Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:14
Received 12 May 2003

Mr Tony Healy
Research Software Engineer
PO Box 2045
BONDI JUNCTION BOXES NSW 1355
☎
E-mail:

Submission to Parliamentary Joint Committee on the Australian Crime Commission Inquiry into Cybercrime:

Failures in Internet Banking Protections

Submission by Tony Healy
Research Software Engineer

(Submission in private capacity)
PO Box 2045
Bondi Junction 1355
netgames@magna.com.au

09 May 2003

Thankyou for the invitation to make a submission to the PJC's Inquiry. My submission relates to crime involving internet banking.

Over the past two years we have seen several cases where customers of internet banking facilities have had their money stolen. The latest involves customers of St George bank. [1]. Almost all those thefts could have been easily prevented by the banks, but instead the banks knowingly chose directions that expose their customers' money to theft.

Traditional Tenets of Bank Security

It has always been a fundamental precept of bank security that, to access their money, customers must present a physical token, such as a passbook or ATM card, and also know or display some secret information, such as PIN numbers and personal signatures.

This combination of physical token plus secret information is effective in preventing unauthorised access, because account holders can protect their accounts by safeguarding the physical token. Even if a criminal discovers a customer's PIN or learns to forge their signature, the criminal can't access the customer's money unless he also acquires the passbook or ATM card.[2]

When banks such as NAB and CBA started deploying internet banking systems, they initially preserved this approach by requiring customers to have digital certificates on their computers. Digital certificates are small, encrypted files that customers obtain from the bank and install on their computer. They serve to uniquely identify customers, in the same way as passbooks and ATM cards, and effectively fill the role of a physical token.

Telstra and the Australian Taxation Office require internet customers to use digital certificates.

How Have The Banks Exposed Customers' Money to Theft?

Westpac and, I believe, ANZ, chose a simpler, much less secure approach. When they established their systems, they required nothing more than a password entered into any web browser. This means that anyone obtaining the customer's user ID and password can instantly log on to that user's account, from anywhere in the world, and manipulate that customer's money. For example, if a virus on a customer's computer sent the customer's user ID and password to someone in Russia, that person could log on to the customer's account.

For the banks, this weak approach provides several benefits. First, it's much easier and cheaper to implement, and it frees the bank from the cost of issuing digital certificates to customers. Second, it attracts more customers, because they can access their money from internet cafes, from computers overseas, and from multiple computers at work.

NAB and CBA found they were losing customers to Westpac and ANZ because of this convenience factor. Accordingly, in Q3 2001, NAB and CBA ditched their original internet systems and replaced them with weak systems.

Tellingly, at that same time, all the banks rewrote their electronic banking contracts in ways that would absolve the banks of responsibility for thefts and fraud, if the banks chose. They did this by making the customer directly responsible for losses arising from failure to adequately safeguard the customer's password.

In other words, having removed one critical part of the protections for customers' money, the banks then made sure that exposure of the sole remaining protection, the password, would ipso factor constitute negligence by the customer and absolve the bank of responsibility.

Why Passwords Alone Are So Weak

Relying on passwords alone for protecting customers' main financial holdings in the internet environment is extraordinarily weak. First, as mentioned, if someone anywhere in the world obtains that password, along with the user ID, they can access the customer's account without further ado.

Second, information such as passwords can and has been captured by various viruses that send information back to other computers, and can also be captured deceitfully by web sites and email requests.

Third, modern browsers store passwords automatically once a person enters them. This means that, after someone logs onto their bank account, the next user at the computer can often log on to the account using the passwords and information that have been stored automatically by the browser. Knowledgeable users can prevent this, but probably about 90 percent of computer users would not know how to do this, nor know the need for it.

Fourth, proprietors of internet cafes are not beyond capturing user passwords precisely for this purpose.

Steps The Banks Take To Ameliorate The Exposure

The banks do take steps to preserve security as much as possible within the above, weak scenario. Their main technique is to accept that there may be unauthorised log-ons, but to then try to prevent the easy transfer of money out of customers' accounts. This is why transfers from internet accounts can only be to designated theoretically valid accounts.

However there have been cases where criminals set up bogus "authentic" accounts purely to receive the transferred money, and probably there will be more.

Conclusion

The banks would argue that, in choosing weak systems, they are just catering to customer demand. However there has been a noticeable lack of discussion around the central issues. Also, the banks' decision, made to benefit themselves, makes customer money more vulnerable than it needs to be. As well, the redrafting of the electronic banking contract at the time they knowingly adopted weak systems points to the banks being well aware of what they were doing.

This situation, like others, highlights the extent to which organisations providing services over the internet may themselves deserve some blame for cyber crime. If a bank left its money sitting in bags at the front door, we would have no problem seeing them as negligent. If they further wrote their contract to make customers liable for any removal of those bags, we would have no difficulty seeing that as extraordinarily arrogant. That is the situation pertaining to internet banking in Australia.

Recommendations

My recommendations relating to this issue are:

1. There should be public discussion of security standards for consumer financial systems, and the fairness of accompanying contracts. In particular, the decision of Australian banks to dispense with traditional levels of security for marketing reasons should be examined.

2. Some customers may indeed prefer easy access to their accounts from internet cafes and the like. However customers who prefer appropriate protection for their money should be given a choice of using digital certificates or similar more rigorous protections.

3. Cyber crime legislation in general should consider whether public providers of personal data or access to financial accounts exercise suitable levels of care in protecting that information and access.

References:

1. Bina Brown: St George Hit By Net Scam, The Australian, 10 May 2003 http://australianit.news.com.au/articles/0,7204,6408318%5E15306%5E%5Enbv%5E,00.html

2. Sydney has recently seen a scam where Malaysian nationals were duplicating customer ATM cards in order to steal from customer accounts. Although they were successful until caught, they needed sophisticated equipment and elaborate access procedures in order to capture the customer information necessary to duplicate ATM cards, allowing them to be caught once the scam was detected.