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

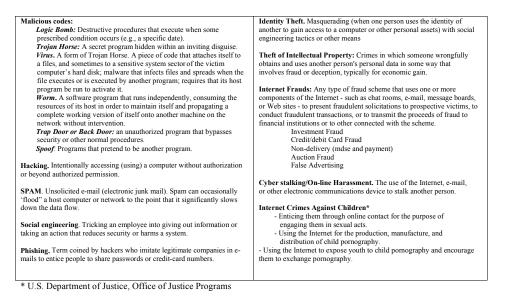


Table 2. Increase in reported incidents and fraud complaints over time

	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 Respons (b) Internet Fraud Complaint Cent					CC Statisti	cs 1988-200	14.

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

Online Sisterhood: Women, Income Generation, and Online Social Capital in Urban Indonesia

Ariane J. Utomo (2016). *Gender Considerations in Online Consumption Behavior and Internet Use (pp. 208-227).* www.irma-international.org/chapter/online-sisterhood/148840

Career Management Concerns for Women in IT

David M. Kaplanand Fred Niederman (2006). *Encyclopedia of Gender and Information Technology (pp. 84-89).* www.irma-international.org/chapter/career-management-concerns-women/12719

Gender Inclusion in the Information Society

Wendy Faulknerand Merete Lie (2006). *Encyclopedia of Gender and Information Technology (pp. 636-642).* www.irma-international.org/chapter/gender-inclusion-information-society/12803

Outsourcing to the Post-Soviet Region and Gender

Elena Gapova (2006). *Encyclopedia of Gender and Information Technology (pp. 952-956).* www.irma-international.org/chapter/outsourcing-post-soviet-region-gender/12855

Male Dominated Industries: Jobs for the Boys

(2013). Gendered Occupational Differences in Science, Engineering, and Technology Careers (pp. 26-63). www.irma-international.org/chapter/male-dominated-industries/69600