Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)

Practical Assignment V1.4

OPTION 2 Case Study

INTERNET BANKING FRAUD INVESTIGATION

Author: Narelle Wakely

Date: July 2003

Version: 1.0

File Name: Narelle_Wakely_GSEC.doc

Table of Contents

Summary

As part of an IT Security Investigation and Response team I was assigned six separate Internet banking cases to investigate from the Business Fraud team. The scope of my investigation effort was to help identify the source of the Internet banking sessions where the suspected fraudulent transactions were committed and determine if the cases were linked. Additionally by examining how the frauds were committed offer some advice for preventative measures.

The cases occurred over January, February and March 2003 and involved individual exposure of funds ranging from six thousand dollars to half a million dollars.

The approach taken was to utilise technical detail, such as the reported IP address, provided in Internet banking application reports. By using familiar security tools such as WHOIS, NSLOOKUP and TRACERT I was able to clarify the sources of the banking sessions. Further analysis of the available data also revealed a predictable pattern to how the frauds were committed. The six cases were linked. To reduce the fraud risk recommendations were made back to the Business unit regarding authentication, application design, detection and education. Since completing this particular investigation our team has also seen a trend towards more sophisticated ways of social engineering customers to gain access to funds by stealth, indicating the threat is increasing which adds weight to the recommendations made for these cases.

Before Snapshot

The investigation of these six Internet banking cases revealed weaknesses in the authentication processes used by the application and helpdesk, the processes that allow further privileges such as increases to transaction limits, the detection and reporting of misappropriated funds and the education of end-users.

These process weaknesses are vulnerabilities. With the threats of social engineering, identity theft and system compromises increasing the risk of fraud to the Internet banking customer and the financial institution is high.

Authentication
This Internet banking application uses a numeric eight-digit customer identifier and password for authentication of its retail customer base. The password is an alphanumeric containing six characters. It is managed by the customer and is not forced to change by the application. The Internet banking Terms & Conditions (T&Cs) state the password 'should' be changed and 'recommend' it be changed regularly, for example every six months. There are some guidelines about not selecting easy passwords, such as birth dates, and how to manage the password's safe custody such as not storing it with the customer identifier, not recording it in a recognisable way.

When a password is forgotten a customer can contact the helpdesk and request a password reset. The helpdesk procedure is for the caller to provide their telephone banking, a separate application's, 3 digit access code. Alternatively the helpdesk will ask five out-of-wallet questions to ascertain the identity of the caller. When the operator is satisfied with the caller's identity the Internet banking password is reset to a one-time use password and the caller is immediately informed of what this is. The application forces the customer to change this password the first time it is used.

Authorisation -Increasing Transaction Limits
For retail customers value transactions such as transfers, third party transfers and bill payments via Bpay[1] can be performed to a standard limit of Au$1500 per day. This limit can be increased to Au$5000 per day and requires the customer to request this change online. An access code will be mailed out within 5 days to the customer to activate the request. The T&Cs do point out that by increasing the transfer limit it will increase the risk to the account holder for unauthorised larger withdrawals for which the account holder could be liable.

Business customers performing unrestricted value transfer transactions are issued with an authentication token to be use when initiating this particular transaction. A business customer has the initial Internet banking sign-in password authentication and a stronger two-factor authentication process for authorising potentially high value transactions.

Detection and Reporting
Typically the financial organisation waits for a customer to complain about misappropriated funds. In fact the T&Cs state it is the customer's responsibility to notify

[1] Bpay is a registered bill payment system used in Australia. Companies register to the Bpay organisation and receive a biller code that they make available to their customers. Each customer receiving a bill has a unique reference number. At a participating financial institution customers can then transfer their money online to the biller to pay their bill using the biller code and their reference number.

the finance organisation first if a mistake is suspected. There has been an increase in customer complaints of misappropriated funds during the period of these six cases. This has made the Business Fraud team suspect a more organised approach is being taken to commit fraud in the Internet banking channel.

The Internet banking application will produce on request from authorised business personnel a trace report for a specified customer and date range. This report provides some technical detail such as an IP address for each Internet banking session in the specified period. A session id is then assigned to all the system and application events performed using that session IP. Other sections in the report also detail the value transactions with the transaction type, from/to accounts, amount, currency and date and time. This information could be considered an application log. The Business Fraud team have requested the trace reports for the six customers covering the period of the suspected fraudulent transactions. The report is the information given to assist in my part of the investigation.

Although the business fraud team can perform their own analysis on the reported application details such as the accounts receiving funds, times, types of value transactions used and whether or not a password reset has occurred or not, they do not have the technical know-how to get a more meaningful identification of the session IP. A number tells them little about the source country or region, type of connection used eg dialup or broadband and therefore whether the session location and connection were normal customer behaviour or not, and whether the sources have been used in other cases.

The customer is liable when they are careless with their authentication credentials, which is why identifying the source of the disputed transactions and any linkages to other cases can help determine the intent or not of fraud and the subsequent liability.

During Snapshot

This fraud investigation became an IT Security Incident for our team to manage and therefore follows our internal response process as follows:

1. Incident notification and acknowledgement
2. Obtain reported information
3. Verify the information is an incident
4. Determine severity
5. Formulate plan of action to:
   - Contain the threat
   - Eradicate
   - Recover
   - Protect
   - Followup
6. Execute required communication

Incident notification

The Internet banking cases were notified direct to our team at the end of March 2003. I was assigned the case. I assigned a case number, created our necessary files and reported back to the Business Fraud team to gain a better understanding of their requirements.

Obtain reported information

Discussion took place with the Business Fraud team regarding the scope of the investigation, as the cases were several weeks old. The scope was defined as simply to help identify the source of the Internet banking sessions where the suspected fraudulent transactions took place and determine if, and how, the cases were linked. Also by examining how the frauds were committed offer some advice for preventative measures. Basically what is the threat and how can we minimise the risks.

Therefore the case became more of a consultative investigation rather than an incident response and it would not follow all our normal incident response steps.

The Business Fraud team forwarded the Internet banking application reports they had retrieved for the six cases in question.

Verify the information is an Incident

At this stage the cases were being treated as fraud by the Business Fraud team but they were not willing to divulge any further information regarding other actions underway. I asked if any of the customers had reported a theft and this information was provided verbally. Based on the information provided the cases would be treated as a fraud incident.

Determine the Severity

Fraud is classified as a high severity incident.

Plan of Action

The six reported cases were analysed sequentially and then correlated. The steps conducted were:

1. Analysing each Internet banking application trace report and check for
    - The likely access method and transaction pattern used to conduct the value transactions – was a password reset present?
    - The time of day when activity occurred – normal sociable hours or not?
    - The accounts receiving funds – any the same?
2. Resolving the session IPs to a more meaningful identity and location
    - Using WHOIS[2]
3. Tracing and analysing IP ownership
    - Using NSLOOKUP and TRACERT[3]
    - Reverse DNS lookup when required
    - Company checks using Australian Securities and Investments Commission (ASIC)[4] online enquiries

Results

The analysis revealed the six cases were linked in three ways

1. Two common computer source locations, i.e Internet Protocol (IP) address, for Internet banking sessions

    One set of IP addresses resolved to the same Internet Service Provider (ISP). Generally if the IP address is sourced to an ISP provider I am unable to ascertain directly the owner or location of the computer activity due to privacy and legal constraints.[5] The sourcing of this information can generally only be progressed by law enforcement agencies.

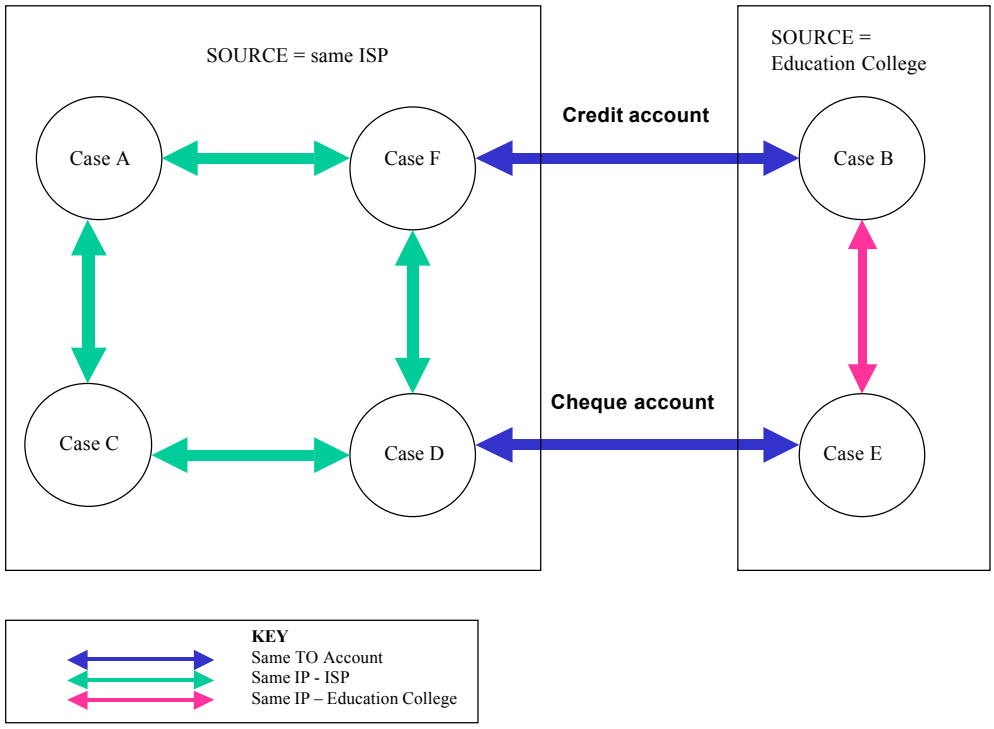
    However in this instance by performing a little of my own social engineering I have been able to ascertain that an IP resolving to this Internet Service Provider 's accounts that are prefixed by "PR" are Asynchronous Digital Subscriber Line (ADSL) accounts. Furthermore the ISP has identified that Internet Cafes, as opposed to individuals, lease the majority of their ADSL accounts. ADSL is a technology for transmitting information at a high bandwidth on existing phone lines to homes and businesses. Unlike regular dialup phone service, ADSL provides continuously available, "always on" connection. Accounts of this type are valuable in the course of an IT Security investigation because they are leased for a far longer period of time than IPs that are temporarily assigned to the users of dial up accounts. This in turn supports the ISPs to identify the account holder before system logs roll over.

[2] Geektools WHOIS http://www.geektools.com/cgi-bin/proxy.cgi
[3] Optus Looking Glass NSLOOKUP and TRACERT http://looking-glass.optus.net.au/
[4] ASIC company checks http://www.asic.gov.au/asic/asic_srchlodg.nsf
[5] Telecommunications Act 1997 (Cth) and Privacy Act (Cth) 2000

The second common IP resolved to a private Education College. Education institutions are renowned for being used for illegitimate purposes but in this case the college was again forced to prove its innocence having been accused of inappropriate activity six months before. The college no longer owns the IP addresses in question or even uses the same ISP provider. They have brought this current matter to the attention of their previous ISP provider again. Unfortunately the offending ISP has been the target of multiple business takeovers resulting in it now being owned by a collapsed global telecommunications company. A poorly run ISP is a soft target for those wanting to abuse the IPs under their management and to hide their identities.

2. Two target accounts receiving funds - a credit card and a savings account belonging to the same financial institution, but not this Internet banking institution. This indicates the fraudsters are likely to have set themselves up with a false identity using stolen or forged credentials. In this country it is colloquially referred to as the '100 point check' and is normally verified using paper based documents. The normal pattern is then to withdraw the stolen money as quickly as possible from these new receiving accounts at the other financial institution.

Internet Banking Case Connections



3. In these cases social engineering was the method used to gain access to the system and remove funds. The predictable pattern was as follows:
   - Obtain identification details by theft, then use the identity details to socially engineer a password reset for the Internet banking sign-in or to create a false Internet banking account

   Once access was achieved
   - conduct value transactions to the daily limit

- attempt to increase that limit to enable execution of higher value transactions
- use third party payments or Bpay payments to execute the value transfer to target receiving accounts
- check the transactions were executed soon after midnight or even after known end of day batch processing

Summary of Fraud Pattern

Case	Identity Theft	Password Change	Limit Increase	Sessions in abnormal hours
A	None reported	Reset at Helpdesk 10/01/03	No	No
B	Yes	Internet Banking account created 31/01/03	No 3rd party trans = 4 x $1500	03/03/03 @ 00:30
C	Helpdesk call successful for reset	Password changed 23/2/03	Yes Transfer = 1 x $8000 3rd party trans = 2 x $1500	No
D	None reported	Password changed 01/03/03	Yes Transfer = 1 x$1500 3rd party trans = 2 x $1500 Bpay =1 x $4000	2/3/03 @ 00:26
E	None reported	Password changed 2/3/03	Yes Transfer = $1500 3rd party tran = 1 x $1500 Bpay =1 x $8000 1 x $5000	03/03/03 @ 00:17, 04:18
F	Theft via house break-in and wallet stolen in separate incident	Password changed 20/2/03	No (increase already in place) 3rd party tran = 2 x $2000 1 x $5500 1 x $9000	21/03/03 @ 01:36, 03:59, 04:15

Application Reporting Error
During the analysis it was discovered that some of the reported IP addresses for the Internet banking sessions were reserved for local network addressing. This masks the true source IP for the Internet banking session.

Recommendations
Along with the results of the investigation the following recommendations were put forward to the Business Fraud team for their consideration to reduce the risks of ongoing Internet banking fraud:

1. The Internet banking password reset process and procedures are reviewed and strengthened.

   1.1. Changes to the identification part of the process-

   These few cases have shown it is too easy to social engineer the identification requirements of the Internet banking customer used at the Helpdesk. The process of either using the customer's Telephone Banking access code or the same out-of-wallet questions for each call is too predictable and makes the social engineering task easy and successful.

   To help strengthen the existing process some variation needs to be added to the question and answer method for example randomly choosing 3 questions from a possible list of 10. There would be little cost to implement this small change to the existing process. Alternatively there are other techniques to the question and answer model such as the use of customer generated questions and answers. However this technique will require system changes to store the details and there is little control over the quality of the question and answers chosen. Easy to remember questions become easy to guess as well.

   1.2. Changes to the response part of the process-

   The new reset password could be issued to the customer via another channel, for example a call-back using system stored registration details, an e-mail response like that used in our business environment. When using e-mail responses it is recommended webmail accounts are excluded. By using an alternative channel for delivering the new password it enables the process to be strengthened by:

   - the customer's identification is again confirmed using previously supplied information
   - the customer is alerted to an attempt to compromise their password if a fraudster is at work
   - the fraudster is required to compromise not only identification material but also the target's delivery channel for example the email or phone. This is extra work and often more technically difficult to achieve thus reducing the likelihood of a breach occurring.

2. The Internet banking application sign-in process could be strengthened with the introduction of a two-factor authentication process, like the use of tokens being used with business customers for unlimited transfer transactions. This could be an optional authentication process presented and made available to all customers. The cost, for example of a token, could be at the customer's own expense when they assess their risk of a password sign-in is not acceptable to them. It would then transition the change and in time could become the authentication process.

To enhance the existing authentication process introduce stronger passwords rules such as a minimum of eight characters not six, must contain a numeric, a special character and is forced to changed on the recommended six monthly time frame.

This would reduce the threat of passwords being easily guessed, socially engineered or cracked by malicious code. The simplest technique is to suggest customers use a phrase and selecting first letters from the phrase with a number or special characters added for good measure.

The disadvantage to stronger password rules is the likely increase to helpdesk calls due to forgotten passwords. Justification is the cost compared to the increasing costs of the frauds being purported by this weakness.

3. Review the process that enables change to withdrawal limits.

   A simple change would be to again introduce a separate notification channel to the Internet banking customer that this limit change has occurred for example via their e-mail (not webmail). This would at least enable earlier detection of a fraud attempt if the requested change were not valid.

4. The IP sessions reported as local network IP addresses is an application logging error due to the introduction of a web-based single sign-on facility. This single sign-on module is not passing on the source IP details to the Internet banking application and others. Explicit development guidelines have now been developed and passed to the system teams to ensure traceability and auditability of customer transactions at the application level.

5. The education of the customer base to use, and to use effectively, anti-virus and anti-spyware software, such as personal firewalls, when using the Internet is critical. It must be recognised the financial institutions can, and are, implementing security measures on their side of the business transaction. More often it is the client PC that is left vulnerable to malicious attack. The customer must take some responsibility to prevent this but can only do so when educated to know they are vulnerable. Additionally education programmes need to cover preventative measures to avoid being the target of identity theft. These education programmes would aid the introduction and acceptance of any changes used to strengthen the existing Internet banking processes.

6. Review the availability and cost benefits of introducing a software diagnostics tool to analyse, cross reference and report abnormal customer transaction behaviour used in the Internet banking channel.

   It is observed that most of the fraudulent activity occurs in the late evening or very early in the morning. For the majority of customers this would be abnormal behaviour. In most cases the fraudster signs in again soon after midnight to see if their transactions were processed. In some cases it can be seen they are even aware of the time overnight batch processing is completed.

   Customers usually log onto the Internet banking system from predictable locations using known device types such as work, home or banking kiosk facility.

   These are all triggers that could alert the organisation and their customers to fraudulent activity in a timelier manner. Detection is an added defence mechanism for securing systems, as prevention measures are rarely hundred percent.

After Snapshot

The risk of fraud conducted via the Internet banking channel is increasing with the vulnerabilities still in existence and the threats expanding. The business is currently accepting the risk. They do recognise however they are more aware of where the vulnerabilities lie and the preventative measures they can implement when ready to reduce the vulnerabilities and overall risk.

In regard to the uptake of my recommendations as a result of the investigation:

Review and strengthening of authentication process

The cost to the business of implementing two-factor authentication, such as tokens, and selling to the customer base with the added admittance that this financial institution's Internet banking channel may be at risk is at present too costly both in funds and reputation and has not been accepted.

It is interesting to note that another financial institution in our region is now using SMS text messages to a customer's mobile phone in place of an issued token thus helping to reduce the cost and inconvenience of a carry a token around for this two-factor authentication process.[6]

With the recent added incentive to meet government requirements to prevent terrorist funding via fraud, the business case for two-factor authentication may gain additional support for the benefits of the process.

The maturing of biometric authentication techniques and technologies, increase in consumer awareness and the wider implementation in work places may make this the more preferred second piece in the authentication equation instead of tokens in the longer term.

I believe a two-factor authentication process for retail Internet banking customers needs the strength of an industry wide uptake, or directive, with all the financial institutions agreeing to implement a solution by an agreed planned date, much like the upgrade to use triple DES encryption in the ATM / EFTPOS arena.

To date no changes have been made to the password rules, helpdesk identification procedures, alternative channel for delivery of the response or limit increase processes. Again the business case costs to make the changes are not acceptable and yet they would reduce known vulnerabilities as well as aid in detection of suspicious activity.

Development Guidelines

I have been able to progress some explicit development guidelines for web-based application development to ensure traceability and auditability of all transactions by communicating and recording the original source IP. Heightened security awareness has also been achieved in these system teams.

Education of the Customer Base.

Changes to the T&Cs have occurred where customers are now warned about the different methods of frauds, to avoid using public computers found in Internet cafés and

[6] Staff Writers, ZDNet Australia "Bank secures Internet logins via mobile messages"

libraries, what to look for to ensure they are logged into the legitimate secure banking site and how the organisation will communicate with them if required.

Unfortunately these important details are buried in the T&Cs or to a linked security information document on the Internet banking site and rarely catch a customer's attention. This communication is a step forward but not explicit enough for education. It is up to the customer to go and read the documentation. How do they know if there is a new security issue or the guidelines have changed?

The local finance industry association has recognised the need for consumer education in transacting in the online environment but does not see it as solely their responsibility. It has recommended 'There is a significant role for Government in educating the general public on their responsibilities in relation to cybercrime and on preventative measures.' [7].

There is an industry review in progress to assess new identification requirements for customer account creation, colloquially referred to as the '100 point check'[8]. With the sophistication of technology and print media the required documentation is today too easy to forge. This may also flow into a change in the Helpdesk arena as one identification proposal is to link directly into the systems used for identification to bypass paper documentation such as the traffic authority for a licence check. This would then require an increased effort for the fraudster to compromise other referenced identity systems.

Identity theft stories are now being aired in the media more regularly. Some stories turn into a bank bashing exercises because the banks are seen as not protecting the consumer's funds and privacy. Thick- skinned as the financial institutions have become this new reputation damage may provide the impetus for the banks to invest some money in process change and end-user security education.

Detection

The Internet banking application has been changed to report and display at sign-in the last logged-in session. This is a simple trigger that could warn the customer of unauthorised access to their account in a timelier manner.

The analysis of several software diagnostic tools is in progress by the business application team for their appropriateness to the Internet Banking channel. Like Intrusion Detection System (IDS) is a detection tool for infrastructure compromises so can software diagnostics tools be detection tools for the application layer and processes. To support the security defence in depth model greater industry effort is required in developing, evaluating and adding detection tools to applications and processes not just at the infrastructure layer. Recent legislation enacted in California US[9] to notify the owner of a breach in security regarding their personal information will likely support the development and use of more detection tools.

[7] Australian Banker's Association Submission to Cybercrime Inquiry, page 39
[8] Australian Banker's Association Submission to Cybercrime Inquiry, page 25
[9] Akerman, Nick "Cyberprivacy law – a needed wake-up call"

Impact

Internet banking fraud cases are increasing and are being performed by more organised teams. The cases examined here fitted the common pattern of social engineering a customer's identity to gain authentication details to Internet banking to access funds that are transferred to a pre-determined receiving account.

In the few months since this investigation new online fraud patterns are appearing both in obtaining credentials and how stolen funds are received. Like the emerging trend of blended viruses Internet banking fraud is becoming more sophisticated with the blending of techniques such as Spam, viruses with keystroke loggers and recruitment of middlemen. Continuing customer ignorance ensures a high success rate.

My team are responding to incidents to obtain credentials such as:

1. Web ghosting of Internet Banking sites combined with a mass Spam email requesting customers to visit the bogus site and enter their banking credentials such as Internet banking access and password.
2. Deployment of keystroke loggers in viruses, the use of trojans and port sniffing to obtain credentials with the funds being transferred with no apparent compromise in access to the customer's Internet banking session.

To receive funds:

3. People being contacted via the Internet chat room ICQ and asked whether they can assist in transferring funds owed in advertising contracts to Russia
4. Fake job adverts for labourers, removalists, money transfer agents etc on Australian and overseas websites such as monster.com and seek.com
   The recruiting scam aims to 'hire' individuals to accept funds into their accounts, be paid a nominal fee, and then to send the money onto a designated account using a prescribed method such as overseas telegraphic transfers using Moneygram and Western Union.[10]

In support of the recommendation to better educate the Internet banking customers the 2003 Australian Computer Crime and Security Survey report[11] comments that as these web ghosting incidents do not compromise the confidentiality, integrity and availability of the system itself it is difficult to defend against, and goes on to say, the best defence is the education of the online and system users to not disclose logon information to seemingly trusted entities.

The local finance industry body is recognising the increasing threats of fraud conducted over the Internet. A Fraud Taskforce was launched in December 2002.[12] This taskforce is currently working on several major project which include:

- The development of voluntary Industry Standards on Security and Fraud Prevention.
  This will target all banking transactions and will cover interface requirements, authentication and verification processes and source document validation.
- An Analytical Study of Identity documents
  This will examine the use, exchange and compilation of documents required for validation of a bank customer's identity, particularly when opening an account.

[10] Brown, Bina "Don't be pinned down by scamsters and spamsters"
[11] 2003 Australian Computer Crime and Security Survey
[12] Australian Banker's Association Submission to Cybercrime Inquiry, page 25

- Fraud Education Programme
  To identify the best practice education programmes and to create an education package for customers of financial institutions.

In addition the finance industry association recognises in their report published in June 2003 to the Cybercrime Inquiry 'there is significant opportunity for Government and banks to collaborate on the Critical Infrastructure Protection as a defence against cybercrime locally and internationally.'[13] A statement from the Minister for Justice and Customs supported this collaboration back in May 2003 where '…the Commonwealth and industry agreed to hold Biannual Ministerial Meetings with financial institutions to discuss fraud, in particular banking fraud.'[14] These initiatives may now provide the environment for funding of the recommended changes to the Internet banking system, processes and education of users.

As demonstrated by this case study the risk of fraud being conducted via Internet banking is high and increasing. Vulnerabilities are known and reduction measures can be put in place. As an industry we need to educate the end-users not just provide them with the technology. "The most important element of any security measure, Schneier argues, is people not technology."[15]

[13] Australian Banker's Association Submission to Cybercrime Inquiry, page 39
[14] Ellison, Senator Chris "Government and industry tackle fraud against financial institutions"
[15] Mann, Charles C. "Homeland Insecurity"

References

1. Geektools WHOIS http://www.geektools.com/cgi-bin/proxy.cgi

2. Optus Looking Glass NSLOOKUP and TRACERT
   http://looking-glass.optus.net.au/

3. ASIC company checks http://www.asic.gov.au/asic/asic_srchlodg.nsf

4. Commonwealth Of Australia Telecommunications Act 1997 (Cth)
   http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/

5. Privacy Act 1988 (Cth) which incorporates the amendments made to it by the Privacy Amendment (Private Sector) Act 2000 (Cth).http://www.privacy.gov.au/act/

6. Staff Writers, ZDNet Australia "Bank secures Internet logins via mobile messages" 17 June 2003
   http://www.zdnet.com.au/newstech/security/story/0,2000048600,20275442,00.htm

7. Australian Bankers' Association Submission "Cybercrime Inquiry"
   http://www.bankers.asn.au/ABA/PDF/CybercrimeInquiryFinal.doc

8. Ellison, Senator Chris "Government and industry tackle fraud against financial institutions" 14 May 2003
   http://www.ag.gov.au/www/justiceministerHome.nsf/Alldocs/7D56D3B406D4B96BCA256D26002324B0?OpenDocument

9. AusCERT grants permission to link to the *2003 Australian Computer Crime and Security Survey* via this page using the URL:
   http://www.auscert.org.au/crimesurvey

10. Akerman, Nick "Cyberprivacy law – a needed wake-up call" CNET News.com, 30 June, 2003 http://zdnet.com.com/2100-1107_2-1022113.html

11. Brown, Bina "Don't be pinned down by scamsters and spamsters" The Australian, (c) 2003 Nationwide News Proprietary Ltd, 10 May 2003

12. Mann, Charles C. "Homeland Insecurity", The Atlantic Monthly, September 2002

END OF DOCUMENT