STOPPING CHAIN LETTERS AND HOAXES ON THE INTERNET

by M. E. Kabay, PhD, CISSP-ISSMP

Security Leader, INFOSEC Group, AtomicTangerine, Inc.

Some years ago I received the following friendly joke in an e-mail message from an acquaintance

```
You've been hit!
["*" used to draw big letters of the words "SNOW BALL"]
                  Consider yourself hit by a snowball !!
 Send this message to as many people as possible, in the first
               *E-MAIL SNOWBALL FIGHT!*
 Send it back or to people already listed above. Send it to your
 parents, siblings, politicians, teachers, bullies or anyone else
 you've wanted to hit with a snowball. have fun. but don't blame me if
 you're hit back !!
 Remember: e-mail snowballs don't hurt, don't get you soaked and
 don't melt away. Throw one today  !
Xxxx [name removed to protect the foolish]
```

The message header showed it had been sent to a distribution list of a dozen people. You have probably seen many such letters -- either jokes with requests to circulate widely or warnings of terrible things that could happen to you by reading e-mail messages with particular subject lines.

I hope the response I sent my friend will help reduce the incidence of similar mistakes.

* * *

Dear Xxxx,

DON'T SEND CHAIN LETTERS THROUGH THE INTERNET.

Sorry, Xxxx, I have to disagree with you about the e-mail snowball:

>Send this message to as many people as possible<

What you are doing is generating a chain letter. There are several problems with chain letters.

1) There is NO EXPIRY DATE on your joke. Once launched, your message can circulate for years, causing millions of useless messages on the Internet, wasting people's time and Internet bandwidth (capacity). For a look at what this kind of unlimited message

can cause, see the notorious Craig Shergold spam, which has been absolutely impossible to stop. I quote from my "The Year in Review in InfoSec -- 1996" published in the January issue of the NCSA NEWS:

"In a graphic demonstration of the harm that undated, unauthorized, immortal and unauthenticated messages circulating on the Internet can have, the Make-a-Wish Foundation set up an 800 hot line and a Web page begging for the end of one of the many variations of the Craig Shergold urban myth. Craig Shergold is a kid who had a brain tumor but it was removed and he's now fine. Unfortunately, several thousand messages a day continue to circulate among well-meaning but naive people who think that the poor chap wants their post cards and business cards. He doesn't, and neither does the postal service where he lives. Make-a-Wish have been tarred with this bizarre brush because some nitwit embroidered the story to implicate them in the scheme and now they receive thousands of pieces of unwanted mail for someone they have never been involved with. Lesson: do NOT forward chain letters without verifying their accuracy. [See http://www.wish.org/wish/craig.html or call 800-215-1333, x. 184 for information.]"

2) There is no way for you or anyone else to stop the chain letter once it gets started.

3) Chain letters are a violation of Netiquette (proper behavior on the Internet).

4) You used your corporate account, making your own employer liable for serious trouble if people become annoyed by the useless traffic that includes your address. Possible damages: mail-bombing (large volumes of unwanted mail) to your account or to your postmaster's account at your company; publication of your company's 800 number in various unsavory regions of the Net, resulting in avalanches of unwanted (and expensive) calls the company will pay for. You yourself could be in major trouble for initiating such a sequence of events. If your corporate appropriate use guidelines do not forbid this sort of wasted effort, they ought to. If they do include prohibitions on frivolous use of corporate resources, you may face disciplinary action.

5) There is no way to be sure that the people on person A's list will not send the message to people who include A on their lists. There is a real possibility of extended batches of useless mail circulating from one person to another and back; this phenomenon is known as a mail-storm and is a real problem on the Net.

I am really sorry to rain on your snowball fight, but this is a really bad mistake. I am sending this message to everyone on your list in the hope of stopping a minor disaster.

DON'T SEND CHAIN LETTERS THROUGH THE INTERNET.

Respectfully,

Mich

* * *

I was criticized by one person on Xxxx's list for having made this message public to everyone on her distribution list; the person felt that it was rude to do so. I maintain that providing instruction on appropriate use to innocent victims of a mistake is a responsibility of my position at the NCSA.

Another question is whether writing to everyone who has received false information -- hoaxes about imaginary viruses, for example -- is itself an abuse of bandwidth. I feel that the practice of circulating unverified information is itself much more harmful than the expenditure of bandwidth in a single message explaining why the practice should stop.

The general principle for all corporate appropriate-use policies is that circulating unverified information is irresponsible. Employees who receive a terrifying warning from a friend or colleague should send it to their technical support staff. Technical support staff should verify the accuracy of any such warnings by checking appropriate authorities such as the CERT-CC. No one should circulate unsubstantiated rumors.

The people who invent rumors are malicious; those who circulate them are just dupes of the inventors. There is no reason to be abusive when responding to the innocent victims of these pranks; it's enough to give them the facts and enlist their cooperation in stopping the growing tide of hoaxes on the Net.

* * *

In conclusion, some practical advice:

1) Don't forward warnings about viruses to anyone unless you are qualified to evaluate their accuracy.

2) Use the resources listed below to check the veracity of any warnings you do feel worried about:

Virus hoaxes:

http://www.vmyths.com

http://www.icsa.net/html/communities/antivirus/hoaxes/

Other hoaxes:

http://ciac.llnl.gov/ciac/CIACHoaxes.html

http://www.urbanlegends.com/

http://www.cwrl.utexas.edu/~roberts/gullibility.html

http://www.urbanmyths.com/

For a scholarly (and fascinating) analysis of why hoaxes spread, see the paper by Sarah Gordon entitled "Hoaxes & Hypes" at

http://www.av.ibm.com/InsideTheLab/Bookshelf/ScientificPapers/Gordon/HH.html

and also her excellent overview entitled "Received. . . and Deceived" at

http://www.infosecuritymag.com/sept/cover.htm

3) Ignore warnings that contain exclamation marks, LOTS OF CAPITALS, and terrifying consequences of reading e-mail.

4) Be skeptical of warnings that show no date, no expiration date, no author and no references to where you can verify their authenticity and correctness.

* * *

In the long run, I would like to see this kind of information about rumors and hoaxes filtering into computer and Internet courses taught in universities, colleges, high schools, middle-schools and grade-schools. Today's children can, if instructed effectively, become much better citizens of Cyberspace than their untutored elders.

I urge all computer experts to become involved in outreach to their communities by giving lectures in schools, churches, mosques, synagogues, and social clubs. Get the word out on all the many issues that affect people in cyberspace.