When Computer Viruses Strike

Based on a True Story—Don't Let this Happen to You!

By Tracey Losco
tracey.losco@nyu.edu

Nora-yin Ulysses is a typical student at NYU: she's a good student, belongs to a sorority, has a part-time job, and surfs the Web—a lot. One day, Nora came home from her job, turned on her computer and started a search on Google, when suddenly, to her surprise, her computer automatically rebooted. She hadn't done anything that would have caused this—it was almost as if the computer had a mind of its own.

When her computer came back up again, Nora resumed her search, only to find that once she started typing, her computer rebooted again! At this point, Nora started feeling frustrated because she had a really important project due for one of her classes, and she needed access to the Web to do research.

Nora picked up the phone and contacted NYU's computer support people at the ITS Client Services Center (1-212-998-3333). When she explained her situation to Joe, the support person who answered her call, he said that it sounded as if her computer had been infected with a virus or someone had broken into it. At this point Nora went into panic mode. "I have important information on my computer! What am I supposed to do now?"

"Do you have backups of your hard drive?" asked Joe.

"What's that?" said Nora.

Joe cringed and said, "That sounds like a "no" to me. Do you make copies of all of your important information onto another computer or onto a disk or CD every month or two?"

Nora answered, "No, why would I do that?"

Joe explained, "So that you would be able to get back your important information if something happened to your computer."

At this point, Nora became even more agitated. "No," she said, "I don't have copies of anything!"

"OK," Joe said, "let's move on. Do you run anti-virus software on your computer and do you keep it up to date?"

"Of course I have anti-virus software," exclaimed Nora, "NYU gives it out for free through NYUHome. I installed it, so how could I get infected?"

"Well," responded Joe, "just installing it isn't enough. You have to keep it updated. And, to do that, you have to set it up to automatically check for and download those updates, called "virus definitions." Otherwise the software is useless. New viruses come out daily, so if you have never updated your software, you aren't protected from any of the new viruses. That's important to remember: your software is only useful if the virus definitions are up to date."

Nora, now both frustrated and scared, replied, "Why didn't anyone tell me this? I never updated the software. I thought that all I needed to do was just install it!"

"OK," Joe said gently, "the Read Me file that comes with the software actually explained this, and we also have it on the ITS website and in our publications, but the important thing right now is that we can get your computer running normally again. Let's check a few other things. What operating system are you using?"

Nora replied, "I'm using a PC with Windows ME."

"OK," said Joe, "When was the last time that you checked for a Critical Update to your operating system?"

"What's a Critical Update?"

"Uh oh," said Joe. Nora's answer told him exactly what had happened. He explained, "Critical Updates are important fixes and patches for your operating system that are released by Microsoft

when a new security risk is discovered. You need to check for them and install them on a regular basis. I'm sorry to say it, but it does sound like your computer was attacked by either a virus or a worm. If you didn't have the most recent virus definitions or any of the Critical Updates installed, your computer was basically an open target."

"Wait," Nora exclaimed, "I thought I heard that NYU scans all the University's e-mail to remove any viruses before they get to us? I've seen some of those messages in my inbox that say that ITS caught and removed an infected message. So, how did this virus get to my computer? Is this NYU's fault?!"

"No," said Joe, "let me explain how NYU checks for viruses. When messages arrive at NYU, before they are forwarded to your account, they are sent through a virus filter which catches most infected messages.[1] That virus filter is updated with new virus definitions when they are released, in the same way that you would update your own anti-virus software. So, just as new viruses may slip past your desktop anti-virus software, some mail infected with extremely new viruses may slip in past the NYU mail filter without being detected."

"Okay, then my main question is, what do I do now?!" asked Nora desperately.

"Well," replied Joe, "first we can try and have you download the most recent virus definitions. You'll need to restart your computer in Safe Mode with Networking, and then you should be able to get the definitions and scan for viruses. In order to restart in Safe Mode you will need to go to the "Start" menu, select "Turn Off Computer," and then select "Restart". This will initiate the restarting process. Then, while your computer is restarting, hold down the F5 key. This will cause the computer to display a list of choices. Use the cursor keys to move up through the list in order to select "Safe Mode with Networking."

You should then be able to download the latest virus definitions for your anti-virus software from the Internet and then scan your computer. If your software does find a virus, be sure to have it remove the virus and repair your computer.

"Then, once you finish with that, you'll need to restart again to get out of Safe Mode so that you can access the Windows Update website to download all of the Critical Updates that are available for your computer. This may take a while because, from what you've already told me, it sounds as if you don't have any of these updates.

Start this by opening Internet Explorer and selecting "Windows Update" in the "Tools" menu. Your computer will be scanned, and then you'll see a list of Critical Updates that have been released for your operating system. If a lot of updates appear, select only three or four at a time to install, otherwise you may run into problems. Keep installing updates and rescanning your computer until no more Critical Updates appear. If your computer is a laptop, make sure you have it plugged into the power outlet when you're doing this because these downloads can sometimes take a while."

Nora asked, "So, does this mean that everything is going to be the way it was before I got infected?"

Joe replied, "Unfortunately, no. What this will do is protect you from any new viruses or worms that may be released. The steps we just talked about might fix the problem, but they might not."

Nora asked, "What if my computer keeps acting strange?"

"Well," Joe replied sadly, "you may need to reformat your computer and start from scratch. Sometimes computers are so badly infected that this is necessary."

"What could I have done to prevent this?" asked Nora.

"Everything that we went over earlier," said Joe, "and be sure to set your anti-virus software to automatically check for new definitions and set your computer to automatically check for Critical Updates. We have instructions for doing that on our website at *http://www.nyu.edu/its/faq/security/.*

"But even if you keep up with your virus definitions and Critical Updates, there is still a chance that you might get infected. With viruses, it's a constant game of 'leap frog.' A new virus is released and computers get infected. Then, anti-virus software manufacturers create a new definition to detect and clean this virus, and, if necessary, Microsoft releases a Critical Update to protect your computer. Then, a new virus or a new strain of the virus appears and the process starts all over again."

"Wow," replied Nora, "I never realized that I needed to keep track of all these things. Is there anything else that I can do?"

"Absolutely," replied Joe. "Don't open any e-mail attachments that you receive unless you are expecting them. Even if you know the sender, give him or her a call and ask if the attachment is legitimate before opening it. Some

1. The graphic on page 20 shows recent NYU virus filter statistics.

viruses are very clever in that they have their own mailing capabilities and they send infected messages to everyone in a person's address book…so other people will think it's coming from someone they trust. You should also keep an eye on the Security Alerts channel on the main page of NYUHome; that will tell you about new viruses to watch out for."

Nora sighed, then said, "Okay, thanks for all of your help, Joe; I'll get started on this right away."

Joe said, "Thanks for your understanding, and take care."

Nora spent the next few hours disinfecting and patching her computer, then setting it up to protect it from getting infected again in the future. In the end, she was one of the lucky ones—she didn't have to reformat her computer and none of her important files were lost.

The moral of this story is that no matter whether you're a student, a staff or faculty member, or an administrator at NYU, or a computer owner anywhere, if you haven't taken the steps explained above, it's only a matter of time until you find yourself in Nora's predicament…and you might not be so lucky! For more information about how to protect your computer and NYU's network, see the resources listed below.

Additional Resources

- The ITS Computer and Network Security website: *http://www.nyu.edu/its/security/*
- Computer security FAQs, including instructions on how to help secure your Windows computer: *http://www.nyu.edu/its/faq/security/*
- ITS Computer and Network Security Awareness Month: *http://www.nyu.edu/its/securityawareness/*
- Most NYU community members can download a copy of Symantec AntiVirus through the Files tab of NYUHome. Log in with your NetID and password at *http://home.nyu.edu,* click the Files tab, then select the correct version for your computer.
- The Security Alerts Channel in NYUHome (*http://home.nyu.edu/):* the channel appears under the E-mail channel on the main page that opens.
- ITS classes on viruses and security: *http://www.nyu.edu/its/classes/*
- Windows Update: *http://windowsupdate.microsoft.com*
- Symantec: *http://www.symantec.com/*
- Center for Internet Security: *http://www.cisecurity.org*
- Stay Safe Online: *http://www.staysafeonline.info/*

Tracey Losco is a Network Security Analyst in ITS Network Services.