International Journal of Advanced Research in IT and Engineering

ISSN: 2278-6244
Impact Factor: 6.111

CYBER SECURITY CHALLENGES & ONLINE FRAUDS ON INTERNET

Krishan Tuli*

Dr. Neenu Juneja*

Abstract: *The fast evolution of on-line and mobile channels has etched out new markets and brought large opportunities for aborting and established organizations alike. However, sadly the past decade has additionally witnessed important disruption to ecommerce payment processes and systems. The interconnected, anonymous and fast nature of those channels has inevitably diode to the event of malicious threats targeting ecommerce and retail services corporations, their individuals and their customers.*

These e-crime and digital fraud threats still evolve apace, with attackers utilizing progressively refined techniques to focus on vulnerabilities in individuals, processes and technologies. The e-crime threats, if with success completed, will undermine essential digital services, cause important injury to complete reputations, and end in wide money and operational pain for organizations and their customers.

Cyber crime is rising as a significant threat. Worldwide governments, police departments and intelligence units have begun to react. Initiatives to curb cross border cyber threats are taking form. Indian police has initiated special cyber cells across the country and have started educating the personnel. This text is a trial to supply a glimpse on cyber crime in Asian country. This text is predicated on numerous reports from journalism and news portal.

Key words: *Cyber crime, Hacking, Phishing, Cyber squatting, e-crime and digital fraud*

*Chandigarh Group of Colleges, Landran, Mohali

INTRODUCTION

Worldwide, regulators are also turning their attention to these threats, with enhanced scrutiny of organizational resilience and the introduction of stringent compliance requirements. The challenge that ecommerce services firms are facing is to deliver richer, integrated services, through multiple remote and digital channels, under significant cost restraint, and in the face of sophisticated e-crime threats. Recent cyber-attacks highlight the urgency for retail organizations to contend with ever increasing risks to customer protection, continuity, fiduciary responsibility, and operations. In order to achieve the security objectives, it is necessary to recognize that the security of the services and the protection of the customers' data are essential. To this end, and specifically to support the current security equation, it is necessary to have an enterprise wide target customer security model. This should be designed to deliver enhancements to both customer-facing and back office security capabilities, and in particular to improve existing security defenses for remote online, telephone and mobile banking channels.

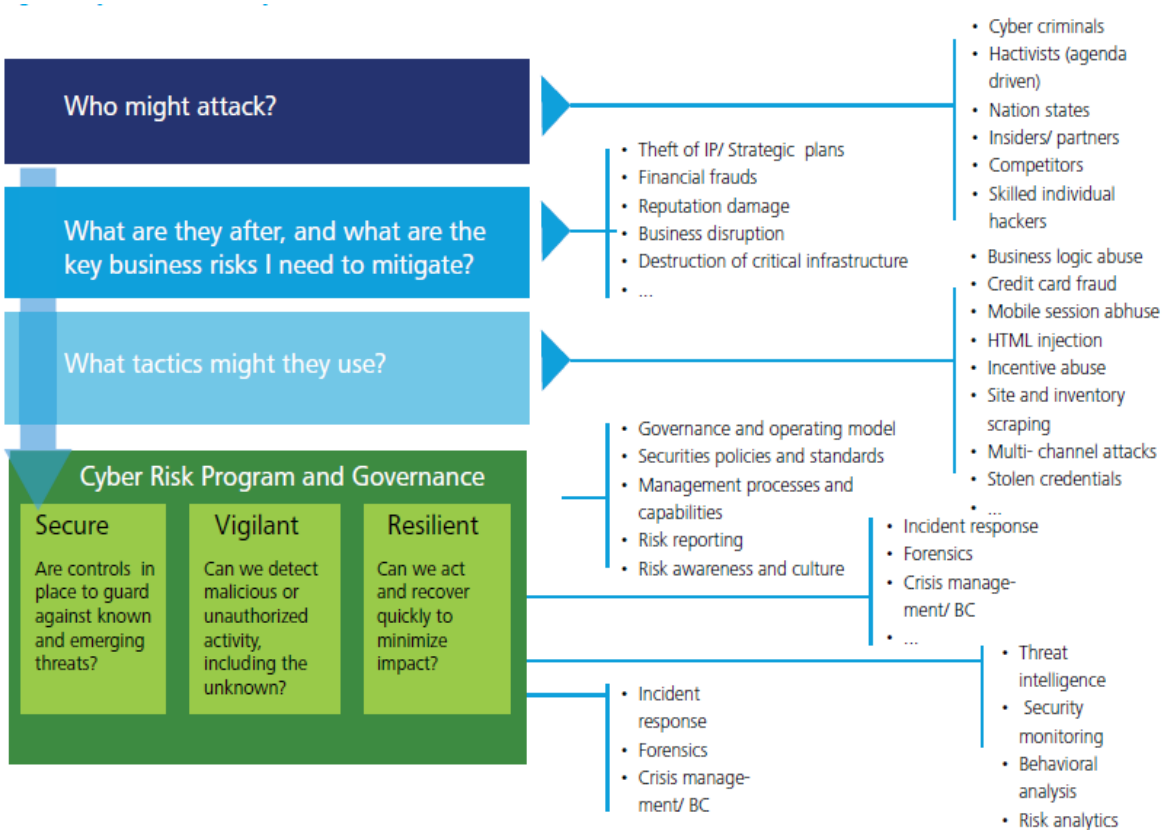
As far back as the early 1990s, the Internet was argued to be a unique medium showing the fastest speed of diffusion in human history (Nguyen and Alexander, 1996). Today, there are very few people whose lives are not affected beneficially and/or harmfully by the technology of the Internet era. On the positive side, the ability to share and exchange information instantaneously has provided unprecedented benefits in the areas of education, commerce, entertainment and social interaction. On the negative side, it has created increasing opportunities for the commission of crimes – information technology has enabled potential offenders to commit large-scale crimes with almost no monetary cost and much lesser risk of being caught. Compared to perpetrators of traditional economic-motivated crimes (e.g., burglaries, larcenies, bank robberies), online fraudsters are relatively free of worry from directly encountering law enforcement and witnesses.

With the continuous advancement of Internet technology and personal computing devices in recent years, Internet crimes have risen to an alarming level. For instance, in the U.S., the National White Collar Crime Center reported a 33.1% increase in citizen complaints of Internet crimes between 2007 and 2008, and this figure is reflective particularly of the increased incidence of identity theft. Another source of information also indicated that the number of identity thefts increased more than tenfold within a 9-year period – growing

from 31,140 incidents in year 2,000 to 313,982 in 2008. In addition, identity theft remained the top one complaint category filed by the victims across years. Evidence from victimization survey also pointed out that about 5% of Americans aged 16 and above was victims of successful and attempted identity theft within two years, and the direct financial damage to the victims were as high as 16 billion dollars. These statistics coincide with the notion of —Crime of the New Millennium as the phenomenon quickly emerged in the 21st century.

On the basis of this upward trend, we aim to examine identity theft from an analytic angle with a focus on the expanded versatilities of this contemporary crime. In the present article, the mechanism of identifying an individual is first discussed, followed by the definition and typology of identity theft. Elements and methods of identity theft will be deconstructed for classification, and subsequent discussions will be emphasized on recent variations in online fraud. The study will conclude with the implications of the close relations between identity theft and the fast growing Internet, and suggestions for improved means of identity protection.

CYBER RISK TAXONOMY



EVOLVING DEGREE OF THREATS

The threat landscape is ever evolving and increasingly challenging. Customer data with retailers and e-commerce firms has been increasing at a rapid pace. As per the incremental service provisioning in e-commerce, more data will be generated in the next two years than was generated ever before. Access to all this data has made the retail industry one of the primary targets for cyber-attacks. Some of the key threats today's organizations are vulnerable to include:

- User account takeover via robotic attacks, password guessing, HTML injection and Man-in the-Middle or Man-in-the-rower. Account peeking is a very common behavior by fraudsters as it allows them to validate the login credentials, identify higher value accounts and understand the controls which must be defeated to complete future unauthorized transactions.
- Business Logic Abuse or the use of portal's functionality for malicious or exploitative purposes (e.g., abuse of loyalty point programs or shopping cart functionality, fraudulent account set up, Scripted attacks to find valid coupon codes.). Impact of such abuse may include effect on the genuine customer due to unauthorized use of coupon offers, overall decrease in revenue due to offer abuse, incremental portal overhead due to scripted attacks and site scraping by resellers or coupon aggregator sites.
- Distributed-Denial-of-Service or DDOS attack on the application layer where a deluge of page requests coordinated by a bad actor overwhelms the server and brings the site down.
- Site or Architecture Probing to gather as much information about site structure and security vulnerabilities as possible to prepare for an attack on that site.
- Site & Inventory Scraping or data theft perpetrated by copying large amounts of data from a website, typically via automated scripts.

ISSUES

Cyber Security issues lead to brand degradation and change in consumer behavior. Attacks are exploiting weaknesses in traditional controls, some very destructive. Traditional controls around Point of Sale and other IT systems are necessary but not adequate – greater emphasis must be placed on preventative controls, rapid detection, and rapid response.

Retail innovations that drive growth (e.g. Digital, Omni-channel retailing, social etc.) also create cyber risk. Cyber risk management strategy must be a component of business strategy, and can't simply be delegated to IT.

1. Lack of appropriate control and transparency add to cyber security risk. Despite growing frequency and sophistication of cyber-attacks on the ecommerce industry, payment settlement agreements between credit card networks, the banks and the merchants have remained a closely guarded secret. Neither the government nor any database shares the list of defaulters with the public. Banks and credit card companies determine fault on a case-by-case basis through private contracts with individual merchants. Fines and the reasons for them remain sealed. Due to the lack of transparency, the majority of customers is not aware of any cyber security breaches and remains vulnerable to cyber attackers.
2. E-commerce firms and retailers face heat to increase efforts to ensure greater cyber security. In the wake of recent data-security breaches at large retail corporations, retailers have been pushed to spend more to ensure tighter customer data security. While the traditional retailers have been investing millions of dollars to compete with online retailers the cyber-security threats have multiplied their operational expenditures.
3. Third-party cyber risk As firms look to exploit the competitive edge they gain from the data they capture about their customers, they are increasingly leveraging the expertise of third parties Such as analytics specialists and social marketers. Couple this with increasingly lengthy and complex supply chains; retail organizations are increasingly becoming enmeshed in very complex, interconnected value chains where sensitive data is shared and dependencies are introduced between business critical systems. Firms are rapidly waking up to the realization that they often have very little visibility in these areas, and that they do not have a good understanding of where their customers data is travelling, and what their risks are. We should focus on to map these interconnections, develop robust risk management frameworks, and provide firms with assurance that they have understood and actively managed the risk of each partner relationship.

4. Inadequate joint efforts by banks and retailers to counter cyber security threats While collaborated efforts are expected to ensure tighter cyber-security, banks and retailers differ in terms of responsibility sharing. Banks want retailers to bear more of the costs of replacing cards after breaches occur whereas retailers say banks have been slow to adopt new, more secure debit card technology.

IDENTITY THEFT BREEDERS AND DAMAGES

Breeder identification can be gained by any means; its significance is in its use for obtaining additional, separate, false, or fraudulent means of identification controlled exclusively by the perpetrator without the victim‘s knowledge, or ability to know. An identity thief can fraudulently use obtained personal information to generate other means of identification, ranging from open new accounts, apply for loans and credit cards, to receive governmental benefits (General Accounting Office, 1998). Breeder ID means occur most often in the course of committing credit card fraud for the purpose of establishing the —authenticity required to obtain a new account, although their incidence is fairly frequent in conjunction with check fraud, document fraud/counterfeiting, signature forgery, and bank/loan fraud as well.

Thus, as long as the identity thieves have knowledge of or keep a record of the stolen identities, deeper and long-term damage to the victims can explode or surprise the victims at any time after the initial damage. For that reason, in addition to financial and credit damages, some victims of identity theft may suffer from varied psychological, social, and/or legal disturbances. These hidden costs are considerable but usually are not addressed. The recent supplement of the National Crime Victimization Survey shed some light in this regard – the emotional distress experienced by some types of identity theft victims (e.g., open new account, stolen personal information) were comparable to an average violent crime victim.

THE ELEMENTS AND OFFENDING METHODS OF IDENTITY THEFT

An identity thief may reach others identifying information through various means. The examples of identity theft are, probably, limited by each individual‘s imagination but expandable by the escalation of technology advancement. Here, we employ two dimensions to deconstruct the seemingly complicated incidents of identity theft.

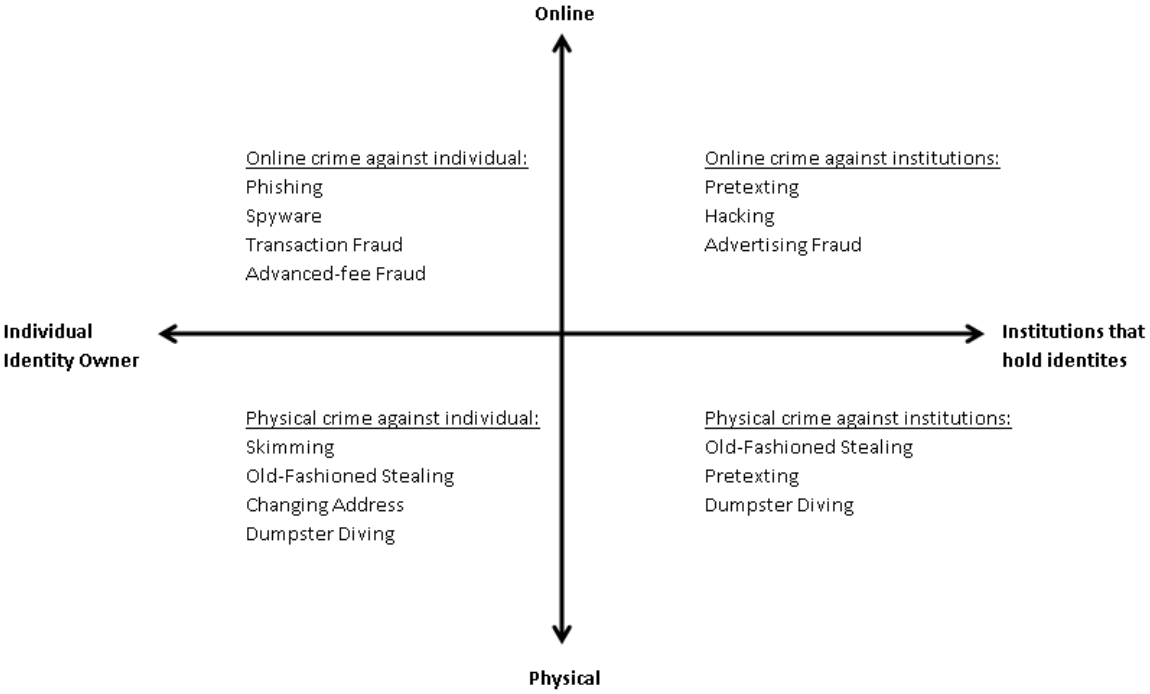


Figure 1: Deconstructing Types of Identity Theft

The horizontal dimension is the source from which identity thieves obtain the identifying information. On one end of this dimension is the individual victim; on the other end are institutions that legitimately store client personal information. Stealing each individual's personal information generally is easier than penetrating institutions security protocols. However, once identity thieves penetrate layers of protection employed by those institutions, the loss of identity information is often massive and the damages are much more substantial.

The vertical dimension is the place where the identity-stealing conduct occurs. Identity thieves either violate social rules implemented in the physical world (e.g., steal individual victim's mails like bill statements containing personal information; bribe or coerce institutions employees who have access to clients personal information) or deceive Internet users of different services. Sometimes, the financial damage of identity theft does not begin until fraudsters purchase identity information that was collected illegitimately in the first place. The underground data warehouses that sell identity information online can contribute greatly to financial disaster for individuals.

The purpose of recognizing these two dimensions is threefold. First of all, these two dimensions help identify major dimension of paths that those identities are or can be stolen (cyberspace vs. physical space; individuals vs. institutions). The classification also lays out a

framework for detailed examinations of each type of identity theft. Without this foundation, further elaboration and analysis are limited.

Dumpster Diving/Trashing

Identity thieves can rummage through trash of residences or businesses looking for bills, paper documents, storage devices, and even discarded credit cards containing personal information. This way of stealing identifying information is fairly labor-intensive and is restricted to limited geographic areas. Consequently, suspects are relatively easy to locate by law enforcement agencies.

Old-Fashioned Stealing

Via traditional stealing methods, identity thieves either target goods that include personal information or obtain victims personal identification as a byproduct of pickpockets. The targets are those usually containing personal identifying information, such as wallets and purses, mail, especially bank and credit card statements, pre-approved credit offers, new checks, and tax information. Old-fashioned stealing can also occur when offenders steal personnel records from institutions or bribe/coerce/deceive employees who have the access.

Changing Address

Identity thieves divert victim's mail, particularly billing statements, to another physical location by completing a change of address form. This type of identity theft is usually conducted by filing the change-of-address form with the U.S. Post Office. Thus, the U.S. Postal Inspection Service is intuitively the corresponding law enforcement agency accountable for preventive/deterring actions.

Skimming

Skimming occurs when legitimate transactions are processed by swiping credit/debit cards in retail stores or any other type of institutions where swiping cards is required. Generally, the credit/debit card numbers are stolen by a special storage device built in or attached to the swipe machines. The card information is stolen simultaneously when a legitimate business transaction occurs. The thief can be anyone who has access to the swipe machine, including, but not limited to, technicians of swipe machine vendors, and retail stores' staffs/owners. Skimming sometimes can be completed by perpetrators who attach a slim seem-like-real cover on a given ATM machine.

Pretexting

Pretexting involves a series of deceptive actions that obtain victim's personal information from the owner of the information, institutions that hold the information, and/or other individuals who may have knowledge of the information. Pretexters may pretend to have different roles (e.g., customer service representatives, survey researchers, the victims or the victim's authorized representatives) in order to collect pieces of victim's personal information. In sum, as a technique of social engineering, pretexting is a cluster of pretenses with the ultimate intention of taking financial advantage of the victims.

Hacking

Hacking was perceived as a creative activity that helped overcome the limitations of computers about a half century ago when such machines were not common, but the image of hacking changed, largely influenced by the media, to a threatening force in 1980s (Britz, 2009). The developed categories of hackers (e.g., white hat, black hat, and gray hat) are usually not mutually exclusive (McQuade, 2006; Parker, 1998) because whether their intention is malicious is uncertain from discovered evidence. Even though contemporary hacking is usually associated with stealing valuable information other than personal information (e.g., business secrets, confidential documents) and properties (e.g., copyrighted artifacts, billing) in cyberspace, it can be used as a means to obtain identifying information. Stolen identity information sometimes can be a —by-product of hacking for other purposes. Hacking is attractive for the reason that offenders do not have to physically appear at the —crime scene to —rob or —steal from institutions. Instead, exploiting online financial and billing systems is enough to illegitimately gain privileged information. Especially after database technology is widely utilized by varied institutions to store and manage huge amounts of data, a copy of the database itself is very valuable in the black market. As more money, transactions, and even resources are moved to and managed in the virtual space for the sake of efficiency and convenience, it is likely hacking will remain a seductive means of identity stealing.

Phishing

Phishing is the pursuit of personal financial information with the intent to commit fraud by relying upon the recipient's inability to distinguish bogus emails, messages, web sites, and other online content, from legitimate ones – they all designed to appear with legitimacy.

Phishers can use a combination of tricks involving web sites, emails, and malicious software to deceive potential victims for the purpose of stealing their personal identity information and financial account credentials. The significance of phishing is that it enables remote identity theft. Precisely, phishing significantly reduces the risk and the costs to identity thieves because no physical contact, such as dumpster diving or old-fashioned stealing, is needed to complete the crime. Consequently, the chance of being caught at the crime scene is virtually eliminated. Another significance of phishing is its popularity in the U.S. where the largest proportion (25%) of phishing sites are hosted, compared to other countries in the world.

A typical phishing attack begins when phishers (offenders) send out massive amounts of email (spam) or messages with bait, which is intended to trigger the targeted victim's intuitive interests. Usually, the unsolicited emails ask recipients, with a sense of urgency often exaggerated by an alleged security breach, to log onto the provided URL and confirm their personal information details, particularly their password of access. Typically these fraudulent emails are designed to look like they are from large and well-known financial institutions, such as Bank of America, Citigroup, or PayPal. In the past several years, however, observers have witnessed that phisher's Spyware (Malicious Software).

ONLINE FRAUDS

In general, fraud refers to the act of taking advantage of others, largely motivated by economic reasons, via varied deceptive means. Online fraud intuitively refers to those conducted and/or facilitated by the Internet. As discussed earlier, identity theft is the inception of many fraudulent and criminal activities, but it does not necessary means that identity theft is the start of all online frauds.

Business Transaction Frauds

The network of computer networks creates a cyberspace where business transaction platforms, such as stores, can be operated virtually. In some cases, the same products demonstrated in a company's physical stores or printed catalogues can be found in their corresponding online stores. The most significant difference between buying from a physical or virtual store is the method of business transactions, including both the payment and the delivery of products or services, and this joint venue is where online frauds usually emerge.

Online Advertising Frauds/Advertisement Click Frauds

Cyberspace has created new business models, as well as new ways to advertise. One of the most common, and probably the least intrusive forms of advertising online is a banner on Web sites that invites interested customers to click on it and view the details. Once an Internet user clicks on the banner, s/he is linked to another site of products/services and the information system automatically records the click for later cumulative counts. The corresponding business model for charging the advertising fee is typically based on how many times the banner was clicked. Consequently, a particular fraudulent behavior online is to defraud Internet advertising billing systems by employing individuals or software to massively click on the advertisements. Outsourcing the task of fraudulent massive clicks to countries with cheap human labor becomes a rational choice to offenders.

Advanced-Fee Frauds

Advanced-fee frauds, again, is not something new in civilized human history, but this type of fraud has regained attention for its rapid increase use of email. The latest version of this fraudulent form is frequently referred as Nigerian 419 scam, named after the Nigerian criminal code section (Edelson, 2003). Online advanced-fee frauds generally begin with the receipt of a fake formal letter claiming a large amount of money needs to be transferred through a third-party bank account.

CONCLUSION

The rapid pace at which technology is changing has provided large opportunities for organizations to develop new business models, services, and products. While the digital revolution has transformed the way we do business, it has also created complex and sophisticated security issues. Assets and Information that were once protected within the organization are now accessible online; customer channels are vulnerable to disruption; criminals have new opportunities for theft and fraud. With organizations growing organically and inorganically, complexity of managing businesses & security operations are also becoming complex.

Identity theft and online frauds are contemporary crimes for profit. As the world market continues to progress toward transferring and managing money conveniently on the Internet, online frauds and scams are inescapable. As long as identity theft and online frauds are relatively easy paths to financial gain, the use of these fraudulent means will increase

with the growth of the Internet. With the movement of processing transactions totally online, online fraud has gradually transformed from a hybrid cybercrime to a true cybercrime. Collectively, cyberspace has become such an attractive place where suitable targets like personal information increase in value while effective guardians typically fall behind. Anti-fraud efforts must be accelerated and orchestrated proficiently to make online scams difficult for offenders.

REFERENCES

1. Crume, J. (2000). Inside Internet Security: What Hackers Don't Want You to Know. Harlow: Addison-Wesley.
2. Cukier, W. and A. Levin. (2009). Internet fraud and cyber crime. In Frank Schmalleger and Michael Pittaro (ed.) Crimes of the Internet. Upper Saddle River, NJ: Pearson Education Inc.
3. Economic Crimes Policy Team (1999). Identity Theft: Final Report. United States Sentencing Commission.
4. Albert, M. R. (2002). E-buyer beware: Why online auction fraud should be regulated. American Business Law Journal, 39(4): 575.
5. Britz, M. (2009). Computer Forensics and Cyber Crimes: An Introduction. Upper Saddle River, NJ: Pearson Education Inc.
6. Federal Trade Commission. (2003). Overview of the Identity Theft Program: October 1998 – September 2003. [online]. Available from: http://www.ftc.gov/os/2003/09/timelinereport.pdf [Accessed 28/08/2010].
7. Federal Trade Commission. (2009). Consumer Fraud and Identity Theft Complaint Data: January – December, 2008. [online]. Available from: http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf [Accessed 20/08/2011].
8. Federal Trade Commission. (2010). Consumer Fraud and Identity Theft Complaint Data: January – December, 2009. [online]. Available from: http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf [Accessed 20/08/2011].
9. Huang, W. & Wang, S. K. (2009). Emerging Cybercrime Variants in the Socio Technical Space. In B. Whitworth & A. de Moor (ed.) Handbook of Research on Socio-Technical Design and Social Networking Systems. Hershey, PA: Information Science Reference, IGI Global.
10. Jasper, M. C. (2002). Identity Theft and How to Protect Yourself. Dobbs Ferry, NY: Oceana Publications.