Vulnerability to Internet Crime and Gender Issues

Tejaswini Herath
State University of New York at Buffalo, USA

S. Bagchi-Sen
State University of New York at Buffalo, USA

H. R. Rao
State University of New York at Buffalo, USA

INTRODUCTION

A tremendous growth in the use of the Internet has been observed in the past two decades. More than 75% of Americans participate in online activities (University of Southern California Annenberg School Center for the Digital Future, 2004) such as e-mail, Web browsing, working from home, accessing news stories, seeking information, instant messaging, using the Internet in lieu of the library for school work, playing games, and managing personal finance. For professionals, the Internet is an important medium for networking and building social capital. However, along with all positive impacts, there are also negative outcomes. One such negative outcome includes Internet crimes. Dowland, Furnell, Illingworth, and Reynolds (1999) state that "with society's widespread use of and, in some cases, reliance upon technology, significant opportunities now exist for both mischievous and malicious abuse via IT systems" (p. 715).

Internet crimes (cyber crimes) consist of specific crimes dealing with computers and networks (such as hacking, spreading of viruses, and worms) and the facilitation of traditional crime through the use of computers on the Internet (such as child pornography, hate crimes, telemarketing/Internet fraud). This article focuses on Internet crimes, especially those affecting individual users, and offers a discussion of issues regarding Internet crimes and gender.

BACKGROUND

Cyber Crime

Computer crimes can be categorized by who commits them and what their motivation might be (e.g., professional criminals looking for financial gain, angry ex-employees looking for revenge, hackers looking for intellectual challenge), or by the types of computer security that ought to prevent them (e.g., breaches of physical security, personnel security, communications and data security, and operations security). These crimes can also be understood by how they are perpetrated (e.g., by use of the Internet or by use of physical means such as arson). For the purpose of this article, we will consider the method of perpetration, that is, crime committed via the Internet to hurt individual users, as the focus of the discussion below. Table 1 lists some common types of Internet crimes.

The 2004 Computer Crime and Security Survey, recognizes that Internet crime continues to be a significant threat. The E-Crime Watch Survey conducted by CERT Coordination center notes that nearly 70% of their survey respondents reported at least one intrusion while 43% of survey respondents reported an increase in electronic crimes. Organizations are harmed by insiders, such as employees or contractors, and outsiders (Computer Emergency Response Team Coordination Center, 2004, p. 6). CERT 1988-2004 statistics shows that incidents of

Copyright © 2006, Idea Group Inc., distributing in print or electronic forms without written permission of IGI is prohibited.

Table 1. Selected examples of Internet crimes

Malicious codes: ***Logic Bomb:*** Destructive procedures that execute when some prescribed condition occurs (e.g., a specific date). ***Trojan Horse:*** A secret program hidden within an inviting disguise. ***Virus*.** A form of Trojan Horse. A piece of code that attaches itself to a files, and sometimes to a sensitive system sector of the victim computer's hard disk; malware that infects files and spreads when the file executes or is executed by another program; requires that its host program be run to activate it. ***Worm*.** A software program that runs independently, consuming the resources of its host in order to maintain itself and propagating a complete working version of itself onto another machine on the network without intervention. ***Trap Door or Back Door:*** an unauthorized program that bypasses security or other normal procedures. ***Spoof***: Programs that pretend to be another program. **Hacking.** Intentionally accessing (using) a computer without authorization or beyond authorized permission. **SPAM**. Unsolicited e-mail (electronic junk mail). Spam can occasionally 'flood" a host computer or network to the point that it significantly slows down the data flow. **Social engineering**. Tricking an employee into giving out information or taking an action that reduces security or harms a system. **Phishing.** Term coined by hackers who imitate legitimate companies in e-mails to entice people to share passwords or credit-card numbers.	**Identity Theft.** Masquerading (when one person uses the identity of another to gain access to a computer or other personal assets) with social engineering tactics or other means **Theft of Intellectual Property:** Crimes in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. **Internet Frauds:** Any type of fraud scheme that uses one or more components of the Internet - such as chat rooms, e-mail, message boards, or Web sites - to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to other connected with the scheme. Investment Fraud Credit/debit Card Fraud Non-delivery (mdse and payment) Auction Fraud False Advertising **Cyber stalking/On-line Harassment.** The use of the Internet, e-mail, or other electronic communications device to stalk another person. **Internet Crimes Against Children*** - Enticing them through online contact for the purpose of engaging them in sexual acts. - Using the Internet for the production, manufacture, and distribution of child pornography. - Using the Internet to expose youth to child pornography and encourage them to exchange pornography.

* U.S. Department of Justice, Office of Justice Programs

Table 2. Increase in reported incidents and fraud complaints over time

	1990	1995	2000	2001	2002	2003	2004
Incidents reported at CERT (a)	252	2,412	21,756	52,658	82,094	137,529	-NA-
Complaints received via IFCC website (b)			16,838	49,959	75,063	124,509	190,143

Sources: (a) Computer Emergency Response Team Coordination Center--*CERT/CC Statistics 1988-2004*.
(b) Internet Fraud Complaint Center–*IC3 2004 Internet Fraud Report*

systems or data intrusions are continuously increasing. In 2003-2004, the reported incidents increased by nearly 67% (see Table 2).

Internet Crimes Targeting Individuals

The Internet Fraud Compliant Center (IFCC) report shows that traditional crimes such as fraud, identity theft, and harassment are on the rise. Furthermore, these crimes are now committed with the use of the Internet (Internet Fraud Complaint Center 2004). IFCC, which deals with Internet fraud, also receives complaints regarding child pornography (redirected to National Center for Missing and Exploited Children), computer intrusion (redirected to National Infrastructure Protection Center), SPAM e-mail, and identity theft (redirected to Federal Trade Commission). Victims of the well-known Nigerian letter fraud, which has been in existence since the early 1980s, have lost millions of dollars. The Nigerian letter fraud and other credit card frauds are handled by the U.S. Secret Service.

The financial loss incurred through the above fraudulent activities is extensive but the new emergence of crime against children and crime against women using the Internet are even more disturbing (Sones, n.d.). In the recent past, Internet crime against children, such as child pornography, has also been on the increase. Some of the common types of crime against children include enticing them through online contact for the purpose of engaging them in sexual acts, using the Internet for the distribution of child pornography, using the Internet to expose youth to child pornography, and encouraging them to exchange pornography.

Cyber-stalking or online harassment, where one individual harasses another individual on the Internet using various modes of transmission such as electronic mail, chat rooms, newsgroups, mail exploders, and the World Wide Web is also on the rise (National

4 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/vulnerability-internet-crime-gender-issues/12894

Related Content

ICTs for Economic Empowerment in South India
Shoba Arun, Richard Heeksand Sharon Morgan (2006). *Encyclopedia of Gender and Information Technology (pp. 793-797).*
www.irma-international.org/chapter/icts-economic-empowerment-south-india/12828

A Concluding Pledge: With Technology and Justice for All
Mary Kirk (2009). *Gender and Information Technology: Moving Beyond Access to Co-Create Global Partnership (pp. 260-302).*
www.irma-international.org/chapter/concluding-pledge-technology-justice-all/18813

The Computer Game Industry, Market, and Culture
(2014). *Gender Divide and the Computer Game Industry (pp. 28-50).*
www.irma-international.org/chapter/the-computer-game-industry-market-and-culture/95699

Understanding the Mommy Tracks in the IT Workforce
Jeria L. Quesenberryand Eileen M. Trauth (2006). *Encyclopedia of Gender and Information Technology (pp. 1178-1183).*
www.irma-international.org/chapter/understanding-mommy-tracks-workforce/12891

Femenist Standpoint Theory
Clancy Ratcliff (2006). *Encyclopedia of Gender and Information Technology (pp. 335-340).*
www.irma-international.org/chapter/femenist-standpoint-theory/12757