Global Information Assurance Certification Paper

Internet Hoaxes: *The Truth is Out There*

Jeff Henning
September 4, 2000

Introduction

What is an Internet hoax? Where do they originate? I hope this project will shed some light on what Internet Hoaxes are and why they prey on our sense of good nature, greed or willingness to help others in need.

The Internet is constantly being bombarded with bogus computer virus warnings and chain letters. These are typically scare warnings started by malicious people and passed on by naive users who think they are helping the community by spreading the warning. While these hoaxes do not infect systems, they can cause a "Denial of Service" attack on email servers from all the messages that are forwarded to everyone in the company.

History

Since 1988, computer virus hoaxes have been circulating the Internet. In October of that year, according to Ferbrache ("A pathology of Computer Viruses" Springer, London, 1992) one of the first virus hoaxes was the 2400 baud modem virus. [1]
Internet Hoaxes now arrive in many forms. From chain letters to deadly viruses, they all have one thing in common. They're just not true!

How to Identify an Internet Hoax

How do you avoid being tricked by Internet hoaxes? Learn ways to identify them. The best method is to educate yourself and others about Internet hoaxes and how to spot them.
Here are some examples to look out for.

- Any email message that states **"This is not a hoax"** probably is.

- The ever so popular phrase **"Forward this to everyone you know."** This will help propagate the message around the Internet. Do not forward this type of message, they only slow your email system down or clog the network.

- **Did the message originate from the person who sent it to you?** Hoaxes are usually forwarded from people you know, but it's hard to know where they started.

- **Offers too good to be true!** They promise you money, free products and luck if you forward them, bad luck to those who don't.

- **Don't be fooled by technical sounding language.** This is only to impress you into believing the email. If you carefully read these hoax messages, you can break down the technical jargon, used to confuse and scare those who aren't computer experts. This jargon usually talks about systems of a computer that don't exist or things that aren't possible. Unfortunately, the inexperience Internet users, falls prey to these hoaxes everyday.

- **Look for UPPERCASE LETTERS and lots of exclamation points!!!** Hoaxsters like to over empathize the language to push your emotional buttons. Who wouldn't want to forward an email so little Johnny can have his dying wish of millions of emails bouncing around the Internet.

- **Check the Internet Hoax web sites.** There are numerous web sites, dedicated to the cause of debunking Internet Hoaxes and chain letters. Check these sites first to validate the information's authenticity.

Examples

Take some time and read these examples. Some are really funny. Do people really fall for these? All examples are links to CIAC Web Site. [1]

Internet Cleanup Day
Good Times
Bud Frogs Screen Saver
Boy With Just A Head Spoof
Win A Holiday
AOL4FREE

More

Sample Email Policy

All companies need to have a corporate policy that relates to their email system. Here is a sample email policy that most companies could use.

2.0 Corporate Email Policy

2.1 Electronic media may not be used for knowingly transmitting, retrieving or storage of any communications of a discriminatory or harassing nature, or which are derogatory to any individual or group, or which are obscene or X-rated communications, or are of a defamatory or threatening nature, or for "chain letters," or for the spread of “Internet Hoaxes,” or for any other purpose which is illegal or against company policy or contrary to the company's interest.

2.2 Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

2.3 Any messages or information sent by an employee to one or more individuals via an electronic network (e.g., bulletin board, on-line service, or Internet) are statements identifiable and attributable to our company. While some users include personal "disclaimers" in electronic messages, it should be noted that there would still be a connection with the company, and the statement might still be legally imputed to the company. All communications sent by employees via a network must comply with this and other company policies, and may not disclose any confidential or proprietary company information.

2.4 Any messages that may warn of viruses should be directed to the I.S. Department for review. Under no circumstance should these warnings be forwarded to anyone other than the I.S Department. It is the job of the I.S. Department to send out warnings of viruses or hoaxes and warnings from other sources should be ignored.

2.5 Any employee found to be abusing the privilege of company-facilitated access to electronic media or services will be subject to corrective action and/or risk having the privilege removed for him/herself and possibly other employees.

Conclusion

Internet Hoaxes are here to stay, they may disappear for awhile, only to resurface and fool again. As security professionals, it is our job to inform/educate users in ways to identify Internet Hoaxes. These users are our first line of defense against these hoaxes. As stated in this paper and on every hoax site, **“Please do not forward these hoax messages,”** they only encourage others to write more. As an example, The Urban Legend Generator allows you to create your own Urban Legend to email to your friends. I would not encourage anyone to do this. It will only hurt the cause. Another useful web site, The Hoaxkill service will extract the addresses of all previous recipients from the message and inform them all that the message is a hoax.

In closing, just remember one thing, by sending out a false Internet Hoax warning at your

company, everybody will remember your name.

References

[1] WWW.CIAC.org. "CIAC Hoax Page,"
URL: http://HoaxBusters.ciac.org/HBHoaxInfo.html#identify (24 Aug. 2000)

Author Unknown. "Hoaxkill.com," URL: http://www.hoaxkill.com/index2.shtml (1 Sept. 2000).

Rosenberger, Rob. "Vmyths.com," Computer Virus Myths Home Page.
URL: http://www.Vmyths.com/hoax.cfm (26 Aug. 2000).

Emery, David. "How to Spot an Email Hoax," Urban Legends and Folklore.
URL: http://urbanlegends.about.com/science/urbanlegends/library/howto/hthoax.htm (26 Aug. 2000).

Emery, David. "Best Hoax Busting Resources," Urban Legends and Folklore. 16 June 1999.
URL: http://urbanlegends.about.com/science/urbanlegends/library/weekly/aa061699.htm (25 Aug. 2000).

Cosper, John. "I Swear It's All True!," Handystreet.com Web Page.
URL: http://handystreet.com/hoax/index.html (24 Aug. 2000).

Arthor Unknown. "Virus Hoaxes," Symantec AntiVirus Research Center Web Site.
URL: http://www.symantec.com/avcenter/hoax.html (24 Aug. 2000).

Austin, Bill. "Virus Hoax Busters," Virus Hoax, Alert, Fraud, Chain Letter and Urban Legend Information. URL: http://www.stockhelp.net/virus.html (25 Aug. 2000).

Crispen, Patrick. "The Urban Legend Combat Kit," NetSquirrel.com Web Site. 5 Sept.2000.
URL: http://www.netsquirrel.com/combatkit/index.html (5 Sept. 2000).

Author Unknown. "The Urban Legend Generator,"
URL: http://toybox.asap.net/legend (24 Aug. 2000).

Network Associates, Inc. "NAI Web site,"
URL: http://www.mcafeeb2b.com/asp_set/anti_virus/library/hoaxes.asp (24 Aug. 2000)