Computer Security: Types Of Security Risks In Online Banking

1.0 Introduction

Online Banking has become popular among people in the world. It is because it can easily and useful for Internet users to manage their bank accounts from anywhere. Banks have been encouraged for this trend for years, since Online Banking also saves lots of resources for the banks regarding of staff training, investment for ATMs and branches, and other operations costs.

However, since the Internet is not originally designed for Online Banking, Online Banking now is facing a wide range of security risks for both the banks and Online Banking users such as brute-force attacks, distributed attacks, and social phishing. The banks have to increase their Online Banking security system constantly, which means the banks have to keep investing on the security systems all the time. Compared with the possibility of the lost from the potential risks, the banks may not want to update their current security systems, because the cost of upgrading security is too expensive and the risks of loss are low. Then this will leave a lot of security responsibilities to the Online Banking users. However, the customers' PCs actually are always the weakest link for Online Banking security. The customers would rather to choose convenient and easy-to-use than complex login procedures for Online Banking. In other words, they would choose a great user experience with foolproof security.

This paper will discuss and analyze the Online Banking security issues. In this paper, Online Banking security is a wide range of topic. This paper will discuss and analyze the important security issues related to the security to online banking.

1.1 Definition of Computer Security Risks

A computer security risk is really anything on your computer that may damage or steal your data or allow someone else to access your computer, without your knowledge or consent. There are a lot of different things that can create a computer risk, including malware, a general term used to describe many types of bad software. We commonly think of computer viruses, but, there are several types of bad software that can create a computer security risk, including viruses, worms, ransomware, spyware, and Trojan horses. Misconfiguration of computer products, as well as unsafe computing habits, also pose risks. (P, 2018)

Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your computer system. Often people confuse computer security with other related terms like information security and cybersecurity. One way to ascertain the similarities and differences among these terms is by asking what is being secured. So, Computer security can be defined as controls that are put in place to provide confidentiality, integrity, and availability for all components of computer systems. (Choudary, 2019)

A computer security risk is anything that can negatively affect confidentiality, integrity or availability of data. Examples of computer risks would be misconfigured software, unpatched operating systems, and unsafe habits that cause vulnerabilities. (Hobb, 2018)

1.2 Types of Security Risks

There are several types of security risks such as malicious code, viruses, worms, and Trojan horses.

1.2.1 Malicious Code

Malicious code can be found in the computer when someone downloads attachment in emails or download files from unknown resources. It also happens when any code is added, changed or removed from a software system. Malicious code is unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. There is three main type of malicious code such as virus, worm and trojan horse. (H. L. Capron, J. A. Johnson, 2004) (CISA, 2018)

1.2.1.1 Virus

The virus is malware that is attached to the system's files that may attack the software, files and computers' boot which can affect someone's computers by changing the computer works without the user's knowledge. Viruses have the ability to damage or destroy files on a computer system and spread by sharing already infected removable media, opening malicious email attachments, and visiting malicious web pages. Viruses also can copy themselves into a new device that is connected to the affected computers. Then, the viruses can spread to other computers using the infected medium. A virus will might be attached to a program and runs together with the program. There are many types of viruses such as Overwrite virus, Macro virus and Boot Sector virus. There are two types of computer viruses which are 'parasitic' and 'boot' viruses. Parasitic virus activated when the host program is executed while boot virus is designed to enter the boot sector of a floopy disc. Examples of viruses that we can found are melissa, tiny, sircam and tequila. (Hooi, 2014) (CISA, 2018)

1.2.1.2 Worm

The worm is a program that can spread by copying itself repeatedly and possibly to transmit through the network. It copies itself to the new machine using the security hole, and starts replicating from there. Worms have the ability to spread themselves on their own. They know how to attach to portable devices such as USB drives or removable hard drives, or to move through the network. Its functionality is to use all of your computer's resources, which can cause your computer to stop responding. Michelangelo and MS Blast worms are the most popular examples. Other than that, nimda, blaster, mimail and sobig also examples of worm. (Hooi, 2014)

1.2.1.3 Trojan Horse

Trojan horse is a program that conceals or looks like a lawful program until triggered. It is a type of software that spreads by downloading applications from the Internet. When the application

has already been installed, part of the malware that was installed together will infect the computer. When you run Trojan horses, it will damage your programs which means it will erase your hard disk. Some of the trojan horses disguise themselves as gaming software to attract users to download and install them. Examples of the trojan horses are back orifice, beast trojan and net bus, Trojan-Banker, Trojan-Downloader and Trojan-Dropper. (H. L. Capron, J. A. Johnson, 2004)

1.2.2 Unauthorized Access and Use

Unauthorized access is the illegal use of a computer or network while unauthorized use refers to the use of data for unapproved activities or illegal purposes. Both of these unauthorized access and use mostly come together. A user can lawfully access a computer to get what they want but if they search for illegal web pages or applications such as Facebook during they working hours, this is called as unauthorized use. Examples of this types are hackers and crackers. Hacker means that someone who tries to access into a network without permission while cracker has the intend of harming and stealing data and information. (Hooi, 2014)

1.2.3 Hardware Theft

Hardware theft is an act of stealing computer materials. Hardware theft may happen in the office, cars or in public areas. This allows devices like smartphones, notebooks and others which are often targets. Hardware loss may occur when the collections are misplaced during delivery. Even though it can be covered by insurance but it still causes a major problem for unbacked-up data. An example of hardware vandalism is when people does not have civic awareness that will make the computer equipment destroyed by cutting cables, deleting software and smashing computers. (Choudary, 2019)

1.2.4 Software Theft

Software theft is also known as software piracy. It involves taking and selling pirated software to the public. As an example, downloading movies, music files or other software from the Internet without permission from the publisher are also illegal actions. This is because every software has its own owner in terms of law. So, making copies from the original software is an infringement of the rights of others. Software theft includes sending instructions to remove installed software in the computer.

Software theft occurs when someone took software media that contain the software and hardware of the media, intentionally remove or disable programs they have already written from other computers, illegally copies or stole piracy from software manufacturers and illegally registers or activates a program. (Beal, 2019)

1.2.5 Information Theft

Information theft is stealing data from other computers by transferring to a hard drive or sending via e-mail in the network. In an organization, data is a valuable resource. Confidential data cannot be exposed to outsiders. Information theft works when a person who steals data from other computers by transferring to a hard drive or sending via e-mail in the network is committing information theft. Information theft can access by two methods. Firstly, Pharming. Creating fraudulent websites which is identical to the original website and asking the user to key

in their personal details into the websites. Secondly, Phishing. A link was created in an e-mail to request that customers update their personal details, at the same time revealing their password and credit card number. (Choudary, 2019)

1.3 Definition of Security Measure

Security measure is a professional who develops security plans to protect an organization's network is the computer security expert. Security measures can be used to prevent this invader from getting the account information. Security measure is a measure taken as a precaution against theft or espionage or sabotage. (Syafiqa, 2017)

1.4 Types of Security Measure

There are several types of security measures such as data backup, cryptography, anti-virus, anti-spyware, firewall, physical access control and human aspect awareness.

1.4.1 Data Backup

Data backup is an action to make a copy of original data such as files, programs or disk and save it in different media storage such as flash drives, hard disk, DVD or cloud storage. This is one of the ways to make sure that the old file can be restored by copying the backed-up files to the original location in case of system failure. Nowadays, cloud storage is the most popular backed-up data location. It can back up for large files as online storage. After the backup operation has been done, the devices must be placed in a safe place. Owners also can put a password to make sure no one can open it illegally. (Hooi, 2014)

1.4.2 Cryptography

Cryptography is a technology of encoding data and information so it only can be read by authorized individuals. It can be divided into two which are encryption that transforms the readable data into an unreadable character to avoid unauthorized access and decryption which are processes to decode encrypted data. To read the data, it must decrypt into readable form. The unencrypted data is called plaintext while the encrypted data is called ciphertext. To encrypt, the plaintext is converted into ciphertext using an encryption key. It is important to the process of proving one's identity and ensuring that no one can read the message except the intended receiver. (Hooi, 2014)

1.4.3 Anti-Virus

Anti-virus is a program that scans for viruses and solves detected threats to protect computers from malware attacks. It is important to protect computers against viruses and other malware. An antivirus scans for programs that attempt to modify the boot program, the operating system, and other programs. The anti-virus program scans memory, disks, and incoming email messages and attachments for viruses and attempts to delete any viruses it finds. (H. L. Capron, J. A. Johnson, 2004)

1.4.4 Anti-Spyware

Anti-spyware is software designed to detect and prevent spying activities. This software can remove spyware tools from hiding in our computers. One type of anti-spyware is malware. It is installed on the computer to get information about others but they do not know about it. (Hooi, 2014)

1.4.5 Firewall

A firewall is part of a computer system or network which is designed to block unauthorized access while permitting outward communication. This implements a security policy and it might permit limited access from the network parameters. Type of firewall is Norton Personal Firewall, Tiny Personal Firewall, and Black ice Defender. (Rouse, TechTarget, 2017)

1.4.6 Physical Access Control

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization. There are two types of access control which is physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. But the organization use different access control modem. (Rouse, Tech Target, 2018) (Rouse, TechTarget, 2017)

1.4.7 Human Aspect: Awareness

Users have to do maintenance for their personal computers. Various utility programs can help users to perform the necessary maintenance tasks. Users can perform full scanning of the system, clear up unwanted icons on the desktop, etc.

2.0 Scenario of the Problem: Online Banking Security

Refer to the question given

2.1 Security Risk 1: Information Theft

From the scenario, there is information theft based on the sentence “The modus operandi of this activity is to use spoofing techniques to gain names and passwords of account holder” that has been detected. Information theft is a crime in which an imposter obtains key pieces of personally identifiable information. Like other ways that they can do is PIN capturing. After they have already gotten the PIN number, they check for the discarded receipt, and unfortunately, they have both PIN and card numbers. (Rouse, TechTarget, 2017)

2.2 Security Risk 2: Malicious Code

Malicious code is a term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Based on the scenario, the sentence “The impact is the breach of information security through the compromise of confidential data” shows for malicious code. There is an example of a system or boot infection. A virus can infect a system by installing itself as a part of the operating system, so remain in the RAM and booted when the computer is shut down. (Beal, 2019)

2.3 Security Risk 3: Unauthorized Access and Use

The sentence “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 perpetrator’s own advantage”, it shows unauthorized access and use. Unauthorized access and use mean the use of a computer or network without permission by connecting it and logging in as a legitimate user. For another example of scenario, criminals keep trying someone's password for an account. If they can access your account this means all of your information are in criminals' knowledge. (Paul, 2012)

2.4 Security Measure 1: Anti-Spyware

Based on security risks information theft, the best security measure is anti-spyware. Anti-Spyware functions as a cleaner, remove and adware from your computers. This is depending on what types of software that you use because each of them have their own function. Ant-spyware will immunize the computer from spyware that it has already destroyed by blocking the spyware from accessing your computer in the future.

2.5 Security Measure 2: Anti-Virus

Based on security risks malicious code, the best security measure is anti-virus. Anti-virus helps to protect your computer from malware and cybercriminals from illegal use. You can install anti-virus and keep the software updated. Even though someone needs to pay for the anti-virus installed, but it can give advantages for them. This will remain free if you have Windows on your machine, you are granted access but you did pay for a Windows license. May users are not aware of this program, but this actually decent protection.

2.6 Security Measure 3: Firewall

Based on security risks of unauthorized access and use, the best security measure is a firewall. A firewall is software or firmware that enforces a set of rules about what data packets will be allowed to enter or leave a network. There are two types of firewalls which is hardware firewalls and software firewalls. Software firewall helps you to protect the software that you install from unauthorized incoming and outgoing data. This will only protect the software that you only installed. Nowadays, there are many antivirus scanners that include their own version of the software firewall. (Rouse, Tech Target, 2018)

3.0 Conclusion from The Scenario Problem

In conclusion, the popularity of online banking has attracted to internet criminals to attack online banking customers. Based on the scenario, I can conclude that every security risk has its own security measure to prevent internet criminals. In my opinion, the government should invest to educate online banking clients to safeguard their transactions and customer data from criminals. Other than that, every bank in Malaysia should upgrade their security measure. By doing that way, each account can be saved properly. Users will not worry about their account’s safety anymore. They can save their money in the bank and buy something using online banking.