Computer Crime: Computer as an Instrument of Crime
(October 2009)

Definition

Computers can be utilized as an instrument or tool to facilitate criminal activity. As defined by the U.S. General Accounting Office, Office of Special Investigations, computers can be “used as tools to commit traditional offenses.” This means that the functions specific to computers, such as software programs and Internet capabilities, can be manipulated to conduct criminal activity.

How It Happens

As computers proliferate at work and home, there are more opportunities for criminals to interact with law-abiding citizens. The computer offers relative anonymity to criminals who use it to commit crimes. With the advances in technology and user friendly software, a criminal’s computer knowledge may consist of only the most basic skills. Consequently, for even the least sophisticated of computer users, a single computer provides a medium for conducting an array of crimes. Criminals can use the computer to initiate and maintain contact with victims via the Internet, to conduct fraudulent financial transactions, to illegally replicate and distribute legitimate products or information, or to obtain confidential, personal information.

Computer crimes frequently overlap each other during their commission.

The computer is a doorway to a world of opportunity on the Internet that is not policed by any single law enforcement agency. The potential for financial gain coupled with the ease of commission has resulted in many crimes via the Internet that previously occurred via mail or over the telephone. According to the U.S. Department of Justice, “the same types of fraud schemes that have victimized consumers and investors for many years before the creation of the Internet are now appearing on-line (sometimes with particular refinements that are unique to Internet technology).” Examples of on-line crimes include fraudulent marketing schemes, on-line auctions, work-at-home schemes, gambling operations, and Spam. The Internet provides criminals with a quick and efficient means of communicating large quantities of information to a wide range of victims via chat rooms, e-mail, message boards, or Web sites. In addition, the Internet allows for anonymity whereby a victim may only know the offender by their e-mail address or Web site.

For example, on-line banking has created new opportunities for con-artists and money launderers. Criminals can gather confidential personal information by spoofing a valid Web site, creating a deceptive Web site, or even touting a legitimate sounding scam in a chat room. Once a criminal is in possession of detailed bank account information, unauthorized transfers of money can occur in one quick transaction. Offshore money laundering also provides a lucrative opportunity for white collar criminals, organized crime groups, and terrorists. As reported by the U.S. Department of the Treasury in the 2001 National Money Laundering Strategy, “criminals target foreign jurisdictions with liberal bank secrecy laws and weak anti-money laundering regulatory regimes as they transfer illicit funds through domestic and international financial institutions often with the speed and ease of faceless Internet transactions.” The International Monetary Fund organization summarizes the issue by stating that “various forms of financial system abuse
may compromise financial institutions’ and jurisdictions’ reputations, undermine investors’ trust in them, and therefore weaken the financial system.8

The illegal reproduction and distribution of intellectual property and physical property can be effortlessly facilitated with a computer. From the piracy of electronic videos, books, music, and software to the cloning of cellular telephones, a single computer can function as a replication and distribution center. Individuals who knowingly buy or download pirated intellectual property (such as recorded music) perpetuate the problem. Victims include both individuals who created the intellectual property and the companies who have purchased exclusive distribution rights and have that privilege taken from them by unauthorized “pirates.” The Better Business Bureau Web site specifies a variety of methods in which Internet piracy may be facilitated: “Peer-to-Peer (P2P), E-mail, News Groups, Internet Relay Chat (IRC), Mail Order/Auction Sites, File Transfer Protocol (FTP), Circumvention Information, Site Links, Direct Links, Remote Links, “Elite” Activities”.9

There is an incredibly large amount of personal information that is appropriated illegally by criminals. Personal information, such as a social security number, mother’s maiden name, bank PIN number, or photograph, has become a marketable commodity. Such personal information is crucial to the infrastructure of many businesses that deal in information. By co-opting your name, credit card number, or some other piece of your personal information for their own use, criminals can conduct identity theft.10 One method for acquiring personal information occurs when an employee in a position of trust steals confidential information from clients by accessing electronic files. Another means of attaining information is by illegally replicating credit card numbers with a computer during the course of a legitimate business transaction. Often victims of identity theft may never know the person who appropriated their information.

Two additional areas of computer crime are child pornography and cyberstalking. Individuals trafficking in child pornography on the Internet can create, access, sell, replicate, and transmit graphics with their computer. According to Mark Pollitt, FBI Computer Analysis Response Team Unit Chief, over half of their work falls into two categories: traditional white-collar crime and child pornography.11 Cyberstalkers use the Internet to pursue and harass Internet users with on-line insults, taunts, or threats. The interactive nature of on-line chat rooms provides an ideal opportunity for anonymously posting intimidating and menacing statements directly to a participant. The organization WHOA, Working to Halt On-line Abuse, compiled statistics that indicate e-mail and chat rooms were the first and second most common forums in which harassment began.12 In some cases, offenders use information obtained in chat rooms to physically stalk or assault the victim.

**Cost / Statistics**

There is no precise cost estimate for computer crimes, but several surveys exist which indicate the severity of the problem.

The Computer Security Institute has conducted an annual survey of computer security practitioners. Twenty percent of respondents in 2002 acknowledged theft of proprietary information. In addition, the 2002 survey reported that total losses of the 41 respondents were $170,827,000. The increase in the financial loss is explained by Naomi Fine of Pro-Tec Data as being due to “1) increased recognition that information has value and 2) increases in perceived value of information.”13

Complaints filed with the Federal Trade Commission’s (FTC) Consumer Sentinel indicated that identity theft comprised 39 percent of the 635,173 complaints filed in 2004.14 Internet services and computer complaints (consisting of undisclosed Web site charges and problems with computer software and equipment) totaled 6 percent of all the complaints filed with the FTC.15

In a survey released by the Business Software Alliance in the spring of 2002, “85 percent of users surveyed agreed that intellectual property rights must be protected so companies continue to invest in research and development.”16 However, the survey of 1,026 Internet users found that “nearly half have downloaded commercial software at some time and that 81 percent of them have failed to pay for all the copies they
made.” In 2001, International Planning and Research completed a study of piracy in the U.S. by state and the implied economic impacts. The estimates for the total packaged software industry include total retail dollar losses of $8.3 billion, total wage and salary losses of $5.7 billion, and total tax losses of $1.6 billion. Adobe Software's anti-piracy statements summarize the implications of the piracy problem: “Piracy stifles innovation. The money spent to combat software piracy, and the revenues lost to piracy, could be spent on research and development.”

**High Profile Examples/ Case Studies**

- Researchers at Sunbelt Software discovered an identity theft ring during the audit of the “CoolWebSearch” program, in which systems were placing callbacks to remote servers distributing sensitive information from personal computers. Upon discovery they found key logger transcript files of chat sessions, usernames, passwords and bank account information being uploaded to the server. According to Sunbelt's president, Alex Eckelberry, this was the work of a “massive identity theft ring,” which used keystroke loggers to obtain information that could be used to create fake online identities. The files held login information connected to a business bank account containing more than $350,000 as well as the names and addresses of the people owning the accounts. Sunbelt alerted the account owners, who appeared to be at risk of losing a considerable amount of money.

- In March of 2007, Robert Soloway, known as the “Spam King,” was arrested by federal authorities on 35 charges of fraud, money laundering, and identity theft. Soloway's criminal activities involved hijacking computers from unsuspecting customers and using them to disseminate Spam that advertised his fraudulent marketing services. Over a four year period, Soloway sent tens of millions of Spam messages using the hijacked computers, or zombies. He was able to elude positive identification by using 50 different web sites to foist his fraudulent services. The charges brought against Soloway mark the first time federal prosecutors have used identity theft laws to prosecute a Spam case.

- In 2002, the State of New York sued the bulk e-mailer MonsterHut Inc. for sending more than 500 million unsolicited commercial e-mail messages to consumers. The company falsely claimed that consumers had requested the e-mail that advertised a variety of goods and services. The unsolicited e-mails included, among other ads, promotions for natural marriage enhancers and weight loss products. New York sought a court order to stop MonsterHut from falsely representing the source of its e-mail and to force it to reveal how it obtained consumer e-mail addresses. The court order also required MonsterHut to pay fines and cover court costs.

- In 2002, the Federal Trade Commission ended an on-line scam designed to subject Internet users to pop-up ads. The scam, run by John Zuccarini, involved registering Internet domain names that were misspelled versions of popular, legitimate domain names and then redirecting Internet users who inadvertently accessed the sites. For example, Mr. Zuccarini registered 15 variations of CartoonNetwork.com and 41 variations of pop star Britney Spears' name involving more than 5,500 Web site addresses. The court order permanently bars Zuccarini from engaging in this activity in the future without the permission of the user.

**The Response / Current Efforts**

Developed by the Department of Justice, the National Cybercrime Training Partnership (NCTP) provides guidance and assistance to local, state, and federal law enforcement agencies in an effort to ensure that the law enforcement community is properly trained to address electronic and high technology crime. The NCTP's vision is to develop a 21st century paradigm for law enforcement training in electronic and high-technology crime which will be available to multiple types of law enforcement personnel (e.g., investigators, prosecutors, and specialists), decentralized to reach law enforcement personnel in all geographic regions and all levels of government, and continuous to remain current with the rapidly changing technology and associated threat.
The Business Software Alliance (BSA) is an international association of corporations whose mission is to educate computer users on software copyrights and cyber security, advocate public policy that fosters innovation and expands trade opportunities, and fight software piracy. The BSA includes corporate members such as Adobe Systems, Microsoft, and Symantec and a policy council that includes corporations such as Dell, IBM, and Novell.\(^{26}\)

There are several prevention methods for individuals to avoid computer crime victimization. The most important step is to stay informed about current crime trends. On-line news sources provide timely crime information. Several of the surveys mentioned above are updated annually with trend information. In addition, government and private Web sites provide specific prevention tips for different types of crime. Also, a general awareness of accepted business practices in an industry, such as securities and investments, provides a critical frame of reference for conducting on-line transactions. Often, crime victims who relied upon false product or service information provided by the offender could have found truthful information with a little independent research. Finally, implementing encrypted on-line communications and utilizing secure Web sites will also help protect individuals from becoming victims of a computer crime.

**Additional Resources**

- U.S. Customs - http://www.customs.ustreas.gov/xp/cgov/home.xml
- Working to Halt Online Abuse - http://haltabuse.org/
- Business Software Alliance - http://bsa.org/

*Maintenance and revisions:* Rodney Huff, NW3C Research Assistant
Endnotes


