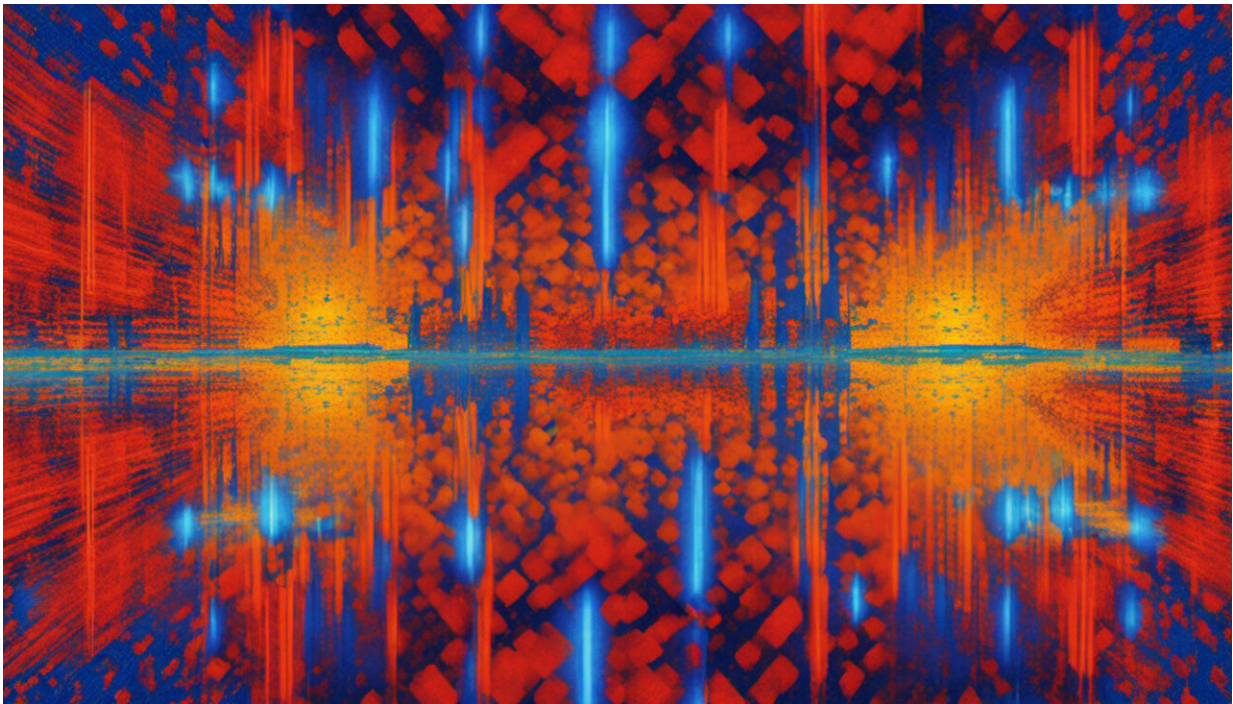


# Probing Question: What are computer viruses and where do they come from?

July 20 2006

---



Credit: AI-generated image ([disclaimer](#))

Just as the flu can spread from human to human, a well-engineered computer virus can transfer from machine to machine--with a bad outbreak affecting tens of thousands, or even millions, of systems. Indeed, in a high-tech age, the potential for a large-scale mechanical meltdown makes computer viruses almost as much of a threat as the

biological kind.

Given the havoc a virus can wreak, its makeup is surprisingly simple. "Virus writing is very basic," says Lisa Johansen, a doctoral candidate in computer science and engineering at Penn State. "There are websites galore which explain how to hack into a computer." These sites include both specific lines of system-jamming code and descriptions of which vulnerabilities to target. With these resources, says Johansen, creating a virus definitely "doesn't require a college education."

Why would someone deliberately write a bad code?

"Writing a computer virus is an intentional action," says Johansen. Thrill-seeking teenagers may find out how easy it is to write harmful code and take it up as their outlet for rebellion. Techies may turn virus-writing into a sport. Entire hacking communities are spawned to see who can produce the most destructive code. The same incentives are behind street-racing or graffiti, Johansen explains: the adrenaline rush of defying authority, the promise of "prestige or respect within a certain group."

Beyond the bored kids and the ego-driven super-hackers, there are also people who write viruses by accident. Johansen says many are simply curious about their ability to affect the lives of others. They might write snippets of code to see how they will spread, she explains, not intending to do harm. "They create something they didn't mean to create, and soon, they're responsible for a virus which they can no longer control."

"A virus is a self-propagating piece of software." Johansen adds. Malware is the blanket term which refers to any malicious software that runs on a computer. It includes viruses, worms, spyware and trojan horses, among many others. A worm is so named because of its ability to burrow into a system and spread on its own. Spyware accesses a computer, obtains information from the system and sends it back to the

spyware's creator or a central server. A Trojan Horse is software that looks harmless, but on opening, infects the targeted computer.

These are only a few examples of malware, Johansen notes. Malware can be either active or passive. An active virus, she explains, will cause an obvious malfunction like the deletion of files from the hard drive or even a total crash. "A passive action," on the other hand, "is not necessarily noticed by the user." Spyware, for example, relies on being undetectable to collect a computer's information without the user knowing. In addition to invading the user's privacy, however, it may slow the system down. "All malware," Johansen says, "take up both system and network resources," so even the least imposing kind will have some effect on a computer's activity.

Is there a malicious hacker out there on the verge of releasing the most paralyzing worm yet? Is there a precocious 11-year-old dedicating his summer to the creation of a crippling Trojan Horse? Johansen has good news and bad.

First, the bad: "New viruses are being created all the time," she says, "and protecting computers against them is as difficult as protecting a human against the flu." To make things worse, unprotected and out-of-date systems continue to allow the spread of viruses over the Internet, hazarding protected systems as well.

Now for the good: Virus protection software is readily available and increasingly effective. Today, patches, firewalls, and antivirus programs can prevent, scan for, or remove many viruses that might otherwise end a session of web-surfing in an unexpected crash.

Aside from taking advantage of anti-virus software, Johansen says the most effective defense against viruses is a reasonable level of caution when accessing the 'net. "Be aware," she says "that the Internet is not a

safe place, and be careful when using its resources. Knowing that something's out there is the first step to protecting against it."

Source: By Lauren Clark, Research/Penn State

Citation: Probing Question: What are computer viruses and where do they come from? (2006, July 20) retrieved 23 April 2024 from <https://phys.org/news/2006-07-probing-viruses.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.