Framed for child porn -- by a PC virus

November 8 2009, By JORDAN ROBERTSON , AP Technology Writer

In this June 13, 2008 photo, Michael and Robin Fiola sit for a photo with the forensics report, at left, that exonerated Michael in their North Scituate, R.I. home. The Fiolas said recently, they have health problems from the stress of the case. They say they've talked to dozens of lawyers but can't get one to sue the state, because of a cap on the amount they can recover.(AP Photo/The Boston Herald, Matthew Healey) BOSTON GLOBE OUT; METRO BOSTON OUT; MAGS OUT

(AP) -- Of all the sinister things that Internet viruses do, this might be the worst: They can make you an unsuspecting collector of child pornography.

Heinous pictures and videos can be deposited on computers by viruses - the malicious programs better known for swiping your credit card numbers. In this twist, it's your reputation that's stolen.

Pedophiles can exploit virus-infected PCs to remotely store and view their stash without fear they'll get caught. Pranksters or someone trying

to frame you can tap viruses to make it appear that you surf illegal Web sites.

Whatever the motivation, you get child porn on your computer - and might not realize it until police knock at your door.

An Associated Press investigation found cases in which innocent people have been branded as pedophiles after their co-workers or loved ones stumbled upon child porn placed on a PC through a virus. It can cost victims hundreds of thousands of dollars to prove their innocence.

Their situations are complicated by the fact that actual pedophiles often blame viruses - a defense rightfully viewed with skepticism by law enforcement.

"It's an example of the old 'dog ate my homework' excuse," says Phil Malone, director of the Cyberlaw Clinic at Harvard's Berkman Center for Internet & Society. "The problem is, sometimes the dog does eat your homework."

The AP's investigation included interviewing people who had been found with child porn on their computers. The AP reviewed court records and spoke to prosecutors, police and computer examiners.

One case involved Michael Fiola, a former investigator with the Massachusetts agency that oversees workers' compensation.

In 2007, Fiola's bosses became suspicious after the Internet bill for his state-issued laptop showed that he used 4 1/2 times more data than his colleagues. A technician found child porn in the PC folder that stores images viewed online.

Fiola was fired and charged with possession of child pornography, which

carries up to five years in prison. He endured death threats, his car tires were slashed and he was shunned by friends.

Fiola and his wife fought the case, spending $250,000 on legal fees. They liquidated their savings, took a second mortgage and sold their car.

An inspection for his defense revealed the laptop was severely infected. It was programmed to visit as many as 40 child porn sites per minute - an inhuman feat. While Fiola and his wife were out to dinner one night, someone logged on to the computer and porn flowed in for an hour and a half.

Prosecutors performed another test and confirmed the defense findings. The charge was dropped - 11 months after it was filed.

The Fiolas say they have health problems from the stress of the case. They say they've talked to dozens of lawyers but can't get one to sue the state, because of a cap on the amount they can recover.

"It ruined my life, my wife's life and my family's life," he says.

The Massachusetts attorney general's office, which charged Fiola, declined interview requests.

At any moment, about 20 million of the estimated 1 billion Internet-connected PCs worldwide are infected with viruses that could give hackers full control, according to security software maker F-Secure Corp. Computers often get infected when people open e-mail attachments from unknown sources or visit a malicious Web page.

Pedophiles can tap viruses in several ways. The simplest is to force someone else's computer to surf child porn sites, collecting images along the way. Or a computer can be made into a warehouse for pictures and

videos that can be viewed remotely when the PC is online.

"They're kind of like locusts that descend on a cornfield: They eat up everything in sight and they move on to the next cornfield," says Eric Goldman, academic director of the High Tech Law Institute at Santa Clara University. Goldman has represented Web companies that discovered child pornographers were abusing their legitimate services.

But pedophiles need not be involved: Child porn can land on a computer in a sick prank or an attempt to frame the PC's owner.

In the first publicly known cases of individuals being victimized, two men in the United Kingdom were cleared in 2003 after viruses were shown to have been responsible for the child porn on their PCs.

In one case, an infected e-mail or pop-up ad poisoned a defense contractor's PC and downloaded the offensive pictures.

In the other, a virus changed the home page on a man's Web browser to display child porn, a discovery made by his 7-year-old daughter. The man spent more than a week in jail and three months in a halfway house, and lost custody of his daughter.

Chris Watts, a computer examiner in Britain, says he helped clear a hotel manager whose co-workers found child porn on the PC they shared with him.

Watts found that while surfing the Internet for ways to play computer games without paying for them, the manager had visited a site for pirated software. It redirected visitors to child porn sites if they were inactive for a certain period.

In all these cases, the central evidence wasn't in dispute: Pornography

was on a computer. But proving how it got there was difficult.

Tami Loehrs, who inspected Fiola's computer, recalls a case in Arizona in which a computer was so "extensively infected" that it would be "virtually impossible" to prove what an indictment alleged: that a 16-year-old who used the PC had uploaded child pornography to a Yahoo group.

Prosecutors dropped the charge and let the boy plead guilty to a separate crime that kept him out of jail, though they say they did it only because of his age and lack of a criminal record.

Many prosecutors say blaming a computer virus for child porn is a new version of an old ploy.

"We call it the SODDI defense: Some Other Dude Did It," says James Anderson, a federal prosecutor in Wyoming.

However, forensic examiners say it would be hard for a pedophile to get away with his crime by using a bogus virus defense.

"I personally would feel more comfortable investing my retirement in the lottery before trying to defend myself with that," says forensics specialist Jeff Fischbach.

Even careful child porn collectors tend to leave incriminating e-mails, DVDs or other clues. Virus defenses are no match for such evidence, says Damon King, trial attorney for the U.S. Justice Department's Child Exploitation and Obscenity Section.

But while the virus defense does not appear to be letting real pedophiles out of trouble, there have been cases in which forensic examiners insist that legitimate claims did not get completely aired.

Loehrs points to Ned Solon of Casper, Wyo., who is serving six years for child porn found in a folder used by a file-sharing program on his computer.

Solon admits he used the program to download video games and adult porn - but not child porn. So what could explain that material?

Loehrs testified that Solon's antivirus software wasn't working properly and appeared to have shut off for long stretches, a sign of an infection. She found no evidence the five child porn videos on Solon's computer had been viewed or downloaded fully. The porn was in a folder the file-sharing program labeled as "incomplete" because the downloads were canceled or generated an error.

This defense was curtailed, however, when Loehrs ended her investigation in a dispute with the judge over her fees. Computer exams can cost tens of thousands of dollars. Defendants can ask the courts to pay, but sometimes judges balk at the price. Although Loehrs stopped working for Solon, she argues he is innocent.

"I don't think it was him, I really don't," Loehrs says. "There was too much evidence that it wasn't him."

The prosecution's forensics expert, Randy Huff, maintains that Solon's antivirus software was working properly. And he says he ran other antivirus programs on the computer and didn't find an infection - although security experts say antivirus scans frequently miss things.

"He actually had a very clean computer compared to some of the other cases I do," Huff says.

The jury took two hours to convict Solon.

"Everybody feels they're innocent in prison. Nobody believes me because that's what everybody says," says Solon, whose case is being appealed. "All I know is I did not do it. I never put the stuff on there. I never saw the stuff on there. I can only hope that someday the truth will come out."

But can it? It can be impossible to tell with certainty how a file got onto a PC.

"Computers are not to be trusted," says Jeremiah Grossman, founder of WhiteHat Security Inc. He describes it as "painfully simple" to get a computer to download something the owner doesn't want - whether it's a program that displays ads or one that stores illegal pictures.

It's possible, Grossman says, that more illicit material is waiting to be discovered.

"Just because it's there doesn't mean the person intended for it to be there - whatever it is, child porn included."