Chapter 1
Introduction

CHAPTER OVERVIEW

This introductory chapter gives a detailed overview of the book. This chapter explores the historical aspect of victimization of women users in the internet. This includes the discussion on why mostly women are targeted in the cyberspace and what methods the offenders use to attack them in the cyber space. The time periods or the spaces in which women are attacked are also discussed. We have also provided the reasons why we chose to write a book on only women victims of internet crimes. This chapter also gives a detailed description on the research done to write this book. This chapter also gives the aims and the audience that the book is aiming to attract. In addition, the scope and the expected implications of the book are presented.

1.1 INTRODUCTION

I am feeling panicked. I am ashamed of my womanhood; I am tired of the constant pricking in the cyber space; can I ever live a normal happy life? Oh God!! Why I had to be born as a woman? Why can’t I be spared even in the cyber space? - A women victim of cyber crime.

Rosy (name changed due the victim’s request) was a new internet user and she immensely enjoyed cyber socializing after she and her husband moved to a remote township from a busy city hub in Florida. She started frequenting a particular online chatting site, chatted with her friends, accepted new friends irrespective of gender and even exchanged her residential address. She invited everyone to visit her town, which she described as a “serene place”. One quiet afternoon, when she logged in the chat room,
she received a request from a user to talk to him in one of the ‘private rooms’ that could be created by the users. She knew this user for quite sometime and she had chatted with this person in the public chat frequently. Therefore, she agreed to move into a “private room” where only two users can chat. The first question posed by the user to her was, did she ever miss her husband when he went for long business tours? When she answered affirmatively, this friend who had a gender-neutral name asked her whether she would like to stay with this friend during those “short holidays” as “she” (friend) also stays nearby. Rosy was eager to have real life friends in this new area. She readily consented and promised to visit the friend very shortly.

Strangely, on the very next week when her husband went for a week long tour, she received an email from a stranger asking her to meet him at a local pub for dating as she might be “missing her husband”. She was afraid and never replied to that mail; neither went to the “meeting place”. Next morning she received an angry mail from the same stranger who threatened her to mail her husband that she was having an illicit relationship with him, if she fails to show up the following evening. She replied to him that she does not meet strangers. That was the beginning. Every fortnight whenever her husband went for official tours, she received “mating call” from this stranger who used to send her emails from various email ids. She was perplexed and opined “I never knew how this man understood that my husband was out of the station”. However, the “friend” in the regular chat room never gave any reason to suspect “her” as “she” used to be in Rosy’s “comfort zone”. “She” became her best friend during those “hard days” and used to hear her agonies with great patience and sympathy. It was only after the “friend” mentioned about the probable meeting place (the same local pub where the stranger invited her) “finally” to have a “girly” get together, that Rosy understood that she had fallen a victim of a big trap laid by the virtual “friend”, who is actually the “stranger” who have stalked her.

This is not an uncommon experience for majority of women in the internet. Victimization of women continues in the internet era through myriads of such ‘traps’. Indeed, few researches (Citron, 2009; Halder & Jaishankar, 2008&9; Bartow, 2009) have established the Internet as the most chosen mode of the offenders to harass and victimize women. The foremost aim of such sorts of victimization remains the same as that of pre-internet era, i.e., damaging the reputation of the woman victim and creating fear factor in the victim’s mind (Citron, 2009). The behavioral factors that contribute to such victimization may include broken relationships, ex-partner harassments, professional rivalry, male dominance and chauvinism, sudden exposure to digital technologies, mischievous intentions to experiment with online adult entertainment in a digital way (Citron, 2009a, Whitty, 2005, Halder, 2009a) and even for monetary gains (Bartow, 2009). Victimization may begin by numerous methods, such as, either befriending the victim with original name but portraying as a ‘good Samaritan’, or winning her trust under a camouflaged identity, or shadowing her cyber activities, or encouraging others to add to the ongoing victimization process of the victim. Cyber technology has become a prime tool to carry out such victimizations in an almost successful manner due to digital ways and similarly, cyber space has provided the biggest platform to harass women in a most cruel way as the victimization can be viewed by millions of digital audiences. Emails, public and private chat rooms, search engines, social networking sites and web sites along with various digital technologies are the chosen modes of many offenders who victimize innocent women.

There could be three factors for offenders choosing these unique methods for victimizing women; viz.

1. It successfully generates instant fear and trauma in the minds of the victims;
2. The perpetrator is omnipresent, yet no one can find him out and prevent his atrocious activities;
Related Content

A Simulation Model of IS Security
[www.irma-international.org/chapter/simulation-model-security/60950](www.irma-international.org/chapter/simulation-model-security/60950)

An Improved Encryption Scheme for Traitor Tracing from Lattice
[www.irma-international.org/article/an-improved-encryption-scheme-for-traitor-tracing-from-lattice/210134](www.irma-international.org/article/an-improved-encryption-scheme-for-traitor-tracing-from-lattice/210134)

Blind Image Source Device Identification: Practicality and Challenges
[www.irma-international.org/chapter/blind-image-source-device-identification/252690](www.irma-international.org/chapter/blind-image-source-device-identification/252690)

Reliable Security Strategy for Message-Oriented Middleware
[www.irma-international.org/article/reliable-security-strategy-for-message-oriented-middleware/193017](www.irma-international.org/article/reliable-security-strategy-for-message-oriented-middleware/193017)

Forensic Statistics in Health Sciences
[www.irma-international.org/chapter/forensic-statistics-health-sciences/52294](www.irma-international.org/chapter/forensic-statistics-health-sciences/52294)