Muhammad Hasmi Abu Hassan Asaari & Noorliza Karia (2001). "Disastrous Impact: Shortage of Knowledge Workers in Organization," *Refereed Proceeding,* The 2nd. International Conference on Disaster Management: Preparing for the Future, Surabaya, Indonesia, 3-5 May 2001, 8p [ISBN 983-2078-16-4].

IDENTITY THEFT: WHAT CAN WE LEARNED?

Noorliza Karia
Muhammad Hasmi Abu Hassan Asaari
Universiti Sains Malaysia, Penang, Malaysia

Abstract

In this digital world, we are no longer known as an individual. The communications and transactions are carried out through computers. Therefore, the case of identity theft has been a major issue to the advanced nations. Malaysia as a developing country needs to learn from them in combating the issue of identity theft. Therefore, various types of identity theft can be categorized as misuse of other people's information through the on-line transactions. Solutions to the identity theft are proposed in the Malaysian context.

Introduction

Cyber crime has been an issue to the advanced nations as most of the daily transactions were done through computers. Nevertheless, identity theft is one of the rising numbers in complaints and issues to be solved by the relevant authorities. In the cyber world, who we were is unimportant (Spoore, 2001). Moreover, what matters were that our computers had a better chance to be known than we do. Due to the technology advancement in the cyber world, perpetrators took advantage of the situation by gaining unauthorized use of others identity for their financial advantage.

Eventhough the issue of identity theft has yet to be at the alarming rate in Malaysia, individuals, businesses, and government need to take measures towards curbing the issue of identity theft from happening in this nation as we move into the digital world. Hence, this paper will explore and discuss the experience of various parties in their handling of the issue of identity theft. Further, it will give views and opinions on the manner of handling the identity theft issue in the Malaysian context.

Definition of Identity Theft

Identity theft can be defined as when someone uses someone else's personal information, usually a social security number (SSN) or credit card number, and acts as if he or she is that person (Anonymous, 2001). Further, Poore (2001) stated that identity theft occurred through the theft of card numbers, expiration dates, and your name. Meanwhile, Arnold (2001) indicated that identity theft as a person steals such information as another person's SSN, credit card number, and checking account information. Using these "proofs" of

identity, the criminal pretends to be someone else, running up charges against the dupe's accounts.

Type of Identity Theft

Estimates indicated identity theft reached 900,000 new victims a year. Some victims' accounts have been fraudulently charged for $200, others for $200,000 (Anonymous, 2001). Moreover, Grassley (2001) indicated that FBI estimated 350,000 cases of identity theft occurred each year. It was known as the fastest growing crimes in the new economy. Further, this was stimulated as people increasingly rely on credit cards for electronic commerce and daily business transactions. Further, Trans Union reported that fraud line increased from 35,000 in 1992 to more than 500,000 in 1997. Further, the U.S. Secret Service made nearly 9,500 ID theft-related arrests in 1997 involving losses of $745 million. MasterCard reported that, in 1997, 96% of its fraud losses of $407 million involved ID theft. In 1999, the Social Security Administration received nearly 39,000 complaints about the misuse of SSN (Bernstein, 2000).

Identity theft can be grouped as follows:

Social security number (SSN)
Majority of the identity theft was the misuse of SSN. In 2000, the Social Security Administration reported it had received 46,839 complaints regarding the misuse, many of them had to do with identity theft. Further, the figure was almost six times greater than just four years ago when the number totaled 7,868 in 1997 (Arnold, 2001; Feinstein, 2001).

Credit card
Further, Lim (2001) indicated that in 1999 more than 25,000 Americans became victims, with half the cases involving credit-card fraud. Even, Microsoft Corp. Chairman Bill Gates and former president Bill Clinton were among the possible victims (Verton, 2001). Further, it was estimated that 3,000 stolen credit card numbers traded in chat rooms each month (Brown and Ploskina, 2001). Moreover, criminals were using real names and credit card numbers in their fraud attempts instead of phony names and credit card or SSN (Bernstein, 2000).

Lost wallets/purses
Federal Trade Commission (FTC) reported that they received 2,000 calls per week due to identity theft. But less than 1% of all reported cases to date can be linked to the Internet. Further, the two most common causes are lost wallets or purses, and mail theft (Verton, 2001).

E-mail address
Anyone can obtain an e-mail address. With some persistence, you can obtain an e-mail address that clearly represents someone else's name. Therefore, free e-mail services exist for which you need not present even a means of payment (e.g. credit card number or debit

card number) through which a third party (in this case a financial institution) might vouch for you (Poore, 2001).

Birth certificate

A copy of birth certificate can be purchased for $10 from the state agency by a con man. Further, the con man used the certificate and convinced the driver license clerk to create a duplicate driver's license. With the license, birth certificate, and SSN, the con man called the bank. Using the lost-my-wallet story, the con man asked for checking account information. Finally, the con man used the information to open new checking accounts and make purchases (Arnold, 2001).

In-side job

Moreover, a crime ring bought car rental agreement from a clerk at a car rental agency. The customers' personal information in the agreements was used to open bank accounts, get credit cards, and obtain lines of credit – all in the customer's names. Even the perpetrators could be the family member, co-worker, ex-spouse, or acquaintance that had access to someone's personal information and uses it to open new accounts in that person's name (Bernstein, 2000).

In conclusion, identity theft can be listed from theft of name, address, SSN, credit card number, checking account number, birth certificate, e-mail address, and the list is exhaustive. As indicated by Bernstein (2000), ID thieves used a variety of ways to get your personal information. They will used any of the following ways:

1. stealing wallets and purses with identification and credit and bank cards.
2. pilfering mail, including bank statements, preapproved credit offers, telephone calling cards, and tax information.
3. completing a change of address form to divert mail to another location.
4. rummaging through trash for personal data.
5. fraudulently obtaining a credit report by posing as a landlord, employer, or someone else who may have a legitimate need for the information.
6. getting business or personnel records at work.
7. finding personal information at your home.
8. using personal information you share on the Internet.
9. purchasing personal data from "inside" sources.

Occurrence of Identity Theft

The main question on identity theft -- how can you detect that your identity had been theft? Few instances that you may encountered such as you got a call from your creditor, stating it suspects "unusual activity" on your account; received a call from a collector, demanding payments, or denied a car loan, view the credit report and see a host of overdue bills you never knew about (Anonymous, 2001). Moreover in this digital world, organizations gave precedence to computer databases over the testimony of real people, an error may result in denied credit, denied employment, denied medical coverage, false

arrest, improper medical treatment, defamation, unauthorized transfer of assets, and just plain bad things (Poore, 2001). Then you discovered that your identity had been theft.

The Internet allows a person who steals a credit card or another's identity to avoid detection (Arnold, 2001). Moreover, Poore (2001) indicated that cellular telephones and similar handheld computers (e.g. PDA) usually authenticate as if they were the end users. Further, successfully cloning such computers equates to stealing the identities of the legitimate owners.

Further, identity theft could occurred as you entered the Internet zone such as (Arnold, 2001):

1. online shopping; as you ran on credit card transactions.
2. monitoring actions; as you clicks, downloads, preferences, purchases, electronic mail, voice messages sent via Internet telephony – all these actions can be watched, processed, and counted.
3. data mining; as your information was captured into retailers' databases.
4. password poaching – intruder obtained user names and passwords; and entered the new system with the identity of the original users.
5. account takeover – intruder used the accounts of the true user for his own purposes (e.g. credit card scams).
6. fraudulent transactions – intruder used the existing accounts to make fraudulent purchases, and arranged for a third-party to sign for the packages.
7. new account creation – intruder created new accounts in the name of one or more people whose information was hijacked.

Moreover, stolen identity nightmares afflict about 500,000 Americans annually and account for more than $2 billion recorded in fraud losses (Arnold, 2001). Further, the perpetrators targeted prominent members of the nation's business community and obtained personal information about them. They impersonated their victims in telephone calls to banks and credit card companies. Further, they charged the billing address on the account to hotels in various states.

Meanwhile, millions of Internet users key in their name, address, home and work telephone, facsimile, electronic mail address, and credit card number with only a moment's hesitation, and sometimes not even that (Arnold, 2001). Further, he indicated the types of systems leave digital footprints:

1. mobile telephones.
2. banks that surreptitiously sell financial secrets.
3. computer technology that secretly profiles as you go online.
4. a healthcare system that shares medical information.
5. airport scanning devices that see and "sniff" for trace gases on your person and in you luggage.
6. tiny surveillance cameras: workplaces, campuses, lobbies, elevators, restaurants, and locker rooms.

7. growing pressure to require all Americans to carry a national identification card and DNA registries for everyone that would permit tracking.

As the perpetrators obtained the information, they will used the information in the following ways (Bernstein, 2000):

1. they call your credit card issuer and, pretending to be you, ask to change the mailing address on you credit card account.
2. they opened a new credit card account, using your name, date of birth, and SSN.
3. they established phone or wireless service in your name.
4. they opened a bank account in your name and write bad checks on that account.
5. they filed for bankruptcy under your name to avoid paying debts they have incurred under your name.
6. they counterfeit checks or debit cards and drain you bank account.
7. they purchased vehicles by taking out auto loans in your name.

Solutions

Laws

In the US, various acts were passed in order to curb the seriousness of the identity theft cases. The Identity Theft and Assumption Deterrence Act of 1998 made it a Federal crime when someone "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or to abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under an applicable state or local law." According to the law, a name or SSN was considered a means of identification. So was a credit card number, cellular telephone electronic serial number, or any other piece of information that may be used alone or with other data to identify a specific individual (Bernstein, 2000).

Introduction of legislation, Social Security Number Misuse Prevention Act, to curb the growing epidemic of identity theft by making it harder for criminals to steal another person's SSN (Feinstein, 2001). This legislation was fundamental to protecting the identity of our citizens. Further, the act introduction prohibited anyone from selling or displaying a SSN to the general public without the Social Security holder's consent.

The Identity Theft Prevention Act of 2001 was introduced to make it harder to steal someone's identity. It imposed additional duties on credit issues and credit bureaus to ensure the accuracy of information in credit applications. Moreover, the bill also speeds up the paperwork process after an identity theft has been committed so that victims can more quickly reclaim their good credit (Grassley, 2001).

Biometric

Biometric might offer some help against identity theft (Poore, 2001). Moreover, the effectiveness of biometric identification depended on the effectiveness of the registration process and the security and controls over the authentication process. By associating a biometric with the wrong person and the person with that biometric became the person

with whom its associated – at least until that person could prove through his actual biometric that he was not the person whose biometric points to him.

Credit card companies

Proactive measures by the three major credit card companies, American Express, MasterCard International, and Visa International Service Association – all had programs aimed at giving merchants more online security muscles (Brown and Ploskina, 2001). Further, MasterCard unveiled their Site Data Protection Service, a set of security products and measures offered to its merchants; and also rules for them to follow when processing and storing credit card information. Visa launched its Cardholder Information Security Program, which required vendors that collect and store credit card information remotely to meet asset of security standard, from installing firewalls to encrypting stored data. Meanwhile, American Express started using VeriSign's Pay flow, which gave merchants the option to let American Express process and store all American Express charges.

Police report

If you're the victim of identity theft, you need to report to the police and get their report. Further, you need to forward the report to the security division of the credit card company. Next call the three reporting bureaus: Trans Union, Equifax, and Experian; and place a "fraud alert." Asked for their reports and examine them. Do informed your creditors that fraudulent activity had occurred and asked them to freeze the old account and issue a new card and account number (Anonymous, 2001; Bernstein, 2000).

Digital signatures

Digital signatures and encrypted messages can diminish this risk but these techniques have weaknesses of their own (Poore, 2001). Finally, periodically review your credit bureau records. Carefully examined monthly billings for unauthorized or expected charges (Poore, 2001).

In summary, a solution to the identity theft lies on the individual person. If the individual do not reveal his or her personal information, then he or she will be in a good position from being a victim of identity theft.

Discussion

As Malaysia is moving towards an e-government and transactions to be done through computers, we need to learn a lesson from the incidents and cases of identity theft which occurred most in the developed countries such as the US. Further, identity theft remains at the top of the list of privacy violations (Arnold, 2001).

Further, on-line banking needs to be monitored on the implementation and the security aspects as the system will not know who is on the line doing all the banking transactions. In this electronic age, your finances can be damaged within a matter of seconds by this easy, popular crime. The damage to your credit can take years to undo, but if you take swift action, you have a better chance of restoring your good name and keeping your finances intact (Anonymous, 2001). Therefore, a measure needs to be taken by Bank

Negara Malaysia and all the banks in Malaysia to safeguard all the interests of Malaysians from being a victim of identity theft.

As indicated by Bernstein (2000), tips to fight identity theft and consumer fraud:

1. keep your personal information private; such as address, SSN.
2. read all of your bills carefully; look for unauthorized charges.
3. order a copy of your credit report each year from all three credit bureau reporting agencies to check for anything that could indicate fraud.

As for cases in Malaysia, specific laws need to be passed in combating the presence of identity theft. The creation of such laws can be viewed from the perspective of the Bank Negara Malaysia, relevant Ministries, Communications and Multimedia Commission, Securities Commission, Judiciary Department, and other relevant agencies and organizations.

Conclusion

In cyber space, who we are is unimportant. All that matters is who we appear to be. If the user ID and password are correct, than is who we are. If the digital signature verifies, that is who we are (Poore, 2001). Finally, the failures had a great del to do with human nature. Despite the increased vulnerabilities of certain types of online transactions, security boils down to individual behavior (Arnold, 2001). Therefore, no matter what laws that were passed in protecting the individual and agencies from identity theft, we as community must safeguard ourselves from the perpetrators by keeping our personal information as confidential as it can be.

References

Anonymous (2001). "Identity Theft: How to Fight the Scam," *Ebony*, Aug2001, Vol.56, Issue 20, p24.

Arnold, S.E. (2001). "Internet Users at Risk: The Identity/Privacy Target Zone," *Searcher*, Jan2001, Vol.9, Issue 1, p24.

Bernstein, J. (2000). "Protect Yourself Against Identification Theft," *USA Today Magazine*, Sep2000, Vol.129, Issue 2664, p54.

Brown, D. and Ploskina, B. (2001). "E-Theft: Who's Liable?" *Inter@ctive Week*, 8/13/2001, Vol.8, Issue 31, p11.

Feinstein, D., Senator (2001). "Senators Feinstein and Gregg Introduce Bipartisan Measure to Combat Identity Theft," *FIDCH Press Releases*, 05/09/2001.

Grassley, C., Senator (2001). "Grassley Takes Aim at Identity Theft," *FDCH Press Releases*, 09/04/2001.

Lim, P.J. (2001). “Sounding an Identity-Theft Alarm,” *U.S. News & World Report*, 04/23/2001, Vol.130, Issue 16, p74.

Poore, R.S. (2001). “Identity Theft: Who Are You Anyway?” *Information System Security*, Jul/Aug2001, Vol.10, Issue 3, p10.

Verton, D. (2001). “Identity Thefts Skyrocket, but Less than 1% Occur Online,” *Computerworld*, 02/12/2001, Vol.35, Issue 7, p7.