EDITORIAL

Identity related Crime in the Cyberspace: Examining Phishing and its impact

K. Jaishankar

Last November/December 2007, I was invited to two prestigious events of Cyber Criminology. The POLCYB International Summit on Policing Cyberspace, 2007, Bangkok, Thailand and the UNODC core group meeting of Experts on Identity related Crime and ISPAC Conference at Courmeyeur, Italy. I was also entrusted the task of preparing the Bangkok Declaration of the International summit on Cyberspace by the Society for the Policing of Cyberspace (POLCYB), Canada and that is published as a special paper in this issue. Hence in this editorial I would like to focus about identity related crime and its impact in the cyberspace.

Identity is a holistic term to portray "an individual's comprehension of him or herself as a discrete, separate entity" (Identity, 2008, para 1). Finch (2007, *pp.29-31*) provides a brief typology of identity:

> *"Identity is a complex and multi-faceted concept … and it can be divided in to three categories: personal, social and legal. Personal identity relates to the self as experienced by the individual… social identity is the identity that is perceived by others; it is the external view of the self as viewed by others in society… Legal identity is …the way in which an accumulation of information distinguishes one individual from all others….".*

The importance of identity gains greater significance in this wired era. The use of identity in the cyberspace is greater nowadays. People tend to shop, bank, sell, and have relationship in internet. In these processes their identity plays a superior role, which, however, is being misused by the miscreants. The perpetrators try to misuse the identity of a person for personal gain. This criminal misuse of identity is called identity related crime, which the United Nations Office of Drugs and Crime (UNODC), Vienna, Austria prefers to use and as a member of the core group of experts on Identity-related crime, UNODC[1], I also advocate the use of this term.

[1] "Starting with the release of a study on "Fraud and the criminal misuse and falsification of identity" in 2007 and on the basis of its mandates arising from ECOSOC resolutions 2004/26 and 2007/20, UNODC has launched a consultative platform on identity-related crime with the aim to bring together senior public sector representatives, business leaders, international and regional organizations and other stakeholders to pool experience, develop strategies, facilitate further research and agree on practical action against identity-related crime. In this context, a core group of experts was established to exchange views on the best course of action and the most appropriate initiatives that need to be pursued

Koops & Leenes (2006) were the first to "propose to use the term 'identity-related crime' as an umbrella term. This covers all punishable activities having identity as a target or a principal tool." However, there is no universal definition of identity related crime, as it invariably comprises of many types of crimes such as identity theft, identity fraud, intellectual property abuse and other related crimes (UNODC, 2007a, 2007b). Though, Koops & Leenes (2006) have defined Identity-related crime, as the one that "*concerns all punishable activities that have identity as a target or a principal tool*", it is not recognized as a final definition of Identity related crime.

Identity related cyber crime is on the rise, both in developed and developing countries. In this decade alone millions of people around the world are victimized of identity related cyber crime. The identity related cyber crime is perpetrated with ease when compared to the identity related crime in the physical space (Smith, 2007). It should be noted that the impact of identity related cyber crime is larger. The transnational nature, velocity and its relationship with other criminal activities such as fraud, organized crime, money-laundering and terrorism makes this crime more unique. UNODC (2008a, para 30) describes Identity related crime as the crime of the 21st Century:

> "*In serious cases, millions of dollars are stolen using false ID. Millions of smaller cases result in personal loss and frustration for victims. Because of under reporting, lack of common definitions, and insufficient legislation, this is probably just the tip of the iceberg. Nor are the costs purely economic: identity-related theft can pose a major threat to security. The problem is serious, and it is growing. No wonder it has been called "the crime of the 21st century".*

While we explore identity related cyber crime, we cannot avoid analyzing Phishing. Phishing is the main identity related cyber crime, though, malware to a certain extent, can be construed as an individual identity-related cyber crime, but predominantly Phishers also use malware. Though, identity related crime "was – and still is – committed through techniques such as dumpster diving (also known as —bin raiding); payment cards' theft; pretexting, shoulder surfing; skimming; or computer theft" (Acoca, 2008, p. 16), the internet related cyber crime is done by a method known as Phishing which and it is mostly done by the "use of malware and spam" (Acoca, 2008, p. 16). Acoca (2008) describes Phishing's origin:

> "*Phishing is a term that was coined in 1996 by US hackers who were stealing America Online (—AOL) accounts by scamming passwords from AOL users. The use of ph in the terminology traces back in the 70's to early hackers who were involved in phreaking, a hacking of telephone systems. Phishing is today generally described as a luring method that thieves use to fish for unsuspecting Internet users' personal identifying information through e-mails and mirror-websites which look like those coming from legitimate businesses, including financial institutions, or government agencies" (Acoca, 2008, p. 17).*

The AntiPhishing working group (2008) defines Phishing as:

> "*Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use spoofed e-mails purporting to be from legitimate businesses and agencies to lead*

---

under the platform. The group has so far met twice in Courmayeur, Italy, on 29-30 November 2007, (I participated in this meeting) and in Vienna, Austria, on 2-3 June 2008" (UNODC, 2008a, para . 31)

> *consumers to counterfeit websites designed to trick recipients into divulging financial data such as usernames and passwords. Technical-subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using systems to intercept consumers online account user names and passwords - and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes)" (APWG, 2008, p.2).*

Phishing based on social engineering and malware dominates the identity related cyber crime scenario. The use of malware in phishing is by methods of "Pharming" (crimeware that misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning), "SMiShing" (Use of SMS in cell phones) and "Vishing" (Use of Voice over protocol) (For a more detailed analysis on phishing see Acoca, 2008).

Phishing attacks are growing day by day, but the rates are always fluctuating (APWG, 2008). The Anti-Phishing Working Group (APWG) a group dedicated to work against phishing has been publishing Phishing Activity Trends Report from 2004. The latest report is of the first quarter and it has revealed that "Crimeware-Spreading URLs rose rapidly doubling previous high. However on the positive side, the number of phishing reports and new phishing websites decreased at the end of Q1 2008 period" (CircleID Reporter, 2008, para 1). The summary of key findings in the report is provided by CircleID Reporter (2008, para 1):

- *Numbers of unique phishing reports submitted to APWG declined by 12.5% by the end of the period, after a spike in February, attributable to IRS-related attacks*
- *Unique phishing websites detected by APWG ended down by 12 percent from January, at 25,630 in March, spiking in February to 36,002, due to IRS-related attacks*
- *The number of hijacked brands rose from 131 to 141 within the period, well within the average for the year*
- *Financial Services was the most targeted sector during the quarter, running between 92 and 94 percent*
- *While the United States remains the top country hosting phishing sites, China dropped to fifth at the end of the period*
- *The number of unique Keyloggers and malicious code applications detected rose to a record 430 in the period*

The above statistics explain the prevalence of Phishing. There is also a need to analyze the vulnerability of victims, in this form of crime. Gartner 2007 statistics have warned an increase 40% rise in the victims of phishing and governments should note this. Most of the victims are lured in to the trap of phishers and they are defrauded. Also many new surfers of the internet become victims of this crime. Hence, it is difficult to prevent and protect the victims from phishing. There is also no systematic data on the victims of phishing and this should be taken care of criminal statistics bureaus of various countries. There is a need for NGO's and Governments to create awareness among the masses about phishing victimization.

Apart from United States, international statistics on identity related cyber crime is not systematically developed. Countries like UK and Australia has recently developed various reports on identity theft, which provide base level statistics, but not on identity related cyber crime. An international repository of data related to identity related crime for analysing its occurrence is the need of the hour. Even though some researches (JSR,

2006) feel that Identity related crime is more prevalent in the physical space than in cyber space (Acoca, 2008), I feel that there will be certainly a greater rise in the identity related cyber crime as a larger number of people are entering cyber space daily. The efforts of UNODC core group of experts on identity related crime (UNODC, 2008b) are laudable and it has to further specifically look in to the identity related cyber crime and provide solutions for its prevention and protection of victims.

This issue has six articles and two book reviews. The first one is a special paper. The Bangkok International Summit (2007) declaration on Policing Cyberspace by Jaishankar, Pang and Hyde is an outcome of the 7th Annual Policing Cyberspace Summit of POLCYB held at Bangkok, Thailand during 5-9, November 2007. It summarizes the findings of the conference and has made various recommendations including the usage of specific open source software packages and securing communications forum for use of police officers and cyber crime investigators globally.

The second article by Lynne Roberts on 'Cyber stalking' highlights the increasing avenues of a novel crime in cyber space. Cyber-stalking is defined as an interpersonal crime that challenges notions of the requirement for physical proximity for harm to occur. Building on the notion of what off-line stalking is, the article explores the crime of cyber stalking. The author has emphasized upon developing typologies of cyber-stalking and chalking out possible relationships between cyber-stalking and off-line stalking. The article further brings out the possible constraints that could come forth in dealing with cyber stalking. The major issue lies in the realm of determining the jurisdiction for trying the offence as the victims and perpetrators of cyber-stalking are generally geographically separated by physical borders when the offences occur. Effective law enforcement and legal responses to cyber-stalking are dependent firstly upon the formulation of laws that recognize both the harms that can result from cyber-stalking and the cross-jurisdictional nature of the crime. There is a need to extend the boundaries of our perceptions of stalking to include current conceptions of cyber-stalking and future methods of stalking that may arise as the proliferation of new information and communication technologies continues. These laws need to be supported through co-operation between jurisdictions and the continued training of law enforcement and legal officers to increase their technological sophistication and understanding of cyber-stalking behaviours.

The study by Seigfried, et.al., is an attempt to understand the psychology of the child pornography consumer. It tries to distinguish between an internet CP consumer and a non internet CP consumer using Bandura's theory of reciprocal determinism. The sample was drawn from a population of Internet users via an anonymous survey through examination of demographic, personality, and behavioral characteristics for ascertaining the existence of any discriminating traits or factors between the users and non-users of Internet child pornography. Subjects were voluntarily recruited via the Internet by publicizing or advertising the survey using various online resources, such as chat rooms, bulletin boards, and email discussion forums. The analysis has provided valuable information, regarding the types of individuals who utilized Internet child pornography, where there was previously a significant gap in the literature. Statistical analyses revealed a relationship between higher scores on exploitive-manipulative amoral dishonesty (EMAD) traits, lower scores on internal moral choice, and the viewing of child pornography. Furthermore, the study suggests women are engaging in Internet CP consumption more often than previously suggested. The author concludes that the consumption of child

pornography over the Internet is likely to increase unless researchers decide to make this area of study a priority.

Kimberly Young in her article on sexual addiction in the internet, argues, that the internet anonymity promotes pedophilia within the otherwise normal populace. The study emphasizes to corroborate an association of sexually compulsive or addictive behavior with social isolation. Clinical research suggests that deviant sexual fantasies carried out online do not always originate from individuals with a pre-existing disposition for deviancy, but cases document how once pro-social citizens will engage in this same behavior. Based upon a study of 22 forensic interviews, the paper outlines a framework for understanding the psychology of the sex offender from a clinical perspective. The paper outlines five stages from inception to incarceration that the virtual sex offender follows. The research attempts to provide insight in relation to it for use by treating professionals, academia, and the general public. New and continued research in the area of online sex offenders will also assist the courts in achieving learned, accurate and just evaluation of such matters as they become presented with increasing frequency.

The article by Kyung-shick Choi emphasizes to present the causes of computer-crime victimization by examining an individual's lifestyle patterns. The central argument revolves on creating a distinction between an individual's actual personality vis a vis virtual presence. It presents an overview of lifestyle-exposure theory and routine activities theory, how routine activities theory is merely an expansion of lifestyle-exposure theory, and an overview of computer crime and victimization. The author has substantiated his point through conducting empirical research on college students by analyzing their behaviour patterns, specifically by looking at where they are on the Internet, what their behaviors are on the Internet, and what they are doing to protect themselves while they are on the Internet. The purpose sought is to create a link between the elements of an online lifestyle and the level of computer-security protection, with the resultant levels of computer-crime victimization that are experienced by the students. A better computer-crime victimization model based on routine activities theory is the end result that the author wishes to achieve.

Tina Freiburger & Jeffrey S. Crane in their article have done a systematic examination of terrorist use of the Internet. The anonymous design of the internet has made it a haven for the terrorists to carry out their activities in an organized manner. The article seeks to present an appraisal of the existing literature on cyber terrorism vis a vis the social learning theory. Social learning theory asserts that individuals learn deviant behavior from significant groups. This learning specifically operates through the four main concepts of differential association, definitions, differential reinforcement, and imitation. This paper examines the manner in which mechanisms of social learning theory is used by terrorist groups on the Internet. These methods are then examined to determine how they might be used for better purposes by antiterrorism groups.

Acknowledgments:

I would like to thank all the reviewers of this issue who have helped me in reviewing articles. I sincerely thank Ms. Bessie Pang, the Executive Director of POLCYB for giving me the wonderful task of preparing the Bangkok International summit Declaration of Policing cyberspace. From the bottom of my heart, I would like to thank Dr. Peter Carrington, the Editor of Canadian Journal of Criminology and Criminal Justice for granting permission to republish the Crime online book review by Travis Moriss, in

this issue of IJCC. My earnest thanks are due to the voluntary intern of the journal Mr. Dhruv Sharma, a law student from NALSAR University, Hyderabad for helping me in the corrections and formatting for articles of this issue.

References

Acoca, B. (2008). Scoping Paper on Online Identity Theft of OECD. Presentation at OECD Ministerial Meeting on the Future of the Internet Economy during 17-18 June 2008 at Seoul, Korea.

CircleID Reporter (2008). APWG Releases 2008 First Quarter Phishing Activity Trends Report. Retrieved, September 21, 2008, from http://www.circleid.com/posts/89922_apwg_phishing_activity_trends_report/

Finch, E. (2007). The problem of stolen identity and the Internet. In Jewkes, Y. (Ed.,), *Crime Online* (pp.29-43) Portland, Oregon: Willan Publishing.

Identity theft. (2008, September 21). In Wikipedia, The Free Encyclopedia. Retrieved, September 21, 2008, from http://en.wikipedia.org/w/index.php?title=Identity_theft&oldid=240027522

Koops, B., & Leenes, R. (2006). Identity theft, identity fraud and/or identity-related crime: Definitions matter. *Datenschutz und Datensicherheit - DuD*,30 (9), September, 2006.

Smith, R. (2007). Biometric solutions to Identity-related crime. In Jewkes, Y. (Ed.,), *Crime Online* (pp.44-59) Portland, Oregon: Willan Publishing.

UNODC (2007a). Study on "Fraud and the criminal misuse and falsification of identity". Retrieved September 21, 2008, from
http://www.unodc.org/documents/organized-crime/E_CN_15_2007_8.pdf

UNODC (2007b). Report of the first meeting of the core group of experts on identity-related crime (Courmayuer, Italy, 29-30 November 2007). Retrieved September 21, 2008, from http://www.unodc.org/documents/organized-crime/Courmayeur_report.pdf

UNODC (2008a). UNODC and organized crime: Identity-related crime. Retrieved September 21, 2008, from http://www.unodc.org/unodc/en/organized-crime/index.html

UNODC (2008a). Report of the second meeting of the core group of experts on identity-related crime (Vienna, Austria, 2-3 June 2008). Retrieved September 21, 2008, from http://www.unodc.org/documents/organized-crime/Final_Report_ID_C.pdf