

People do reply to email spam!

Written by [David Kelleher](#) of GFI on August 12, 2009 – 12:42 pm

I sometimes wonder how spammers can be so successful in what they do. They send out millions of emails every day promising the world – get rich offers, a pile of cash waiting just for you to claim ownership, pills and creams that work wonders, financial advice and dozens of other schemes and offers. Junk, literally.

One look at the email, its content and the name of the person sending the email should be enough to convince email users that the trash can is the best place for it. In theory yes, but there are still people who open spam emails, click on the links or visit spammer-recommended websites.

Spam numbers

According to a survey released in July by the Messaging Anti-Abuse Working Group (MAAWG), one in six consumers “responded to a message they suspected might have been spam”.

Although one in six is a relatively small number in terms of those using email, we should not forget that spammers send out hundreds of millions of emails; economies of scale ensure that even though a very, very low percentage actually ‘buy’ something, it is enough to generate millions of dollars in revenue.

Another survey by the University of California showed that the number of people who actually bought something after receiving a spam email is extremely small. They monitored three spam campaigns for a total of 350 million messages; of these just over 10,500 visited the advertised site and only 28 tried to purchase. According to the university, this represents just 0.000081%. The researches, however, they did make it clear that even at such a low rate, up to \$3.5 million could be generated in annual revenue.

Good enough reason for keep spammers to stay in business.

Spam is no longer limited to email delivery. Spammers are maximizing the potential offered by new technologies and communication methods such as social networking sites, instant messaging, blogs, search engine searches and so on to disseminate spam.

Combine all the methods and platforms and you quickly get an idea of the reach and versatility that spammers have. It also explains why spam is more than just huge volumes of unsolicited commercial mail – spam is a huge load of trouble if not properly dealt with.

Controlling spam

Unfortunately, it is impossible to eradicate spam, but that doesn’t mean companies should sit back and look on helplessly. Whilst legal attempts to stop spammers have had little success so far due to the inherently unregulated nature of the internet, there are other options.

The first step is to install anti-virus and anti-spam software at the server level. Anti-spam solutions come with a variety of technologies – IP filtering, Bayesian filtering, whitelists and blacklists, for example – each one identifying and stopping different types of spam.

The next step is to educate users on the use of email, social networking sites, basic internet security and how to protect their data using strong passwords, for example. Unfortunately, employee awareness is often given low priority by IT professionals, especially in small organizations with limited IT human resources. Yet, with the bulk of spam targeting end-users and their inquisitiveness and/or fear of legal-sounding content, employees need to be told what the dangers are. The message that needs to filter down to employees is:

1. Be wary of any emails that come from unknown sources.
2. Do not open attachments that you were not expecting or where the sender is unknown.
3. Do not reply to spam email. Replying only verifies that the email is active, resulting in more spam.
4. Do not click on links in emails.
5. If it’s too good to be true, it probably is not. Just hit the delete button.

6. Do not provide personal details, passwords or credit card details in reply to genuine-looking emails from banks or other well-known online merchants. These organizations never ask for such details via email.
7. Forward all suspicious emails to an IT administrator to have it checked.

Spam will not go away on its own – it has proved too successful – and will remain the bane of every email user. Reducing spam is as much a question of technology as it is an issue of education and employee awareness. Together, they can be a successful weapon in the fight against spammers and spam email.

