Chapter 1.1
Internet Crime:
How Vulnerable Are You? Do Gender, Social Influence and Education Play a Role in Vulnerability?

Tejaswini Herath
State University of New York, USA

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

Shambhu Upadhyaya
State University of New York, USA

ABSTRACT

It is estimated that over 1 billion people now have access to the Internet. This unprecedented access and use of Internet by individuals around the world, however, is accompanied by malicious and mischievous activities online. With the traditional crimes such as fraud, identity theft, and harassment now being committed with the use of the Internet, and networked home computers being exploited to carry out attacks such as denial of service, spamming, phishing and virus/worm propagation, it has become important to investigate security and privacy issues as they pertain to individual Internet users. To date very little is known about what characteristics of internet users affect their computing and on-line behaviors as they relate to security online. While some attention has been paid to understand the security issues affecting corporations, research investigating security issues as they relate to home users is still in infancy. Drawing from disciplines such as criminology, sociology, consumer fraud, and information security, this study seeks to find the role of computing skills and computer training, social influence, and gender on person's vulnerability to Internet crimes. Our findings are significant and shed light in this important area of Internet crime contributing to the information security literature.

DOI: 10.4018/978-1-61350-323-2.ch1.1

INTRODUCTION

Explosive growth in the use of the Internet around the globe has been noted by several surveys. The web statistics compiled by Internet World Stats (http://www.internetworldstats.com/stats.htm) indicates that estimated over 1 billion people around the world now have access to the Web. The 2005 UCLA Internet Report notes that Internet use at home has increased consistently in the past five years. Typically, internet users participate in online activities 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 (Center for the Digitial Future, 2005). With the wide use of Internet, there now exist a significant opportunities to carry out malicious and mischievous activities (Dowland *et al.*, 1999). This is evident through the staggering numbers available on the numbers of crimes committed over internet and losses they pose.

With the traditional crimes such as fraud, identity theft, and harassment now being committed with the use of the Internet, and networked home computers being exploited to carry out attacks such as denial of service, spamming, phishing and virus/worm propagation, it is important to investigate what characteristics of individual internet users affect their computing and on-line behaviors. According to statistics gathered for the E-Crime Watch Survey the chances of falling victim to a computer virus, phishing attack, malicious hack attempt or other cyber security dangers are currently running at 70% (http://news.bbc.co.uk/2/hi/technology/3708260.stm).

Sparse yet some information security literature has focused on behavioral components of information security in an attempt to understand the security related behaviors of individuals (for example, (Hazari, 2005; Hu & Dinev, 2005; Sasse & Brostoff, 2001; Stanton *et al.*, 2004; Stanton *et al.*, 2005). While many of these studies have been conducted in organizational settings others have focused on behaviors pertaining only to the software use behaviors. Although, as discussed in detail later, we can draw valuable insights from these studies, many other online risks faced by individual internet users in home setting such as social engineering tactics or awareness issues were outside the scope of these studies. Drawing from disciplines such as criminology, sociology, consumer fraud, and information security, this paper lays a theoretical foundation to evaluate the role of computing skills and computer training, social influence, culture, individual values, age and gender on person's vulnerability to online risks. We take the approach of understanding on-line risks and vulnerabilities and factors that relate to them. Such understanding will allow us to effectively design defense mechanisms to overcome these issues. Although, consumer fraud literature in marketing has used such approach, this approach is new to online risks and information security area.

This article is organized as follows. We first discuss various types of crimes committed on-line that affect individual citizens. Then we define vulnerability related to on-line activities based on distinct characteristics of each. Drawing from the disciplines of criminology, sociology and marketing (specifically consumer fraud literature in marketing), we present a theoretical model along with propositions to understand the role of computing skills and computer training, age and gender on person's vulnerability to internet crimes.

Nature of Cyber Crime

Wide range of crimes that affect individual citizens are now being committed through the Internet. The Internet Fraud Compliant Center (IFCC) report shows that traditional crimes affecting individuals such as fraud, identity theft, and harassment are on the rise, and are now committed with the use of the Internet ((IFCC), 2004). These crimes include Internet fraud, child pornography, com-