Hoax E-Mails Invade MTA Computer Network

By FRANKLIN A. HOLMAN

(Aug. 29, 2003) In the aftermath of last week's real and hoax computer virus attacks, the damage that electronic viruses can cause is beginning to sink in.

"The truth is that as every day goes on, the electronic world that we live in is becoming more dangerous," says Chief Information Officer Elizabeth Bennett.

Earlier today, federal agents arrested Jeffrey Lee Parson, 18, of Hopkins, Minn., on suspicion of creating the computer program responsible for the hoax e-mails and other viruses that have plagued computers – including MTA's – worldwide.

READ ALL ABOUT IT: Computer worm suspect arrested.

Last Thursday, a few MTA employees received the hoax e-mail virus and unknowingly sent it to coworkers. Once the e-mails were sent, ITS realized something was going on in the network.

"Like too many cars on a freeway, all these e-mails slowed things down," says Bennett.

As a little caution is all it takes, here are some tips on how to protect MTA's computer network:

Dos and Don'ts of Computer Viruses

Do...

- Call the ITS Help Desk at ext. 2HELP if you suspect a virus.
- Sign off computers every day so anti-virus updates can be automatically loaded when signing-on.
- Be suspicious of e-mails that ask you to do something that is not of a business nature (for example, the e-mail may ask you to check out an attached file that contains the virus).
- Delete e-mails that are suspicious or forward them to the ITS Help Desk for analysis.

Don't...

- Take matters into your own hands.
- Open attachments from senders you don't know.
- Be a participant in spreading viruses or hoaxes.

When viruses hit, employees can't access the network to do business; consequently, dollars and productivity are lost.

Last week for example, CSX, a major rail transportation company located in the eastern United States, was hit by a virus that crippled its dispatching and signal systems. As a result, passenger and freight traffic was halted for several hours until CSX was able to contain the damage sufficiently to resume service.

"ITS is very diligent in protecting the health of MTA's electronic environment. The payoff … we have been able to dodge the onslaught of virus attacks," says Bennett.

Employees can help avoid virus attacks by keeping an eye on the e-mails they receive. E-mails that could contain viruses may have a vague subject line or no subject line at all. They also are notable for subject lines that don't match the body of the e-mail.

"Looking out for viruses is like a neighborhood watch, says Bennett. "If you want a neighborhood to be safe, everyone has to keep an eye out for problems and report them."

Top

Computer Worm's Suspected Creator Due in Court

(Aug. 29, 2003) CNN reports that Jeffrey Lee Parson, 18, of Hopkins, Minn., is scheduled to appear before a U.S. magistrate in a St. Paul, this afternoon, to answer charges that he created a computer virus that has affected thousands of computers.

Federal officials said the suspect is known online as "teekid."

The damaging viruslike infection, known as "Blaster," LovSan" and "MSBlast," struck the Internet weeks ago. Some experts said it has infected more than 500,000 computers across the globe.

One of the most widespread computer worms this year, the virus does not damage data or programs, but replicates itself repeatedly, eating up computer capacity.

Some versions of the worm began spreading via e-mail attachments with such subject lines as "Thank you," "Re: Details" or "Re: approved."

The fast-spreading Blaster worm took advantage of a flaw in Microsoft's Windows software. Experts urged computer users to install a free patch offered on Microsoft's site since the software giant acknowledged the vulnerability July 16.

Top

Back to Bulletin Board