Deviant Behavior

ISSN: 0163-9625 (Print) 1521-0456 (Online) Journal homepage: https://www.tandfonline.com/loi/udbh20

Differentiating Hackers, Identity Thieves, Cyberbullies, and Virus Writers by College Major and Individual Differences

Kathryn C. Seigfried-Spellar & Kellin N. Treadway

To cite this article: Kathryn C. Seigfried-Spellar & Kellin N. Treadway (2014) Differentiating Hackers, Identity Thieves, Cyberbullies, and Virus Writers by College Major and Individual Differences, Deviant Behavior, 35:10, 782-803, DOI: 10.1080/01639625.2014.884333

To link to this article: https://doi.org/10.1080/01639625.2014.884333

Deviant Behavior, 35:782–803, 2014

ISSN: 0163-9625 print/1521-0456 online
DOI: 10.1080/01639625.2014.884333

Routledge
Taylor & Francis Group

Differentiating Hackers, Identity Thieves, Cyberbullies, and Virus Writers by College Major and Individual Differences

Kathryn C. Seigfried-Spellar and Kellin N. Treadway
The University of Alabama, Tuscaloosa, Alabama, USA

This study examined the personality characteristics of 296 self-reported computer deviants and non–computer deviants with different college majors. Results indicated hackers majoring in the Arts were more hedonistic compared to the hackers majoring in Business. The identity thieves majoring in Business were more extraverted and open to experiences compared to the identity thieves majoring in "Both." The virus writers majoring in the Arts were more likely to make moral decisions based on hedonistic, social, and internal moral values compared to the virus writers majoring in Business. There were no significant differences in the personality characteristics of cyberbullies with different majors.

INTRODUCTION

Computer criminality is a serious problem that affects individuals, businesses, and our nation's security. While the exact damage caused by computer criminals is open for debate, the activities' existence and increase in numbers is unquestioned (Rogers et al. 2006a). First, consider that approximately 39% of the world's population has Internet access (ITU 2013), which is up from 20% in 2006. Second, global penetration of mobile-cellular subscriptions has reached 96%. Worldwide, 37% of all women and 41% of all men are Internet users, and 41% of households have Internet access. In the developed world, nearly 80% of all households have Internet access (ITU 2013). This globalization of technology facilitates the ever-increasing risk of cybercrime and computer criminality due to the sense of anonymity or "cloak of safety" offered by the Internet, which lessens social risk and lowers inhibitions (Morahan-Martin and Schumacher 2000).

Originally, the term "hacker" was a badge of honor bestowed upon those who had the intelligence and skills to implement shortcuts, or "hacks," within slow-moving computer programs, but over the years, this term has taken on a negative connotation (Fötinger & Ziegler 1993; Schell and Holt 2009). In the past, research has focused on hacking in general, lumping nearly every form of computer deviancy into this category, with little attention given to the fact that not all computer deviants are the same. Different forms of computer deviant behavior require different levels of technical knowledge and skillsets; so lumping pirates, hackers, and virus writers into an overall

Received 6 August 2013; accepted 26 November 2013.
Address correspondence to Kathryn C. Seigfried-Spellar, Ph.D., The University of Alabama, 425 Farrah Hall, Box 870320, Tuscaloosa, AL 35487, USA. E-mail: kseigspell@as.ua.edu

cybercriminal category may convolute our ability to discriminate between computer deviants and non-computer deviants.

With cybersecurity at the forefront, the field of cybercrime and digital forensics has focused on the technology, and specifically, devising approaches to protect digital information and the security of associated networks and systems. The approach to understanding cybercrime and efforts to hone in on cybercriminal activity through efforts like digital forensics are changing from the more traditional—that is, a focus on technology—to one wherein society realizes the need to understand *the people* involved and their motives, essentially the *who* and *why* of cybercrime (Crossler et al. 2012). Overall, the general term "cybercriminal" includes a variety of computer deviant behaviors, each with different motivations and technical skillsets (see Rogers 2010). As the present study shows, in order to understand *the people* involved in computer deviant behavior, it is important to discriminate between the different types of computer deviants (e.g., hackers, virus writers, identity thieves, and cyberbullies).

LITERATURE REVIEW

The Internet Crime Complaint Center of the National White Collar Crime Center (NW3C) stated that in 2012 the Internet Crime Complaint Center (I3C) received 289,874 computer crime complaints (approximately 24,000 complaints per month; IC3 2013). In only one year, the IC3 reported an 8.3% increase in reported financial losses due to computer criminal activity. Specifically, 39.6% of the complaints reported financial loss for a total of $525.4 million, with an average of $4,573 per victim reporting a financial loss (I3C 2013). For example, a total loss of approximately $135,000 was due to malware extorting money through intimidation tactics (e.g., ransomware), and almost $4.7 million in total loss was the result of government impersonation e-mail scams (I3C 2013). In addition, the Computer Security Institute (CSI) released the findings from their annual Computer Crime and Security Survey. The survey was sent to 5,412 security practitioners and a total of 351 surveys were returned (Richardson 2010). Similar to last year's report, malware infection, such as viruses and worms, was the most common attack reported (67.1%). Furthermore, approximately half of the respondents experienced at least one security incident, and 45.6% of these respondents stated they were the specifically targeted (Richardson 2010).

Not only does the globalization of technology continue to make it easier for individuals to engage in computer criminal behaviors, but it also increases the number of possible victims and targets, which is especially impactful on the issue of cyberbullying. Hinduja and Patchin (2008) and Mesch (2009) found the amount of time spent on-line is one of the greatest risk factors associated with cyberbullying, because the more time that an individual spends on-line, the more opportunity they have to bully and be bullied. In addition, the more time individuals spend on the Internet engaged in consumer behavior (e.g., shopping), the more likely they will be the victim of identity theft or Internet fraud (Pratt et al. 2010). Overall, consistent with Routine Activities Theory, research shows that the Internet facilitates an environment where motivated offenders have access to numerous targets, and there is an absence of guardianship in cyberspace (Bossler and Holt 2010; Pratt et al. 2010).

Just like traditional crimes, not everyone with access to technology, such as the Internet, chooses to engage in illegal computer behaviors. According to Loch and Conger (1996),

"individual characteristics all appear to be important in determining ethical computing decisions" (p. 82). Research indicates computer hackers may exhibit individual traits associated with certain personality disorders. For example, some computer hackers may be prone to higher rates of hostility and exhibit a greater propensity for egotistical qualities (Campbell and Kennedy 2009; Schell and Holt 2009). As discussed by Campbell and Kennedy (2009), Narcissistic Personality Disorder is characterized by an excessive perception of entitlement, as well as a lack of empathy, both of which are associated with some subsets of criminal computer behavior, especially insider hacking. In addition, computer criminal deviants may exhibit a lack of empathy, insincerity, dishonesty, and enhanced intellect, all of which are consistent with Antisocial Personality Disorder, as individuals with the disorder do not believe their actions cause harm to others or break the law (Campbell and Kennedy 2009). In particular, these traits may be more likely to manifest in hackers who excel in social engineering, or the manipulation of others to obtain certain means through hacking (Chiesa et al. 2009; Kirwan and Power 2012). Finally, Bachmann (2010) suggested that hackers who exhibit high risk-taking behaviors engage in a higher number of hacking behaviors, but with less success overall.

In Shaw and colleagues (1999), the information technology specialists who committed insider threats (i.e., employees with legitimate access commit computer crimes within an organization) were more likely to be introverted and computer dependent. In addition, insiders reported a history of work and family problems, ethical flexibility, sense of entitlement, and reduced loyalty and empathy (Shaw et al. 1999). Rogers and colleagues (2006b) found that lower levels of internal moral choice and social moral choice correlated negatively with computer deviancy, meaning criminal computer behavior was more likely when an individual had loose personal morals and did not conform to societal norms (formal social control). In addition, Rogers et al. (2006b) suggested individuals who self-reported computer deviance scored higher on exploitive-manipulative amoral dishonesty and lacked social norms. Finally, a preliminary study by Seigfried-Spellar and colleagues (2010) found that undergraduate students who engaged in computer crime were less agreeable (high antagonism) and more open to experiences (low constraint) compared to non-computer deviants.

Against expectations, Rogers et al. (2006b) and Seigfried-Spellar et al. (2010) reported no significant difference in the levels of introversion for computer deviants and non-computer deviants. However, Rogers et al. (2006a) found self-reported computer criminals were more likely to score low on extraversion, meaning they were more likely to exhibit an introverted, or less social and gregarious, personality. This inconsistency in the trait "extraversion" may be due to the sampling procedures themselves. Shaw et al. (1999) and Rogers et al. (2006a) sampled information technology specialists or undergraduate students enrolled in the College of Technology, respectively. On the contrary, Rogers et al. (2006b) sampled undergraduate students from an introductory psychology course, and Seigfried-Spellar et al. (2010) randomly sampled undergraduate students campus-wide, and the final dataset yielded an even distribution of arts and sciences majors. Therefore, computer deviance and introversion may be related for those individuals majoring or working in technology-related related fields, whereas introversion is not significantly related to computer deviants in the softer sciences (see Rogers et al. 2006a).

Since cyberbullying is a relatively new form of cyber deviance, few empirical studies have assessed whether personality characteristics discriminate between cyberbullies and non-cyberbullies. Coyne et al. (2009) reported the factor most often associated with this type of cyber deviance is achievement or "the motivation to enhance power, to dominate, and a desire

to provoke and annoy" (p. 215). This need for power and achievement may be related to the higher levels of narcissism, specifically the traits entitlement and superiority, which indirectly effect cyberbullying (see Ekşi 2012; Menesini and Spiel 2012). In addition, Aricak (2009) found a significant relationship between high levels of hostility and psychoticism for cyberbullies compared to non-cyberbullies. Although only a few studies exist, the research indicates that certain individual differences, such as narcissism and aggression, are related to cyberbullying behaviors.

Overall, previous research suggests there are personality differences between computer criminals and non-computer criminals, but in the past, this literature has not distinguished the individual differences of those engaging in different forms of computer deviance. First, some literature categorizes respondents as "computer criminals" by lumping together crimes where the computer was the "target" (such as hacking) and crimes where the computer was the "tool" (such as cyberbullying; Rogers 2001; Rogers et al. 2006a; Rogers et al. 2006b; Seigfried-Spellar et al. 2010). However, these different categories of computer deviance involve different degrees of technical knowledge and skills; for instance, less technical knowledge is typically necessary for a cyberbully to harass someone on social media, whereas a virus writer must have fairly extensive knowledge of computers and technology to code and/or implement malware. Second, research has yet to determine the relationship between individuals who engage in crimes where the computers are the "target" versus crimes where the computers are the "tool." In other words, are computer hackers more or less likely to also be cyberbullies? Third, respondents are often labeled as computer criminals based on their endorsement of several questions related to different forms of computer hacking behavior, such as guessing passwords and virus writing— these types of hacking behaviors, again, involve different degrees of technology knowledge. Lastly, there are inconsistent findings regarding the differences in personality characteristics between computer deviants and non-computer deviants, specifically related to introversion. This inconsistency may be the result of sampling respondents from different fields of study, specifically from the technology versus liberal arts-related fields.

THE CURRENT STUDY

Three primary objectives were the focus of the current study. First, the authors investigated whether degree major/minor (Arts, Sciences, Business, or "Both") distinguished between computer deviants and non-computer deviants. That is to say, are computer hackers compared to non-computer hackers more likely to major in the sciences versus the arts? The second aim of this study was to determine whether individual differences distinguished between computer deviants and non-computer deviants with different degree majors/minors. In other words, are there differences in the personality characteristics (e.g., extraversion) of computer criminals and non-computer criminals majoring in the Arts? Finally, the third aim of this study was to determine whether individual differences distinguished between individuals who engaged in different forms of computer deviance (hacking, virus writing, cyberbullying, and identity theft). For instance, are there personality differences between computer hackers and cyberbullies?

Based on the previous research, the authors expected to find significant differences in the personality characteristics and degree majors/minors of computer deviants and non-computer deviants. The following three hypotheses were tested in the current study:

H_1. There are differences in the degree majors (Arts, Sciences, Business, "Both") of computer deviants (hackers, virus writers, cyberbullies, and identity thieves) when compared to non-computer deviants.

H_1.a. Hackers, virus writers, and identity thieves will be more likely to major in the hard sciences.

H_2. There will be individual differences between computer deviants (hackers, virus writers, cyberbullies, and identity thieves) and non-computer deviants.

H_2.a. Computer deviants will be less agreeable (more antagonistic) and less likely to follow social moral norms compared to the non-computer deviants.

H_3. There will be individual differences for computer deviants (hacker, virus writers, cyberbullies, and identity thieves) with different degree majors (Arts, Sciences, Business, "Both").

METHOD AND DATA

Method

A convenience sample of approximately 600 undergraduate students from a large, Southern university was recruited for participation in the current study. Three hundred and ninety-eight undergraduate students voluntarily participated, resulting in a 66% response rate. It is unknown why some students did not participate in the study—although, one reason could be because the students had to be at least 19 years of age or older to participate, and it is possible there were 18-year-old students in the solicited classrooms. The undergraduate students were recruited from all degree majors and minors by information sessions given on a class-by-class basis with permission from the instructor. Both upper-level (300 or 400) and lower-level (100 or 200) courses were sampled from different colleges within the university in order to obtain a wide variety of majors and minors; for example, professors were contacted who taught courses in the College of Arts and Sciences as well as the College of Engineering. Trained research assistants recruited the students during class by advertising the study as assessing "attitudes toward computer behaviors." Next, the professors e-mailed the link to their students and also posted it on the university's e-Education platform, Blackboard Learn. Participants did not receive any incentives from the researchers to complete the survey. The undergraduate students were recruited for approximately three weeks.

The study was conducted electronically using an Internet-based survey. Once the respondents accessed the website, the home page explained the study while acting as a consent form to which the respondents had to agree or decline to participate. In order to participate in the study, the individual had to also indicate that he/she was at least 19 years of age or older (based on the State's definition of a "minor") and currently enrolled as a student at the university. The waiver of consent stressed the voluntary nature of the study, the anonymity of the data collected, and the ability for respondents to quit the Internet survey at any time with no repercussion. If the prospective respondents met the study's requirements and agreed, they had to click on the "I Agree" button in order to participate in the study, which took approximately 15 minutes to complete in total.

No identifying information (e.g., names, IP address) was recorded or collected in the survey or asked of the respondent at any time, so identification of the participants was impossible. Anonymity and confidentiality was important in order to increase the participants' confidence

in self-disclosing criminally sanctioned behaviors (e.g., virus writing). All survey items were forced-choice, but the respondents were able to select ''decline to respond'' to any item, as required by the Institutional Review Board (IRB). At the end of the questionnaire, once participants had submitted their responses, they were directed to a page thanking them for their time and participation, and contact information for the research team was provided. All respondents were treated in accordance with the ethical standards set forth by the American Psychological Association (APA).

Data

The survey comprised of several questionnaires, which were previously used or adapted from studies in the areas of computer deviant behavior (e.g., Rogers 2001; Rogers et al. 2006a; Rogers et al. 2006b; Seigfried et al. 2008; Seigfried-Spellar et al. 2010). In addition, these scales have consistently shown acceptable levels of reliability in research related to computer deviant behavior. The current study comprised of the following questionnaires/scales: demographics, Computer Crime Index–Revised, Five-Factor Model Rating Form (FFMRF), and the Moral Decision-Making Scale (MDKS). First, the respondents' basic demographic information was self-reported via an on-line questionnaire, which included items such as sex, age, and college major/minor. The demographics survey appeared at the beginning of the study for all of the respondents and was advertised as assessing "attitudes toward computer behavior." By placing the demographics questionnaire prior to the questions regarding computer criminal behavior, this method increased the accuracy of self-reported demographics, such as sex, for this study (cf., Birnbaum 2000).

Dependent Variables

Individual differences, meaning the respondents' personality and cognitive characteristics, were the dependent variables of the current study. In order to assess the personality characteristics of the respondents, the Five-Factor Model Rating Form (FFMRF) measured the following individual differences, which are considered to be the five key traits of personality: Neuroticism (emotional instability), Extraversion (positive affect), Openness to Experience (unconventionality), Agreeableness (vs. antagonism), and Conscientiousness (constraint; Mullins-Sweatt et al. 2006; Widiger 2004; Widiger and Lowe 2007). The FFMRF displays 30 polar opposites on a Likert scale of 1 (extremely low) to 5 (extremely high). For example, the neuroticism item, Impulsivity, is measured with "tempted, urgency" at one end of the spectrum and "controlled, restrained" on the polar end. In the current study, the FFMRF had acceptable Cronbach's alpha levels for the five factors: Neuroticism = .66, Extraversion = .75, Openness = .70, Agreeableness = .74, and Conscientiousness = .87.

In addition, the cognitive disposition of the individual was assessed using the Moral Decision-Making Scale (MDKS), which focuses on the respondents' "moral compass," meaning whether or not decisions are based on hedonistic, internal, or social values (Rogers et al. 2006a). The MDKS included 15 items, scaled from 1 (not important in my decisions) to 8 (very important in my decisions), for statements such as "if I could be punished for my decision." Using the instrument's standardized scoring procedures, certain items will be summed together in order to score each respondent on the three decision-making values: hedonism, internal, and social values. The Moral Decision-Making subscales had the following reported Cronbach's alphas: Social ($\alpha = .74$), Internal ($\alpha = .87$), and Hedonistic = ($\alpha = .83$).

Independent Variables

The respondents' cybercriminal behavior was treated as a grouping variable (independent variable) in the current study. Previous research has categorized individuals based on their computer deviant behavior, as either computer deviant or non-computer deviant (cf., Rogers 2001; Rogers et al. 2006a; Rogers et al. 2006b; Seigfried-Spellar et al. 2010). However, computer deviancy includes a wide range of criminal behaviors, which involve different technical skillsets and motivations. Therefore, the current study grouped the respondents into different categories of computer deviants in order to better understand the individual differences between hackers, cyberbullies, virus writers, and identity thieves.

Roger's et al. (2006a) Computer Crime Index–Revised (CCI–R) measured the frequency and prevalence of self-reported deviant computer behavior. Based on item response, respondents were classified as hackers, cyberbullies, identity thieves, and/or virus writers. Individuals who did not self-report computer deviant behavior were classified as a non-computer deviant. For example, an individual who engaged in hacking behaviors was classified as a hacker (1) and individuals who did not self-report computer hacking behaviors were classified as non-hackers (0). Although pirating was measured in the CCI–R, it was not considered for inferential statistics since this behavior has become marginalized in society. The following statements are examples from the CCI–R, which were used to classify the respondents' computer deviant behavior:

1. Cyberbullying: knowingly harassing, annoying, or stalking someone through the use of e-mails, social media, or other forms of technology.
2. Hacking: knowingly accessing a computer system or network without authorization.
3. Identity theft: knowingly electronically obtaining another person's credit card information without permission.
4. Virus writing: knowingly writing or using a program that would infect a computer or network.

In total, 6 items assessed cyberbullying behaviors, 36 corresponded with hacking, and 9 items addressed identity theft and virus writing, each. There were more items related to hacking because hacking involves a wider range of behaviors, including guessing passwords and website defacement, for example.

In addition, the current study treated the respondents' college major/minor as a grouping variable (independent variable) based on the previous research that suggested that there might be personality differences between computer deviants from different college samples (liberal arts vs. technology). As part of the demographics questionnaire, respondents self-reported their current major(s) and minor(s) as an open-ended question. Based on their responses, respondents were classified into one of four categories: (1) Arts, (2) Sciences, (3) Business, or (4) "Both." Individuals classified as majoring in the "Arts" included the social sciences, humanities, and fine arts, such as theater, psychology, languages, criminal justice, and music. Majors and minors in the "Sciences" category included the traditional hard sciences: computer science, engineering, chemistry, biology, and physics, to name a few. Majors and minors in the "Business" category included general business, management, accounting, operations management, finance, marketing, and other business-related programs. Lastly, students who had some combination of the previous categories (i.e., Chemistry major and Spanish minor) were classified as "Both."

These categories were chosen because: (1) computer deviants from different college samples (arts vs. technology programs) may exhibit different personalities; (2) research has shown computer hackers are more likely to choose career paths related to information technology and science; (3) the authors wanted to eliminate any overlap in categories so a "Both" category was created; and (4) There are different skillsets (technical) required for committing various forms of computer deviant behavior. The creation of a "Both" category was important because the University where the students were sampled from requires that all students graduate with a major and minor (or double major), which is not a common practice at other major Universities. By creating "pure" categories (i.e., Art-only, Science-only, Business-only) and a "Both" category, the authors attempted to eliminate a possible source of error in the data. In addition, computer deviancy may be considered a continuum of low to high levels of technical skills (Rogers 2001). For instance, cyberbullying requires less technical skill than hacking, and both require less technical skills than virus writing. Thus, the authors were investigating whether computer deviancy was related to degree majors; for example, are students majoring in business more likely to engage in identity theft whereas students majoring in the hard-sciences would be more likely to engage in virus writing?

ANALYTIC STRATEGY

Two-tailed statistical significance was set at the alpha level of 0.05 prior to any analyses; however, due to the exploratory nature of this study, marginal significance levels of .10 were discussed in some cases. First, a zero-order correlation was conducted to identify if any personality characteristics (e.g., extraversion) were significantly associated with the different types of cybercrime (hacking, identity theft, cyberbullying, and virus writing). In an attempt to minimize chance associations, findings from the zero-order correlation were further validated by a one-way analysis of variance (ANOVA). When assessing the best predictive model for each type of cybercrime behavior, only the significantly related personality characteristics were entered into a backward stepwise (Wald) logistic regression (LR). Logistic regressions are appropriate for exploratory analyses, for they are more robust with fewer violations of assumptions, such as small and unequal sample sizes (Tabachnick and Fidell 2007). Finally, in order to determine significant mean group differences in the personality characteristics of cybercriminals with different degree majors, post hoc analyzes were conducted.

FINDINGS

Descriptives

Three hundred and ninety-eight undergraduate students from a large, Southern university voluntarily participated in the current study. Final data analyses included 296 due to missing data (incomplete item responses). As shown in Table 1, the sample of participants was evenly split between males and females. The majority of the participants were white (80%, $n = 236$), Christian (83.4%, $n = 247$), and under the age of 21 years (87%, $n = 257$). As shown in Table 1, students majoring and minoring in the Arts made up the largest category with 35% ($n = 103$).

TABLE 1
Demographics of Computer Deviants and Non-Computer Deviants

	Computer		
Variable	*Deviant (n =179)*	*Non-Deviant (n = 117)*	*Total (N = 296)*
Sex			
Male	88 (49.2)	62 (53.0)	150 (50.7)
Female	90 (50.3)	55 (47.0)	145 (49.0)
Decline	1 (0.5)	0	1 (0.3)
Age (yrs)			
19	85 (47.5)	56 (47.9)	141 (47.6)
20	47 (26.3)	33 (28.2)	80 (27.0)
21	22 (12.3)	14 (12.0)	36 (12.2)
22	14 (7.8)	6 (5.1)	20 (6.8)
≥ 23	11 (6.1)	8 (6.8)	19 (6.4)
College Major/Minor			
Art	61 (34.1)	42 (35.9)	103 (34.8)
Science	34 (19.0)	29 (24.8)	63 (21.3)
Business	42 (23.5)	16 (13.7)	58 (19.6)
Both	32 (17.9)	23 (19.7)	55 (18.6)
Decline	10 (5.5)	7 (5.9)	17 (5.7)
Ethnicity*			
Caucasian/White	151 (84.4)	85 (72.6)	236 (79.7)
Black	16 (8.9)	16 (13.7)	32 (10.8)
Asian	5 (2.8)	9 (7.7)	14 (4.7)
Hispanic/Latino	5 (2.8)	1 (0.9)	6 (2.1)
Other	2 (0.6)	6 (5.1)	8 (2.7)
Religion			
Christian	145 (81.0)	102 (87.2)	247 (83.4)
No Religion, Secular	18 (10.0)	8 (6.8)	26 (8.7)
Atheist/Agnostic	9 (5.0)	2 (1.7)	11 (3.7)
Other	7 (4.0)	4 (3.4)	11 (3.7)
Decline	0	1 (0.9)	1 (0.5)

Values represent frequencies with percentages in parentheses.
*Two-Tailed Fisher's Exact Test, $p = .027$.

21% ($n = 63$) of the undergraduate students were Science majors, 20% ($n = 58$) were Business majors, and 19% ($n = 55$) had a major/minor in at least two of the previous categories ("Both"). Of the 296 respondents, 179 (60%) reported engaging in some form of cybercrime. Only 40% ($n = 117$) of the respondents reported never engaging in hacking, cyberbullying, identity theft, or virus writing. 57% ($n = 170$) of students reported engaging in hacking behaviors, 13% ($n = 38$) reported engaging in identity theft, 23% ($n = 66$) reported engaging in cyberbullying, and 8% ($n = 23$) engaged in virus writing.

As shown in Table 2, there was a significant relationship between the categories of computer deviant behavior in that individuals who engaged in one form of computer deviance (e.g., hacking) were also more likely to engage in another (e.g., cyberbullying; all were significant at $p < .01$). 4.7% ($n = 14$) of the respondents reported engaging in all types of cybercrime behaviors (hacking, identity theft, cyberbullying, and virus writing). Of the 170 hackers, 45% ($n = 76$) of

TABLE 2
Zero-Order Correlation between Computer Deviant Behaviors

	Computer Deviant Behavior			
	Hacking	*Identity Theft*	*Cyberbullying*	*Virus Writing*
H	1.0	0.28*	0.36*	0.24*
IT		1.0	0.33*	0.57*
CB			1.0	0.37*
VW				1.0

*$N = 290$; $p < .01$ (2-tailed)

TABLE 3
Prevalence of Computer Deviance by College Major/Minor

	College Major/Minor				
Computer Deviant	*Art*	*Science*	*Business*	*Both*	*Total (N = 168)*
Hacker-only	32 (36.4)	18 (20.4)	19 (21.6)	19 (21.6)	88 (52.4)
Identity Thief-only	0	0	1 (50.0)	1 (50.0)	2 (1.2)
Virus Writer-only	0	0	0	0	0
Cyberbully-only	2 (33.3)	1 (16.7)	1 (16.7)	2 (33.3)	6 (3.6)
Hacker & Virus	1 (50.0)	0	0	1 (50.0)	2 (1.2)
Hacker & Identity	4 (40.0)	3 (30.0)	1 (10.0)	2 (20.0)	10 (6.0)
Hacker & Bully	12 (36.4)	9 (27.3)	8 (24.2)	4 (12.1)	33 (19.6)
Hacker, Identity, Virus	2 (40.0)	1 (20.0)	2 (40.0)	0	5 (3.0)
Hacker, Identity, Bully	2 (28.6)	1 (14.3)	4 (57.1)	0	7 (4.2)
Hacker, Virus, Bully	1 (100)	0	0	0	1 (0.5)
All types of crimes	5 (35.7)	1 (7.2)	5 (35.7)	3 (21.4)	14 (8.3)

Values represent frequencies with percentages in parentheses.

11 of the original 179 computer criminals were dropped from this analysis due to missing data on the other computer criminal behaviors.

the hackers were engaging in other forms of cybercrime. Only 31.8% ($n = 94$) of the respondents *only* engaged in computer hacking. Less than 1% ($n = 2$) of respondents self-reported solely engaging in identity theft, where as 2.4% ($n = 7$) of respondents were only engaging in cyberbullying (see Table 3). Finally, none of the respondents were sole virus writers, which is to be expected since computer deviancy follows a Guttman-like progression in that individuals start with the least technical computer deviant behavior and progress to more technically challenging computer deviant behaviors (see Hollinger 1988). Overall, the descriptive results suggested individuals who engaged in one form of cybercrime were more likely to self-report engaging in another. Hacking was the only cybercrime with distinctive specific versus general cyber deviance groups: hacker-only ($n = 94$) versus hacker + other cyber deviance ($n = 76$).

Hypothesis Testing

H_1: There are differences in the degree majors (Arts, Sciences, Business, "Both") of computer deviants (hackers, virus writers, cyberbullies, and identity thieves) when compared to non-computer deviants.

A chi-square analysis was conducted in order to determine if hackers, virus writers, cyberbullies, and identity thieves were more likely to major in the Arts, Sciences, Business, or "Both" compared to non-computer deviants. As shown in Table 4, there was no significant difference between the hackers and non-hackers, χ^2 (3) = 3.67 with $p > .05$, and the cyberbullies and non-cyberbullies, χ^2 (3) = 5.23 with $p > .05$, regarding degree majors. In addition, there was no significant difference between the identity thieves and non-identity thieves, χ^2 (3) = 5.05 with $p > .05$, regarding degree majors. Due to small cell counts, Fisher-Freeman-Halton exact test was conducted for the virus writers and non-virus writers, which also determined no significant differences in degree majors, Fisher-Freeman-Halton test = 3.39 with $p > .05$. Overall, this hypothesis was not supported in that there were no differences in the degree majors of computer deviants and non-computer deviants. However, the author would like to note that there was a sex difference in degree majors for computer hackers and identity thieves; the authors plan to discuss these findings in detail in a separate manuscript.

H_2: There will be individual differences between computer deviants (hacker, virus writers, cyberbullies, and identity thieves) and non-computer deviants.

Hacking. As shown in Table 5, there was no statistically significant difference in personality characteristics between the hackers and non-hackers. However, there was a moderately significant relationship between hacking and Agreeableness, $r_{pb}(268) = -.11$ with $p = .07$, meaning hackers scored lower on the trait Agreeableness (more antagonistic) compared to the non-computer hackers. Although the relationship was only moderately significant, exploratory analyses were conducted. An ANOVA suggested significant group differences existed for the self-reported

TABLE 4
Computer Criminal versus Non-Computer Criminal Behavior by College Major/Minor

	College Major/Minor				
Computer Behavior	*Art*	*Science*	*Business*	*Both*	*Total*
Hacker	59 (36.9)	33 (20.6)	39 (24.4)	29 (18.1)	160
Non-Hacker	44 (36.7)	31 (25.8)	19 (15.8)	26 (21.7)	120
Identity Thief	13 (34.2)	6 (15.8)	13 (34.2)	6 (15.8)	38
Non-Identity Thief	90 (37.5)	56 (23.3)	45 (18.8)	49 (20.4)	240
Cyberbully	22 (35.5)	12 (19.3)	19 (30.6)	9 (14.6)	62
Non-Cyberbully	79 (37.4)	48 (22.7)	38 (18.0)	46 (21.9)	211
Virus Writer	9 (40.9)	2 (9.1)	7 (31.8)	4 (18.2)	22
Non-Virus Writer	94 (36.7)	60 (23.3)	51 (20.0)	51 (20.0)	256

Values represent frequencies with percentages in parentheses.
Overall total (*N*) differs for each category of computer behavior due to missing data.

TABLE 5
Zero-Order Correlation between Computer Criminal Behavior and Individual Differences

	Individual Differences							
	N	*E*	*O*	*A*	*C*	*IV*	*SV*	*HV*
Hacking	0.08	0.07	−0.02	−0.11*	.01	−0.03	−0.03	0.03
Identity Theft	.15**	−.14**	−.11*	−.13**	−.15**	−.26***	−.18***	−.17***
Cyberbully	.18***	.03	.01	−.15**	−.10*	−.18***	−.11*	−.09
Virus Writing	.08	−.04	.02	−.17***	−.17***	−.23***	−.14**	−.14**

N = Neuroticism, E = Extraversion, O = Openness, A = Agreeableness, C = Conscientiousness, SV = Social Value, IV = Internal Value, HV = Hedonistic Value.
$^{*}p < .10$; $^{**}p < .05$; $^{***}p < .01$.

hackers ($M = 3.32$, $SD = .65$) and non-hackers ($M = 3.47$, $SD = .65$) regarding their scores on Agreeableness, $F(266) = 3.24$ with $p = .07$. Based on these analyses, a binary logistic regression (enter) was conducted to determine if Agreeableness significantly predicted self-reported hacking. Results suggested low scores on the agreeableness trait was a moderate significant predictor of hacking ($W = 3.14$, $p = .07$). The Hosmer and Lemeshow test was non-significant, $\chi^2(8) = 10.54$ with $p = .23$; however, the model explained only 1% of the variance between hackers and non-hackers.

Identity Theft

Next, identity theft was significantly related to the following personality and cognitive differences variables (see Table 5): Neuroticism, $r_{pb}(268) = .15$ with $p < .05$; Extraversion, $r_{pb}(268) = -.14$ with $p < .05$; Agreeableness, $r_{pb}(268) = -.13$ with $p < .05$; Conscientiousness, $r_{pb}(268) = -.15$ with $p < .05$; Social Values, $r_{pb}(268) = -.18$, $p < .01$; Internal Values, $r_{pb}(268) = -.26$, $p < .01$; and Hedonism, $r_{pb}(268) = -.17$, $p < .01$. As suggested by the zero-order correlation, there were significant group differences between identity thieves and non-identity thieves on Neuroticism, Extraversion, Agreeableness, Conscientiousness, Social Values, Internal Values, and Hedonism (see Table 6). Based on these analyses, a backward stepwise (Wald) logistic regression was conducted to determine the best predictive model for self-reported identity theft (see Table 7). Results suggested the best predictive model for distinguishing between identity thieves and non-identity thieves included high scores on the neuroticism trait ($W = 3.83$, $p < 05$) and low scores on internal moral values ($W = 14.11$, $p < .01$). The Hosmer and Lemeshow test was non-significant, $\chi^2(8) = 7.55$ with $p = .48$, indicating the final model fit the data. The Hosmer and Lemeshow's measure (R_L^2) suggested this model explained 10% of the variance in identity theft.

Cyberbullying

The authors investigated whether there were personality and cognitive differences between cyberbullies and non-cyberbullies. As shown in Table 5, cyberbully behavior was significantly related to the following individual differences: Neuroticism, $r_{pb}(268) = .18$ with $p < .01$;

TABLE 6
Means and Standard Deviations for Individual Differences by Computer Criminal Behavior

	FFMRF					*MDKS*		
Computer Behavior	*N*	*E*	*O*	*A*	*C*	*IV*	*SV*	*HV*
Hacker	2.52 (0.60)	3.45 (0.68)	3.27 (0.63)	3.32 (0.65)*	3.67 (0.73)	5.25 (1.26)	4.76 (1.14)	5.14 (1.12)
Non-Hacker	2.42 (0.63)	3.36 (0.68)	3.30 (0.63)	3.47 (0.65)*	3.66 (0.73)	5.31 (1.15)	4.82 (1.16)	5.08 (1.18)
Identity Thief	2.27 (0.79)***	3.16 (0.72)**	3.10 (0.75)*	3.17 (0.81)**	3.37 (0.90)***	4.44 (1.34)***	4.24 (1.38)***	4.59 (1.33)***
Non-Identity Thief	2.44 (0.58)***	3.45 (0.67)**	3.31 (0.61)*	3.42 (0.63)**	3.70 (0.69)***	5.39 (1.14)***	4.86 (1.10)***	5.19 (1.10)***
Cyberbully	2.66 (0.56)***	3.44 (0.69)	3.29 (0.63)	3.21 (0.66)**	3.53 (0.73)*	4.88 (1.17)***	4.55 (1.12)*	4.93 (1.18)
Non-Cyberbully	2.42 (0.62)***	3.40 (0.68)	3.28 (0.63)	3.44 (0.64)**	3.70 (0.72)*	5.39 (1.19)***	4.86 (1.15)*	5.17 (1.13)
Virus Writer	2.64 (0.69)	3.32 (0.67)	3.34 (0.58)	2.98 (0.80)***	3.22 (0.78)***	4.30 (1.39)***	4.23 (1.44)**	4.55 (1.48)**
Non Virus Writer	2.46 (0.61)	3.42 (0.68)	3.28 (0.63)	3.42 (0.63)***	3.70 (0.71)***	5.35 (1.15)***	4.83 (1.12)**	5.15 (1.10)**

Values represent means with standard deviations in parentheses. FFMRF (Five-Factor Model Rating Form): N = Neuroticism, E = Extraversion, O = Openness to Experience, A = Agreeableness, C = Conscientiousness. Scale ranges from 1 (Extremely Low) to 5 (Extremely High); MDKS = Moral Decision-Making Scale: IV = Internal Values, SV = Social Values, HV = Hedonistic Values. Scale ranges from 1 (Not Important) to 7 (Very Important).

*$p < .10$; **$p < .05$; ***$p < .01$.

TABLE 7
Backward Stepwise (WALD) Logistic Regression of Individual Differences and Computer Deviance

Variable	*B*	*SE B*	*Exp (B)*
		Hacking	
Step 1			
A*	−0.34	0.19	0.71
		Identity Theft	
Step 1			
N*	0.56	0.34	1.75
E	−0.45	0.31	0.64
A	−0.18	0.36	0.84
C	−0.13	0.35	0.88
IV**	−0.78	0.33	0.46
SV	0.16	0.31	1.18
HV	0.22	0.29	1.25
Step 6 (last)			
N**	0.61	0.32	1.58
IV***	−0.59	0.16	0.55
		Cyberbullying	
Step 1			
N**	0.56	0.25	1.75
A	−0.36	0.25	0.70
IV*	−0.23	0.13	0.79
Step 2 (last)			
N**	0.55	0.25	1.74
IV***	−0.31	0.12	0.73
		Virus Writing	
Step 1			
A	−0.6	0.43	0.56
C	−0.38	0.44	0.69
IV***	−1.05	0.42	0.35
SV	0.48	0.39	1.61
HV	0.38	0.37	1.46
Step 5 (last)			
IV***	−0.64	0.18	0.53

For brevity, only the first and last step of the logistic regression was included. N = Neuroticism, E = Extraversion, O = Openness to Experience, A = Agreeableness, C = Conscientiousness, IV = Internal Values, SV = Social Values, HV = Hedonistic Values.

*$p < .10$; **$p < .05$; ***$p < .01$.

Agreeableness, $r_{pb}(268) = –.15$ with $p < .05$; and Internal Values, $r_{pb}(268) = −18$, $p < .01$. As suggested by the zero-order correlation, there were significant group differences between cyberbullies and non-cyberbullies for Neuroticism, Agreeableness, and Internal Values (see Table 6). Based on these analyses, a backward stepwise (Wald) logistic regression was conducted to determine the best predictive model for cyberbullying behaviors. Results suggested the best predictive model for cyberbullying included high scores on the neuroticism trait ($W = 4.95$, $p <$

05) and low scores on internal moral values (W = 6.36, $p < .01$). The Hosmer and Lemeshow test was non-significant, $\chi^2(8) = 4.55$ with $p = .80$, indicating the final model fit the data. The Hosmer and Lemeshow's measure ($R_L{}^2$) suggested this model explained 5% of the variance in cyberbullying.

Virus Writing

As shown in Table 5, virus writing was significantly related to the following individual differences: Agreeableness, $r_{pb}(268) = –.17$ with $p < .01$; Conscientiousness, $r_{pb}(268) = –.17$ with $p < .01$; Social Values, $r_{pb}(268) = –.14$, $p < .05$; Internal Values, $r_{pb}(268) = –.23$, $p < .01$; and Hedonism, $r_{pb}(268) = –.14$, $p < .05$. As suggested by the zero-order correlation, there were significant group differences between virus writers and non-virus writers for Agreeableness, Conscientiousness, Social Values, Internal Values, and Hedonism (see Table 6). Based on these analyses, a backward stepwise (Wald) logistic regression was conducted to determine the best predictive model for virus writers. Results suggested the best predictive model for virus writing included low scores on Internal Moral Values ($W = 12.52$, $p < .01$). The Hosmer and Lemeshow test was non-significant, $\chi^2(8) = 9.95$ with $p = .27$, indicating the final model fit the data. The Hosmer and Lemeshow's measure ($R_L{}^2$) suggested this model explained 9% of the variance in cyberbullying.

H_3: There will be individual differences for computer deviants (hackers, virus writers, cyberbullies, and identity thieves) with different degree majors (Arts, Sciences, Business, "Both").

The following analyses only included those individuals who self-reported hackers, virus-writers, cyberbullies, or identity thieves. For each category of cybercrime, a one-way ANOVA was conducted to determine if there were personality differences, which discriminated between hackers, cyberbullies, virus writers, or identity thieves with degree majors. If the ANOVA yielded significant group differences, post hoc pairwise comparisons were conducted; specifically, Bonferroni guarantees control over Type 1 error rate and is generally more conservative; Gabriel's pairwise test performs well if sample sizes are different; and the Games-Howell test copes well for cases where population variances may differ. For large differences in sample sizes, Hochberg's GT2 test was conducted in addition to the other *post hoc* analyses (see Field 2013).

Hacking

For the hackers, the results suggested a significant mean difference on Hedonism, $F(3, 136) = 3.87$ with $p < .01$. The hackers majoring in the Arts ($M = 5.56$) were significantly more hedonistic than the hackers majoring in Business ($M = 4.82$; Bonferroni, $p = .01$; Gabriel, $p = .01$; Games-Howell, $p = .01$).

Identity Theft

For the identity thieves, there were significant group differences on Extraversion, $F(3, 29) = 5.15$ with $p < .01$; and Openness to Experience, $F(3, 29) = 3.35$ with $p < .05$. The identity

thieves majoring in Business were significantly more extraverted ($M = 3.65$) from the hackers majoring in "Both" ($M = 2.50$; Bonferroni, $p < .01$; Gabriel, $p < .01$; Games-Howell, $p = .06$; Hochberg GT2, $p < .01$). Also, identity thieves majoring in "Both" were less open to experiences ($M = 2.36$) compared to the Science ($M = 3.58$) and Business ($M = 3.28$) majors (Bonferroni, $p = .05$; Gabriel, $p = .05$; Games-Howell, $p = .09$; Hochberg GT2, $p = .05$; and Bonferroni, $p = .06$; Gabriel, $p = .05$; Games-Howell, $p = .20$; Hochberg GT2, $p = .06$; respectively).

Cyberbullying

There were no significant differences in the personality characteristics of cyberbullies with different degree majors.

Virus Writing

For the virus writers, significant group differences were only investigated for the Art, Business, and "Both" degree majors; Science was dropped from all analyses due to the small sample size ($n = 1$). For the virus writers, there were significant group differences on Social Values, $F(2, 15) = 5.31$ with $p < .05$; Internal Values, $F(2, 15) = 4.95$ with $p < .05$; and Hedonism, $F(2, 15) = 4.96$ with $p < .05$. For Internal Values, the virus writers majoring in the Arts ($M = 5.30$) were more likely to make decisions based on internal moral values compared to the virus writers majoring in Business ($M = 3.53$; Bonferroni, $p = .05$; Gabriel, $p = .05$; Games-Howell, $p = .06$; Hochberg GT2, $p = .05$).

In addition, the virus writers majoring in the Arts ($M = 5.25$) were significantly more likely to make decisions based on social values compared to the virus writers majoring in Business ($M = 3.46$, Bonferroni, $p = .05$; Gabriel, $p = .05$; Games-Howell, $p = .07$; Hochberg GT2, $p = .05$) and "Both" ($M = 3.20$, Bonferroni, $p = .05$; Gabriel, $p = .04$; Games-Howell, $p = .05$; Hochberg GT2, $p = .06$). Finally, the virus writers majoring in the Art were significantly more hedonistic ($M = 5.50$) compared to the virus writers majoring in Business ($M = 3.60$, Bonferroni, $p = .03$; Gabriel, $p = .03$; Games-Howell, $p = .05$ Hochberg GT2, $p = .03$).

Summary

Overall, the authors' expectation of significant group differences was supported; *post hoc* analyses yielded significant differences in the personality characteristics of hackers, identity thieves, and virus writers with different college majors. The hackers majoring in the Arts were more hedonistic compared to the hackers majoring in Business. The identity thieves majoring in Business were more extraverted and open to experiences compared to the identity thieves majoring in "Both"; Science majors were also more open to experience compared to the identity thieves majoring in "Both." Finally, the virus writers majoring in the Arts were more likely to make moral decisions based on hedonistic, social, and internal moral values compared to the virus writers majoring in Business; the Art majors were also significantly more likely to make moral decisions based on social values compared to the virus writers majoring in "Both."

DISCUSSION

Consistent with previous research (Rogers et al. 2006a; Rogers et al. 2006b), there is a greater prevalence of computer deviant behavior than non-computer deviant behavior in college samples, with 60% of the 296 respondents in the current study reporting that they had engaged in some form of cybercrime. However, the current study reported fewer virus writers compared to the Rogers et al. 2006a study (9% vs. 17%, respectively), but the prevalence of identity theft/fraud in the current study was comparable to Selwyn's (2008) study (13% vs. 6%, respectively). Finally, only a few studies have assessed the prevalence of cyberbullying in college student samples (see MacDonald and Roberts-Pittman 2010); the current study reported a higher prevalence rate of cyberbullying (23%) compared to the MacDonald and Roberts-Pittman (2010) study (8.6%). Although, the current study was consistent with the Chapell et al. (2006) study, which reported that 21.8% of college students engaged in cyberbullying. Overall, the prevalence rates for computer deviance in the current study are consistent with the limited number of studies, which have assessed the prevalence of different computer deviant behaviors (hacking, virus writing, cyberbullying, and identity theft) among undergraduate college students.

In addition, the current study suggested individuals who engaged in one form of computer deviancy were also significantly more likely to engage in another form of computer deviance, such as cyberbullying. Although previous research has found most hackers to originate from the hard sciences (Chiesa et al. 2009; Coldwell 1993; Fötinger and Ziegler 1993; Rogers et al. 2006b; Rogers 2010; Schell and Holt 2009; Shaw et al. 1999), results from the present study contradict this finding. In regards to degree major, no significant difference was found between computer deviants and non-computer deviants (hackers and non-hackers; cyberbullies and non-cyberbullies; identity thieves and non-identity thieves; and virus writers and non-virus writers).

Previous research is also contradicted in many ways by findings from the present study on the topic of individual differences between computer deviants (hackers, cyberbullies, identity thieves, and virus writers) and non-computer deviants. It should be noted that the Rogers et al. (2006a), Rogers et al. (2006b), and Seigfried-Spellar et al. (2010) studies were assessing "general computer deviance" versus non-computer deviance. In other words, individuals were not classified based on the "type" of computer criminal behavior (hacking, virus writing); instead, computer deviance was coded as a dichotomous variable (computer deviant = 1, non-computer deviant = 0), making it difficult to make comparisons between the different studies regarding findings on individual differences, specifically agreeableness and introversion.

Schell and Dodge (2002) and Schell and Holt (2009) suggested most hackers have creative problem-solving capabilities, and Bachmann (2010) believed hackers are also more likely to take more risks than the overall population. However, the present study found only a moderately significant difference between hackers and non-hackers, specifically on levels of agreeableness; hackers were found to be more antagonistic than non-hackers. These marginal findings were consistent with the Seigfried-Spellar et al. (2010) study, which suggested undergraduate students who engaged in computer crime were less agreeable (high antagonism) compared to non-computer deviants. If the current study treated computer deviancy as a dichotomous variable, the results were consistent with the previous findings in that computer deviants were more antagonistic than non-computer deviants, $F(1, 271) = 5.66$ with $p = .02$.

Previous research also suggests introversion is the most common personality trait in computer hackers (Fötinger and Ziegler 1993; Shaw et al. 1999). However, the current study did not identity

introversion/extraversion to be a significant predictor of any computer deviant behavior (hacking, virus writing, cyberbullying, identity theft). In the current study, when computer deviance was treated as a dichotomous variable, there was still no evidence of a significant relationship between introversion and computer deviancy, $r_{pb}(271) = .03$ with $p > .05$. The current study improved on the previous methodologies by identifying computer hackers and non-computer hackers with different degree majors/minors, and the only consistent finding was that computer hackers are more antagonistic than non-computer hackers. Due to the globalization of technology, the hacker subculture may be changing to include individuals beyond the stereotyped, specifically the introverted information technologist.

The Millennial Generation, sometimes referred to as the Net Generation, were the first demographic cohort born with computer technology readily available at home (Junco and Mastrodicasa 2007). Individuals with and without a specific interest in computer science or information technology now have access to a variety of means for developing a skillset in computer hacking (e.g., Google search, YouTube videos). Overall, the traditional "hacker" may no longer reference a specific demographic (e.g., introverted) as previous research suggests due to the influence of technology (e.g., Internet, social media) on the current and future generations experiencing its globalization. The difference in extraversion/introversion may distinguish between the different types of computer criminal behavior (hacker versus identity thief) rather than the non-criminal population.

The present study found significant differences between virus writers and non-virus writers across several traits. Virus writers were more antagonistic, exhibited constraint, and were less likely to follow social norms or make decisions based on internal moral or hedonistic reasons compared to the non-virus writers. In addition, low internal moral values were significantly related to individuals who engaged in identity theft and cyberbullying. These results are consistent with Rogers et al. (2006b), which showed computer deviancy was more likely when an individual had loose personal morals. Furthermore, Rogers (2010) believed identity thieves to rank on the lower end of Kohlberg's scale of moral development, in the pre-conventional stage, involving attention-seeking behavior and little respect for authority. In the present study, high neuroticism also predicted identity theft behavior, and neuroticism is often associated with impulsivity, hostility, and the inability to control urges (Widiger and Lowe 2007).

Finally, previous research suggests the most common factor among cyberbullies is the achievement derived from aggressive behavior (Coyne et al. 2009; Holt 2011; Kirwan and Power 2012). In the present study, significant group differences were found between cyberbullies and non-cyberbullies in levels of neuroticism, agreeableness, and internal values, meaning cyberbullies were found to be more neurotic and antagonistic, as well as less reliant on internal moral values for behavioral choices. This elevated level of antagonism is consistent with previous findings that claim cyberbullies are more prone to display dominance and hostility (Aricak 2009; Coyne et al. 2009). Furthermore, as mentioned previously, high neuroticism and low agreeableness are traits associated with hostility, deception, and opposition (Widiger and Lowe 2007). Overall, high antagonism (low agreeableness) was the most consistent trait, which distinguished between the computer deviants and non-computer deviants. Excluding hackers, a lack of personal moral values was the most consistent trait among virus writers, cyberbullies, and identity thieves.

When distinguishing between the categories of computer deviants, significant differences emerged for the relationship between personality characteristics and degree majors/minors. Hackers majoring in the Arts were significantly more hedonistic than the hackers majoring in

Business, while the identity thieves majoring in Business were significantly more extraverted from the hackers majoring in "Both." Again, extraversion may be a trait that distinguishes between different categories of cybercriminals rather than a non-deviant comparison sample. Furthermore, the identity thieves majoring in "Both" were also less open to experiences (more conventional) compared to the Science and Business majors, and virus writers majoring in the Arts were more likely to make decisions based on internal moral values, social values, or hedonism compared to the virus writers majoring in Business. In other words, virus writers majoring in Business follow a different moral compass and are less likely to follow social norms compared to virus writers majoring in Art. However, no significant differences were found between the degree majors for cyberbullying behavior.

Although the study sampled undergraduate students from a large, Southern university, the findings may not be generalizable to the entire population of computer deviants. However, the purpose of the current study was to utilize a college sample in order to compare the differences in degree majors/minors for computer hackers, cyberbullies, identity thieves, and virus writers. Besides pirating, computer hacking was the most prevent form of computer deviance, and few to none reported only being an identity thief or virus writer. Thus, the current analyses included overlaps between categories where individuals who were engaging in virus writing were also engaging in other forms of computer deviance, such as computer hacking (see Table 3). Due to this overlap, the authors were unable to compare the personality and cognitive characteristics of individuals who were solely engaging in certain forms of computer crime, such as sole virus writers versus sole computer hackers. It may be that certain individuals (virus writers) are more likely to engage in a variety of computer deviant behaviors, whereas others (hackers) are more heterogeneous in that their level of engagement in other computer deviant behaviors varies. Level of engagement in other computer deviant behaviors may be due to differences in technical knowledge, skillset, or motivation (see Rogers 2010).

Computer crimes are often described as "burglaries" in that whenever a house is broken into, the first thing society does is call the locksmith, because once the lock is changed, the problem is resolved. However, even if the lock is changed, the person is still in the room. Research should not only focus on information assurance and security from a technical standpoint, but on the personality and cognitive characteristics related to computer criminality across individual, organizational, and national contexts. Law enforcement needs-analysis surveys for computer crime investigations indicate the ability to obtain reliable and valid offender profiles and rigorous investigative protocols are pressing issues (Institute for Security Technology Studies 2004; Rogers and Seigfried 2004). In addition, the digital forensic community may be able to identify the evidence, but the judicial system will eventually expect the field of digital forensics to "put someone behind the keyboard" (Rogers and Seigfried-Spellar, 2012). By understanding the type of person who engages in computer deviance, investigators may be able to link the perpetrator to the digital forensic evidence.

Like with any "real world" crime, individual differences play a key role in the decision behind choosing to engage in such behavior. From a preventative standpoint, individuals who exhibit certain individual differences putting them at greater risk for engaging in computer deviancy may be identified prior to them engaging in computer deviancy. For example, talented students with computer skills who express lower moral values are at a greater risk for engaging in computer hacking (see Xu et al. 2013). Although the hackers and non-hackers did not differ in their moral values in the current study, virus writers, cyberbullies, and identity thieves displayed lower moral values.

As empirical research consistently suggests that morality is a key issue in computer deviance, various initiatives are forming related to cyber education and ethics, including the National Initiative for Cybersecurity Education (NICE). It will become important to identify those students who display a "different moral compass" in order to curb their potential computer deviancy.

Overall, the current study suggests that not all cybercrimes should be treated equally—the term "cybercriminal" is too general, and does not allow for the individual differences between hackers, cyberbullies, virus writers, and identify thieves. Technology is the medium, not the equalizer, for individuals who engage in computer criminal behavior. Low agreeableness (high antagonism) was the only personality trait exhibited by all four types of computer deviants examined for this study. Against previous research and traditional myths of cybercrime, computer deviants were not more likely to major in the hard sciences compared to non-computer deviants in the current study. Again, the use of technology may be so proliferate for the current and future generations of students that engaging in computer deviancy does not automatically suggest computer hackers are more likely to choose career paths related to the hard sciences. In other words, students do not need to have an overt interest in technology in order to seek it out; instead, they are growing up in a society where technology is the norm rather than a "special interest."

There is an unquestioned increase in the prevalence of cybercrime, and as technology becomes more global, it will only be easier for individuals to engage in computer criminal behaviors. Future research should continue to assess the personality and cognitive characteristics of computer deviants while distinguishing between the different types of computer-related crimes. As technology evolves, so does the computer criminal, and the stereotypes of the past may no longer be relevant.

ACKNOWLEDGMENT

The authors acknowledge Ms. Emily Schmidt for her assistance with participant recruitment and data coding on this project.

REFERENCES

Aricak, Osman Tolga. 2009. "Psychiatric Symptomatology as a Predictor of Cyberbullying among University Students." *Eurasian Journal of Educational Research* 34:167–184.

Bachmann, Michael. 2010. "The Risk Propensity and Rationality of Computer Hackers." *International Journal of Cyber Criminology* 4(1&2):643–656.

Birnbaum, Michael (Ed.). 2000. *Psychological Experiments on the Internet*. San Diego, CA: Academic Press.

Bossler, Adam and Thomas Holt. 2010. "Online Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory." *International Journal of Cyber Criminology* 3(1):300–333.

Campbell, Quinn and David Kennedy. 2009. "The Psychology of Computer Criminals." Pp. 140–160 in *Computer Security Handbook* (4th ed.), edited by S. Bosworth and M. E. Kabay. New York: John Wiley & Sons.

Chapell, Mark, Stefanie Hasselman, Theresa Kitchin, Safiya Lomon, Kenneth MacIver, and Patrick Sarullo. 2006. "Bullying in Elementary School, High School, and College." *Adolescence* 41(164):633–648.

Chiesa, Raoul, Stefania Ducci, and Silvio Ciappi. 2009. *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*. Boca Raton, FL: Auerbach Publications.

Coldwell, Robert. 1993. "University Students' Attitudes towards Computer Crime: A Research Note." *Computers & Society* 23(1&2):11–14.

Coyne, Iain, Thomas Chesney, Brian Logan, and Neil Madden. 2009. "Griefing in a Virtual Community: An Exploratory Survey of Second Life Residents." *Journal of Psychology* 217(4):214–221.

Crossler, Robert E., Allen Johnston, Paul Lowry, Quig Hu, Merrill Warkentin, and Richard Baskerville. 2012. "Future Directions for Behavioral Information Security Research." *Computers & Security* 32:90–101.

Ekşi, Füsun. 2012. "Examination of Narcissistic Personality Traits Predicting Level of Internet Addiction and Cyber Bullying through Path Analysis." *Educational Sciences: Theory & Practice* 12(3):1694–1706.

Field, Andy. 2013. *Discovering Statistics Using IBM SPSS Statistics* (4th ed.). Thousand Oaks, CA: SAGE Publications.

Fötinger, Christian and Wolfgang Ziegler. 1993. "Understanding a Hacker's Mind: A Psychological Insight into the Hijacking of Identities." RSA Security. Retrieved June 3, 2011 from (http://www.donau-uni.ac.at/de/department/gpa/Informatik/DanubeUniversityHackersStudy.pdf).

Hinduja, Sameer and Justin W. Patchin. 2008. "Cyberbullying: An Exploratory Analysis of Factors Related to Offending and Victimization." *Deviant Behavior* 29(2):129–156. doi:10.1080/01639620701457816.

Hollinger, Richard C. 1988. "Computer Hackers Follow a Guttman-Like Progression." *Sociology and Social Research* 72(3):199–200.

Holt, Thomas. J. (Ed.). 2011. *Crime On-Line: Correlates, Causes, and Context*. Durham, NC: Carolina Academic Press.

Institute for Security Technology Studies. 2004. "Law Enforcement Tools and Technologies for Investigating Cyber Attacks: Gap Analysis Report." Retrieved December 2, 2012 from (http://www.ists.dartmouth.edu).

International Telecommunication Union (ITU). 2013. "The World in 2013: Facts and Figures." Retrieved January 14, 2013 from (www.itu.int/ict).

Internet Crime Complaint Center. 2013. "2012 Internet Crime Report." Retrieved February 18, 2013 from (http://www.ic3.gov).

Junco, Reynol and Jeanna Mastrodicasa. 2007. "Connecting to the Net Generation: What Higher Education Professionals Need to Know about Today's Students." Washington, DC: NASPA.

Kirwan, Gráinne and Andrew Power. 2012. *The Psychology of Cyber Crime: Concepts and Principles*. Hershey, PA: Information Science Reference.

Loch, Karen D. and Sue Conger. 1996. "Evaluating Ethical Decision Making and Computer Use." *Communications of the ACM* 39(7):74–83.

Menesini, Ersilia and Christiane Spiel. 2012. "Cyberbullying: Development, Consequences, Risk and Protective Factors." *European Journal of Developmental Psychology* 9(2):163–167.

Mesch, Gustavo S. 2009. "Parental Mediation, Online Activities, and Cyberbullying." *Cyberpsychology & Behavior* 12(4):387–393. doi:10.1089/cpb.2009.0068.

Morahan-Martin, J. and P. Schumacher 2000. "Incidence and Correlates of Pathological Internet Use among College Students." *Computers in Human Behavior* 16:13–29.

Mullins-Sweatt, Stephanie N, Janetta E. Jamerson, Doublas B. Samuel, David R. Olson, and Thomas A. Widiger. 2006. "Psychometric Properties of an Abbreviated Instrument of the Five-Factor Model." *Assessment* 13:119–137.

Pratt, Travis, Kristy Holtfreter, and Michael Reisig. 2010. "Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory." *Journal of Research and Crime and Delinquency* 47(3):267–296.

Richardson, Robert. 2010. "2010/2011 Computer Crime & Security Survey." Retrieved October 29, 2012 from (http://gocsi.com/survey).

Rogers, Marcus. 2001. "A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study." Unpublished dissertation, University of Manitoba, Canada.

———. 2010. "The Psyche of Cyber criminals: A Psycho-Social Perspective." Pp. 217–235 in *Cybercrimes: A Multidisciplinary Perspective,* edited by S. Ghosh and E. Turrini. Heidelberg, Germany: Springer-Verlag Law Division.

Rogers, Marcus and Kathryn Seigfried. 2004. "The Future of Computer Forensics: A Needs Analysis Survey." *Computers and Security* 3:12–16.

Rogers, Marcus and Kathryn Seigfried-Spellar. 2012. "Applied Predictive Behavioral Modeling: The Role of Behavioral Sciences in Digital Forensics." Presentation at the American Academy of Forensic Sciences 64th Annual Scientific Meeting, Atlanta, GA.

Rogers, Marcus, Kathryn Seigfried, and Kirti Tidke. 2006a. "Self-Reported Computer Criminal Behavior: A Psychological Analysis." *Digital Investigation* 3:116–120.

Rogers, Marcus, Natalie D. Smoak, and Jia Liu. 2006b. "Self-Reported Computer Criminal Behavior: A Big-5, Moral Choice and Manipulative Exploitive Behavior Analysis." *Deviant Behavior* 27:1–24.

Schell, Bernadette and John Dodge. 2002. *The Hacking of America: Who's Doing It, Why, and How*. Westport, CT: Greenwood Publishing Group.

Schell, Bernadette and Thomas Holt. 2009. "A Profile of the Demographics, Psychological Predispositions, and Social/Behavioral Patterns of Computer Hacker Insiders and Outsiders." Pp. 190–213 in *Online Consumer Protection: Theories of Human Relativism*, edited by K. Chen and A. Fadlalla. Hershey, PA: Information Science Reference.

Seigfried, Kathryn, Richard Lovely, and Marcus Rogers. 2008. "Self-Reported Consumers of Internet Child Pornography: A Psychological Analysis." *International Journal of Cyber Criminology* 2(1):286–297.

Seigfried-Spellar, Kathryn, Marcus Rogers, and Donald Lynam. 2010. "Psychological Analysis of Computer Criminal Behavior: Preliminary Findings." American Academy of Forensic Sciences 62nd Annual Scientific Meeting, Seattle, WA.

Selwyn, Neil. 2008. "A Safe Haven for Misbehaving?: An Investigation of Online Misbehavior among University Students." *Social Science Computer Review* 26(4):446–465.

Shaw, Eric, Jerrold Post, and Kevin Ruby. 1999. "Inside the Mind of the Insider." *Security Management* 43(12):34–42.

Tabachnick, Barbara and Linda Fidell. 2007. *Using Multivariate Statistics* (5th ed.). Boston, MA: Pearson Education.

Widiger, Thomas. 2004. "Five Factor Model Rating Form (FFMRF)." Retrieved (www.uky.edu/∼widiger/ffmrf.rtf).

Widiger, Thomas A. and Jennifer Ruth Lowe. 2007. "Five-Factor Model Assessment of Personality Disorder." *Journal of Personality Assessment* 89(1):16–29.

Xu, Zhengchuan, Qing Hu, and Chenghong Zhang. 2013. "Why Computer Talents become Computer Hackers." *Communications of the ACM* 56(4):64–74.

KATHRYN C. SEIGFRIED-SPELLAR, Ph.D., is an Assistant Professor in the Department of Criminal Justice at The University of Alabama. She earned a Ph.D. in Cyberforensics from Purdue University and a Master of Arts degree in Forensic Psychology at John Jay College of Criminal Justice. She earned a Bachelor of Arts degree with highest distinction from Purdue University in Psychology and Law and Society. Dr. Seigfried-Spellar has multiple publications, book chapters, and conference paper presentations, including international presentations in India, Ireland, and Russia. Her research merges the behavioral sciences with cybercrime, specifically the personality and cognitive characteristics of computer deviants.

KELLIN N. TREADWAY is a senior at The University of Alabama, pursuing a Bachelor of Science degree in Psychology, a Bachelor of Arts degree in Criminal Justice, and minors in Creative Writing and Computing Tech & Applications. Along with being a research assistant to Dr. Seigfried-Spellar in the Criminal Justice Department at The University of Alabama, Ms. Treadway is also President of the University's Cybercrime Club.