AN INSIGHT INTO THE DIFFERENCES OF PSYCHOLOGICAL DISPARATE MOTIVATIONS BETWEEN HACKERS AND CRACKERS

Syed Muzaffar Hussain
School of Applied Psychology, Social Work and Policy, College of Arts and Sciences, Universiti Utara Malaysia

Dr. Sarwat Sultan
Department of Applied Psychology, Bahauddin Zakariya University Multan-Pakistan

Venothiney Dewi Muniandy
Student Counselor, Student Affairs Division, Multimedia University, Cyberjaya, Malaysia

Noor Haslindawati binti Abd
Commercial Crime Investigation Department, IPK Kedah, Malaysia

Abstract

This article studies two different types of computer hackers, and particularly it focuses on disparate inspirations of hacking. Hackers' psyche is discussed in detail on the media platforms but not by psychologists almost. This article uncovers the motivation of hackers and crackers which is investigated, using the study of values scale. The study employed 114 participants through an online research tool. The questions about values and demographics were asked. The contributors were divided into hackers and crackers through their responses. Results showed that hackers had a higher level of motivation for knowledge, aesthetic sense, mysticism, and social interactions. While crackers had motivation because of their economic and political interests. The results suggested that hackers hack for the thrill of learning and gathering information to gain intelligence. Hackers hack for the betterment of society. In the contrast, crackers are unable of normal social interactions, and their hacking is based on the motivation of getting power and money.

Keywords: *Hackers and Crackers, Motivation, Prison, Prisoners.*

INTRODUCTION

In the new millennium, hacking is a worldwide phenomenon and is considered a computer crime. Computer crime is well defined as "any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation, or prosecution" (Benson, Jablon, Kaplan, & Rosenthal, 1997). Hacking, in particular, is defined as "the process of accessing computer systems by persons who have no legitimate access to the systems" (Mulhull, 1999). But hacker activity is not limited to breaking into computer systems. It also includes breaking passwords, creating "logic bombs," e-mail bombs, denial of service attacks, writing and releasing viruses and worms, viewing restricted, electronically-stored information owned by others, adulterating Web sites, or any other behavior that involves accessing a computing system without appropriate authorization (Sansone & Harackiewicz, 2000). We restrict our discussion primarily to computer hacking.

Researchers have only vague ideas: what really pushes hackers to hack, i.e. what is their motivation. Although this is the key issue, too little effort has been made to understand the motivation of the modern generation of hackers (Taylor, 2000). Since only anecdotal and self-reported evidence is available, we might conclude that research in this problem area is not advanced enough. This paper presents empirical research of the hackers' motivation.

All hackers are not the same. In order to best deal with their actions and the intent behind their actions, one must understand who they are. Many hackers are not malicious, in that they hack for the thrill of learning and to "look around". However, others are intent upon gathering information for gain (for-profit or intelligence aspects), corrupting data or denying access to the system, or to see what harm they can cause (McGuire, D'Amico, Tomlinson, et al. 2002).

Raymond (2004) is one of the most recognized experts in the context of the hacker topic. He points out: the term `hacker', most having to do with technical adeptness and a delight in solving problems and overcoming limits. There is a community, a shared culture, of expert programmers and networking wizards that traces its history back through decades to the first time-sharing minicomputers. The members of this culture originated the term `hacker'. Hackers built the Internet. Hackers made the Unix operating system what it is today. Hackers run Usenet. Hackers make the World Wide Web work. There is another group of people who loudly call themselves hackers, but aren't. These are people (mainly adolescent males) who get a kick out of breaking into computers and phreaking the phone system. Real hackers call these people 'crackers' and want nothing to do with them. Real hackers mostly think crackers are lazy, irresponsible, and not very bright, and object that being able to break security doesn't make you a hacker any more than being able to hotwire cars makes you an automotive engineer. Unfortunately, many journalists and writers have been fooled into using the word `hacker' to describe crackers; this irritates real hackers no end. The basic difference is this: hackers build things, crackers break them (Sterling, 1992).

Indeed, there does seem to be a difference between good and evil hackers. Having already categorized hackers in the typology earlier, the most important distinction is between 'hackers' and so-called 'crackers'. So if the community per

se is not following evil intentions, who are the people who hack into systems to damage them or for commercial purposes? As we learned, experts and the hacker community itself distance themselves from those people who seek to cause damage and disruption. They call them crackers. Crackers are the evil hackers of the scene (Voiskounsky, Babaeva, & Smyslova, 2000). Now that we know the typology of hackers and we have learned that a hacker is not necessarily a criminal, we should shift our focus to the ideology and intentions: why those 'computer freaks' behave as they do. We will talk about the psychological drivers of hackers and crackers.

Hackers are often portrayed as being pasty white from a lack of outside contact. They bring about the end of the world, with malicious intent, through computers. Bernhardt Lieberman's findings (1994) indicate that hackers are not markedly different from anyone else - with the obvious exception that many commit crimes on a daily basis by hacking into computers. Lieberman says there are two definitions of hackers. A hacker is either someone who does "elegant programming" on computers and is considered positive in the public's eyes, or a hacker is someone who intrudes upon another's a computer and is viewed as someone who does harm.

Lieberman's work (1994) on "Motivation of Hackers" showed that hackers' highest-rated motivations are "intellectual challenge" and to "learn about computers and computing". Their lowest-rated motivations are "to break the law" and "to get to be known,'' But if hackers' intentions are not malevolent, Lieberman said, he does believe they can cause great harm. Hackers responded higher on Social Anxiety and Social Avoidance measures which suggested that hackers are capable of normal social interactions.

Hackers tend to be rather anti-authoritarian while crackers are found to be motivated to gain power. However, hackers are far more likely than most non-hackers to either (a) be aggressively apolitical or (b) entertain peculiar or idiosyncratic political ideas and actually try to live by them day-to-day. Even hackers who identify with a religious affiliation tend to be relaxed about it, hostile to organized religion in general, and all forms of religious bigotry in particular. Hackers are generally only very weakly motivated by conventional rewards such as social approval or money. They tend to be attracted by challenges and excited by interesting toys, and to judge the interest of work or other activities in terms of the challenges offered and the toys they get to play with (Chan & Yao, 2004).

In contrast to hackers, crackers are malicious user's intent on waging an attack against a person or system. A cracker may be motivated by greed, power, or recognition. Their actions can result in stolen property (i.e. intellectual property, data, etc.), disabled systems, compromised security, negative public opinion, loss of market share, reduced profitability, and lost productivity (Tittel, 2004).

Considering this review of the literature, the current study aimed at knowing the differences between hackers and crackers in terms of their disparate motivations. Though the public associate's labels and titles with the actions of a hacker whether these actions are positive or negative, there is a difference in the drivers of hacking of hackers and crackers. It was assumed that hackers and crackers usually hack with different interests and motivations.

METHODOLOGY
Participants

The sample consisted of 114 hackers; 68 hackers and 46 crackers ranging in from 20 to 37 years with a mean age of 29. All the participants were male. 62% of the participants were employed and 38% were unemployed. 14% had less than a high school education and 86% were with master's degree.

Instrument

Study of Values; This scale ((Spranger, 1989)) measures the six relative prominent interests or motives in personality including Theoretical, Economic, Aesthetic, Social, Political and Religious. The scale is basically designed to used with college students or educated adults. The scale has two parts. Part-I contains 30 items with two alternative answers and are scored on 0-3 range representing disagree to agree. Part-II includes 15 items with four alternative answers scored on 4 point rating scale ranging from 1 to 4 representing low to high degree. There are 120 answers for six subscales, 20 of which refer to each of the six motivations. The higher degree in each measured subscale depicts the higher level of motivation. The mean reliability coefficient (for the whole scale) is .90.

1. The Theoretical: Theoretical man is necessarily an intellectualist, empirical, critical, and rationalist as his dominant interest in discovery of truth
2. The Economic: Economic man is interested in what is useful. He is practical, self-preservation and greedy for wealth.
3. The Aesthetic: Aesthetic men tend toward individualism, self-sufficiency and artistic episodes of life.
4. The Social: Social men are more likely to be listed as altruistic, sympathetic and unselfish.
5. The Political: The political man is interested primarily in power for personal bower, influence and renown.
6. The Religious: The religious man is mystical who comprehend the cosmos as a whole and relate himself to its embracing totality.

RESULTS

To study the significance of differences in disparate motivations of hackers and crackers, independent sample t-test were computed using SPSS.

Table 1

Differences in the disparate motivations of Hackers and Crackers (N=114)

Scales	Hackers (N=68)		Crackers (N=46)		t	p
	M	SD	M	SD		
Theoretical	53.74	8.82	41.21	7.97	2.013	0.02*
Economic	38.74	8.05	58.72	9.02	-2.311	0.01*
Aesthetic	46.35	10.20	38.47	10.01	1.999	0.04*
Social	51.82	9.04	44.91	8.56	2.547	0.01*
Political	39.87	9.55	49.03	10.05	3.131	0.001**
Religion	46.73	8.06	40.05	10.61	2.014	0.03*

df = 112, *p < 0.05, **p < 0.01

Results in Table 1 indicate the significant differences in the motivational behavior behind hacking between hackers and crackers. Findings show that hackers are found to be higher on the motivations of theoretical, aesthetic, social and religion as compared to crackers. Findings further show that crackers have higher motivations of economic and politics than hackers.

DISCUSSION

To the best of the authors' knowledge hackers have not been thoroughly investigated by psychologists. Therefore the current study was planned and it was assumed that hackers' community categorizing as hackers and crackers will have different interests and motivations behind the act of hacking. Differences in the Scores of hackers and crackers on six disparate motivations were found significant. Findings indicated that hackers were high on the motivation of getting intellectual knowledge to discover the truth. With the dominance of this theoretical motivation, the hackers are characterized as empirical, critical, and rational. Therefore the aim of hackers' hacking as compared to that of crackers is to order and systemize their knowledge. Crackers were not found interested in seeking knowledge or discovering the truth. Therefore crackers are not intellectualists who may do well for society. Crackers' mind works on the destruction of privacy and truth on computers.

These findings are inconsistent with the work of Verton (2002) who stated that the motivation for hacking varies but a significant proportion of hackers surveyed indicated innocuous reasons for their behavior. 36 percent said they hack to "advance network, software, and computer capabilities," 34 percent claimed they hack" to solve puzzles or challenges," and 5 percent said they hack to "make society a better place to live."

Hackers were also found motivated toward aesthetic value. Lieberman's study (1994) supported these findings that a hacker is someone who understands technology, so they can make it do anything they want it to do," The questionnaire's results indicate that hackers don't generally seek power for negative results. Motivation for power was found higher among crackers. Crackers' hacking can be subjected to the motivation for personal power, influence, and renown. Hackers had moderately high respect toward the law, even though they "repeatedly break the law,"

One another finding of the present study is pertaining to the value of economics. A cracker is one who breaks security on a system to get the money (Gordon & Loeb, 2002). Crackers hack for some practical reasons (for example, if it's necessary to get around some security in order to get some work done, money, or some bodily needs). Crackers usually are hired for hacking and they get huge amounts of money for breaking the privacies of companies. Findings are in tune with the investigations by Hirschman (1992) that crackers usually seemed to be very destructive as they do the job of getting advantages of money even for negative consequences.

CONCLUSION

Currently, very limited research is available to help researchers and firms understand the behavior of hackers. This paper explored the intentions of hackers and crackers. It was important to us to understand the minds of hackers and crackers for their psychological drivers as well as their intentions. It was found that hackers hack with the intentions of getting knowledge, making life better, acceptance from the social group. They also value their religious approach. On the other hand, crackers have intentions of achieving power and politics. They also hack for their economic goals in life. So it is concluded that hackers' communities hack with varying motivations and all hackers don't hack for the purpose of damaging privacy.

Hacking also has the good aspects that may lead to the progress of the use of technology.

REFERENCES

Benson, C., Jablon, A. V., Kaplan, P. J., & Rosenthal, M. E., (1997). Computer crimes. American Criminal Law Review (34-2), pp. 409-443.

Chan, S. H., & Yao, L. J., (2004). An exploratory study on systems security and hacker hiring. Review of Business Information Systems (8), pp. 17-28.

Gordon, L. A., & Loeb, M. P., (2002). The economics of information security investments. ACM Transactions on Information and System Security (5-4), pp. 438-457.

Mulhall, T, (1999). Where have all the hackers gone? Part 3: Motivation and deterrence. Computers & Security (16), 1999, pp. 291-297.

Raymond, E. S., (2004). Retrieved March 23, 2011, from www.catb.org/~esr/faqs.

Sansone, C. & J. M. Harackiewicz., (2000). Controversies and new directions – Is it déjà vu all over again? In Intrinsic and Extrinsic Motivation: The Search for Optimal Motivation and Performance, C. Sansone and J. M. Harackiewicz (eds.), San Diego: Academic Press, pp. 443-453.

Sterling, B. (1992). The hacker crackdown: law and disorder on the electronic frontier. London: Penguin.

Taylor, P. (2000). Hackers. Crime in the digital sublime.London: Routledge.

Tittel, E., Chapple, M., & Stewart, J. M., (2004). "CISSP: Certified Information Systems Security Professional Study Guide" Sybes 2003 (access via http://www.books24x7.com, 5 Feb. 2004).

Lieberman, B., (1964). "i-Trust: A Notion of Trust in Three Person Games and International Affairs", Journal of Conflict Resolution, Vol. 8.

McGuire, S., D'Amico, E., Tomlinson, K., et al. (2002). Teenagers self-reported motivations for participating in computer crime. Presented at the 8th International Conference on Motivation, Moscow.

Voiskounsky, A. E., Babaeva, J.D., & Smyslova, O.V. (2000). Attitudes towards computer hacking in Russia. In: Thomas, D., and Loader, B.D. (eds.). Cybercrime: law enforcement, security and surveillance in the information age. New York: Routledge, pp. 56–84.

Verton, D., (2002). The hacker diaries: Confessions of teenage hackers. McGraw Hill.