E-BANKING RISKS AND SECURITY ISSUES

COSTINELA-LUMINITA DEFTA
UNIVERSITY OF PITESTI, STR. LIVIU REBREANU, NR. 46-58, BUCURESTI,
lumi.defta@yahoo.com

Abstract:
E-banking is a cost-effective way for the bank customers to communicate with their bank. Using e-banking, we can make online banking transactions, money transfer, electronic payments, banking consultancy and check balances 24 hours a day, 7 days a week. Despite these advantages, a considerable number of people still prefer the traditional form of banking, largely due to the concerns related to their transaction security. People worry also that their bank accounts can be hacked and accessed without their knowledge. In this paper we will present the main security risks and issues for customers but also for the banking institutions.

Key words: *e-banking, internet banking, security, risks, transactions.*

JEL classification: *L21, L86, M15*

Introduction

The new trend of worldwide banks is to provide improved customer services based on e-banking systems. E-banking is a service that allows customers to access their bank information, conduct financial transactions, make deposits, withdrawals and pay bills through the Internet without having to physically visit their bank. It provides the convenience of accessing banking facilities from the comfort of their home or office. But as these systems require internet connection, it is normally to appear many security issues. The banking institutions try to apply more stringent security measures to ensure data and accounts protection of users.

In addition to the advantages of the Internet, applications like e-banking are also associated with various security risks – including data being observed, altered or deleted during transmission, or fraudulently obtained by unauthorized persons.

E-banking risks

Online banking continues to present challenges to your financial security and personal privacy. Millions of people have had their checking accounts compromised, mainly as a result of e-banking. If criminals manage to access your online bank account, they can not only access your private information but also transfer money out of your account. If you are going to use online banking to conduct financial transactions, you should make yourself aware of the risks and take precautions to minimize them.
Although banks take various measures to protect you against this threat, one of the biggest risks is actually the computer used to bank with.

A financial institution's board and management should understand the risks associated with e-banking services and evaluate the resulting risk management costs against the potential return on investment prior to offering e-banking services. Poor e-banking planning and investment decisions can increase a financial institution's strategic risk.

For an informational website the list of potential risks include the access to confidential financial institution or customer information if the website is not properly

isolated from the financial institution's internal network, the liability for spreading viruses or other malicious code to computers communicating with the institution's web site and the negative public perception if the institution's online services are disrupted or if its website is defaced or otherwise presents inappropriate or offensive material.

Transaction risk arises from fraud, processing errors, system disruptions, or other unanticipated events resulting in the institution's inability to deliver products or services. This risk exists in each product and service offered. The level of transaction risk is affected by the structure of the institution's processing environment, including the types of services offered and the complexity of the processes and supported technology.

Another type of risk that should be mentioned is the operational risk. This is the risk of occurring damage, either from insufficient, inadequate internal processes and systems, or from human factor, or other external reasons. The operational risk is the risk of damage that is owed, in insufficient or unsuccessful processes, individuals (human faults, failures of administration), or systems (risk of damage or insufficiency of computer systems) or in exterior incidents (natural destruction, fires, etc.). It exists in all the products, the activities, the processes and the bank systems and all the departments and the services of the bank involved. This risk can always arise and cause from negligible damage to essential damage and could lead to bankruptcy. It is also related to the safety of transactions, which depend on the handling and the structure of electronic systems of providing the financial services, the integrity and the right management of records.

Choice of appropriate technology is a potential risk banks face because the technology which is outdated, not scalable or not proven could land the bank in investment loss, a vulnerable system and inefficient service with attendant operational and security risks and also risk of loss of business.

Another risk is related to the bank reputation. The system or product which is not working to the expectations of the customers, system deficiencies or security breach can be the main reasons for this risk. Possible measures to avoid this risk are to test the system before implementation, backup facilities, virus checking, etc.

E-banking security issues

Several types of electronic fraud specifically target online banking. Some of the more popular types are: phishing attacks, malware, pharming attacks, saved usernames and passwords.

Phishing occurs when you receive an email, text message or instant message that appears to be from your bank. If you click on the link provided and input your username and password, you may be giving your information to another person. Hackers will create banking websites that look exactly like your current bank but is not. Your bank will not try to communicate with you in these matters nor will they ever ask you to provide your username and password.

Malicious software (or malware) can be automatically and silently downloaded onto the computer when browsing the Internet. Malware silently captures login information and transfers it to criminals while users log-in to their bank's website. It is also capable of silently changing the transactions executed as directed by criminals.
This type of malicious software is designed to thwart online security technology implemented by many financial institutions that allow their customers to monitor and make changes to their accounts via the Internet.

A trojan, or trojan horse, is a type of malware that is disguised as legitimate program in order to entice users to download and install it. In contrast to viruses and worms, trojans are not directly self-replicating. A new type of financial malware has the

ability to hijack customers online banking sessions in real time using their session ID tokens. For example, the oddjob trojan keeps sessions open after customers think they have logged off, enabling criminals to extract money and commit fraud unnoticed. This is a completely new piece of malware that pushes the hacking envelope through the evolution of existing attack methodologies. It shows how hacker ingenuity can side-step many commercial IT security applications traditionally used to defend users' digital and online monetary assets.

Like phishing attacks, pharming involves the creation of look-alike Web sites that fool people into giving away their personal information. But where phishing attacks encourage victims to click on links in spam messages to lure them to the look-alike site, pharming attacks direct the victim to the look-alike site even if they type the address of the real site into their browser. If the scam site is made to resemble the legitimate website of the targeted institution, a victim could enter account numbers, passwords and other sensitive information before he or she realized what was happening.

In order to make pharming work, scammers may compromise a victim's system directly by secretly installing malicious software on his or her computer or modifying the browser's hosts file. Alternatively, the scammers may use "DNS cache poisoning" to effectively compromise the DNS server.

E-banking security protection

Anti-virus, firewalls and other security software are important but unfortunately not enough. Various studies and recent incidents show that these tools are not always effective in preventing criminals from taking money from your account. As criminals become more sophisticated, your bank strongly recommends additional layers of protection on your computer to enable safe online banking.

There has been an increase in reported cases of phishing scams over the years and the techniques used are becoming also becoming more sophisticated, therefore it is important that we to know how to recognize and prevent from phishing activities.

Some advices to help us protecting against phishing are:

- keep your password and PIN code safe, and change them regularly. If you conduct transactions in a number of websites, use different passwords for each. Create unique passwords that are difficult to guess, e.g. use combination of letters and numbers.
- verify that the internet bank site uses a SLL connection
- be sure that the email attachments before you open are from trusted sources. Do not respond to emails asking for personal information, login information or change password notification via email.
- never click on the link in email messages. Manually key-in URL address into the browser’s address bar.
- memorize your password and if possible, do not write it down anywhere. Report identity theft or any suspicious activity immediately to the bank.
- check your account balances regularly to ensure that no fraudulent withdrawal has taken place.
- when visiting your e-banking site, check that the date and time matches the date and time when you last signed in.

To help protect yourself from pharming, you should make sure that the secure website you are visiting has a valid certificate of authority from a trusted service such as VeriSign. Before entering sensitive personal data on the website, click the ‘lock’ icon in the browser's status bar to view the certificate. Ensure that the name on the certificate corresponds to the site you are viewing. You should also run anti-virus and anti-spyware software, keep your operating system and browser updated with the latest security

patches and use a reliable firewall. Also I good idea is to use the replication system for the data storage. The replication process increases the security of the system and also improves the speed of data operations.

As with all aspects of online security, simple vigilance is a crucial defensive weapon. For example, if your e-banking site suddenly seems subtly different in layout and styling and /or some of the links don't work as expected, it is possible that you have been secretly redirected to a scam site.

Conclusions

E-banking is an enormously popular and safe way to access your bank account, but it pays to be aware of the ways in which criminals can try to gain access to your account and to learn how to protect yourself and your money. There are many potential problems associated with the e-banking industry due to imperfection of the security methods.

In order for electronic banking to continue to grow, the security and the privacy aspects need to be improved.

While the threats presented in this paper are real and pose a serious risk to users of e-banking, it cannot be denied that online banking has benefits that outweigh the issues. As long as users are aware of potential problems that may compromise their accounts, and take security seriously, these threats can be avoided and users can enjoy the convenience of e-banking without falling victim to fraud.

With the security and privacy issues resolved, the future of electronic banking can be very prosperous.

REFERENCES

1. Cezar B., Dardac N. – "Riscuri bancare. Cerinte prudentiale. Monitorizare" - EDP, 1999;
2. Iacob N., "Data replication in distributed environments" - Journal "Constantin Brancusi" University of Targu Jiu Annals - Economics Series, 2010;
3. Makowski M., "Security in Electronic Banking" – Bundesverband deutscher Banken – 2007
4. Ramakrishnan G., "Risk management for Internet Banking" – ISACA – 2001
5. Yang Y., "The security of electronic banking" – National Computer Security Center – 1997
6. Zota R., "Elemente de securitate pentru Internet Banking" – Revista Informatica Economica, 2000;
7. http://www.banksafeonline.org.uk/
8. http://www.esecurity.org.my/adult-banking.htm
9. http://www.hoax-slayer.com/pharming.html