USE OF SOCIAL ENGINEERING IN FINANCIAL INDUSTRY FOR IMPERSONATING

February 27, 2020

MUKESH KUMAR PILANIYA - MT2019068
PEEYUSH PANDEY - MT2019075
SHASHANK SHEKHAR MISHRA - MT2019101

Department of Computer Science and Engineering

ABSTRACT

Social Engineering has been hot topic for a while, In brief terms Social Engineering is a process of tricking the employees and getting access to secured data of the firm. This project discusses the topic Impersonation (a type of Social Engineering) in financial Industry.

INTRODUCTION

Social Engineering is among one of the most used cyber attack form. In Impersonation Social Engineering attack, impersonator plays the role of a person to whom employee trusts or the one who convinces employee using human behavior and manipulates him to get the confidential information or security policies of the company. This attack is less about technical skill but more about the non-technical skills of the impersonator.
Coming to what this project contains ahead, it has what is Impersonation attack, Impersonation attacks in financial industry, How to stop such attacks followed by Conclusion References in the end.

PROJECT REASON

Various secure systems have been developed in recent times but a loop hole always exist, to which hackers/malicious social engineers find to attack the system. Impersonation is one of the social engineering technique which is very handy to perform hacking or malicious activity. Seeing the tools like lanturtle which can be used to gain remote access and to do man in the middle attack by just plugin into the target device. An IT support guy, a security guard or a friend can easily plugin this device into the targeted computer and because it looks like a simple USB-drive it is hard to detect it.

After reading the case studies about impersonation attacks in the financial industry and seeing a number of devices in the class, we decided to read more about this topic and hence elected social engineering in the financial industry using impersonation as our project topic.

0.1. What is Impersonation Attack:

Impersonation is one of the social engineering technique that is used to gain access to a system or a company network to commit fraud.

Impersonation technique differs from other social engineering techniques because in impersonation a person is vulnerable rather than a system or a network. In impersonation attack, impersonators can be someone whom we likely to trust and they are trying to fool us to get access to the server room or office room. This type of social engineering is very common and easiest to exploit. Impersonation uses human behavior to collect information and the security policies of a bank rather than using technical knowledge to attack a system.

Also, for the financial industry, it is very difficult to understand this type of attack because of the complex nature of a banking system. Impersonator can use human behavior as a tool to attack the system by manipulating a person towards the target.

0.2. Impersonation for Financial Industry:

The financial service sector is extremely growing and the financial services include thousand of banking institutions, product-based companies like Microsoft, Google and services based companies like Wipro, Infosys. Financial sectors are very extensively in size as some of the largest global banking companies with thousands of workers and billions of assets. Financial sectors form the backbone of the global sector. For a financial industry like banking, impersonation requires a lot of preparation so it occurs less than that of other forms of social engineering because social engineers prefer more anonymous rather than as Impersonates. However, in impersonation, nobody ever knows the impersonator was ever there because impersonator also looks like a normal person like a repairman, IT support guy, a fake employee or a trusted third-party service provider. Most of the roles fall under the category of IT support guy which leads to integration. It is human nature when someone wants to help, we will accept and may provide information like where the server room or manager office is located because we suppose that this is an IT support guy that require some information.

Sometimes comparator company **A** may send their employee to other comparator company **B** as an employee of company **B**, So it is hard to detect these types of impersonation attacks because company **B** has to trust his employee. For those type of attack, the employee may demand more money from company **A** and can leak all the information of company **B** like what are the technologies they are using or what are the projects they are planning so after that it becomes easy for company **A** to gain more revenue compared to company **B**.

Sometimes security guard works as an impersonator and they are involved in major security breaches that are happening nowadays. The reason is that generally, security guards know all the infrastructure of a company and can access all the departments, hence for an external attacker it's easy to maintain a relationship with a security guard by giving him more money and assets. An employee of a company can be an impersonator, sony hack is an example of this type of hack where an internal employee(developer) founded as an impersonator. Once inside the building, the impersonators will look forward to gaining access to a computer or shoulder surf to uncover passwords, pins or trying to eavesdrop on employee conversations and try to learn more about the organization and its employees.

Impersonation attack is well explained in the Mr. Robot series where an employee name Elliot wants to company server and data name as Evil Crop organization. Besides the impersonation attack can be a single person or an organization help. Most of the cybersecurity reports have shown that trend is increasing in social engineering in the financial sector. A cyber threat can affect a bank's financial infrastructure and reputation. Social engineering attacks on the banking industry generally involve legitimate access using impersonation, device control and credentials theft.

Kevin Mitnik a hacker, got access to digital equipment corporation' OS development servers simply by calling the company and claiming that he is one of their lead developers and he was facing trouble in login. He was immediately provided a new login and password. Now many organizations do have barriers that prevent these kinds of impersonations, but they can often be circumvented easily. Humans are a factor of impersonation, an individual may exhibit emotions depending on their character, habits or surroundings. These emotions and circumstances may be utilized by an attacker to make an attack successful. Company not aware of its employee may be the weakest link in exposing the business to a data breach but the point is that employees can also contribute to cybersecurity incidents in a variety of both intentional and accidental ways. The biggest hack in the financial industry is hijacking servers and the stolen data can be sold on dark websites

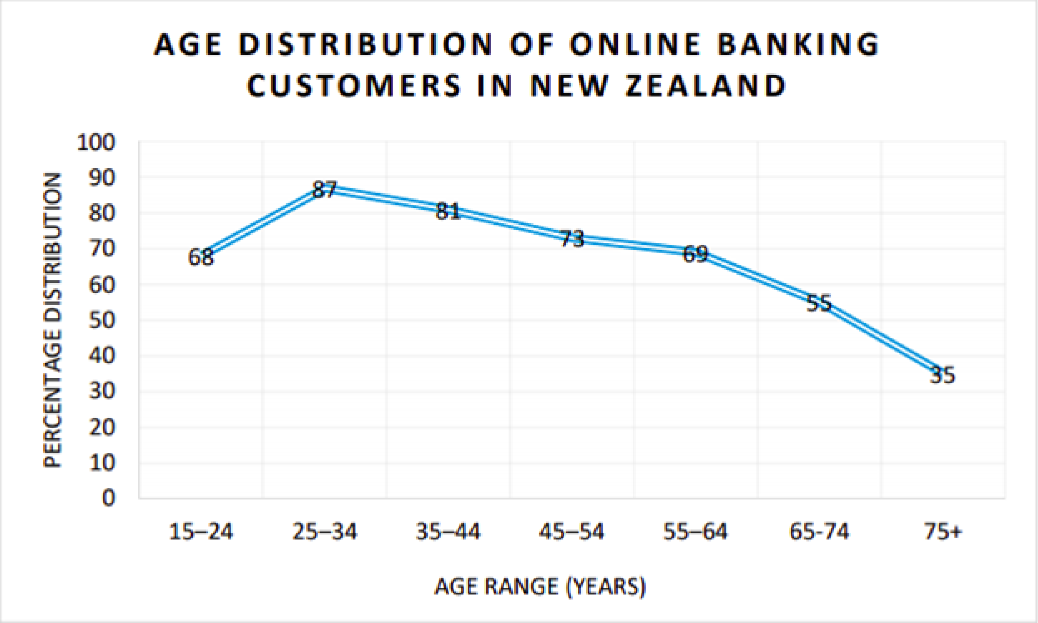

Figure 1

like midnight city etc.

0.3. How Impersonation works:

Impersonation attacks are malware-less attacks and conducted through email/calls using social engineering to gain the trust of a targeted employee. An attacker may know employee personally or can research a victim online by gathering information from social media account which can be used in text or email to prove authenticity. An impersonation attack is typically directed to an employee that has access to sensitive information or credentials. The employee receives an email that appears to be from a legitimate source like a high-level executive within the company.

0.4. How to stop Impersonation Attack:

To prevent impersonation attack the organizations have adopted a multi-layered approach to email security that includes, security awareness training educate their employee about what impersonation attack looks like and how to prevent them and what kind of damage can be arise using impersonation. The impersonator may request out-of-ordinary requests or try to claim the authority, name dropping, card cloning or emergency meeting with the CEO.

Oftentimes, companies invest a lot of time and money into their security technology but fail to invest in their employee's awareness but they should highly invest in employees education as it has significant returns.

Verification is the key to security because a social engineers goal is to fit in the crowd and to look like someone who should be there. Because they may be disguised as any number of people who are frequently present in the organization. Your best defense is being alert and verify the identity card of everyone who enters inside the organization

0.5. Conclusion

Technology evolution offers both opportunities and challenges to financial sectors. Cybercriminals are also becoming creative in exploiting human emotions. To prevent impersonation attacks in the financial sector new ways and tools needs to be developed. A better approach towards impersonation is needed to determine the threats at the operational level, which can help in taking better decisions quickly and effectively to prevent the attack.

REFERENCES

https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC$_{G}eneral i_{T}he-Impact-of-Cybersecurity-Incidents-on-Financial-Institutions-2018.pdf$

$http://ijcsn.org/IJCSN-2014/3-6/A-Review-on-Shoulder-Surfing-Attack-in-Authentication-Technique.pdf$