

Cybercrime Victimization

A pilot Computer Security Survey of U.S. businesses found that nearly 75 percent of responding companies had detected at least one incident of cybercrime in 2001. Over half of the victimized businesses experienced multiple incidents of computer virus, denial of service, and fraud. (Bureau of Justice Statistics. 2004. *Cybercrime Against Businesses*. Washington, D.C.: U.S. Department of Justice.)

In the same survey, 68 percent of the companies reported financial effects due to cybercrime, resulting in \$61 million in losses and recovery costs. Estimated recovery costs for computer viruses were nearly \$22 million. Costs from computer fraud were an estimated \$18 million and denial of service caused losses of approximately 14 million. (Ibid.)

The most common forms of cybercrime detected by companies in 2001 were computer virus infections (64.1 percent), denial of service attacks (25.3 percent), and vandalism or sabotage (18.7 percent). Hacking and spamming are other common breaches of computer security that occur with frequency. (Ibid.)

Between March 1998 and October 2003, the CyberTipline operated by the National Center for Missing and Exploited Children received a total of 140,593 reports of child pornography, and 2,048 reported cases of child prostitution. There were 908 cases of child sex tourism, and 5,522 cases of child molestation (not in the family). Also, there were 9,377 reported cases of online enticement.

(National Center for Missing and Exploited Children, "Cybertipline Fact Sheet." http://www.ncmec.org/en_US/documents/cybertipline_factsheet.pdf. Accessed September 21, 2004.)

Working to Halt Online Abuse (WHOA) received 198 reports of cyberstalking in 2003: 35 percent began as e-mail communications, 16.5 percent from a message board conversation, 17 percent from instant messaging, 7.5 percent from a website, and eight percent from chat rooms. (Working to Halt Online Abuse. "Online Harassment Statistics." <http://www.haltabuse.org/>. Accessed September 23, 2004.)

A survey of the cyberstalked victims reporting to WHOA between 2000 and 2003 reveals that over 75 percent are Caucasian; 78 percent are women, and 39 percent are between the ages of 18 and 30 years old. (Ibid.)

In 2003, 52.5 percent of the cyberstalkers reported to WHOA were male, 38 percent were female and in 9.5 percent of the cases, the gender was unknown. (Ibid.)

According to the North American Securities Administrators Association (NASAA), the most recent figures show cybercriminals stole \$122 million from victims through Internet fraud in 2002.

(North American Securities Administrators Association. "January 14, 2004, Press release." http://www.nasaa.org/nasaa/scripts/pre_display.asp?rcid=244. Accessed September 21, 2004.)

The FBI's Internet Fraud Complaint Center received 48,252 complaints in 2002 that were referred to enforcement agencies. The Center also received an additional 37,000 complaints that did not constitute fraud, but were cases of unsolicited e-mail, illegal child pornography, computer intrusions, as well as many other violations of the law.

(Federal Bureau of Investigation's Internet Fraud Complaint Center. <http://www.ifccfbi.gov/>. Accessed September 28, 2004.)

The total costs of Internet fraud cases reported to the FBI's Fraud Complaint Center was \$54 million in 2002. The victims of the Nigerian Letter fraud averaged \$3,864, Internet identity theft averaged a \$2,000 loss, and victims of check fraud averaged a \$1,100 loss. (Ibid.)

PRESENTED AS A PUBLIC SERVICE BY: