Global Information Assurance Certification Paper

SANS Security Essentials
GSEC Practical Assignment
Version 1.2e

Prepared by Darren Grocott

Virus hoaxes – are they just a nuisance?

Virus hoaxes require little or no technical skill to initiate and are becoming as common as the virus problem itself.

Should information security professionals be concerned about virus hoaxes? After all, it is commonly opinion that they are just a prank that doesn't really hurt anybody.

This paper aims to:

- Outline the risks and/or impact that virus hoaxes pose to an organisation;
- Provide some simple steps that can help organisations minimise the risk and / or impact of virus hoaxes; and
- Discuss the dilemma that virus hoaxes create for organisations, and the potential future for virus hoaxes.

A Brief History of Virus Hoaxes

Computer Viruses are well reported and analysed due to their potentially destructive nature. However virus *hoaxes* receive minimal analysis because the damage they cause to organisations is not easily quantifiable and therefore the history of virus hoaxes is not well documented.

One of the earliest virus hoaxes to be reported was in October 1988 (the '2400 baud modem' hoax[1] claimed that a virus was being spread on the modems sub-carrier which would cause corruption of a users hard disk). Since that time there has been a steady increase in the number of virus hoaxes reported (and other internet hoaxes), with approximately 50 hoaxes identified in the last 12 months according to the F-Secure, Security Information Center [1]. Unless there is a concerted effort to manage the impact of virus hoaxes, the time when they will pose as serious an issue as malicious code is fast approaching.

There have been a number of virus hoax web sites created to assist in managing this increasing threat. These resources can help information security professionals minimise the impact of a virus hoax by providing up to date information. Some of

[1] Virus hoax extracts discussed in this paper are detailed in the description section (page 8) of this paper

the sites that provide extremely useful information are:

- Vmyths web site; [2]
- Urban Legends web site; [3]
- CIAC's Hoax buster site; and [4]
- Most of the major anti-virus vendors.

As the impact of this form of attack is better quantified virus hoaxes will become better documented over time.

There have been famous virus hoax examples that have raised awareness of this issue including:

- Good Times (was supposedly an e-mail virus that would delete the contentts of your hard disk);
- Pen Pal Greetings (was supposedly an e-mail borne virus that would infect the boot sector of your PC and delete the contents of your hard drive);
- Deeyenda (supposedly an e-mail virus that re-writes your hard drive);
- Sulfnbk.exe - particularly destructive because it requested users to delete (of which many did) this executable which is used to restore and backup long file names in Windows 95/98.; and [5]
- Bud Frogs –of which I received a virus while writing this paper claims that if you download the screen saver it will crash your hard drive.

To see a full list of virus hoaxes visit one of the sites listed in sources section of this paper.

Why do people start virus hoaxes

There is no definitive reason why somebody would start a virus hoax. According to Hoaxbusters "Why People Send Chain Letters and Hoax Messages" [6] there are a variety of reasons why people send hoaxes. Virus hoaxes are sent by people to:

- See how far it will go;
- Harass another person (include an e-mail address and ask

everyone to send mail, e.g. Jessica Mydek Hoax which requested users to forward the message and contact American Cancer Society for further information);

- To milk money out of people using a pyramid scheme;
- To kill some other chain letter; and
- To damage a person's or organisation's reputation.

This list could be enlarged to include more menacing motives, such as sending a virus hoax as a prelude to a more destructive malicious code attack. This form of attack relies on the user community becoming aware of a virus hoax and letting down their guard. This type of threat places additional pressure on information security professionals to manage this situation effectively.

Irrespective of why people send virus hoaxes, if users did not forward hoaxes they would not perpetuate the problem nor create any significant damage. There is also an increasing trend to create variants of the original virus hoax message which adds to the confusion. Sarah Gordon of The IBM Anti-virus Research Center [7] states the there are five central factors as to why people transmit/forward hoaxes. The five factors are:

- Trust in Authority (referred to by Rosenberger [2] as the False Authority Syndrome);
- Excitement of being involved;
- Lack of appropriate scientific skepticism of the facts;
- Sense of importance or belonging by passing along information; and
- Furthering their own goals / self interest / agenda

The ability of the virus hoax to prey on the goodwill of the receiver is the delivery mechanism that these viruses use to further their impact. There is only one sure way to stop virus hoaxes – don't send it!!

The cost of Virus Hoaxes

What is the cost of virus hoaxes? Well this really depends on whether you or your organisation is the recipient of a virus hoax warning or whether you are the subject of a virus hoax. In either case there is definitely a cost.

The recent media attention to viruses like the 'Melissa', 'Anna Kournikova' and 'I Love You' virus warnings has raised the awareness of users to a level that information security professional can only dream of. This atmosphere of awareness also increases the risk of virus hoaxes having a much larger impact on organisations.

It is estimated that virus hoaxes could cost an organisation as much as a genuine virus incident. An example of the cost of virus hoaxes is discussed on The CIAC Hoaxbusters site [8]. The example displayed on this site estimated the potential cost of a virus hoax to be in the vicinity of $41.7 million.

The cost of a virus outbreak is relatively easy to quantify: there is the damage inflicted by the virus; the resource cost to repair and return to normal operation; and the financial cost of implementing anti-virus tools etc. The cost of a virus hoax is hidden but includes:

- Loss of productivity of users;
- Network utilisation damage as messages are sent;
- Reputation of your organisation (when responsible for forwarding virus hoax warnings); and
- A relaxing in attitude of users to real virus warnings.

The following diagram demonstrates the impact that a virus hoax can have on an organisation based on an employee salary averaged at $50 per hour and 1 minute of lost productivity per employee in forwarding the message.

Diagram 1 – Cost of Virus Hoax

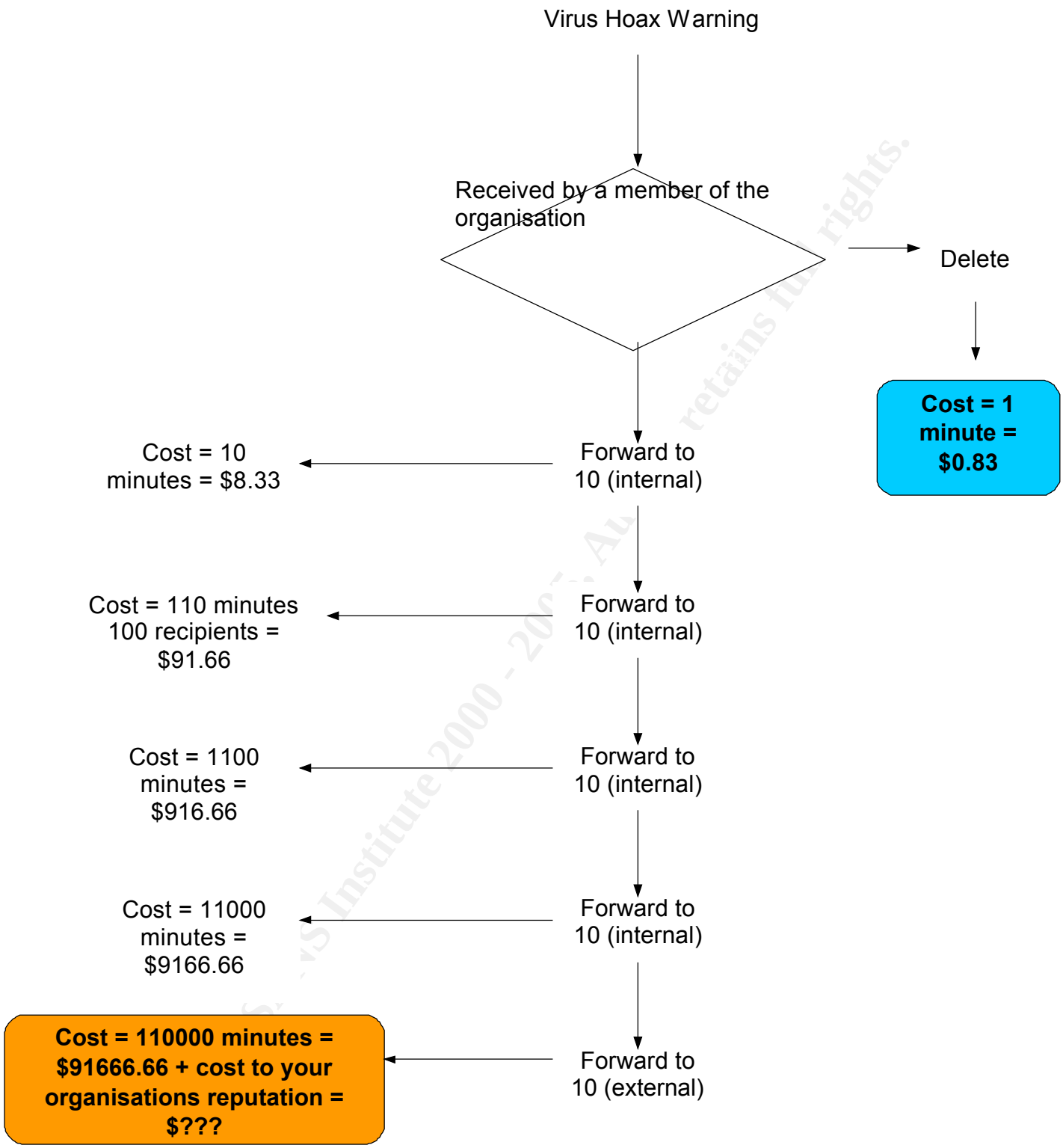

Diagram 1 clearly shows that there is a real cost to virus hoax warnings. The action of one person at the beginning of the process can make a real difference to the cost to an organisation. The loss of production and damage to reputation are only two of the potential costs to an organisation. The Blue Mountain Arts virus hoax is a prime example of the damage that can be caused in this manner. As reported by

Sullivan [9] this virus hoax threatened the Blue Mountain Arts company's core business by stating that all cards issued by the company contained a virus. The Blue Mountain Arts virus hoax claimed that there was a virus infecting all virtual cards being downloaded from their site.

Virus hoaxes potentially pose a greater risk to an organisation than viruses because there is no anti-virus engine that will detect quarantine and clean a virus hoax. It is possible with some intelligent content filtering to minimise an incident of this sort, but a typical response will almost certainly be reactive in nature. The issue of virus hoaxes clearly indicates where a non-technology countermeasure will be the most effective.

A method for handling virus hoaxes

Organisations generally ignore virus hoaxes as a nuisance. But as is displayed in Diagram 1 there is a real cost that an organisation needs to manage. Every organisation should determine the most appropriate method to handle the virus hoax problem within their environment, which will also help the larger Internet community to manage this problem. The 'Catch 22' for an organisation is that they need to be careful not to implement a solution that compounds the problem and perpetuates the loss of productivity.

A technological solution will not eradicate this problem; a policy and intelligent awareness campaign will be the most effective method. The policy should clearly articulate who is responsible for sending any virus warning messages and should highlight that virus warning messages are not to be transmitted except by that person. It should be the nominated person's responsibility to verify the integrity of a virus warning message.

Sophos [10] provides an example policy that could be used by an organisation.

> "You shall not forward any virus warnings of any kind to **anyone** other than… . It doesn't matter if the virus warnings have come from an anti-virus vendor or been confirmed by any large computer company or your best friend. **All** virus warnings should be sent to …, and alone. It is …'s job to send round all virus warnings, and a virus warning which comes from any other source should be ignored."

The aims of a security awareness campaign (in relation to virus hoaxes) should be to:

- Increase awareness of the problem;
- Minimise the impact on the organisation, the end user, the information security professional; and
- Leverage of this issue to increase security awareness in general.

Below is an example of a method being used to handle the virus hoax problem.

Countermeasure 1 – Company A has a clearly articulated and publicised policy on what the end user should do when they receive a virus warning (similar to the policy above).

Countermeasure 2 – The company intranet site is the only authoritative source for advice on virus warnings. This is employed to minimise the impact on the external gateways and networks.

Countermeasure 3 – The intranet site displays this information on the very first page and is updated regularly. To minimise the loss of productivity impact they also include other security messages with the announcement of hoaxes. For example:

> The Good Time Virus warning message has been declared a hoax. Anybody receiving this warning should discard it.
>
> Remember when receiving email you should never open attachments that are not from a trusted source and expected.

Countermeasure 4 – If the virus warning is not listed staff are to forward the warning to the designated person. They are also advised there will not be a response to their message. The response will be articulated on the intranet site within 48 hours. This is implemented to minimise the impact that virus hoaxes have on the information security area

Countermeasure 5 – The other facet of the awareness campaign forms part of an ongoing security awareness effort. Through newsletters, presentations etc, users are educated in methods of identifying virus hoaxes.

This enhanced awareness will hopefully minimise the impact of virus hoaxes in general.

Sarah Gordon of the IBM Anti-Virus Research Center [7] states there are hoax heuristics that are common to all virus hoaxes. These heuristic's are:

- It's a warning message about a virus;
- It's usually from an individual, occasionally from a company but never from the cited source;
- It warns the reader not to read or download the supposed virus, and preaches salvation by deletion;
- It describes the virus as having horrific destructive powers and often the ability to send itself be e-mail;
- The message usually has many words in caps and exclamation marks;
- It urges the reader to alert everyone they know, and usually repeats this message;
- It seeks credibility by citing some authoritative source as issuing the

warning. Usually the source says the virus is 'bad' or has them 'worried'; and

- The message seeks credibility by describing the virus in specious technical jargon.

Conclusion

On an almost daily basis, virus hoaxes continue to surface. Even though the costs to organisations are not reported in the end of year spreadsheet, they are real and need to be managed. By identifying that there is an issue with virus hoaxes that needs to be managed, the first step is to minimise this cost. How an organisation will handle the virus hoax issue may vary greatly, but the fact that it is being managed can only be good for the organisation, and the wider Internet community.

Finally, **do not forward virus warning messages**, you are only encouraging their continued prevalence.

Descriptions

The details contained below have been extracted from the CIAC Hoaxbusters and Symantec web sites (see sources list).

2400 Baud Modem Hoax

SUBJ: Really Nasty Virus
AREA: GENERAL (1)

I've just discovered probably the world's worst computer virus yet. I had just finished a late night session of BBS'ing and file treading when I exited Telix 3 and attempted to run pkxarc to unarc the software I had downloaded. Next thing I knew my hard disk was seeking all over and it was apparently writing random sectors. Thank god for strong coffee and a recent backup.
Everything was back to normal, so I called the BBS again and downloaded a file. When I went to use ddir to list the directory, my hard disk was getting trashed again. I tried Procomm Plus TD and also PC Talk 3. Same results every time. Something was up so I hooked up to my test equipment and different modems (I do research and development for a local computer telecommunications company and have an in-house lab at my disposal). After another hour of corrupted hard drives I found what I think is the world's worst computer virus yet. The virus distributes itself on the modem sub-carrier present in all 2400 baud and up modems. The sub-carrier is used for ROM and register debugging purposes only, and otherwise serves no othr (sp) purpose. The virus sets a bit pattern in one of the internal modem registers, but it seemed to screw up the other registers on my USR. A modem that has been "infected" with this virus will then transmit the virus to other modems that use a subcarrier (I suppose those who use 300 and 1200 baud modems should be immune). The virus then attaches itself to all binary incoming data and infects the host computer's hard disk. The only way to get rid of this virus is to completely reset all the modem registers by hand, but I haven't found a way to vaccinate a modem against the virus, but there is the possibility of building a subcarrier filter. I am calling on a 1200 baud modem to enter this message, and have advised the sysops of the two other boards (names withheld). I don't know how this virus originated, but I'm sure it is the work of someone in the computer telecommunications field such as myself. Probably the best thing to do now is to stick to 1200 baud until we figure this thing out.

Mike RoChenle

Good Times Virus Hoax

Here is some important information. Beware of a file called Goodtimes. Happy Chanukah everyone, and be careful out there. There is a virus on America Online being sent by E-Mail. If you get anything called "Good Times", DON'T read it or download it. It is a virus that will erase your hard drive. Forward this to all your friends. It may help them a lot.

PenPals Greetings Virus Hoax

FYI!

Subject: Virus Alert
Importance: High
If anyone receives mail entitled: PENPAL GREETINGS! please delete it WITHOUT reading it. Below is a little explanation of the message, and what it would do to your PC if you were to read the message. If you have any questions or concerns please contact SAF-IA Info Office on 697-5059.

This is a warning for all internet users - there is a dangerous virus propogating across the internet through an e-mail message entitled "PENPAL GREETINGS!". DO NOT DOWNLOAD ANY MESSAGE ENTITLED "PENPAL GREETINGS!"
This message appears to be a friendly letter asking you if you are interested in a penpal, but by the time you read this letter, it is too late. The "trojan horse" virus will have already infected the boot sector of your hard drive, destroying all of the data present. It is a self-replicating virus, and once the message is read, it will AUTOMATICALLY forward itself to anyone who's e-mail address is present in YOUR mailbox!
This virus will DESTROY your hard drive, and holds the potential to DESTROY the hard drive of anyone whose mail is in your inbox, and who's mail is in their inbox, and so on. If this virus remains unchecked, it has the potential to do a great deal of DAMAGE to computer networks worldwide!!!!
Please, delete the message entitled "PENPAL GREETINGS!" as soon as you see it!
And pass this message along to all of your friends and relatives, and the other readers of the newsgroups and mailing lists which you are on, so that they are not hurt by this dangerous virus!!!!

Deeyenda Virus Hoax

**********VIRUS ALERT**********

VERY IMPORTANT INFORMATION, PLEASE READ!

There is a computer virus that is being sent across the Internet. If you receive an email message with the subject line "Deeyenda", DO NOT read the message, DELETE it immediately!

Some miscreant is sending email under the title "Deeyenda" nationwide, if you get anything like this DON'T DOWNLOAD THE FILE! It has a virus that rewrites your hard drive, obliterates anything on it. Please be careful and forward this e-mail to anyone you care about.

Please read the message below.

Alex

FCC WARNING!!!!! -----DEEYENDA PLAGUES INTERNET

The Internet community has again been plagued by another computer virus. This message is being spread throughout the Internet, including USENET posting, EMAIL, and other Internet activities. The reason for all the attention is because of the nature of this virus and the potential security risk it makes. Instead of a destructive Trojan virus (like most viruses!), this virus referred to as Deeyenda Maddick, performs a comprehensive search on your computer, looking for valuable information, such as email and login passwords, credit cards, personal inf., etc.

The Deeyenda virus also has the capability to stay memory resident while running a host of applications and operation systems, such as Windows 3.11 and Windows 95. What this means to Internet users is that when a login and password are send to the server, this virus can copy this information and SEND IT OUT TO UN UNKNOWN ADDRESS (varies).

The reason for this warning is because the Deeyenda virus is virtually undetectable. Once attacked your computer will be unsecure. Although it can attack any O/S this virus is most likely to attack those users viewing Java enhanced Web Pages (Netscape 2.0+ and Microsoft Internet Explorer 3.0+ which are running under Windows 95). Researchers at Princeton University have found this virus on a number of World Wide Web pagesand fear its spread.

Please pass this on, for we must alert the general public at the security risks.

SULFNBK.exe virus hoax

Subject: BAD virus - act quickly!!
Date: Tue, 29 May 2001 21:57:22 -0400

Subject: Please Act Urgently
VIRUS COULD BE IN YOUR COMPUTER it will become activate on June 1st and will delete all files and folders on the hard drive. No Anti-Virus software can detect it because it doesn't become a VIRUS until 1/6/2001. It travels through the e-mail and migrate to your computer. To find it please follow the following directions:
Go To "START" button
Go to "Find" or "Search"
Go to files and folders
Make sure to search in drive C
Type in; SULFNBK.EXE
Begin Search
If it finds it, highlight it and delete it
Close the dialogue box
Open the Recycle Bin
Find the file and delete it from the Recycle Bin
You should be safe. The bad part is you need to contact everyone you sent ANY e-mail to in the past few months. Many major companies have found this virus on

their computers. Whatever you do, DO NOT open the file.

Bud Frogs Virus Hoax

DANGER!!! VIRUS ALERT!!!

THIS IS A NEW TWIST. SOME CREEPOID SCAM-ARTIST IS SENDING OUT A VERY DESIRABLE SCREEN-SAVER (THE BUD FROGS). BUT IF YOU DOWN-LOAD IT, YOU'LL LOSE EVERYTHING!!!!! YOUR HARD DRIVE WILL CRASH!!

DON'T DOWNLOAD THIS UNDER ANY CIRCUMSTANCES!!!

IT JUST WENT INTO CIRCULATION YESTERDAY, AS FAR AS WE KNOW. BE CAREFUL. PLEASE DISTRIBUTE TO AS MANY PEOPLE AS POSSIBLE...THANX

BELOW IS WHAT THE SCREENSAVER PROGGIE WOULD LOOK LIKE!

File: BUDSAVER.EXE (24643 bytes)
DL Time (28800 bps): <1 minute

Little Girl Dying Chain Letter

LITTLE JESSICA MYDEK IS SEVEN YEARS OLD AND IS SUFFERING FROM AN ACUTE AND VERY RARE CASE OF CEREBRAL CARCINOMA. THIS CONDITION CAUSES SEVERE MALIGNANT BRAIN TUMORS AND IS A TERMINAL ILLNESS. THE DOCTORS HAVE GIVEN HER SIX MONTHS TO LIVE. AS PART OF HER DYING WISH, SHE WANTED TO START A CHAIN LETTER TO INFORM PEOPLE OF THIS CONDITION AND TO SEND PEOPLE THE MESSAGE TO LIVE LIFE TO THE FULLEST AND ENJOY EVERY MOMENT, A CHANCE THAT SHE WILL NEVER HAVE. FURTHERMORE, THE AMERICAN CANCER SOCIETY AND SEVERAL CORPORATE SPONSORS HAVE AGREED TO DONATE THREE CENTS TOWARD CONTINUING CANCER RESEARCH FOR EVERY NEW PERSON THAT GETS FORWARDED THIS MESSAGE. PLEASE GIVE JESSICA AND ALL CANCER VICTIMS A CHANCE.

IF THERE ARE ANY QUESTIONS, SEND THEM TO THE AMERICAN CANCER SOCIETY AT ACS@AOL.COM

Blue Mountain Arts Virus Hoax

"Just received a call from family. A friend of theirs opened a card from Blue Mountain Cards and system crashed. Do not open Blue Mountain Cards until further notice. Virus has infiltrated their system..pass it on....."

Sources

[1] F-Secure URL: www.datafellows.com/hoaxes_new.shtml (access date 23 June 2001)

[2] Rosenberger, Rob "Vmyhts.com", Computer Virus Myths Home Page URL: www.vmyths.com (access date 23 June 2001)

[3] Emery, David. Urban Legends and Folklore, "Virus Hoaxes. URL: http://www.urbanlegends.about.com/science/urbanlegends/cs/virushoaxes/index.htm

[4] Author CIAC. "CIAC Hoax Page", URL: http://hoaxbusters.ciac.org/HBHoaxInfo.html (access date 23 June 2001)

[5] Author Sophos Anti-Virus. "SULFNBK: Virus Hoax… or both?", 30 May 2001 URL:http://www.sophos.com/virusinfo/articles/sulfnbk.html (access date 23 June 2001)

[6] Author CIAC. "Why People Send Chain Letters and Hoax Messages ' URL: http://hoaxbusters.ciac.org/HBHoaxInfo.html#whychain (access date 23 June 2001)

[7] Gordon, Sarah, IBM Anti-Virus Research Center "Hoaxes & Hypes" October 1997,URL: www.research.ibm.com/antivirus/SciPapers/Gordon/HH.html (access date 23 June 2001)

[8] Author CIAC, "The Risk and Cost of Hoaxes' URL: http://hoaxbusters.ciac.org/HBHoaxInfo.html#risk (access date 23 June 2001)

[9] Sullivan, Bob 'Blue Mountain victim of virus hoax' 17 March 1999, www.zdnet.com/zdnn/stories/news/0,4586,2227229,00.html (access date 23 June 2001)

[10] Author Sophos Anti-Virus. "Don't fall for a virus hoax" 23 November 1999, URL: http://www.sophos.com/virusinfo/articles/hoaxes.html#prevent (access date 23 June 2001)

Additional Sources for Information

McAfee, Hoax Home Page URL: http://vil.nai.com/VIL/hoaxes.asp

Trend Micro, Virus Information Centre, URL: http://vil.nai.com/VIL/hoaxes.asp

Symantec, Anti-Virus Center, URL: http://www.symantec.com/avcenter/index.html