South African Journal of Information Management
[DoE accredited]

Peer Reviewed Article

Vol.7(4) December 2005

Identity theft escalation – you may need to change your life

D. Augustyn
Department of Business Information Technology
University of Johannesburg
Johannesburg, South Africa
daveaugu@twr.ac.za

Contents

Key words: Identity theft, identity fraud, risk awareness, impersonation, privacy, information risk

1 Introduction

'MasterCard: 40million Credit Card Accounts Exposed' – this made the headlines on Internetnews.com on 20 June 2005. Hackers gained access to databases containing more than 40 million credit card numbers and some personal details of the card owners in May 2005. More than two hundred thousand of these numbers were downloaded from the CardSystems servers in the United States (Boulton 2005).

Since the 1980s, knowledge workers have experienced a drastic transformation in the way information and knowledge are accumulated, recorded and stored and the ways in which the volumes of information are transported over network media. Information technology has changed our world and brought with it a completely new array of security risks. This new world also brought new ways for fraudsters to commit identity theft – stealing and using another person's identity for fraudulent purposes. A single corporate database may yield hackers millions of records, which can have catastrophic consequences for the victims and

the credibility of the compromised business.

To reduce the risks to corporate and private information as far as possible, it has become increasingly more important for users of digital information to understand knowledge security risks. At the same time, it has also become very difficult to keep up with technological development. The average knowledge worker cannot stay up to date with rapid advances and developments in information technology, much less with the associated security risks brought along with these developments. Knowledge workers do not understand the technology well enough, nor are they fully aware of the risks to which corporate and private information are constantly exposed to.

Recent trends indicate that identity theft is escalating among fraudsters. Hackers attempt to gain entry into corporate networks in their endeavour to obtain customer databases, which are then sold on the black market. Crime syndicates use these personal details to provide new or temporary identities to criminals to defraud businesses and persons or they provide them to illegal immigrants (News24.com 2005; ITWeb staff writer 2005).

Even persons who do not use the Internet or corporate networks are at risk of identity theft. As with almost all people with any type of client affiliation with any institution, their personal details are also stored somewhere in a database on a corporate computer network. This poses the following question:

> Are knowledge workers well-informed about the risks of identity theft and may they unknowingly perform unsafe practices, placing their identities at risk?

To inform knowledge workers of unsafe practices that may expose them to possible identity theft risk, it is necessary to investigate reports on identity theft worldwide and to explore typical identity theft methodologies. The most effective method to determine the extent of this crime is to study and compare reports from the most current publications on the subject available in online forums, news media, international surveys and other publications. To confirm the reality of hacker attacks and the potential risk to Internet users in general, firewall logs were monitored over a period of one month for an ADSL connection and over one week for a dial-up connection. The findings of the intruder attempts recorded by the logs were compared with strategies reported on by security forums and Web sites. A series of phishing attempts were also studied to determine the methodology used.

The article starts by highlighting some media publications and surveys and then reports on knowledge workers' awareness of the realities of identity theft. To make knowledge workers more aware of the risks, some typical methodologies used by intruders are explored as well as what measures can be taken by knowledge workers to minimize identity fraud risk.

top

2 Identity fraud is rife

Identity fraud takes several forms, for example:

- financial identity theft – impostors using a victim's personal information, such as name and identity number, to open credit accounts, obtain loans, make purchases or obtain services;
- criminal identity theft – criminals use another person's identity for criminal acts; and
- identity cloning – an impostor uses the victim's stolen personal details to establish a new life (Foley, Foley, Pletcher, Miranda, Colins and Nelson 2003).

Identities are stolen in the following ways:

- From papers, such as bank statements or invoices containing personal information found in waste;
- from service provider or merchant records – personal information may be leaked by staff from companies providing a service or product, for example a video store or restaurant;
- from a stolen or lost wallet, personal computer, laptop or Personal Digital Assistant (PDA);
- by providing information to fraudsters – details may unwittingly be provided over the phone or in person to a criminal masquerading as a legitimate business person;
- from digital information – information may be stolen from a database of a service provider or merchant, such as a bank;
- Internet users could fall victim to online scams where an infected e-mail attachment is opened or by following a link included in an e-mail; and
- hackers may steal information from a computer over the Internet (Foley *et al*. 2003; Privacy and American Business 2003).

Not only does the recent increasing flood of identity fraud incidents place the unfortunate victim in a financially precarious position, but it also takes many hours to resolve, both for the victims and the defrauded companies involved. Furthermore, and perhaps even more importantly, it could potentially place a strain on the economical growth of e-commerce globally, by hurting consumer confidence in the industry (Berner 2003; Williams 2000).

In their 2005 *Global Security Survey Report*, Deloitte Touche Tomahtsu (2005) reported that financial companies have increased spending on identity and vulnerability management for the second year in a row. Almost 70% of the financial institutions surveyed now have a programme in place to manage privacy. The report further lists identity theft as 'the fastest growing white collar crime in the US', which now accounts for 42% of all fraud complaints to the US Federal Trade Commission. This comes as no surprise when we consider media reports on identity theft and fraud over the past few years.

White-collar crime, including identity theft, is costing South Africa billions of rand each year since organized crime became involved (Fraud Investigator 2003). As a result, identity fraud could lead to bankruptcy for companies. Identity theft is also much more widespread than it appears according to the *Privacy and American Business's ID Theft Survey 2003*. Between January 2001 and May 2003, more than 13 million Americans became victims of identity theft, roughly one out of every 30 American citizens, of which 34% were victims of credit card fraud. This survey also confirms that identity theft is on the increase. Westin, who designed the survey, stated in the findings that 'no one institution, industry or government agency is to blame', implying that there is no easy solution to this growing phenomenon (Privacy and American Business 2003).

Identity theft is a worldwide phenomenon, which costs the United Kingdom £1.3 billion a year. Fraudulent credit card purchases account for most of these costs and fraud is mostly only detected after a considerable sum of money has been involved. In many cases, personal information and card numbers are obtained when handheld computer devices, such as PDA devices, are stolen. Other factors that contribute to identity theft include online scams, poor password management and theft of confidential documents such as bank statements (Privacy and American Business 2003).

Financial identity theft involves the use of another person's credentials to obtain credit facilities (credit cards, loans, leases, etc.). In the case of identity cloning, an impostor will attempt to establish a new identity for him or herself, which is typically the objective of

illegal immigrants and criminals attempting to cover their own tracks (Foley *et al*. 2003). In the survey, *Identity theft: The aftermath 2003. A comprehensive study to understand the impact of identity theft on known victims*, 88% of victims reported that their information was used to open credit accounts (Foley *et al*. 2003). The implications ranged from inconvenient to devastating. Almost 50% of victims took more than a year to resolve damages done by fraudsters and 17% took more than three years, spending an average of more than 600 hours to resolve these problems. Another 62% of respondents reported that they had no idea how impostors could have obtained their information. In some cases, it took more than three years for victims to discover that their identity had been stolen. This is the time it took for unpaid accounts in their name to be processed legally and be placed on the databases of credit bureaux.

One of the latest strategies employed by fraudsters is 'phishing'. This involves the luring of potential victims to a bogus Web site where the victims are requested to 'confirm' their personal information by typing it into a Web-based form. Attackers will typically send an e-mail to targeted victims, requesting them to visit a Web site provided for this purpose. The fact that many persons fall victim to this and other scams indicates ignorance on the part of the general knowledge worker (Federal Deposit Insurance Corporation 2004). In their 'phishing trends' survey, IT decision makers confirmed that 45% of employees who received a phishing attack e-mail, clicked the link in the e-mail (Global Research Partners 2005).

In an article on the findings of the Andersen Internet Privacy Survey (1998), *Business Times* reporter Greg Gordon reported that 75% of South Africa's top 200 companies ignored Internet security. The same survey confirmed that 61% of these companies did not have a security awareness programme for users (Gordon *s.a*.).

top

3 Understanding the risk and implications of identity theft

From studying various publications, it has become clear that the average knowledge worker and Internet user is not informed and concerned enough about the threat of identity theft and network intrusion. Internet users still open unsolicited e-mails and even click their hyperlinks (Global Research Partners 2005).

Identity theft can have a tremendous impact on the life of the victim. His or her credit record appears to be the greatest risk. Once a person's credit record is stained, it may take months or even years to rectify. In surveys, respondents have also indicated that banks and other institutions blamed them for the theft of their identities (Foley *et al*. 2003)

Knowledge workers are simply not always aware of how easily a hacker or fraudster can obtain their personal information, particularly those persons who do not work with information technology on a regular basis and who fail to understand the risks involved with new and developing technology. Wireless networking is a good example of new technology that which brought its own new set of vulnerabilities. Simply adding a wireless subnet to expand an existing network holds excellent benefits over adding a cabled section. Furthermore, the technology is so simple to install, configure and use, that often little thought is given to the security of the newly added technology. An unsecured wireless subnet, however, provides easy access into the entire network.

The Deloitte Touche Tomahtsu survey (2005) provides an indication of privacy vulnerability. The networks of financial institutions compromised in the 12 months during 2003/2004 were: Canada – 50%; Europe and Middle East Africa – 35%; and USA – 26%. Financial institutions are notoriously careful about their networks for obvious reasons, and

the fact that these could be compromised indicates that network security is never a guarantee. It could be argued, therefore, that organizations less concerned about their networks than financial institutions are even more vulnerable to hacking (Deloitte Touche Tomahtsu 2005).

The Synovate survey report of 2003, compiled for the Federal Trade Commission, indicates that approximately 27 million Americans fell victim to identity theft during the period 1998 to 2003. This number represents 12.7% of the United States population – more than one out of every ten Americans. The implications of these numbers are frightening. Indicative of the escalation rate of this crime are the percentages of the respondents who have discovered that they have been victimized: from 4% in 1997/8 to 26% in 2002/3 (Synovate 2003).

When surveying media articles reporting stolen databases from banks and other institutions, it becomes clear that many victims might not even know that their identities had been at risk. Several companies admitted that large databases with thousands of records were compromised by hackers. The knowledge worker should be aware of such possibilities and remain alert (Gordon *s.a.*).

The faceless world of the Internet certainly provides the biggest risk of impersonations. Hackers have no problem with impersonating a victim over the Internet and, since there is no verification of identity in person, fraud can take place much easier (Bergstein 2005; Krim 2005).

The Internet also provides the required anonymity to hackers targeting databases that contain personal details of potential victims. Hackers themselves might not intend to use the details for their own purposes, but could sell the database to a crime syndicate (Fraud Investigator 2003).

top

4 Network intrusion strategies and methods

Identity theft mostly takes place when fraudsters get hold of personal information via documentation or social engineering (this term is explained below) and by stealing information from computers, networks or the Internet.

The concept of privacy is well known, but the value of personal information to network intruders is clearly underestimated. Knowledge workers often believe that information about themselves and their company does not pose any threat to the organization's security. However, the reality is that network intruders only require a basic user account on the network from where it can be escalated to an administrator or 'root' account. With such a 'super user' account, intruders can cripple the organization's entire network or get hold of its databases.

To obtain access to a network through a user account, the intruder only needs to know two things: the username and the password. Many organizations use a standard naming scheme for user accounts, that is, the username is constructed from the user's name/surname or his/her position in the company. Very often, the username is also the first part of an employee's e-mail address. As such, it is relatively easy for an intruder to obtain this piece of information. Once the username is known, the intruder is halfway there; only the password remains. On a network where users select their own passwords, privacy is extremely important, since many users select an 'easy to remember' password relating to a personal interest. If enough personal information about the user is known to intruders, they can start guessing possible passwords.

'Social engineering' is a term used to describe an activity where a hacker engages in social

contact with a potential victim to extract personal or confidential information for malicious use. By getting to know the interests of a person, the hacker has a better chance to guess the person's password or to learn important information about his/her employer's network or its security measures. For example, a specific user might be interested in fly fishing and may model his or her password on a term related to the sport, such as the name of a favourite fly, like woollybugger, walkerskiller or royalcoachman. Similarly, Star Wars fans might select passwords such as: skywalker or darthvader. If the intruder can establish whether the person has a strong interest in a specific area, it will assist the intruder in guessing the password (Lemos 2004).

Intruders will typically use software to do the guessing for them, automating the process, which requires little effort on their part. It should be remembered that intruders are not just persons from outside the company, but are often employed by the company itself. Should fellow employees, for whatever reason, want to acquire information from the network without having the required permission, they would not want to run the risk of snooping around the network under their own logins, but rather those of another employee. This strategy would provide them some anonymity and, if used together with spoofing (this term is explained below) and other techniques, they have a real chance to prevent being identified (Shimonsky 2002).

Should intruders be successful in breaching a system, they might be able to get hold of files with personal information, mailing lists, address books or password lists. They may even install worms or other malicious software such as key loggers, to monitor a user's keystrokes. Key loggers can record keystrokes when users log into their bank accounts online and retain the information for the intruder, without the user knowing it. The intruder may also install software on a remote system allowing it to scan or attack other computers without the users' knowledge. This strategy has the added benefit (for hackers) of anonymity, while they are also not using their own resources (bandwidth and processors).

To further confirm the risks of using the Internet, logs from firewall software were studied for a one-week period over a dial-up Internet connection, and for a period of one month over a permanent ADSL connection. A standard dial-up Internet connection to the ISP Interprise in Rosebank Johannesburg and an ADSL connection through Axxess in Durban were used. A fully licensed version of McAfee Personal Firewall Plus was used to log intrusion attempts in both cases. The Internet connections were used for Web browsing and e-mail. The logs recorded all potentially malicious activities or attempts from other computers on the Internet to connect to the test systems for whatever purpose. The results show that a total of 481 attempts were blocked during a total of five hours and 19 minutes of use, or 1.5 attacks per minute on average over the dial-up connection. Logs from the connection over the ADSL connection showed that a total of 1567 intrusion attempts were made over a period of one month. The reason for the reduced number of attacks over the ADSL connection is the fact that Internet access was obtained through another computer with yet another firewall program installed. This is also a reason for concern, since that implies that the recorded intrusions were only stopped by the second firewall on the test system. The severity of the attempted intrusions ranged from relatively harmless to potentially dangerous. The average, non-technical knowledge worker or user is often unaware of these intrusions or potential attacks. They might not even be aware that the safety of their computers may have been breached.

There are several reasons why hackers would attempt to access a network, for example:

- to obtain a storage place for files, such as illegal software or pornography. Hackers might even use a corporate FTP server or Web server for this purpose, which allows them to make such software available to Internet users without being implicated;

- for the personal challenge, or to 'see if they can';
- they may want to use your computing power. Servers often have very powerful processors able to crack passwords or decrypt code much faster than the average desktop computer. By installing the required software on your servers and running the processes remotely, intruders again maintain their anonymity and use their own processors for other tasks;
- hackers may want to use your bandwidth. By obtaining access to your network, they will also be able to use your network's bandwidth for Internet access;
- when intruders perform illegal activities from within your network, it provides them with anonymity for possible fraudulent transactions, spamming and/or other computer crimes. They may run a mail server from within your network to distribute spam or conduct attacks against other targets; and
- stealing intellectual property, databases and privileged information to sell to crime syndicates.

Information about a target network can be obtained through freely available software, such as network sniffers, scanners and mappers. Once hackers have some information about the network and the software running on the network, they will start looking for exploits to breach the security. Again, information on such exploits is freely available. In short, no network is perfectly secure and if professional hackers want to breach the security, it is really just a question of time before they succeed.

An important aspect of hacking is anonymity. Good hackers always cover their tracks. You might not even be aware that your system had been compromised. One of the techniques used to prevent tracking, is spoofing. This implies the use of fictitious IP addresses and media access control addresses to prevent successful tracing of the perpetrator.

The Deloitte Touche Tomahtsu Survey (2005) clearly indicates an increase in the number of internal attacks: 10% (2003), 14% (2004) and 35% (2005) of the total number of attacks was from inside the network. This trend indicates a need to make knowledge users more aware of the risks inside their own offices so that they can notice suspect activities around them more easily.

Mass e-mailing strategies are often aimed at luring large numbers of people to bogus Web sites from where information can be collected on Web forms, on the false pretence that they stand a chance to win prizes or that they need to update their account details. The link on such an e-mail could also be spoofed – the text of the link seems legitimate, for example www.ligitweb.com, however the underlying hyperlink may be to another site altogether and if clicked, could install a worm or other malicious software. Such strategies are also used to pull off so-called 'phishing' scams – luring users to a spoofed Web site and convincing them to provide their personal details under false pretences.

Phishing e-mails from the 'eBay' scam were studied to determine the typical design of these scams. In this scam, a series of e-mails gave the impression that the intended victim's eBay account was under investigation from a so-called fraud investigations team (FIT). A great deal of care was involved in constructing the message to make it appear authentic and the message in the e-mail also included an idle threat to victims who did not intent to respond, that they would be liable for the costs of the investigation. The return e-mail address provided appeared to be a legitimate eBay e-mail address. On closer inspection, it became clear that the e-mail was sent via Yahoo.com, with the message identification of: ZZGFQPYKDUEQDKTZWNIL@yahoo.com. A DNS lookup for the Internet address 75.146.202.64 from where the mail originated revealed that the address was probably spoofed, since neither the address or the domain (http://ebaysignin.info) were registered. The e-mail prompted victims to follow the included link:

http://ebaysignin.info/ws/eBayISAPIdllSignIn.htm to update their information. This Web site has since been removed, but the intention of the fraudster was to lure Internet users to the 'fake' Web site where they were presented with an online form to enter their details. Once the details were entered and the form submitted, the information entered (the victim's name, username, password and all his or her personal details) was written to the fraudster's database. This particular phishing scam operated during July 2005.

top

5 Limiting the risks of identity theft

In some surveys, articles and publications studied, guidelines are provided to point out safe Internet and network practices to knowledge workers. The reality is, however, that identity theft is still increasing and most victims might not yet be aware that their privacy was compromised as their identity could have been stolen from a corporate database, a reseller or government network. During 2002, 44% of United Kingdom businesses suffered security breaches (PricewaterhouseCoopers 2002).

In their *Global Information Security Survey* (2004), Ernest & Young found that respondents listed 'Lack of security awareness by users' as the major obstacle to effective information security. However, in the same survey it was found that only 28% of respondents listed security and awareness training as top priority (Ernest & Young 2004). Most other publications cite the fact that security is not ensured through a single activity or by having the correct policies and equipment in place, but rather through a total combined strategy, which includes awareness training.

The United States Federal Trade Commission and Berner (Computer Associates *s.a.*; Berner 2003) provided a comprehensive list of guidelines to prevent identity theft. The following are additional recommendations:

- Have at least the following security software installed and maintained on your computer: antivirus, firewall and anti-spyware;
- constantly ensure that your software (operating system, programs and applications, antivirus software, anti-spyware and firewall) is updated regularly.
- never open any links in unsolicited e-mails;
- be very careful when providing any personal information on the Internet. Read the site's privacy policy first and only provide information if you are satisfied that the information would not be passed on to third parties. Also, check the security certification of so-called secure Web sites;
- do not indiscriminately store personal information on a computer. If you have to, encrypt the information, using a 'strong' password to do so; and
- take care to wipe storage mediums securely before disposing of them. Simply erasing files does not necessarily destroy the information on them.

In addition, popular so-called 'peer' software, such as iMesh and Kazaa, should never be allowed on any networked computer. The purpose of this type of software is to allow other Internet users access to a shared folder on your computer and, in return, allows you access to shares on other computers on the Internet. There are several loopholes in such a system that could be exploited by knowledgeable hackers.

On the social front, avoid giving personal information to others, unless you are perfectly certain that it is safe to do so and that the information will only be used for legitimate reasons. Special care should be taken with personal information typically carried on your person, for example identity documents and driver's licenses.

Patrick Evans, regional manger at Symantec, suggests that the first of the top five priorities for security should be awareness, which he calls the creation of 'human firewalls'. Part of the awareness training must include the usage and storage of passwords (Evans 2005).

Biometrics and chip implants will most certainly provide a solution for personal identification, and chip implants even offer an economically and logistically viable option. Several studies have been done on biometrics as a possible solution for improved authentication but the costs and logistics of the implementation of biometrics present huge challenges (Willox and Thomas 2001). Since the person should physically be present for the authentication process, biometrics does not provide an effective solution for e-commerce either. Human chip implants, which is still a very contentious issue, could also be considered as a possible solution, but the person also has to be present for identification and implants are therefore not a solution for personal online authentication.

top

6 Conclusions

Continued increase of identity theft worldwide potentially holds devastating consequences for the victims and, from an economic point of view, the impact could also spark a decrease of consumer confidence in global economy. Many online e-commerce businesses have not only survived the so-called dotcom era, but became exceptionally successful and are sources of income for large numbers of staff. Should such businesses fail as a result of reduced consumer confidence, it will leave families without an income worldwide and consumers without the convenience of online shopping.

From the reviewed publications on identity theft, it has become evident that awareness training is perhaps the single most important activity to minimize identity theft. There is no single perfect solution to safeguard someone completely from the risk of identity theft and all indications are that this type of theft is going to escalate rather than disappear.

Reports from victims show that identity theft was a life-changing event for them. Knowledge workers and Internet users should almost be paranoid about privacy. Knowledge workers should be made aware of the risks and should be informed about preventative measures. Identity theft and privacy risk awareness training should form part of every organization's training programme. In short, the suggested precautions imply nothing less than a change of lifestyle in an attempt to safeguard someone's personal information. Could it be said: 'Be afraid – be very afraid'?

top

7 References

Bergstein, B. 2005. Credit card hacking not hard. [Online]. Available WWW: http://www.madison.com/wsj/home/biz/index.php?ntid=44402&ntpid=2 (Accessed 30 June 2005).
Berner, S. 2003. Safeguarding that personal bit. [Online]. Available WWW: http://www.sajim.co.za/default.asp?to=trainingvol5nr4 (Accessed 11 July 2005).
Boulton, C. 2005. MasterCard: 40M credit card accounts exposed. [Online]. Available WWW: http://www.Internetnews.com/security/article.php/3513866 (Accessed 10July 2005).
Computer Associates. *s.a.* Identity theft. [Online]. Available WWW: http://www3.ca.com/Solutions/Collateral.asp?CID=38599&ID (Accessed 4 July 2005).
Deloitte Touche Tomahtsu . 2005. *Global security survey in the financial services industry 2005*. [Online]. Available WWW:

http://www.deloitte.com/dtt/research/0,1015,sid=1013&cid=85452,00.html (Accessed 30 June 2005).
Ernest & Young. 2004. *Global information security survey 2004.* [Online]. Available WWW: http://www.ey.com/global/content.nsf/South_Africa/28_Sept_04_Global_Security_Survey (Accessed on 2 July 2005).
Evans, P. 2005. What should an IT manager's top five security priorities be?. [Online]. Available WWW: http://www.networktimes.co.za/Article.ASP?pklArticleID=3236&pklIssueID=301 (Accessed 6 July 2005).
Federal Deposit Insurance Corporation (FDIC). 2004. Putting an end to account-hijacking identity theft. [Online]. Available WWW: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf (Accessed 4 July 2005).
Fraud Investigator. 2003. White-collar crime is costing SA billions. [Online]. Available WWW: http://www.fraudinvestigator.co.za/fraud_news_18_september_2003.htm (Accessed 30 June 2005).
Foley, L., Foley, J., Pletcher, J., Miranda, D., Colins, P. and Nelson, C. 2003. Identity theft: The aftermath 2003 A comprehensive study to understand the impact of identity theft on known victims. [Online]. Available WWW: http://wwwidtheftcentre.org (Accessed 4 July 2005).
Global Research Partners. 2005. Nearly half of IT decision-makers surveyed say employees have 'fallen for the phish'. [Online]. Available WWW: http://www.itweb.co.za/office/securedata/0505250921.htm (Accessed 10 July 2005).
Gordon, G. s.a. Companies leave databases wide open to espionage. [Online]. Available WWW: http://www.btimes.co.za/98/0705/tech/tech9.htm (Accessed 6 July 2005).
ITWeb staff writer. 2005. Alleged phishing writer detained. [Online]. Available WWW: http://www.itweb.co.za/sections/internet/2005/0505231037.asp?A=EBU&S=e-Business&O=E&CiRestriction (Accessed 28 July 2005).
Krim, J. 2005. Net aids theft of sensitive ID data. [Online]. Available WWW: http://www.truthout.org/cgi-bin/artman/exec/view.cgi/37/10093 (Accessed 29 July 2005).
Lemos, R. 2004. Password imperfect. [Online]. Available WWW: http://news.com.com/2100-7355_3-5475264.html (Accessed 30 June 2005).
News24.com. 2005. ID crime rocketing. [Online] Available WWW: http://www.news24.com/News24/South_Africa/News/0,6119,2-7-1442_1666043,00.html (Accessed 30 June 2005).
PricewaterhouseCoopers. 2002. *Information Security Breaches Survey 2002.* [Online]. Available WWW: http://www.securitymanagement.com/library/Infosec_tech0702.pdf (Accessed 14 July 2005).
Privacy and American Business. 2003. P&AB ID Theft Survey 2003. [Online]. Available WWW: http://www.pandab.org/id_theftpr.html (Accessed 4 July 2005).
Shimonsky, R. 2002. Hackingtechniques. [Online]. Available WWW: http://www-128.ibm.com/developerworks/security/library/s-crack/ (Accessed 20 July 2005).
Synovate. 2003. *Federal Trade Commission – identity theft survey report 2003.* [Online]. Available WWW: http://www.consumer.gov/idtheft/stats.html (Accessed 6 July 2005).
Williams, D. 2000. Privacy and e-commerce – getting a competitive edge. [Online]. Available WWW: http://www.ag.gov.au/agd/WWW/attorneygeneralHome.nsf/Page/Speeches_2000_Speeches_Privacy_and_Electronic_Commerce_-_Getting_a_Competitive_Edge (Accessed 6 July 2005).
Willox, N.A. and Thomas, M.R. 2001. Identity theft: authentication as a solution. [Online]. Available WWW: http:// www.nationalfraud.com/identity%20theft%203.13.htm (Accessed 3 July 2005).

Disclaimer

necessarily reflect the opinion of the Editor, Board, Publisher, Webmaster or the Rand Afrikaans University. The user hereby waives any claim he/she/they may have or acquire against the publisher, its suppliers, licensees and sub licensees and indemnifies all said persons from any claims, lawsuits, proceedings, costs, special, incidental, consequential or indirect damages, including damages for loss of profits, loss of business or downtime arising out of or relating to the user's use of the Website.

top

ISSN 1560-683X

Published by InterWord Communications for Department of Information and Knowledge Management, University of Johannesburg