Chapter 7.5
A Profile of the Demographics, Psychological Predispositions, and Social/Behavioral Patterns of Computer Hacker Insiders and Outsiders

Bernadette H. Schell
University of Ontario Institute of Technology, Canada

Thomas J. Holt
The University of North Carolina at Charlotte, USA

ABSTRACT

This chapter looks at the literature—myths and realities—surrounding the demographics, psychological predispositions, and social/behavioral patterns of computer hackers, to better understand the harms that can be caused to targeted persons and property by online breaches. The authors suggest that a number of prevailing theories regarding those in the computer underground (CU)—such as those espoused by the psychosexual theorists—may be less accurate than theories based on gender role socialization, given recent empirical studies designed to better understand those in the CU and why they engage in hacking and cracking activities. The authors conclude the chapter by maintaining that online breaches and online concerns regarding privacy, security, and trust will require much more complex solutions than currently exist, and that teams of experts in psychology, criminology, law, and information technology security need to collaborate to bring about more effective real-world solutions for the virtual world.

DOI: 10.4018/978-1-61350-323-2.ch7.5

INTRODUCTION

Hackers are the elite corps of computer designers and programmers. They like to see themselves as the wizards and warriors of tech. Designing software and inventing algorithms can involve bravura intellection, and tinkering with them is as much fun as fiddling with engines. Hackers have their own culture, their own language. And in the off-hours, they can turn their ingenuity to sparring with enemies on the Net, or to the midnight stroll through systems you should not be able to enter, were you not so very clever. Dark-side hackers, or crackers, slip into systems for the smash-and-grab, but most hackers are in it for the virtuoso ingress. It is a high-stress life, but it can be amazing fun. Imagine being paid—well paid—to play forever with the toys you love. Imagine. –St. Jude, Mondo 2000: User's Guide to the New Edge

Since its appearance in the United States in the second part of the twentieth century, the Internet has been the topic of arduous study from a number of academic disciplines, including the social sciences and criminology, business, law, computer science, and political science. In recent decades, as the Internet has expanded at unprecedented rates, and with different socio-economic interests becoming increasingly involved, the Internet's impact on global citizens' daily lives has been profound. The Internet has become one of the most important ways of communicating internationally in real time (such as is the case with online activism—known in the information technology field as hacktivism). Also, the complex infrastructure of the Internet has on the positive side facilitated a number of common activities—such as e-commerce, Internet banking, online gaming, and online voting—and has provided a more level political and economic "playing field" for citizens residing in both developed and developing nations, particularly in China, India, Russia, and Pakistan.

Moreover, in recent years in developed nations, professionals have been able to broaden their returns to society by adopting Internet-related technologies. For example, using hand-held devices, doctors have been able to access patients' health histories and diagnostic records over the Internet without having to rely on "snail mail" courier services, and high-tech billionaires such as those who started the Google search engine (with a November, 2005, market cap of US$120 billion) have pushed the online entrepreneurial envelope to a whole new higher and societal-beneficial plane (Schell, 2007).

However, with the growth of and diversity in Internet traffic, a dark side has surfaced, particularly since the late 1980s as more and more citizens have become able to afford personal computers (PCs) and online accounts. Thus, tech-savvy criminals have increasingly made use of the Internet to perpetrate online crimes—causing an increase in incidences of online child exploitation, identity theft, intellectual property theft, worm and virus infestations of business and home computers, and online fraud involving its many presentations—e-commerce, voting, and gaming. Consequently, Internet-connected citizens worldwide have become increasingly fearful that their privacy—including personal health histories, banking transactions, social security numbers, and online voting preferences—would be vulnerable to destruction or alteration by mal-inclined computer hackers (known as "crackers"). Too, business leaders have become concerned that not only will their computer networks be tampered by tech-savvy outsiders but also by insider employees determined to destroy critical business data when, say, they leave the firm under less than happy circumstances (Schell, 2007).

In the last decade, in particular, with the growth of the Internet and electronic or e-commerce, the amount of personal information that can potentially be collected about individuals by corporations, financial and medical institutions, and governments has also increased. Such data collection, along with usage tracking and the sharing of data with third parties—especially in