Spam is a pesky problem that has plagued our inboxes since the advent of email. As the level of sophistication spammers have used to evade spam filters and into users' mailboxes has increased, the spam-fighting community has constantly strived to stay two steps ahead. More recently, emails containing HTML attachments that redirect to malicious web content, attempting to infiltrate the user's computer system and gain access to sensitive personal information, have become a widespread spam technique. This paper examines the ongoing battle to protect users from unsolicited bulk email and the ethical implications for computing professionals, particularly their role in advancing the technology that facilitates ever-more sophisticated spam techniques.

Studies have reported that the magnitude of spam has increased dramatically over the years, from approximately 10% of overall mail volume in 1998 to 80% in 2006 (Messaging Anti-Abuse Working Group 2006 cited in Goodman, Cormack & Heckerman 2007:25). In fact, some large email service providers like Hotmail can receive more than a billion spam messages per day (Goodman, Cormack & Heckerman 2007:26). While only a small fraction of that 80% actually reaches end users due to effective spam filtering-software, the spam problem (and its associated scams) remains serious and cannot be ignored.

One particular method used to aggressively attack a user's email system is via HTML attachments, as Constantin (2010) highlights. These attachments redirect to multiple 'scareware' websites that eventually display a fake antivirus scan. The user is then warned that malware was found on their computer, after which a rogue program is encouraged for download and installation. However, this program does nothing but bombard the computer with security alerts involving fictitious infections. By way of fear, users are scammed into paying a license fee for an utterly useless application.

Data from security vendor Sophos (cited in Constantin 2010b) suggests the volume of spam with an HTML attachment surged to 8% of total junk mail traffic in 2010, with the majority of malicious content consisting of phishing pages. 'Phishing' is described as a particularly insidious type of spam where legitimate businesses are impersonated with the intent to steal passwords, credit card numbers, Social Security numbers and other sensitive information (Goodman, Cormack & Heckerman (2007:29). Clearly, this raises some interesting and contentious questions, not just from a financial perspective, but also a legal one.

Traditionally, phishing attacks tend to target customers of organisations such as banks, social networking websites, online auction sites such as eBay and payment processing services like PayPal. So not only are spam victims susceptible to considerable financial losses but they are also vulnerable to identity theft, which may lead to even worse consequences from a legal standpoint. Given the push for global cohesion in legislating against cybercrime today (Redford 2011:34) users face the growing possibility of being implicated in criminal activity as a result of spam.

One example is by 'mule recruitment' where criminals send out millions of fraudulent job and employment offers to random email addresses, hoping to recruit unsuspecting and innocent 'mules'. Mules then receive stolen funds using their bank account, which they subsequently transfer to criminals overseas. In Australia, people who agree to participate in such 'jobs' may be prosecuted (Australian Federal Police 2012).

So given what we know about the evils of spam, it begs the question, "Can legislative attempts to effectively stop spam ever succeed, and if not, what ultimately will?" In the United States, the 2003 CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act) enjoyed only limited success (Grimes 2007 cited in Goodman, Cormack & Heckerman 2007:32), with the level of sophistication that spammers now use making it difficult for them to be tracked down. Marchant (n.d) also suggests that any legislation aimed at regulating Internet content will undoubtedly run into free speech and privacy challenges. Due to these legal shortcomings, technology remains the most powerful tool in the fight against spam.

However, as anti-spam methods improve in line with emerging technologies, spammers actively adapt and devise even more sophisticated ways to circumvent the innovative solutions already in place. A cycle of attack and counter-attack therefore develops, leading to endless escalations and a tit-for-tat battle to protect the inbox from harm (Goodman, Cormack & Heckerman 2007).

Mills (2011) explores the recent trend of HTML files embedded in emails, and the implications for anti-spam researchers and developers. Because browsers like Chrome and Firefox are able to detect phishing sites quite well, phishers have responded with even cleverer ways of evading browser blacklists. One such tactic involves filling out personal information on an HTML form and after the user clicks “submit”, the data is sent through a POST request to a PHP script hosted on a legitimate Web server that has been compromised. The level of technical complexity involved makes such techniques difficult to detect, and thus can avoid triggering a warning from the browser. As months-old phishing campaigns go undetected, email service providers can only issue warnings to their customers about opening HTML attachments from suspicious emails and providing sensitive information in web forms. Until an even more complex countermeasure is developed, of course!

Response times will depend naturally on the severity of the email threat but given the rapid rates at which technology is evolving, are computing professionals doing more harm than good by providing the landscape for spammers, phishers, spoofers and click-frauders? To what end should technology play in combatting cybercrime and capturing cybercriminals? Can end-user education, if administered properly, ever suffice in controlling online abuse? Or is there a legitimate case for endeavours such as The Spamhaus Project and Scambusters.org that appear to have taken on the roles of scam ‘police’ and ‘watchdogs’. These are all important ethical considerations that must come into play when tackling issues like spam or other computer-related problems.

References

Australian Federal Police, ‘Internet fraud and scams’, retrieved 16 April 2012 from http://www.afp.gov.au/policing/cybercrime/internet-fraud-and-scams.aspx

Constantin, L. 2010, ‘Aggressive Scam Campaign with HTML Attachments Leads to Scareware’, retrieved 27 April 2012 from

http://news.softpedia.com/news/Aggressive-Spam-Campaign-with-HTML-Attachments-Leads-to-Scareware-156921.shtml

Constantin, L. 2010a, ‘HTML Attachment Spam Exploded in Recent Months’, retrieved 27 April 2012 from

http://news.softpedia.com/news/HTML-Attachment-Spam-Exploded-in-Recent-Months-159367.shtml

Goodman, J., Cormack G.V. & Heckerman D. 2007, ‘Spam and the Ongoing Battle for the Inbox’, *Communications of the ACM*, vol. 50, no. 2, pp. 25-33. Retrieved 16 April 2012 from ACM Digital Library: Association for Computer Machinery database

Marchant, A., ‘Part of The Picture: Ethics and Issues’, retrieved 12 April 2012 from http://cs.calvin.edu/activities/books/c++/intro/3e/WebItems/Ch01-Web/POP-EthicsAndIssues.pdf

Mills, E., ‘Phishers Use HTML Attachments to Evade Browser Blacklists’, retrieved 28 April 2012 from

http://news.cnet.com/8301-27080_3-20043960-245.html

Redford, M. 2011, ‘U.S. and EU Legislation on Cybercrime’, *2011 European Intelligence and Security Informatics Conference*, pp. 34-37. Retrieved 24 April 2012 from IEEE Explore database

Scambusters.org, ‘Internet Scams, Identity Theft, and Urban Legends: Are You at Risk?’, retrieved 12 April 2012 from

http://scambusters.org

The Spamhaus project, ‘The Definition of Spam’, retrieved 12 April 2012 from http://www.spamhaus.org/consumer/definition