VIRTUAL IMPERSONATION BY ANTISOCIAL PERSONALITIES IN CYBERCRIME

Vilas Padhye* and Manisha Gujar**
*Government College of Arts and Science, Aurangabad, Maharashtra – 431 001
**Government Forensic Science Institute, Aurangabad, Maharashtra – 431 001
(*Email: vilpower@gmail.com)

ABSTRACT

The present study compares Internet usernames by known offenders in cybercrime with ASPD symptoms and college students with the aim of finding differences in the usage patterns in the two groups. The results are quite interesting as no significant differences are seen in the length of the username, or in the usage of alphabet, numerical, and special characters in the two groups. However, the most striking difference is that antisocial personalities are seen to take on false identities while creating a username, while only one subject in the control group was found to do so. The study is relevant in understanding the personality of cybercriminals that is a major concern for crime investigating agencies the world over.

KEY WORDS: Antisocial personality disorder, ASPD, Cybercrime, impersonation

INTRODUCTION

Crime is perhaps old as civilization itself. If we go by religious beliefs, then humanity evolved as a result of Adam's *crime* as he ate the forbidden fruit! Social scientists of course take an objective view of criminal activities in their attempt to understand the causes, study the behavioural patterns, and provide remedial therapy to criminals that would facilitate the process of rehabilitation. There are people who commit acts against the law out of ignorance, others are forced by circumstances, some as a result of improper parenting, and still others simply due to a bad neighbourhood. When we talk about crime and criminals, a picture of break-in, assault, rape or murder comes to the mind almost reflexively. Criminals are presumed to be ugly looking creeps lurking in dark alleys in the underbellies of cities.However, the spectrum of crime has widened in the modern world thanks to use of technology in every walk of life. The deep penetration of the Internet has ushered an era of plastic money, e-banking and e-commerce. While these have brought new business opportunities to entrepreneurs and convenience to customers, it also has its ugly face of fraud and deceit–collectively termed cybercrime. Cybercrime is defined as an unlawful act in which a computer/s is/are used as means of committing a crime against a person, property or the government (Babu and Parishat, 2004). Common cybercrimes include relatively minor nuisance activities like spreading spam to more serious computer assisted criminal acts like stealing home address, family information, hacking into someone's bank account, phishing, stealing vital business information, pornography, economic espionage, and the spread of terrorism.

According to the Norton Cybercrime Report 2011, perhaps the most comprehensive study of cybercrime done so far, the total loss due to cybercrime annually the world over is estimated at $388 billion, out of which 114 billion is a result of direct losses in money stolen by cyberthugs and $274 billion losses are due to time lost in dealing with cybercrime experiences. It turns out that the money lost in cybercrime globally every year is more than the global market in marijuana, cocaine, and heroin combined ($288 million), and more than 100 times the annual expenditure of UNICEF ($3.65 billion). India accounted for direct losses of about $4 billion and another $3.6 billion in time spent on resolving cybercrime, amounting to an alarming annual loss of $7.6 billion. The annual losses reported from China are far bigger at $25 billion, while that of Brazil are about $15 billion. The report also estimates that about 29.9 million people in India fell victim to cybercrime in 2010, out of 431 million people globally. This effectively means that 14 victims fall prey to cybercrime every second, 840 victims every minute, and about 50,000 victims every hour! These figures give us an idea of the extent of the malaise of cybercrime worldwide and a reason why the issue needs to be addressed seriously.

Antisocial personality disorder (ASPD), is routinely associated with traditional criminal behaviour. According to the Diagnostic and Statistical Manual of Mental Disorders, Fourth Edition (DSM–IV) of the American Psychiatric Association (APA, 1994), ASPD is characterized by a pervasive disregard for, and violation of, the rights of other people. According to the criteria of DSM-IV, a person is diagnosed to be suffering from ASPD if he or she displays at least three of the following behavioural patterns before the age of 15 years: repeated criminal acts, deceitfulness, impulsiveness, repeated fights or assaults, disregard for the safety of others, irresponsibility, and lack of remorse. It is further necessary that the person is at least 18 years of age at the time of diagnosis, although there is evidence of the above mentioned behavioural patterns before the age of 15 years. The occurrence of such behaviour should also not be exclusively during the course of another major disorder like schizophrenia or a manic episode. The present study explores the possibility of the role of ASPD in cybercrime, by comparing the crime related behaviour of cybercriminals with a control group. The behavioural pattern of cybercriminals with ASPD traits is compared with non-ASPD individuals. Are there any differences in the behaviour of the two groups when it comes to the cyberworld? Do the two groups differ in specific behaviours about revealing themselves or their identities in the cyberworld? In studying this aspect of their personality, the researchers studied the 'usernames' these people used in cybercrimes and compared them with the usernames of a control group comprising student volunteers. Different aspects of usernames such as length, use of alphabet, numerical, and special characters is studied. Further, the way the subjects in the two groups revealed their identities is also studied.

MATERIALS AND METHODS

The research was carried out in two parts. In the first part, the Cyber Cell, Aurangabad Crime Branch was approached and requested to identify accused in cybercrime who were convicted in the last two years. A checklist for identifying antisocial personality traits was prepared based on DSM IV criterion. Seven cybercriminals with antisocial personality disorder behavioural traits were identified. The usernames used by these convicts in committing cybercrimes were taken from their case files. 30 student volunteers were asked to take the checklist for ASPD traits and the 7 with the lowest scores (all below 3 out of 15) were included in the control group. They were then asked to submit the usernames they used on the Internet while transacting with others. The law enforcing authorities and the volunteers were assured of secrecy in dealing with their personal information during and after the research.

RESULTS

No significant difference was found in the length of usernames or in the use of alphanumerical and special characters in creating usernames in both the groups under study. The length of usernames ranged from 10 to 20 characters in the ASPD group with a mean length of 13 and standard deviation of 3.32. In the control group, the length of usernames ranged between 9 and 19 characters with a mean length of 12.71 and standard deviation of 3.20. Student's independent 't' test was not significant, t (12) = 0.164, p>0.05. Further investigation revealed that the use of alphabet in creating usernames ranged between 18 and 9 for the ASPD group (Mean = 11.29, SD = 3.15) and between 18 and 7 for the control group (Mean = 10.86, SD = 3.53). No significant difference was found in the use of number of alphabet in the two groups, t (12) = = 0.240, p>0.05.

Table – 1. Total Length of Usernames of the ASPD and Control groups

Participants	ASPD Group	Control Group
1	12	14
2	14	11
3	11	13
4	20	19
5	12	12
6	12	11
7	10	9
Maximum	20	19
Minimum	10	9
Mean	13.00	12.71
SD	3.32	3.20

Table 2. Use of Alphabet, Numerical, and Special Characters in Usernames by ASPD and Control groups

Participants	ASPD Group			Control Group		
	Alphabet	Numerical	Spacial Character	Alphabet	Numerical	Spacial Character
1	12	0	0	10	4	0
2	9	4	1	11	0	0
3	10	1	0	11	2	0
4	18	2	0	18	0	1
5	11	0	1	11	0	1
6	9	2	1	8	2	1
7	10	0	0	7	2	0
Maximum	18	4	1	18	4	1
Minimum	9	0	0	7	0	0
Mean	11.29	1.29	0.43	10.86	1.43	0.43
SD	3.15	1.50	0.53	3.53	1.51	0.53

Table 3. Impersonation of Usernames by ASPD and Control groups

ASPD Group	Control Group
07	01

The range for the use of numerical in usernames was found identical for both the groups, between 4 and 0, with the ASPD group having a mean of 1.29 and SD of 1.50, while the control group having a mean of 1.43 and SD of 1.51. No significant difference was found in the use of number of numerical in the two groups, t (12) = = 0.178, p>0.05.
Similarly, the range of special characters (e.g. *, _, #, @) for the two groups was found to be between 1 and 0, with the mean (0.43) and SD (0.53) for the two groups also been identical. With identical mean and standard deviation in both the groups, there was no significant difference in the use of special characters, t (12) = 0, p>0.05. All the 7 subjects in the ASPD group were found to impersonate their identity in creating usernames, while only 1 subject in the control group was found to do so. Chi Square test revealed a significant difference in impersonation by the two groups X^2 (1) = 3.84, p<0.05.

DISCUSSION

Crime, until a few years ago, was limited to the geographical arena in which the criminal could operate. But the Internet has altered the landscape and has made the reach of criminals truly global. There is a false sense of security among most cybercriminals today that they would remain untraceable in the virtual world, and consequently in the real world. Turvey (2002) has pointed out that apart from monetary greed, people are attracted towards cybercrime due to its inherent intellectual challenge, its ability to draw instantaneous attention the world over (as in spreading a virus), and also as it boosts self-esteem (as in the case of hackers). Such acts tend to fuel fantasies, feed power motivation and are rooted in psychological needs that signify an obsessive or addictive personality (Turvey, 2002).

On the face of it, the present study does not suggest any difference in the way cybercriminals present themselves from the rest of the normal population. The length of the username or the use of alphanumerical and special characters does not differ at all with the control group. Hackers and virus writers are known to use flashy pseudonyms and usernames that instantaneously grab attention. But cybercriminals intent on conning another person seem to be more calculative in impersonation. Their usernames appear to be very low profile and convincing. It allows them to appear as any other normal individual, whom one would traditionally call a 'face in the crowd'. Antisocial personality disorder has been widely studied with relation to traditional crime. It has been fairly well established that ASPD is positively correlated with substance abuse (Fridell *et al*., 2008; Hernandez-Avila *et al.,* 2000). Another major group of criminal acts includes theft and conning (Martens, 2000). Antisocial personalities are known to take on a distinctly different name and identity while introducing themselves to their victims. They apparently sound very convincing when impersonating as they display an array of behaviours that would be associated with the assumed role. For instance, they show good domain knowledge of financial matters when appearing as investment agents, credible knowledge of medicine when posing as doctors, or that of law when posing as lawyers. These very traits seem to be associated with cybercrime, as an individual needs to possess good domain knowledge of the working of the Internet and related software in order to commit online financial fraud. The ASPD group in the present study did posses such knowledge and also impersonated in committing fraud.

Relocation by ASPD afflicted individuals after committing fraud on people in order to evade arrest is known. They assume a new identity in each place and get bolder with each new crime as they believe that they can get away with anything. In the cyberworld too, the ASPD group was seen to hold more than one identity, and abandoned one username after another as its utility ended. Another interesting feature that was discovered in the course of the study was that on many occasions, the cybercriminal impersonated his victim, assuming his name and identity and created a username resembling that of the victim's when committing an e-banking related fraud. This has become very easy in the cyberworld where there is no chance of confronting the individual whose identity is impersonated. Such a thing is almost impossible to do in the physical world where one would have to walk in a bank, claim to be another person (the victim), and withdraw money from his account forging his signature. So in a way, the Internet has opened new possibilities of deceit for the antisocially inclined.

Assuming a new identity, even a pseudo-identity, in itself is not a crime. Many people, especially teenagers, are frequently known to pose with different names on different websites. Posting photographs of celebrities or other good-looking individuals as their own on social networking sites like Facebook is extremely common. The problem arises when impersonation, whether deliberate or casual, causes loss to another person or violates the law in some way. There is a very thin line dividing a harmless joke, prank, or an intentional harm because the fallout of any of these actions can be devastating. Many a times the thin line of civility gets crossed unknowingly. Law always looks at the intention or motive behind an act that is defined as crime. And here the difference between the ASPD and control group in the study is apparent. The persons with ASPD had impersonated with an intention to cause economic loss to another person whereas such a motive was not seen in the control group. People with a predisposition to antisocial behaviours use the opportunity of impersonation to con others in cyberspace, whereas those without any such tendency never violate the law. Anonymity has been found to be a major factor that invokes antisocial behaviour in most situations (Baggily and Rogers, 2009). Studies have also conclusively revealed that anonymity is positively correlated with cybercrime (Rogers *et al.,* 2006; Shaw et al., 1998). Individuals high on anonymity and low on pre-employment integrity are found to be most vulnerable to committing cybercrime, although ASPD was not a variable under consideration in the studies (Shaw *et al,* 1998; Baggily and Rogers, 2009). Hinduja (2008) has highlighted the role of deindividuation in Internet software piracy.

Cybercrime is an area relatively unexplored by social scientists and calls for serious research to investigate its correlates with personality traits. This is not only because cybercrime is reaching alarming proportions, but also because its genesis may lie in personality rather than technology. A host of anti-virus software, firewalls, and innumerable precautionary measures by service providers is not deterring cybercriminals from their activities. It seems that people with antisocial predispositions, when exposed to the prospects of crime on the Internet, grab the opportunity that a normal person would not. Hence screening for ASPD traits should be a necessary criterion when hiring professionals in all computer-information technology related organizations. Such precautions may not eliminate cybercrime, but will surely help control it.

CONCLUSION

No significant difference was observed in the way cybercriminals with antisocial personality disorder and the control group of college students formed usernames while transacting on the Internet. Length, use of alphabet, numerical, and special characters in usernames was the same in both the groups. However, impersonation by cybercriminals with ASPD was found to be significantly higher than the control group with only one person in the control group posing with a different identity than his original as compared to all the subjects in the ASPD group.

ACKNOWLEDGEMENT

The researchers express their sincere thanks to Mr. Gautam Patare of the Cyber Cell, Aurangabad Crime Branch, who extended wholehearted cooperation for data collection and also provided deep insights into the behaviour of cybercriminals.

REFERENCES

APA (1994). Diagnostic and statistical manual of mental health disorders (4th ed). Washington DC.

Babu M and Parishat MG. (2004). What is cyber crime? Retrieved November 10, 2009, from http://www.crime-research.org/analytics/702/

Baggily I and Rogers M. (2009). Self-reported cybercrime: An analysis of the effects of anonymity and pre-employment integrity. *Int. J.Cyber Criminol.* **3** (2): 550-565.

CSI Computer Crime and Security Survey. (2008). Retrieved May 25, 2009 from http://i.cmpnet. com /v2. gocsi.com /pdf/ CSIsurvey2008.pdf

Fridell M., Hesse M., Jaeger M.M and Kühlhorn E. (2008). Antisocial personality disorder as a predictor of criminal behaviour in a longitudinal study of a cohort of abusers of several classes of drugs: relation to type of substance and type of crime. *Addictive Behav.*. **33** (6): 799-811.

Hernandez-Avila CA., Burleson J.A., Poling J., Tennen H., Rounsaville BJ and Kranzler HR. (2000). Personality and substance use disorders as predictors of criminality. *Comprehen. Psychiat.*. **41**(4): 276-283.

Hinduja S. (2008). Deindividuation and Internet Software Piracy. *Cyber Psychol. Behavior.* **11**(4): 391-398.

Martens WHJ. (2000). Antisocial and Psychopathic Personality Disorders: Causes, Course and Remission- A Review Article. *Int. J. Offender Therapy Comparative Criminol.* **44**(4): 406-430.

Norton Crime Report (2011). www.norton.com/cybercrimereport

Rogers M., Seigfried K and Tidke K. (2006). Self-reported computer criminal behavior: A psychological analysis. *Digital Investigation*. **3**: 116-120.

Shaw E., Ruby K and Post J. (1998). The insider threat to information systems: The psychology of the dangerous insider. *Security Awareness Bull.* **2**: 1-10.

Turvey B. (2002). *Criminal Profiling*. London: Academic Press.