# The Dangers of Computer Viruses: Implications for 21st Century Educators

By: Rachel Tewari, Jamie Wanty and Elizabeth Stolberg

Today we are living in the 21st century, an age in which the education field is becoming increasingly dependent upon computer technology. From K-12 primary and secondary schools to colleges and universities, educators rely on computer technology to carry out various monotonous tasks with relative ease. Tasks such as formatting lesson plans, distributing learning materials, providing a means of contact between students and teachers, recording attendance, computing grades, conducting research, etc. However, risks also present themselves with this increased use of computer technology; computer viruses: programs written specifically to cause mischief or damage to computer systems and operations (Abrams and Lockard 380), become a significant danger for all educators and learners of the 21st century. Thus, teachers and students from all fields need to be better equipped with knowledge about preventing dangers such as computer viruses. Teachers and students alike should be aware of what computer viruses are and what they are capable of then measures can be taken to protect computers from virus infections.

A computer has oft been likened to the human body; computer viruses have thus been given their title because, in many ways, they share similarities of infecting biological viruses that target the human body. A computer virus passes from computer to computer just as a biological virus travels from human to human, the former causing electronic infection, the latter causing physical

infection. A biological virus is not inherently self-replicating; it is merely a scrap of DNA inside a protective jacket. In order to spread, a biological virus must inject its own DNA into a cell and thus reproduce itself by using the *cell's* equipment. Only then can the virus spread and cause damage. Similarly, a computer virus must piggyback on top of an existing program or document in order to run and infect the computer. However, once it is running, it is capable of both spreading and infecting other programs and documents, just like a virus in the human body (Brain 1).

Also like biological viruses, computer viruses manifest themselves with a series of symptoms. When humans suffer from the flu virus they may feel feverish, achy or perhaps sick to their stomach. They won't feel like functioning at 100 percent. Similarly, according to Software Engineer and computer programmer Benjamin Tewari, if your computer is infected by a computer virus:

> Your computer is going to slow down…some [programs] that normally work will suddenly stop working or [programs] will work sporadically…Unintelligible changes [in files will occur which] a program can read. [These changes are] usually not going to make much sense for a human to read. (Tewari)

To hear this quote, click on the following icon: 

The most common forms of electronic infection are viruses, e-mail viruses, worms and Trojan horses. However they are often lumped into the broad category of viruses and called as such. As previously mentioned, a virus is a piece of software which piggybacks upon another existing program in order to spread throughout the infected computer and others connected to the same network. A virus attached to a program such as Excel would be a small piece of

code embedded within the program. When the Excel program is running, the virus would load itself onto the memory of the computer and then reproduces itself, causing harm and chaos to the infected computer and others connected to the same network. In this manner viruses add, delete and modify files, deny access to users, reformat hard disks and/or reproduce themselves until they take up so much memory and cause the entire system to crash (Abrams and Lockard 381). As educators and their students are constantly opening and using programs, such as Microsoft Word, Excel and Power Point, in order to carry out various tasks, a virus-infected program could cause serious harm to themselves as well as others. According to Tewari because of the increased use by students of the:

> Computer labs in schools…and the Internet…it's important that [students] know what computer viruses are and how to avoid them. You could very easily bring down… the whole computer system at the school by downloading or opening the wrong file [such as a virus program]. (Tewari)
>
> To hear this quote, click on the following icon: 

Computer viruses in a school or University's computer network could also erase or alter student and teacher files and records which could be very dangerous as well as illegal.

An email virus attaches itself to emails, usually reproducing by automatically mailing itself to everyone on the victim's mailing list. The "Melissa" virus in March of 1999 was one such email virus, spreading in Microsoft word documents sent via email. The virus was created by somebody as a Word document and uploaded to an Internet Newsgroup site. Those who downloaded

the document and opened it triggered the virus. The virus would then send the document to the first 50 people in the victims address book. Because the email also included a friendly message and came from a source many people trusted, new victims were created as the people opened the document and thus furthered the spread of the “Melissa” virus infection. As a result, the “Melissa” virus became the fastest-spreading virus unforeseen, causing many businesses to shut down their email systems (Brain 4). Teachers and students keep contact with one another sometimes as often as weekly via email. Email viruses could thus be detrimental if contracted by a teacher and then against the teacher’s will, it is further passed on to students, destroying and altering information and altogether destroying the communication system.

Worms are computer programs that have the ability to duplicate themselves from machine to machine. They typically affect machines through computer networks: once in the network, the worm can copy itself very quickly (Brain 2). “Code Red” is one such worm which wreaked much havoc in 2001. This worm was able to damage and replace web pages on infected servers with a page that declared “Hacked by Chinese” (Brain 3). If a teacher distributes exercise materials or working documents among students electronically via the school or University’s network system, if a worm is contracted, all of the work could be destroyed or altered, causing hassles for both the teacher and his/her students. Students also, who create or post work electronically would be much effected if a worm made it’s way into their school’s computer network.

A Trojan horse is a computer program which claims to do one thing, however, when it is run, does a different thing entirely and causes damage. Trojan horses are capable of erasing the hard disk; however they have no way of replicating themselves automatically (Brain 1).

The teachers and students of today are often not computer programmers and are therefore less knowledgeable concerning the tricks and subtleties of computer viruses. Thus, the teachers and students of the 21st century need to be brought to a heightened awareness of the possibility of contracting a computer virus anytime they use a computer and the best options of protecting their computer.

In order to avoid the hassle of computer virus infection, Marshall Brain suggests practicing safe computing. Safe computing, according to Brain, involves avoiding opening suspicious programs and files from unknown sources, and purchasing commercial software programs that are distributed through CD-ROMs rather than the Internet. Floppy disk booting should also be disabled, which most computers today will allow the user to do. This process will insure that no boot sector viruses, viruses which infect the boot sector of the computer which is a fundamental part of its operating system, infect the computer. By putting its code into the boot sector, a virus can guarantee that it gets executed (Brain 4). Users could also set up a firewall on their computer in order to prevent viruses. Tewari defines a firewall as:

> Something that you can put in place on your computer… to disallow other computers [on the network] from running applications on your computer…it's helpful when [using] the Internet…[and] can be very useful

> in preventing viruses [because]…this limits any computer on the outside world from connecting with your computer. (Tewari)
>
> To hear this quote, click on the following icon: 

Firewalls are often set up by the administrator of the computer network one's computer is connected to, however there are also firewall programs available through the Internet and free for everyone to download. Aside from being aware of the dangers of computer viruses and the risks of contracting one, another important tip for all computer users, especially educators and their students, is the implementation of virus protection software.

Anti-virus software is one of the easiest and best ways of protecting a computer against viruses. Tewari explains that an anti-virus program:

> Monitor[s] the processes running on your computer, so it can tell if there's a new process… it alerts the user to the process that's running…kills the process and gives the user the option of deleting that process in case it is a virus. You can set up daily or weekly scans [with this software] so it will scan your *entire* computer for suspicious files. (Tewari)
>
> To hear this quote, click on the following icon: 

Norton and McAfee are two reputable anti-virus software brands, according to Tewari, equipped with settings on how often the program runs a virus scan. While many people choose to run weekly scans, for the inexperienced user, daily scans may even be better. There are also many anti-virus programs available on the Internet to download; however, their credibility may require more investigation. While anti-virus software is important based on the protection it provides for computer users, it is also important to keep the software updated. Viruses can be rewritten in order to bypass anti-virus software; thus anti-virus

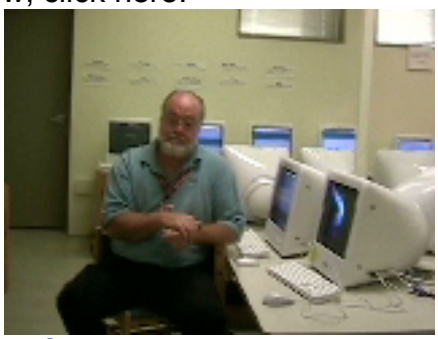
software must be constantly updated in order to successfully protect. If it is not updated, the software is useless.

Computer viruses are a common problem. Society is heavily built upon computer systems so is the whole of the education environment. As such, the implications for 21st century educators concerning viruses are strong as Tewari suggests:

> [K-12 educators and their students] should definitely be educated as to computer viruses…viruses these days are very disguised and the average computer user might not realize that [they're] installing a virus on [their] computer…a lot of them get sent as attachments on emails, if you're not educated… it's very easy to get one on your computer…in the education system so [much] personal and confidential information can be compromised, [altered or destroyed], if you get a virus. (Tewari)
>
> To hear this quote, click on the following icon:

Elementary school Computer teacher and technology support Jeff Flynn advocates awareness as the primary defense against computer viruses:

> Being aware of [them]…and knowing whether you're vulnerable…I think if anyone operates a Windows machine they need to have Spy-ware and Ad-Ware programs…I run three simultaneously…people need to know about [keeping anti-virus software updated]…[viruses] are so prevalent and destructive that machines choke. (Flynn)
>
> To see the interview, click here:



(Quicktime Movie)

Tewari also suggests that knowledge is the best defense:

> Education to users is the biggest thing. Users really need to be educated concerning the risks of viruses and the different malicious programs that can be run computers… if you're not educated, you may unintentionally download things and cause many problems...(Tewari)
>
> To hear this quote, click on the following icon: 

Even though computer viruses are dangerous, knowledge is power. If educators and their students have sufficient knowledge about computer viruses, they can take precautions so as not to be caught unaware when the faceless enemy strikes.

## Work Cited


Abrams, Peter D. and James Lockard. Computers for Twenty First Century Educators. Boston: Allyn and Bacon, 2004.

Aycock, J. and K. Barker. "Viruses 101." 1-8. Department of Computer Science, University of Calgary. ERIC. EMU library, 19 Oct. 2005.

Baker, Monya. "Kill the Bots!" Technology Revolution. 108 (1998): 1-3.

Brain, Marshall. "How computer Viruses Work." 1-7 Howsuffworks Home Page. 2005. <http://www.howstuffworks.com/virus.htm>

Flynn, Jeff. Personal Interview. 28 Oct. 2005.

Kaeli, David and Micha Moffie and Derek Uluki. "Characterizing Antivirus Workload Execution" 1-12.

Tewari, Benjamin. Personal Interview. 30 Oct. 2005