Chapter 3
The General Theory of Crime and Computer Hacking: Low Self-Control Hackers?

Adam M. Bossler
Georgia Southern University, USA

George W. Buruss
University of Missouri-St. Louis, USA

ABSTRACT
Though in recent years, a number of studies have been completed on hackers’ personality and communication traits by experts in the fields of psychology and criminology, a number of questions regarding this population remain. Does Gottfredson and Hirschi’s concept of low self-control predict the unauthorized access of computer systems? Do computer hackers have low levels of self-control, as has been found for other criminals in mainstream society? If low self-control can predict the commission of computer hacking, this finding would seem to support the generality argument of self-control theory and imply that computer hacking and other forms of cybercrime are substantively similar to terrestrial crime. This chapter focuses on the results of a study where we examined whether Gottfredson and Hirschi’s general theory of crime is applicable to computer hacking in a college sample.

INTRODUCTION
The evolution of computer technology and the growth of the Internet have both positively and negatively impacted modern life. Although newer technology makes communication and business transactions more efficient, the same technologies have made it easier for criminals, including malinclined computer hackers, to victimize individuals and businesses without ever being in the same physical space. Computer hacking, as defined in this chapter, can be viewed as the unauthorized access and use or manipulation of other people’s computer systems (Taylor, Tory, Caeti, Loper, Fritsch, & Liederbach, 2006; Yar, 2005a).

Unfortunately, good data do not exist to indicate the frequency and severity of computer hacking (Richardson, 2008), a problem similar to that encountered by white-collar crime scholars.
In general, research has shown that much of our knowledge regarding crime in the physical world applies to cybercrime as well. For example, research has shown that routine activity theory (Cohen & Felson, 1979) can be applied to both on-line harassment (Holt & Bossler, 2009) and malware victimization (Bossler & Holt, 2009). The general theory of crime (Gottfredson & Hirschi, 1990) and aspects of social learning theory (Akers, 1998) have both been extensively applied to digital and software piracy (e.g., Higgins, 2005; Higgins, Fell, & Wilson, 2006).

Although the studying of hackers is not new (see Landreth, 1985), there have been few criminological examinations of these groups or their behaviors (Taylor et al., 2006; Yar, 2005a). Most examinations have focused on hackers as a subculture and have largely ignored other theoretical approaches (see Skinner & Fream, 1997, for an exception). Considering that traditional criminological theories have been successfully applied to other forms of cybercrime, our knowledge on computer hacking could potentially be improved if these same theories, such as Gottfredson and Hirschi’s (1990) general theory of crime, were examined in relationship to hacking.

Michael Gottfredson and Travis Hirschi’s (1990) general theory of crime, or self-control theory, argues that individuals commit crime because they have the inability to resist temptation and, therefore, commit acts having long-term consequences greater than the short-term benefits. Self-control has been demonstrated to be one of the most influential correlates of crime in both the traditional (see Pratt & Cullen, 2000) and digital piracy literature (e.g., Higgins, 2005). Gottfredson and Hirschi would argue that most hacking is simplistic and that hackers take advantage of easy opportunities. Thus, they have characteristics similar to criminals in general. Given this view, the cause of computer hacking is the same as for all other crimes—low self-control.