An examination of hoax computer virus warnings, and their effect on computer users

Barely a day passes without e-mail in boxes being bombarded with messages warning of the potential threat of a virus attack. Indeed, most recently there has been a warning of a virus that would activate itself on June 1st, 2001 which would "wipe out all files and folders" (Symantec, 2001). This, as multitudinous other such warnings, is a hoax.

The concept of e-mail virus hoaxes has been traced back to the *Good Times* hoax first recorded on November 15, 1994 (Ives, 1998), although claims of its existence date back to "April or May" (Jones, 1998). The original *Good Times* hoax was an e-mail that warned of a file being sent via e-mail which if received and downloaded would, the writer understands, "ruin all of your files". It is important to note that this first example does not claim any authority and appears to be a friendly warning.

By December 1994 the warning had metamorphosed to wish everyone "Happy Chanukah", and then discuss the same attachment. However, in this incarnation the message states that the virus exists and "will erase your hard drive" if downloaded. It also encourages the receiver to forward the warning to all of their friends. The warning now contains a concrete threat of potential damage.

The final major textural change was the addition of the statement that "The FCC [US Federal Communications Commission] released a warning […] concerning a matter of major importance to any regular user of the InterNet". Having received a message apparently 'issued' by the FCC immediately gives the warning far more credibility. The FCC edition of the warning also suggested that the 'virus' would put the processor in a "nth-complexity infinite binary loop" – a meaningless piece of jargon that only serves to confuse the receiver into thinking that not only their data, but also their hardware is at risk of irrecoverable destruction. By suggesting that a piece of computer code could physically damage hardware the belief that a hacker's power (as it is perceived that only 'hackers' write viruses) is boundless is reinforced, leading to concern in many other areas of computer security

The majority of virus warnings passing from user to user today appear to have come from a government agency, or a large multinational technology company, and without fail urge the receiver to forward the message to others. As such, people receiving the e-mails not only feel obliged to pass on the message for the good of the computer using public, they are also being asked by a powerful institution to help disseminate critical information. In short, the warnings are little more than chain letters (of which there is also legion traversing the Internet).

The panic that ensues from the receipt of such a warning is due to the existence of genuine viruses of which people are only too aware of having caused technological chaos in the past. The most recent example being the Melissa virus that exploited a loophole in a specific e-mail program to propagate itself: unlike hoaxes, Melissa forwarded itself, rather than requiring any manual intervention. If a warning message was able to forward itself it could not be viewed as a hoax, and would be described as a virus as its behaviour exhibits viral characteristics.

The disruption caused by hoaxes is often ignored, but as Uhlig (1999) reports that "the hoaxes wreak no damage, but instead prompt computer users to flood helplines and company computer departments to switch off their networks as a precaution". This report fails to consider the number of e-mails generated by one person receiving the warning: the circulation of a chain letter is defined by AHDEL (2000) as "increasing in geometric progression as long as the instructions [for forwarding] as followed by all recipients". While the processing power and bandwidth required to handle a single e-mail is negligible, if this is multiplied up to cater for the geometric increase in e-mail traffic, the load can be seen to impact on both the Internet backbone, and individual mail servers.

It is in human nature to communicate ideas, and in trying to establish why certain ideas are communicated more readily, the concept of memes has been proposed. The meme is a “self-replicating pattern of information which propagates via the human mind, interacting with the mind, adapting, mutating, and persisting” (Gordon, Ford, & Wells, 1997). Dawkins first discussed the concept of such a “virus of the mind” in 1976, by suggesting a “cultural replicator analogous to genes” (Jones, 1998). Meme theory is a type of natural selection for non-biological entities such as “sex, danger, profit, love, and fear” (Gordon *et al*, 1997), or “tunes, catch phrases, clothes fashions” (Jones 1998). When these entities are embodied in an idea, be it danger in an e-mail warning, or a catchy tune being hummed, these ideas are more likely, for whatever evolutionary reasons, to get passed between human beings.

While meme theory attempts to explain the reason for succumbing to pass the message on as biological, there are several psychological and social reasons for wanting to disseminate the information. Harley (2001) suggests that altruism and social responsibility are the primary reasons, especially as the number of new users (‘newbies’) using the Internet is increasing dramatically and these warning exploit “their eagerness to learn and help others”. Psychologically, the nature of forwarding an e-mail suggests another reason: when a forwarded e-mail is received the list of previous recipients is visible, showing the number of other people that have seen and sent the e-mail before them. The logical inference to draw is that a plethora of other people cannot be wrong, and as such a longer list of previous recipients “increases the likelihood that the victim will pass it on” (Harley, 2001).

It can be seen that these hoaxes can therefore be viewed as viruses, however, they are nothing to do with technology or illness, they are thought, or social viruses as the only viral activity is displayed by human behaviour. A spokesman for Sophos, an antivirus company, points out that “you can protect yourself against a proper virus, but, ironically, not against a hoax” (Uhlig, 1999).

Leading on from hoaxes, there are concerns outside the scope of this report that should be mentioned for the sake of completeness. The creation of a virus based on information in a hoax could render the hoax a genuine warning (to a point this did happen in the case of the *Good Times* hoax although the resultant virus only tried to utilise the name. It was subsequently renamed the GT Spoof virus by anti virus companies). The specific case of the current SULFNBK.EXE (June 1st) hoax is also worth mentioning as it broaches the fine line between fact and fiction. It warns of a file on the user’s computer, which is in fact part of the operating system, being a virus and encourages the recipient to delete it. The implications of this are twofold: firstly, with the file deleted part of the OS will not function correctly, and secondly, it would be possible for a genuine virus to attack the file, transmogrifying an innocent file into something worth warning against.

The common things that frequently identify a hoax are the urging recipients to “pass this on”, and purporting to come from a well-known organisation. If people were to treat warnings with a little more scepticism, there are various trusted authorities available online to verify the veracity of warnings in a matter of seconds, which would serve to reduce the number of hoaxes causing technical blockages worldwide.

(1244 words)

Bibliography and References

American Heritage Dictionary of the English Language (4th Edition) (2000), Houghton Mifflin, http://www.dictionary.com/cgi-bin/dict.pl?term=chain%20letter [02/06/2001]

Dawkins, R (1976) *The Selfish Gene*, Oxford: Oxford University Press, quoted in Gordon, S, Ford, R, Wells, J (1997) *Hoaxes and Hypes*, http://www.research.ibm.com/antivirus/scipapers/gordon/hh.html [24/05/2001]

Gordon, S, Ford, R, Wells, J (1997) *Hoaxes and Hypes*, http://www.research.ibm.com/antivirus/scipapers/gordon/hh.html [24/05/2001]

Harley, D (2001) *E-Mail Abuse – Internet Chain Letters, Hoaxes and Spam*, http://www.sherpasoft.org.uk/hoaxfaq/mis-it/html [24/05/2001]

Ives, J (1998) *Computer Virus Hoaxes: Urban Legends for the Digital Age*, http://eserver.org/bs/37/ives.html [24/05/2001]

Jones, L (1998) *Good Times Virus Hoax – Frequently Asked Questions*, http://www.public.usit.net/lesjones/goodtimes.html [24/05/2001]

Symantec (2001) *SULFNBK.EXE Warning*, http://www.symantec.com/avcenter/venc/data/sulfnbk.exe.warning.html [31/05/2001]

Uhlig, R (1999) *Hoax computer viruses cause chaos worldwide*, Web page Appendix A

Appendix A