Moral Beliefs, Self-Control, and Sports: Effective Antidotes to the Youth Computer Hacking Epidemic

Qing Hu
Iowa State University
qinghu@iastate.edu

Chenghong Zhang
Fudan University
chzhang@fudan.edu.cn

Zhengchuan Xu
Fudan University
zcxu@fudan.edu.cn

Abstract

While research on computer hackers has a long history, most of the studies in the past three decades have been qualitative and anecdotal in nature. The question why young computer talents become computer hackers remains. Based on the results of a case study, we conducted a survey-based empirical study using the scenario-based research methodology. Statistical analyses show that three primary factors contribute to the likelihood of talents becoming hackers: moral beliefs, self-control, and time spent on computer games vs. sports activities. Our results indicate that individuals who have strong moral beliefs against hacking activities, strong abilities to control temper, and spend more time in sports than on computer games are less likely to be involved in computer hacking activities. The significant implications of these findings for scholars, educators, and policy makers are discussed and future research directions are explored.

Keywords: Hackers, computer hacking, self-control, moral beliefs, computer games, sports.

1. Introduction

The recent computer hacking episodes, e.g., Sony PlayStation Network services where information about 77 million customer accounts were stolen [25], Bank of America where about $10 million were stolen from customer accounts [19], and Google Gmail where hundreds email accounts of US officials and Chinese political activists were targeted [32], highlight the severity of the hacking epidemic in today’s networked global economy. With the emergence of global networks of businesses and finance built on the Internet platform with a fundamentally open architecture, hacking into corporate IT systems and individuals’ computers is not just a sport for bragging rights among talented young computer enthusiasts, but also a major organized economic activity aiming for profits perpetrated largely by underground networks of criminals and organized crimes on a global scale [1,17], as well as for international espionage, political prosecution, and even terrorism.

Studies have shown that the many of the computers hacking activities were perpetrated by talented and computer savvy college even high school students. In a study of college students in three US universities, Cronan et al. [6] found that 34% of the respondents admitted to committing some form of software misuse or piracy and 22% admitted to committing data misuse during their lifetimes, and the percentages are much higher among the computer information systems majors as compared to other non-computer related majors. However, due to the extreme secrecy and stealth nature of hacking, we know very little about this seemingly omnipresent phenomenon and the characters who commit the hacking acts, other than anecdotal accounts when the hackers were caught and prosecuted. Rigorous academic research about computer hackers, especially those with empirical evidence, has been scarce in the literature, other than a few notable exceptions (e.g., [4, 27]).

One important question is how and why these seemingly talented and computer savvy individuals who could have productive careers in the IT profession become computer hackers and even criminals. Some scholars have resorted to criminological theories when studying computer hackers (e.g., [4; 27, 33, 37]), while others seek insights from economic theories (e.g., [20, 21]). However, computer hackers are clearly different from street criminals or delinquent juveniles who often resort to physical violence, and not all computer hackers are motivated by economic factors such as cost and benefits and often do not behave rationally as economic theories would assume [36]. As a consequence, there are no consistent and widely accepted theories or theoretical frameworks in the research literature about why computer hackers emerge, how computer hackers develop, and therefore no clear and effective guidelines about what to do to prevent talented computer savvy high school and college students from becoming computer hackers and criminals.

Motivated by this lack of rigorous and empirical study on the origins and evolution of computer hackers,
we set out to complete two studies about computer hackers. The first was an exploratory case study of known computer hackers to identify and understand how these individuals evolved from talented students into computer hackers. Then, based on the findings of this case study, we developed a survey instrument and collected data from a large student sample to empirically verify and validate the primary factors identified in the case study. Through this effort, we hope not only to identify and confirm the factors that contribute to the evolution of computer hackers, but also to develop a theoretical framework that could serve as a foundation for studying computer hackers and hacking behavior. The details of the case study are described in a separate paper [13]. In this study, we focus on the empirical study and its findings.

The rest of the paper is arranged as follows. We first provide a brief literature review about research on computer hackers and a brief description of the case study. Drawing on this literature and based on the findings of our case study, we then develop an empirical model of computer hacking behavior and related propositions. This is then followed by a description of the data collection process and discussion of the profiles of the subjects. We then proceed to present the results of empirical testing using liner regression models. Finally, we discuss the main findings and the theoretical and practical implications, as well as future research directions and possibilities to extend and improve the current study.

2. Literature Review and Theoretical Development

The word “hack” or “hacker” in the context of electronic computing has not always had the negative connotations as it has today. In fact, the word “hacker” was meant to have positive connotations to indicate a creative person who could alter computer programs and systems to do things beyond what they are designed for [29, 37], even a sign of respect and admiration from peers for superior computer programming skills [22]. However, once the potentially destructive power of hacking computers and systems was unleashed, there was no going back. These talented computer hackers gradually separated into two camps: the white hats and the black hats, based on their motivations and objectives. The white hats are those who hack as a quest for knowledge, discovering and alerting organizations security holes and weaknesses in their systems, and developing better and secure computer systems; in contrast, the black hats are those who hack for revenge, sabotage, blackmail, or outright criminal conducts such as stealing money, products, and services [29]. Naturally, the majority of the research about computer hackers focuses on understanding the black hats who account for billions of dollars in damages to corporations and individuals each year. In this study, we define computer hacking in terms of the behavior and conduct of the black hats, as described above.

Regardless of the variety of views on computer hacking, the black hat computer hackers are considered as deviants, vandals, and criminals in the academic literature and law enforcement community. Thus, it is understandable that the majority of the academic research on computer hackers has adopted a crime perspective and used criminological theories as the lens of analysis. In a qualitative essay, Yar [37] explored the question why there is disproportionate involvement of juveniles in this form of computer crime. He argued that implicit within most non-academic and/or non-criminological accounts of teenage hacking are the recognizable criminological assumptions such as adolescent psychological disturbance, familial breakdown, peer influence, and sub-cultural association. Citing the research literature, Yar [37] attributed two primary causes to the “youth problem” in computer hacking - hackers tend to be predominantly young males and school dropouts in their mid-20s. The first is the adolescence as a period of inevitable psychological turmoil and crisis that helps account for youthful participation in various forms of “delinquent” and “anti-social” behavior. The second is the apparent “ethical deficit” among juveniles which disposes them toward law- and rule-breaking behavior. This argument is consistent with the criminological theories of developmental psychology which argue that when individuals move from childhood to adulthood, they pass through a number of stages of moral learning; and it is only with “maturity” that these individuals are fully able to appreciate and apply moral principles to regulate their own and others’ behavior. As such, juveniles occupy a special space of moral “immaturity” in which they are more likely to act upon their hedonistic impulses with limited regard for the impact of their actions upon others [11].

While the literature is replete with qualitative accounts of hacker behavior and motivations like Yar [36] and Schell and Dodge [29], rigorous quantitative studies that test theoretically derived hypotheses are few and far between, often contradicting to each other. Rogers et al. [27] examined the predicative power of the Big-5 personality dimensions, moral decision making, and exploitive manipulative amoral dishonesty characteristics of individuals on self-reported computer deviant behavior such as password guessing, authorized access of computer files, and use of credit cards of other people. The authors found that none of the Big-5 personality characteristics can differentiate the self-reported deviant group from the non-deviant group. On
the other hand, the moral choice social and internal scores and the exploitive manipulative index scores are significantly related with the self-reported deviant behaviors, indicating that individuals who do not internalize society’s norms or moral compass are more likely to engage in activities that society in general would find unethical and unacceptable.

However, in a study also conducted by Rogers and colleagues [28] using a different sample but with identical measurement instrument and statistical procedures, the authors found that the only significant variable for predicting the deviant computer behaviors is the personality trait of extroversion. The individuals self-reporting deviant computer behaviors are significantly more introverted than those reporting no deviant computer behaviors. This result directly contradicts that of the previous study. The authors attributed this contradiction to the difference between the samples: Canadian students from a liberal arts department in Rogers et al. [27] vs. American students from an information technology department in Rogers et al. [28], even though the demographic and technology use characteristics of the two groups were remarkably similar [28].

The study by Bossler and Burruss [4] focused on testing the applicability of one of the most widely adopted criminological theories – the general theory of crimes by Gottfredson and Hirschi [16] – in predicting computer hacking behavior. The core thesis of the theory is that what differentiate criminals from non-criminals are the characteristics of low self-control which are usually formed early in life and tend to be stable throughout the life of an individual [16]. With the hypothesis that individuals with low self-control are more likely to commit computer hacking, Bossler and Burruss [4] found that when low self-control is entered as the only primary predictor to computer hacking behavior, it is indeed strong and significant, consistent with the prediction of the theory; when social learning construct is also used in the model, however, the effect of low self-control is weaker and opposite to what is hypothesized; rather, it is the social learning that strongly predicts computer hacking behavior. Further examination of the indirect impact of low self-control by the authors suggests that individuals with lower levels of self-control have higher odds to commit computer hacking after they became involved in the hacker social learning process.

In attempting to develop a better theoretical model for understanding and predicting hacking behavior among college students, we were faced with two significant challenges. On one hand, there is a rich body of qualitative discussion about the origins of computer hacking from sociological, economic, and criminological perspectives but lack of clear consensus.

On the other hand, the extant quantitative studies seem to be more contradictory than complementary to each other’s findings. To overcome the lack of theoretical and empirical guidance, we decided to conduct an exploratory case study of hackers first before developing any theoretical models and attempting empirical analysis [13]. In planning for the case study, we were guided by three well-known criminological theories: the general theory of crime [16], the routine activity theory [5], and the situational action theory [35, 36]. Our interview questions were designed to cover all three areas of causes of crime as argued in the theories: the individual propensity to crime attributed to low self-control [16], crime as an outcome of the concurrence of the motivated offender, the opportunity for crime, and the lack of capable guardian [5], and the central role of morality in individual choices in crime situations [35], in addition to a broader range of questions related to individual computing history.

The case study was carried out in a top Chinese university renowned for its computer science and engineering programs, as well as its computer hackers. Five known computer hackers were recruited by the research team, three of whom were still enrolled in the university as undergraduate students, and one graduated from the same university 10 years back and had been working in companies dealing with information security projects, and the fifth graduated from a different university many years ago and had been working as an independent computer security consultant. Their hacking activities including break into university and government agency computer systems, downloading confidential documents, and changing registration or other records. The details of the case study can be found in Hu et al. [13].

Figure 1: Conceptual Model of Research

The findings of the case study led to the development of our conceptual model of computer hacking behavior, as shown in Figure 1. Based on the literature and the case study, we propose the following research propositions:
Proposition 1: Past experience with computer programming, such as participation in computer clubs and programming competitions, learning programming at young age, is a strong predictor of likelihood of future hacking behavior.

Proposition 2: Routine activities and time allocations in regular days, such as hours spent on homework, sports activities, and computer games, are a strong predictor of likelihood of future hacking behavior.

Proposition 3: The level of self-control, such as the degree of impulsiveness, risk taking, temper control, self-centeredness, and preference to simple and physical tasks, is a strong predictor of likelihood of future hacking behavior.

Proposition 4: The strength of moral beliefs about the right or wrong of a specific hacking behavior, such as hacking for fun, hacking for learning, and hacking for profit, is a strong predictor of likelihood of future hacking behavior.

We also identified two categories of hacking behavior with eight specific hacking activities: exploratory hacking - for fun, for friends, for learning, for curiosity, and exploitive hacking – for revenge, for justice, for survival, and for profit. These concepts and relationships were shown in the conceptual model depicted in Figure 1.

In addition to the main concepts, we also included sex, age, GPA, major, and class level as control variables based on the findings of the literature in order to control for the complications of the potential effects of these variables on the main dependent variable – the likelihood of different types of hacking behavior.

3. Data and Method

Based on the conceptual model, the research team proceeded to developing a survey instrument to collect data and testing the conceptual model. Given the similarity between hacking and criminal behavior, we followed the methodology of criminological research when developing the survey instrument (e.g., [24, 26]).

Using scenarios to elicit individual responses has been a common technique in criminology research, and it has been increasingly used by IS scholars in information ethics and security research in recent years (e.g., [2, 7, 10, 23, 31]). The use of scenarios has the advantage of providing a less-intimidating way to respond to sensitive issues and offering realistic scenarios that place the subject in a decision-making role [10]. Using scenario based design also has the advantage of improved reliability of data and the ability to collect data in a much broader population that might have not experienced or committed the activities described in the scenarios.

With the exception of self-control constructs which were measured using the standard items of Grasmick et al. [18] based on a seven-point Likert scale, moral beliefs and hacking behavior which were measured using 11-point scales, the rest of the items were direct measurement of activities, such as hours spent on computer games, in sports, and on homework. This questionnaire was then reviewed by a panel of faculty experts who are familiar with information security research for face validity. Minor changes were made to the questionnaire based on the feedback from these experts.

The data collection was carried out in the same university where we conducted the case study. Undergraduate students enrolled in MIS, Computer Science, and Electrical Engineering classes at the university were selected as subjects of the survey because these students are more likely to have the abilities to conduct computer hacking activities, and perhaps the experience of hacking as well. The data collection was carried out by research assistants with the permission of the instructors in these classes. The assistants handed out the survey to the students in each classroom, informed the students the nature of the study, a small token reward for participating, and the statement that participation was completely voluntary and there would be no negative consequences for not participating. In all, 213 surveys were distributed and all of them were completed, collected, and deemed usable. The effective return rate is 100% primarily because of the cooperation of the instructors and the presence of the assistants in each data collection classroom, the small token gift might also played a role in motivating the students to complete the survey.

The profile data show that about two thirds of the subjects were male students, majority of them were between the age of 20-21, and about 70% have a GPA greater than 3.0, indicating that they were typical college age undergraduates with above average performance. The higher than average GPA may be attributable to the overall high quality of the student population at this top university. Most of the students were in their sophomore or junior years, and 96% were enrolled in computer related majors – computer science, electrical engineering, and management information systems. This concentration of majors in computer related field was by design. We deliberately selected the classes in these three majors to collect data with the belief that they were the best pools for computer hackers to develop thus most appropriate for our study.

Another set of revealing statistics shows the characteristics of our respondents related to their allocation of time in various routine activities as college students. In general, our respondents on average take about 6 courses per semester, and work on computers...
about 3.5 hours per day. They also reported spending about 1.5 hours on social networking, web surfing, and playing computer games each, which totals about 4.5 hours. Thus, the computing hours may have been interpreted differently by these individuals; certain activities may or may not have been counted as computing hours, which resulted in the discrepancies between the total computer use hours and the sum of individual activities. Overall, the statistics fit the general profile of college student activities for those who are majoring in computer science, electrical engineering, and management information systems based on our own knowledge.

One interesting observation is that about 17% of all respondents reported that they had the experience of accessing computers without authorization, a number much higher than we had anticipated. More interestingly, about 6% indicated such activity started when they were in elementary and middle school, and another 5% when they were high school. Together they accounted for 11% of the 17% reported, indicating that about 65% of these who committed unauthorized access to computers started such activity before they entered the college, consistent with the findings of our case study [13].

Another set of revealing statistics shows how early the respondents developed their interests in computers and computer programming. More than one third of the respondents (35%) indicated that they became interested in computers while still in elementary school, and 9% already started learning computer programming and 4% participated in computer clubs and programming competitions while still in elementary school.

### 4. Results and Analyses

We used ordinary least square (OLS) regression to test the effect of different variables on the dependent variables – likelihood of hacking in various scenarios: for fun, friends, curiosity, learning, revenge, justice, survival, and profit. Eight linear regression models were constructed based on these scenarios, using the response to likelihood of hacking in each of the scenarios as the dependent variable, and routine activities (7 variables), past experience (8 variables), and self-control (6 variables), plus one moral belief variable associated with each scenario, as the independent variables. These results are presented in Tables 1 and 2.

Several interesting results stand out from these regressions. First, the role of gender is confirmed. Although we did not hypothesize the influence of gender on hacking behavior, male dominance is clearly manifested in the media reports and studies about hackers and hacking activities (e.g., [15, 37, 38]). Our results show that this popular perception has some empirical truth. Sex, coded as 1 for male and 2 for female, is strongly negatively related to the dependent variable in 7 of the 8 scenarios, with regression coefficients β (values in parentheses are two-tailed t-values) such as -1.815 (-3.721), -1.600 (-3.394), -1.465 (-3.732), -0.369 (-1.236), indicating that male students are more likely to commit hacking than female students. The only exceptional case is model 4 where dependent variable is “Hacking for Learning.” In this case, GPA is stronger predictor (β = -0.298, t = -1.669) than sex (β = -0.369, t = -1.236), indicating that students with higher GPA are less likely to use hacking as a learning activity, which is quite understandable because hackers tend to spend more time on hacking than on class assignments, based on our case study [13].

The second interesting result is that the highly significant but strongly opposite effect of computer game and sports on the likelihood of hacking across all eight scenarios. The number of hours a student spends on playing computer games is strongly related to the likelihood of conducting hacking activities, with regression coefficients β (t) of 1.099 (2.699), 0.999 (2.519), 0.964 (2.941), 0.913 (3.657), 0.738 (3.078), 0.642 (1.752), 0.456 (1.800), and 0.542 (2.433), a strong predictor for identifying potential hackers. On the other hand, the number of hours a student spends in playing sports seems to serve as a strong antidote to the effect to computer games, with regression coefficients of -1.122 (-2.583), -1.562 (-2.663), -0.755 (-1.836), -1.013 (-2.812), -1.408 (-2.105), -1.961 (-3.062), -1.410 (-2.608), and -0.930 (-2.269). One more interesting observation is that the magnitude of the negative effects by sports is stronger than that of the positive effects by computer games on the likelihood of hacking across all eight models, indicating that participation in sports is a stronger antidote than the negative influence of computer games in the fighting against hacking behavior, a silver lining in a gloomy situation.

#### Table 1: Regression Results – Exploratory Hacking as Dependent Variable

<table>
<thead>
<tr>
<th></th>
<th>M1: For Fun (FN)</th>
<th>M2: For Friend (FD)</th>
<th>M3: For Curiosity (CU)</th>
<th>M4: For Learning (LN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Constant)</td>
<td>Beta</td>
<td>t</td>
<td>Beta</td>
<td>Beta</td>
</tr>
<tr>
<td></td>
<td>2.823</td>
<td>1.034</td>
<td>5.689</td>
<td>2.158</td>
</tr>
<tr>
<td>Sex</td>
<td>-1.815</td>
<td>-3.721</td>
<td>-1.600</td>
<td>-3.394</td>
</tr>
<tr>
<td></td>
<td>-1.465</td>
<td>-3.732</td>
<td>-0.369</td>
<td>-1.236</td>
</tr>
<tr>
<td></td>
<td>3.026</td>
<td>1.765</td>
<td>0.964</td>
<td>2.941</td>
</tr>
<tr>
<td></td>
<td>0.913</td>
<td>3.657</td>
<td>0.738</td>
<td>3.078</td>
</tr>
<tr>
<td></td>
<td>0.642</td>
<td>1.752</td>
<td>0.456</td>
<td>1.800</td>
</tr>
<tr>
<td></td>
<td>0.542</td>
<td>2.433</td>
<td>0.306</td>
<td>3.062</td>
</tr>
<tr>
<td></td>
<td>-1.122</td>
<td>-2.583</td>
<td>-1.562</td>
<td>-2.663</td>
</tr>
<tr>
<td></td>
<td>-0.755</td>
<td>-1.836</td>
<td>-1.013</td>
<td>-2.812</td>
</tr>
<tr>
<td></td>
<td>-1.408</td>
<td>-2.105</td>
<td>-1.961</td>
<td>-3.062</td>
</tr>
<tr>
<td></td>
<td>-1.410</td>
<td>-2.608</td>
<td>-0.930</td>
<td>-2.269</td>
</tr>
<tr>
<td></td>
<td>Beta</td>
<td>t</td>
<td>Beta</td>
<td>t</td>
</tr>
<tr>
<td>----------------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>(Constant)</td>
<td>4.775</td>
<td>2.945</td>
<td>6.330</td>
<td>2.620</td>
</tr>
<tr>
<td>Sex</td>
<td>-.570</td>
<td>-1.988</td>
<td>-.1253</td>
<td>-2.856</td>
</tr>
<tr>
<td>Age</td>
<td>.106</td>
<td>.602</td>
<td>-.124</td>
<td>-1.471</td>
</tr>
<tr>
<td>Grade</td>
<td>-.282</td>
<td>-1.199</td>
<td>-.033</td>
<td>-1.092</td>
</tr>
<tr>
<td>Major</td>
<td>.020</td>
<td>.117</td>
<td>-.166</td>
<td>-.640</td>
</tr>
<tr>
<td>GPA</td>
<td>.063</td>
<td>.364</td>
<td>-.113</td>
<td>-.434</td>
</tr>
<tr>
<td>CourseTaken</td>
<td>-.002</td>
<td>-.018</td>
<td>.003</td>
<td>.016</td>
</tr>
<tr>
<td>CompUse</td>
<td>-.043</td>
<td>-1.361</td>
<td>-.199</td>
<td>-1.113</td>
</tr>
<tr>
<td>Homework</td>
<td>-.002</td>
<td>-.015</td>
<td>.254</td>
<td>1.353</td>
</tr>
<tr>
<td>SocNetwg</td>
<td>.303</td>
<td>1.413</td>
<td>-.047</td>
<td>-.144</td>
</tr>
<tr>
<td>WebSurfing</td>
<td>.075</td>
<td>.580</td>
<td>.210</td>
<td>1.073</td>
</tr>
<tr>
<td>CompGame</td>
<td>.738</td>
<td>3.078</td>
<td>.642</td>
<td>1.752</td>
</tr>
<tr>
<td>Sports</td>
<td>-.112</td>
<td>-2.853</td>
<td>-.1562</td>
<td>-2.663</td>
</tr>
<tr>
<td>EarlyInterest</td>
<td>.058</td>
<td>.504</td>
<td>.024</td>
<td>.138</td>
</tr>
<tr>
<td>ProgAbility</td>
<td>.214</td>
<td>1.237</td>
<td>.366</td>
<td>1.396</td>
</tr>
<tr>
<td>ProgClub</td>
<td>.036</td>
<td>.230</td>
<td>-.318</td>
<td>-1.334</td>
</tr>
<tr>
<td>ProgCompetition</td>
<td>-.197</td>
<td>-.660</td>
<td>-.522</td>
<td>-1.158</td>
</tr>
</tbody>
</table>

Table 2: Regression Results – Exploitive Hacking as Dependent Variable
The third interesting result is the strong effect of moral beliefs on the likelihood of hacking. The stronger a student believes that hacking is morally wrong, the less likely this student will be engaged in any type of hacking activities. All regression coefficients related to moral beliefs are strongly negative and highly significant: -0.485 (-5.654), -0.581 (-7.319), -0.353 (-4.111), -0.234 (-3.515), -0.428 (-7.260), -0.683 (-10.734), -0.599 (-9.017), and -0.454 (-7.264). These results suggest that moral beliefs continued to be one of the strong weapons in the fighting against the epidemic of computer hacking, similar to their role in fighting deviant and criminal behaviors in society and computer and systems abuse by employees in organizations.

Last but not the least is the role of self-control in predicting likelihood of hacking. The results are largely mixed but revealing. Among the four hacking activities we classified as “Exploratory Hacking” where the objective is to benefit oneself but do no-harm to others, which include hacking for fun, for friend, for curiosity, and for learning, the “Temper” dimension of self-control has a strong and positive effect on the likelihood of hacking, with regression coefficients β as 0.346 (1.695), 0.445 (2.255), 0.436 (2.660), and 0.242 (1.934), indicating that students with a tendency to lose temper, easily irritated, and become angry are more likely to engaging in hacking activities that belong to this category. Other self-control dimensions, with the exception of “Risk Taking” which has strongly positive effect on “Hacking for Fun” (β = 0.468, t = 2.624), have insignificant effects on the hacking activities in this category. However, among the four hacking activities we classified as “Exploitive Hacking” where the objective is to benefit oneself regardless harms to others, which include hacking for revenge, for justice, for survival, and for profit, the picture is more complex. In the case of hacking for revenge, both “Risk Taking” (β = 0.191, t = 1.834) and “Temper” (β = 0.204, t = 1.699) have strongly positive effects, as expected. The strong and negative effect of “Simple Task” (β = -0.243, t = -1.799) is also expected because preference to simple tasks is opposite of what it takes to be a hacker, especially a hacker that has to respond to a specific event and task, as revenge hacking would require. The more perplexing result is that none of three dimensions has any significant role in the other three type of hacking: for justice, for survival, and for profit. In the case of hacking for justice, only “Impulsiveness” is significant and positive (β = 0.437, t = 2.493). None of the self-control dimensions matters in the case of hacking for survival. And in the case of hacking for profit, only “Self-Centered” has a weak and positive effect (β = 0.213, t = 1.658). We do not have a plausible explanation to these complex and mixed results, which certainly deserve more future research.

5. Discussion

In this study, we tested the main findings of an earlier case study [13] using an empirical study with the general student population and the scenario based methodology. Consequently, our models have shed some lights onto the question why talented students could become computer hackers. Based on the regression results, we highlight three major contributors: moral beliefs, low self-control, and routine activities.

While moral beliefs have been identified as a major antidote to criminal behavior in society [24, 26, 35, 37]
and information security policy violations in organizations [7, 14], our study is among the first that identifies and confirms the critical role of moral beliefs in controlling hacking intentions among the college students. In all eight hacking scenarios, students who believed that the behavior of the characters in the scenarios was morally wrong scored low on the likelihood that they would behave similarly under the circumstances, and those who believed the behavior of the characters was not so wrong scored high on the likelihood of doing similar things given the circumstances, as clearly indicated by the strong and negative regression coefficients across the scenarios. The t-values for the moral belief variable are the highest among all independent variables (all of them are significant at p < 0.001 level), an indication that there is little variance among the responses with regard to how strongly the respondents felt about the relationship between moral beliefs about the hacking behavior and likelihood of perpetrating the hacking behavior. This finding puts moral beliefs about hacking in the forefront of the battle against computer hacking and the prevention of talented and computer savvy college students from becoming professional and criminal hackers. Since the majority, about 65% as shown in Table 4, of the students who had the experience of unauthorized access to computers started such activities before they even entered college, as early as in elementary school, the clear policy implication here is that education on computer ethics needs to start in elementary schools when students were first introduced to computers and computer programming concepts. And this education about what is right and what is wrong about using computers and computer networks needs to continue from elementary all the way to college and must be a center piece of computer education curriculum, if we want to have any hope of controlling and managing the epidemic of computer hacking.

The second major contributor to the likelihood of talents becoming hackers is the individual character of self-control. Although this is not a new concept in the studies about individual behavior, as it was first proposed in the general theory of crime by Gettfredson and Hirschi [16], our study is the first empirical research we are aware of that has tested all six dimensions of the self-control construct based on Grasmick et al. [18] measurement scale. Our results suggest that the impact of self-control on the likelihood of becoming hackers is complex and context specific. First of all, if hacking is for surviving, our results show that self-control characteristics have no impact at all. However, in all other seven hacking scenarios, different dimensions of self-control have different roles. The most consistent is the dimension of “Temper” which is strongly related to five of the seven scenarios. Our results suggest that individuals who easily become angry and have strong tendencies to lose temper are more likely to become computer hackers if they happen to have the computer skills. The second most prominent dimension is “Risk Taking” which is significant in two of the seven scenarios – hacking for fun and hacking for revenge. It is followed by “Impulsiveness” which is significant only in hacking for justice scenario and “Self-centered” which is significant only in the scenario hacking for profit. On the other hand, the dimension “Simple Task” has strong but opposite effect on hacking in the scenario of hacking for revenge. While this is opposite of what has been found in the criminological studies, it is actually consistent with the context: committing computer hacking activities requires sophisticated skills to complete complex tasks, as opposed to criminal acts which usually are physical and unsophisticated. Overall, the results are consistent with the general thesis about self-control and deviant behavior as well as recent findings about self-control and employee information security policy violations [14].

Given the fact that the characteristics of low self-control are formed early in life and remain relatively stable throughout life of an individual [16], the challenge to educators and policy makers who are interested in managing talented and computer savvy college students from sliding into computer hackers is what to do to overcome the effect of low self-control on these students who already possess such characteristics. We argue that the answer lies in our third major finding: the role of computer games and sports activities. After meeting the demand of routine college tasks such as going to classes and doing homework, college students must make the mundane daily decision about how to spend the rest of the hours each day. A talented computer science or management information systems student could choose to play computer games that are omnipresent on the Internet accessible via fixed or mobile computing devices, or choose to participate in on- or off-campus sports activities which are also as easily accessible. Yet, the consequences could not be more disparate in terms of becoming or not becoming a computer hacker. Our results show that across all eight computer hacking scenarios, playing computer games significantly contributes to the likelihood of committing computer hacking while participating in sports significantly reduces the likelihood of committing computer hacking. Therefore, to reduce the likelihood of these talented and computer savvy students becoming computer hackers, university administrators, students advisors, and student organizations should make concerted effort to organize, guide, and monitor on-campus and off-campus sporting events and attract
and retain these students in these events. Along with early and persistent education on computer ethics and morality, sports seem to serve as the strongest antidote to the lure of computer hacking in a significant portion of the youth population.

Our study inevitably has some limitations. Our sample was from the population of college students in one university. A broader sample that includes individuals outside universities might yield even richer insights about the focal phenomenon. In addition, we only examined the effects of individual variables on the likelihood of hacking with linear models. More complex models that consider the interactions of the variables as well as the causal chains in these variables could provide a better understanding of the phenomenon. Finally, our recommendation of using sports as an antidote to computer hacking may have limited effects on the youths who are not inclined to sports activities. Future research is clearly needed to address this critical issue.

6. Conclusion

In this study, we investigated the question why talented and computer savvy college students may become computer hackers. Our study is motivated by the interviews we conducted with five known computer hackers. Based on the results of the case study, we developed a survey instrument and adopted the scenario based research methodology commonly used in criminological studies. Eight computer hacking scenarios were created based on the information acquired from the interviews with the hackers, and responses about the likelihood of committing the same hacking activities were collected, along with moral beliefs about the right or wrong of these hacking activities and a multitude of other predictive and control variables. Consequently, eight regression models were tested, and the results were revealing and interesting. We found that three primary factors that contribute to the likelihood of committing computer hacking by the respondents: moral beliefs, self-control, and time spent on computer games vs. sports activities. Our results indicate that individuals who have strong moral beliefs against hacking activities, strong abilities to control temper, and spend more time on sports than computer games are much less likely to be involved in computer hacking activities. On the other hand, individuals who don’t believe hacking is morally wrong, who have tendencies to lose temper, and who spend more time on computer games are much more likely to develop into computer hackers. These findings have significant implications for scholars, educators, and policy makers.

7. References


