Chapter 1
Computer Hacking and the Techniques of Neutralization:
An Empirical Assessment

Robert G. Morris
University of Texas at Dallas, USA

ABSTRACT

Nowadays, experts have suggested that the economic losses resulting from mal-intended computer hacking, or cracking, have been conservatively estimated to be in the hundreds of millions of dollars per annum. The authors who have contributed to this book share a mutual vision that future research, as well as the topics covered in this book, will help to stimulate more scholarly attention to the issue of corporate hacking and the harms that are caused as a result. This chapter explores malicious hacking from a criminological perspective, while focusing on the justifications, or neutralizations, that cyber criminals may use when engaging in computer cracking--which is in the United States and many other jurisdictions worldwide, illegal.

INTRODUCTION

The impact on daily life in westernized countries as a result of technological development is profound. Computer technology has been integrated into our very existence. It has changed the way that many people operate in the consumer world and in the social world. Today, it is not uncommon for people to spend more time in front of a screen than they do engaging in physical activities (Gordon-Larson, Nelson, & Popkin, 2005). In fact, too much participation in some sedentary behaviors (e.g., playing video/computer games; spending time online, etc.) has become a serious public health concern that researchers have only recently begun to explore. Research has shown that American youths spend an average of nine hours per week playing video games (Gentile, Lynch, Linder, & Walsh, 2004). Video gaming and other similar forms of sedentary behavior among youth may be linked to obesity (e.g., Wong & Leatherdale, 2009), aggression (stemming from violent video gaming—see Anderson, 2004, for a review), and may increase the probability of engaging in

DOI: 10.4018/978-1-61692-805-6.ch001

some risky behaviors (Nelson & Gordon-Larsen, 2006; Morris & Johnson, 2009). In all, it is difficult to say whether increased screen time as a result of technological development is good or bad in the grand scheme of things; the information age is still in its infancy and it is simply too early for anyone to have a full understanding of how humans will adapt to technology and mass information in the long-run. However, we do know that people are spending considerable amounts of time participating in the digital environment, and the popularity of technology has spawned a new breed of behaviors, some of which are, in fact, criminal. One such criminal act is that of malicious computer hacking.[1]

Scholarly attention to cyber-related crimes has gained much popularity in recent years; however, much of this attention has been aimed at preventing such acts from occurring through Information Technology and information assurance/security developments. To a lesser extent, criminologists have focused on explaining the etiology of malicious cyber offending (e.g., malicious computer hacking) through existing theories of criminal behavior (e.g., Hollinger, 1993; Holt, 2007; Morris & Blackburn, 2009; Skinner & Fream, 1997; Yar, 2005a; 2005b; 2006). This reality is somewhat startling, considering the fact that economic losses resulting from computer hacking have been conservatively estimated in the hundreds of millions of dollars per year (Hughes & DeLone, 2007), and media attention to the problem has been considerable (Skurodomova, 2004; see also Yar, 2005a). Hopefully, future research, this chapter included, will help to stimulate more scholarly attention to the issue. The goal of this chapter is to explore malicious hacking from a criminological perspective, while focusing on the justifications, or neutralizations, that people might use when engaging in criminal computer hacking.

Caution must be used when using the term *hacking* to connote deviant or even criminal behavior. Originally, the term was associated with technological exploration and freedom of information; nowadays, the term is commonly associated with crime conduct. In general, hacking refers to the act of gaining unauthorized/illegal access to a computer, electronic communications device, network, web page, data base or etc. and/or manipulating data associated with the hacked hardware (Chandler, 1996; Hafner & Markoff, 1993; Hannemyr, 1999; Hollinger, 1993; Levy, 1994; Roush, 1995; Yar, 2005a). For the purposes of this chapter, I will use the term hacking as a reference to illegal activities surrounding computer hacking. Such forms of hacking have been referred to in the popular media and other references as "black hat" hacking or "cracking" (Stallman, 2002). Again, the primary demarcation here is criminal and/or malicious intent. However, before we fully engage understanding hacking from a criminological perspective, it is important to briefly discuss the history of computer hacking.

The meaning of computer hacking has evolved considerably since the term was first used in the 1960s, and as many readers are surely aware, there still remains a considerable debate on the connotation of the word hacking. The more recent definition of hacking surrounds the issue of understanding technology and being able to manipulate it. Ultimately, the goal is to advance technology by making existing technology better; this is to be done through by freely sharing information. This first definition is clearly a positive one and does not refer to criminal activity in any form.

As time progressed since the 1960s and as computer and software development became less expensive and more common to own, the persona of a hacker began to evolve, taking on a darker tone (Levy, 1984; Naughton, 2000; Yar, 2006); Clough & Mungo, 1992). Many hackers of this "second generation" have participated in a tightly-knit community that followed the social outcry and protest movements from the late 1960s and early 1970s (Yar, 2006). In this sense, second-generation hackers appear to be "anti-regulation" as far as the exchange of information is concerned. As one might expect (or have witnessed), this view typi-