HOW TO MAKE ONLINE BANKING SECURE

By
Ahmad Nasir Mohd Zin *ABCP* and Zahri Yunos *ABCP*
National ICT Security and Emergency Response Centre (NISER)

(This article was published in The Star InTech on 21 April 2005)

Internet banking services have been operational in Malaysia since 2001. Presently, only banking institutions licensed under the Banking and Financial Institution Act 1989 (BAFIA) and Islamic Banking Act 1983 are allowed to offer Internet Banking services here. There are 12 commercial banks (inclusive of Islamic banks) out of a total of 25 in Malaysia currently offering Internet Banking services.

According to the 11th Malaysia Internet Survey conducted by AC Nielson, Internet Banking is the one of the most popular services utilised by Malaysian surfers. The survey found out that 51 percent out of the total respondent base of 8000 used the Internet for online banking once a month.

Security Incidents

However, 2003 and 2004 saw the emergence of fraudulent activities pertaining to Internet Banking or better known in the industry as “phishing”. A total of 92 phishing cases were reported to the Malaysian Computer Emergency Response Team (MyCERT, www.mycert.org.my) in 2004. The modus operandi of this activity is to use spoofing techniques to gain names and passwords of account holders.

The victims reported being deceived into going to a fake website where perpetrators stole their usernames and passwords and later use the information for the perpetrators’ own advantage. Phishing is an attempt to commit fraud via social engineering. The impact is the breach of information security through the compromise of confidential data.

The Association of Banks Malaysia (ABM) has urged both commercial banks and their customers to be extra vigilant following reports of fraudulent email purportedly sent by banks with Internet banking services to online customers.

The fraudulent activities mentioned above are not limited to the Malaysian banking industry. It is a worldwide problem particularly in the United States. There, 2560 new unique phishing sites were reported to the Anti Phishing Working Group (APWG) in this year. (see **http://antiphishing.org/APWG_Phishing_Activity_Report_Feb05.pdf**).

It was an increase of 47 percent over the December 2004 figure. APWG is an industry association focused on eliminating identity theft and fraud that result from the growing problem of phishing and email spoofing. This voluntary based organisation provides a forum to discuss phishing issues, trials and

evaluations of potential technology solutions, and access to a centralised repository of reports on phishing attacks.

In China, it was reported that the National Computer Network Emergency Response Technical Team / Coordination Centre of China (CNCERT/CC) received 223 Phishing reports from over 33 worldwide financial and security organization.

Attack Techniques

Nowadays, the nature of attacks is more active rather than passive.Previously, the threats were all passive such as password guessing, dumpster diving and shoulder surfing. Here are some of the techniques used by the attackers today:

- **Trojan Attack.** The attacker installed a Trojan, such as key logger program, on a user's computer. This happens when users visited certain websites and downloaded programs. As they are doing this, key logger program is also installed on their computer without their knowledge.

  When users log into their bank's website, the information keyed in during that session will be captured and sent to the attacker.

  Here, the attacker uses the Trojan as an agent to piggyback information from the user's computer to his backyard and make any fraudulent transactions whenever he wants.

- **Man-in-the-Middle Attack.** Here, the attacker creates a fake website and catches the attention of users to that website. Normally, the attacker was able to trick the users by disguising their identity to make it appear that the message was coming from a trusted source. Once successful, instead of going to the designated website, users do not realize that they actually go to the fraudster's website. The information keyed in during that session will be captured and the fraudsters can make their own transactions at the same time.

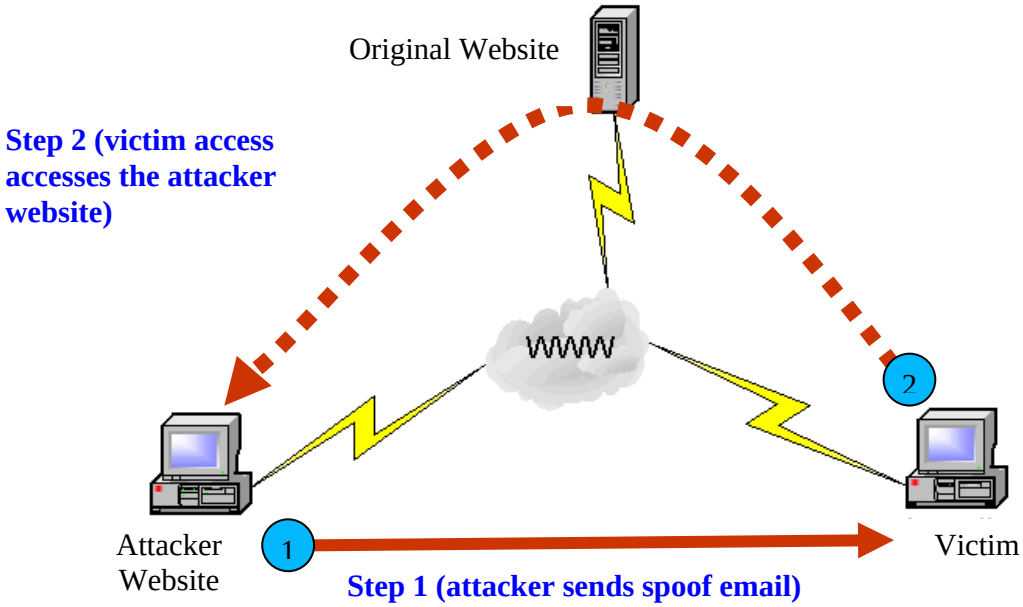

Diagram on how information is being compromised

Striking a Balance

Presently, Internet banking customers only need a computer with access to the Internet to use Internet banking services. Customers can access their banking accounts from anywhere in the world. Each customers is provided a login ID and a password to access the service. It is indeed easy and convenient for customers.

However, the use of password does not provide adequate protection against Internet fraud such as phishing. The problem with password is that when it has been compromised, the fraudsters can easily take full control of online transactions. In such cases, the password is no longer works as an authentication token because we cannot be sure who is behind the keyboard typing that password in.

However, easy access and convenience should not be at the expense and mercy of the security of information. This is important in order to ensure the confidentiality of information and that it is not being manipulated or compromised by the fraudsters.

There are several methods of ensuring a more secure Internet banking:

(1) Minimum Requirement: Two Factor Authentication

Based on the above method, the security measures in place are not adequate to prevent fraud. The current method of using only one factor of authentication

definitely has its weaknesses. The security aspects of Internet banking need to be strengthened. At minimum, a **two-factor authentication** should be implemented in order to verify the authenticity of the information pertaining to Internet banking services.

The first authentication factor can be the use of passwords and the second authentication factor can be the use of tokens such as a smartcard. MyKAD is a good avenue to introduce the second factor.

The above security measures will greatly minimise incidents of Internet banking fraud. The smartcard here provides a second layer of authentication. This will stop a perpetrator even if he manages to obtain the user's password.

Intercepted passwords cannot be used if fraudsters do not have the Smartcard. Besides addressing fraudulent activities, this can instil customers' confidence in Internet banking.

Additional Requirement: Three Factor Authentication

However, for a better security, a three factor authentication process should be considered. The third authentication factor is the use of biometric such as iris or thumbprint recognition. This ascertains who one is, biologically. This method of authentication has been introduced by the Employee Provident Fund (EPF) for it members, but is limited to getting the latest statements of a member.

With a three-factor authentication a more secure method can be implemented - a password to ascertain what one knows, a token (smartcard) to ascertain what one has, and biometric recognition (for example fingerprint or thumbprint) to ascertain who one biologically is.

As such, if passwords have been compromised, fraudsters need to get through another two levels of authentication to access a customers account. Thjs would be difficult, if not totally impossible.

Conclusion

The providers of Internet banking services must be more responsive security requirements. While there is no doubt that Internet banking transaction should have layered protection against security threats, the providers should approach security considerations as part of their service offerings.

Currently, there are no formal processes being put in place to determine the level of security provided by these service providers and to what minimum standards they should be.

Local financial institutions should consider the above-mentioned recommendations to ensure confidentiality of customer information. However, there is a cost implication to the above recommendation. Part of the costs is

already taken care of by MyKAD - a multipurpose digital application card for all citizens over the age of 12.

The additional costs are the hardware and software for the card reader and biometric recognition.

However, this is indeed a serious matter that needs to be looked into by the relevant authorities in this country. In the long run, the cost involved to implement better security will be worth it and beneficial to the banking industry.