicides".

International SOS (ISOS) is one company that is starting to discover just how annoyingly hardy spam is. For the global emergency assistance company, 25-30% of the e-mails that come in everyday is spam. And especially when it is the high-profile management team like the CEO and president who are most badly affected, it is a huge issue.

In addition, ISOS has problems with spoofing, its mail servers are overburdened, and it has to divert its already tight ICT resources to investigate users' complains.

Brett Hay, ISOS' general manager, said his team has been looking at anti-spam solutions for the past two to three months, but they have yet to find anything that is suitable.

"No solution we found can help us," said Hay. ISOS first started looking at installing generic spam filters but the problem is that of false-positives. "Legitimate business e-mail may not get through and we can't afford that."

Then ISOS looked at tools that will make it easy for end-users to manage the filter list themselves. But spammers can always get through using different domain names and it will only shift more work to end-users as they are the ones who will have to maintain that list, said Hay. So now, it is back to the drawing board for Hay.

ISOS' experience reflects the state of the industry in that there is no fool-proof method of combating spam as spammers always seem to get around any new technologies that are put out in the market.

The best way to reduce the amount of spam is to fight it using a combination of

technology, people and policies, said Lionel Phang, managing director of Trend Micro.

"If you have a good technology installed but your people don't know how to use it or disregard the security policies put in place, then technology is of no use," he added.

Tech solutions

To start, spam filters at the gateway are necessary to stop spam before it gets into the corporate network and onto the desktops.

At the gateway, enterprises can apply a whitelist filter, where they create a list of e-mail addresses they expect to receive mail from. Alternatively, a blacklist filter can be used where e-mail from a certain list of addresses or matching a certain list



After you start a few users familiar with the anti-spam system, you get the champions to show the rest how well the system worked for them.

—Ng Kim Hung
IT director for Asia-Pacific, Exel,
on obtaining user support for anti-spam initiatives.

of text patterns are rejected.

However, blacklists and whitelists create the problem of false-positives—as ISOS learnt—and they do not work, said Phang.

He suggested using content filtering with a heuristics scan engine. "This will try to predict whether or not it is spam, quarantine it, tag it, forward it to the end-user, and let him decide whether it is spam. This speeds up resolution of the problem."

Another emerging alternative is the Bayesian filter, which learns from experience what a user personally considers spam. It works by selecting words and numbers from e-mail text and compares their ratio between good mail and spam. Using that ratio, the filter calculates the probability of new e-mail being spam.

However, this is somewhat a coarse-grained tool, said Leigh Costin, director of Product Marketing, Fortinet. "It depends a lot on existing sample data. For a new installation, the accuracy of such tools is not very high and they learn from usage patterns over time. This makes them more effective at the individual users' desktop than elsewhere."

Anti-spam software can also be installed on the mail server to help block spam e-mail from being accepted further into the organisation, added Costin. But he warned that there needs to be the capacity for individual overview of what is, or is not, really spam.

At the desktop level, anti-virus is also a crucial component as there is a convergence between spam and viruses, said John Graham-Cumming, a research director on Sophos' anti-spam task force.

Another solution to consider in time to come, is the ID for e-mail scheme that is in the early stages of being explored in the US. It uses new, yet to be standardised Internet protocols to identify the true sender of each e-mail, eliminating the forged from-addresses used by spammers.

Other IT solutions, which Exel Singapore discovered to be quite effective, include making sure all security patches for its routers are updated and installation of intrusion detection systems (IDS) at all its

support by getting them to understand how spam can negatively impact the company's credibility and productivity.

Only then can the IT department get the investment dollar and support to roll out the anti-spam initiative. Other than getting top management to reinforce the importance of adhering to anti-spam policies, Graham-Cumming suggested appointing a champion to obtain staff's buy-in.

"After you start a few users familiar with the anti-spam system and when you're in the process of rolling it out... you get the champions to show the rest how well the system has worked for them."

But sometimes, even the best intentions can fail as it boils down to just how disciplined individuals are.

Ng has this policy whereby staff must update their anti-virus file daily at 12 noon. But sometimes when he walks round the office, he notices people stopping the automatic virus updates when they pop up.

Legal reinforcements

Would people—end-users and spammers alike—take spam more seriously if there were anti-spam laws in place to punish perpetrators? The Can-Spam Act 2003 which imposes limitations and penalties on spam came into effect in the US this year and already, AOL, EarthLink, Microsoft and Yahoo have filed six lawsuits in four states against spammers.

In response to just how effective such a law would be in Asia, ISOS' Hay said it might discourage enterprises from mass e-mail marketing in case they cross the line. "But they are not the ones who're making lots of money through it!"

"You've got to stop spam from where it is coming from—the spammers. They are making money doing this and have enough to pay [for the consequences] anyway."

For Ryan Chioh, Far East Flora Holding's executive director, who changed his e-mail address of four years to escape from spammers cluttering his e-mail at the old address, such laws are good to have in Asia. However, he thinks it will be too grey an area to regulate, as what constitutes spam to some, may not be spam to others.

Like many others, Chioh conceded that spam is here to stay as it is all part of the "e-mail ecosystem". And since there is no silver bullet to combat spam, the combination of technology, people and policies will have to suffice in minimising spam (see page 18 for a review of a spam filtering solution). □

major computer rooms and data centres.

"The last time spam affected our network was in October last year... and these two measures we've installed since have come into good use," said Ng Kim Hung, Exel's IT director for Asia Pacific. They are so effective that the logistics and supply chain management solutions provider has since never suffered a major spam outbreak in the region.

Staff support needed

But it was not just the IT that did the job for Exel. "More importantly, we do education drives. Whenever we get security alerts from our vendors, we circulate the e-mail to all users, not just the IT people, to keep them aware."

Other policies enterprises can implement include not opening e-mail attachments, sending e-mail in plain text, and determining how long you should quarantine suspicious e-mail before deleting them.

For the anti-spam campaign to work, it is critical to obtain top management's