CRIME PREVENTION ASSIST

No.35 June 2012

Preventing spam

'Spam' is an electronic version of 'junk mail' sent to a large number of people who do not request it, detailing products or services in which they may have no interest. Spam is sent by people who disguise their identity and whom it is difficult, if not impossible, to locate or deter. Senders of spam rely on the fact that, although most will reject the message, a minority of recipients will read and/or respond to it. Criminals have been quick to take advantage of this fact through activities such as 'phishing' – where official-looking 'spoofed' or trick emails (typically purporting to come from banks) attempt to persuade a user to click on a false link leading to a fraudulent web site. Once there, the user is asked to provide their online password, user name and/or other personal information in response to a fake but convincing security check.

Mitigating the impact of spam involves a number of stakeholders including:

1. governments – by enacting legislation to prevent spam;
2. law enforcement agencies – by investigating spam;
3. internet service providers (ISPs) – by filtering all email to remove spam prior to releasing it to customers' inboxes; and
4. corporations – by filtering all email for spam and governing appropriate use of email via an applied email policy.

Individuals can assist in the anti-spam effort by:

- avoiding placing email address in a public domain, for example a chat room;
- if placing an email address in a public domain, disguising it (so, for example, <johndoe@fakesite.com> becomes 'johndoe at fakesite.com');
- using multiple email addresses, so that if one address becomes a target of spam it can be discarded;
- installing and updating spam filters on home computers;
- using longer and more complicated email addresses; and
- simply deleting the spam (never responding in any way, not even by unsubscribing).

Larger stakeholders must also continue to reduce the amount of spam entering computer systems. Corporations could adopt an email policy clearly delineating staff use of email and the internet. ISPs might, as AOL has done, deny their customers access to certain web sites prone to spam. Governments might continue to cooperate with one another in anti-spam campaigns, such as 'Operation secure your server'. Finally, the interception of messages may also assist in the fight against spam. These technological counter-measures include black lists (internet addresses known to be disseminators of spam are blocked), lexical analysis (in which words are analysed in context, so that a word which appears in a group of unrelated words triggers an alarm which blocks the spam) and heuristics (in which particular emails are examined and scored for spam characteristics – if the score reaches a pre-determined level, the email is blocked).

Contact Us

Australia's national research and knowledge centre on crime and justice

www.aic.gov.au

Australian Government

Australian Institute of Criminology

REFERENCES

1 Fallows D 2003. Spam: how it is hurting email and degrading life on the internet. Pew Internet and American Life Project http://www.pewinternet.org/pdfs/PIP_Spam_Report.pdf

2 McCusker R 2005. Spam: nuisance or menace, prevention or cure? *Trends & issues in crime and criminal justice* no 294 Canberra: Australian Institute of Criminology

ISSN 1448-1383