BEHAVIOURAL ANALYSIS: AN INNOVATIVE TOOL TO CONTROL ONLINE BANKING FRAUD

Paritosh Kumar
Manager Faculty, Staff College, Union Bank of India Bangalore, India
Email: paritosh.kumar@unionbankofindia.com

ABSTRACT

Human beings have established tremendous control on various aspects of their life with the use of hi-tech technology. Due to which, things which were deemed unimaginable some few years back, have become a part of everyday life. In case of banking industry, technology has helped to reduce all physical barriers between banks and their customers. Customer can use banking services, any time and from anywhere in the world.

Keywords: Session Hijacking; Phishing; Vishing; Trojan Horses; Identity Theft; Social Engineering; Money Laundering; Pharming

INTRODUCTION

In today’s competitive banking market, banks and other financial institutions are expanding the services that they offer at an unparalleled rate, including online banking and payment options. It is increasingly available on an ever-expanding list of devices, including smart phones, pad based computers, and other mobile devices. At the same time, criminals are always looking for the easiest possible way to steal money. The expanded services being offered by banks are giving criminals more and more opportunity to ply their trade. This creates an ongoing cat and mouse game that is leaving banks and customers with great losses as they fail to keep up with the fraudsters.

OBJECTIVES

1. To study the various IT fraud in banking institutes
2. To analyse existing fraud preventive measures
3. To understand the concept of behavioural analytics as a fraud preventive technique
4. To study future suggestions to banks to prevent IT frauds

Various IT Frauds in Banks

In today’s market, the number of online fraud attacks are increasing, which involves new level of risk for banks and other financial institutions as various new forms of frauds are taking place which makes not only banks but their customers more and more insecure.

Some of the IT frauds in banks are following:

- Session Hijacking: It is a security attack on a user session over a protected network. It involves employing various techniques to tamper with or take over TCP (Transmission Control Protocol) and web application of user’s sessions. If the session hijacker successfully impersonates the user, he gains access to the sensitive information used in the session.
Phishing: It is a criminal activity using social engineering techniques. They attempt to fraudulently acquire sensitive information, such as username, passwords by masquerading as a trustworthy entity in an electronic communication. Phishing emails include links to websites that appear to direct you to legitimate bank’s website. Any information you submit via the web site is gathered by a fraudster. They send thousands of phishing e mails to reach as many potential victims as possible

Vishing: Vishing (voice-phishing) is the practice of sending fraudulent email to consumers that appears to be an email from a local bank, other financially related website and contains what appears to be a local phone number. The fraudulent email will appear to inform the consumer of some type of problem with their account and instruct them to dial a local phone number. Consumers who are used to calling automated tellers are being tricked into using their phone keyword to type in vital account numbers, pin numbers and other financial information into overseas computers.

Trojan Horses: Fraudsters have successfully found a way to extract banking information from computers by using virus programs known as Trojan horse. It lies dormant on your computer, monitors your activity and then activities if you visit a targeted website, such as an online retailer or a financial institution. The program can then record keystrokes, such as usernames and passwords, and other information stored on your computer and sends them to the creator of the Trojan horse. One of the biggest dangers with a Trojan horse is that it can be present on your computer without you even knowing about it. Trojan horses often infect computers through attachment downloads and visiting unsecured websites.

Identity Theft: Identity theft is the fast growing crime. It occurs when someone steals your personal information for their own personal gain. Some examples of personal information which can be used by an identity thief to impersonate you are:

- Debit Cards
- Credit Cards
- PIN (Personal Identification Number)
- Address
- Birth Certificates

Identify thieves gain your personal information by:

- Stealing wallets and purses containing your identification, debit cards, and credit cards
- Stealing your mail, including your debit and credit card statements, preapproved credit offers, telephone calling cards and tax information
- Completing a change of address form to divert your mail
- Rummaging through your garbage or the garbage of business for personal information
- “Shoulder surfing” at ATMs to obtain PIN numbers
- Looking at personal information from personnel or customer files in the workplace
- Social Engineering: It is commonly understood to mean the art of manipulating people into performing actions or divulging confidential information. While it is similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access, in most cases the attacker never comes face to face with the victims.

Money laundering: It refers to the process of concealing the source of illegally obtained money. The banking channel is used for converting black money to white.
Pharming: A man in the middle attack is one in which the attacker makes independent connections with the victims and messages are passes between victims through attacker only. Meanwhile, it appears to the original parties that they are communicating with each other directly. It is called “Pharming” in which the thief actually hijacks the domain name of the website. When you go to your bank’s website, you will actually be on the thief’s website, instead. While there are lots of software programs that are great at detecting schemes like phishing and pharming, occasionally a thief’s design foils even the best software available.

Different Fraud Preventive Methods

Traditionally, banks have used authentication mechanism for identifying the genuine users. There are basically three factors used for authentication of a user:

- Something the user knows (user ID/Password)
- Something the user has (tokens, smart card, cell phone)
- Something the user is (finger print, retinal pattern, voice etc.)

Generally, banks are using first two factors for authentication:

- First Factor: Login Password and transaction Password
- Second Factor: One time password on registered Mobile or smart card etc.

But fraudsters are able to bypass these security controls and perform fraudulent transactions, like online bill payment transactions, online railway reservation payment etc.

Other fraud prevention tools used are:

- Card Verification Codes such as CVV: It is printed on the back side of credit/debit cards and is required for transaction authorization.
- Rules based detection: A set of rules which every transaction must meet are defined. Rules are defined on criteria such as location, demography, order information etc.
- Verified by Master/VISA Secure Code: Transaction Authentication by Master/VISA on basis of registered user ID/Password.

Use of Behavioral Analytics to Achieve Holistic Security

Banks have developed databases of historical service and account data of customers. It provides a basis for analyzing customer value (profitability), channel preferences product affinities, geographic and demographic data all of which are useful for segmenting customers and developing customer management strategy.

This can be used as a tool to fight against frauds.

CONCLUSION AND RECOMMENDATION

- For banks, balancing security with customer ease of use is a constant concern. Anti fraud systems and initiatives should not be deployed at the detriment of consumer convenience.
- Banks while designing new preventive measure tool, should be futuristic rather than mere problem solver.
- In future with advance technology, banks should try to develop such models which would help banks to predict future fraudster’s behavior with past data.
- Banks should be more pro active rather than reactive in nature.
- High professional confidentiality and dignity should be nourished among banks employee and customers.
• A proper and authentic communication is required to educate customers about various online frauds taking place in banks.

• While working on behavioral analytics, banks should not ignore its basic functions.

• People with a deep knowledge of human psychology, human behavior, with technical expertise should be appointed for developing (consumer) behavior analytic tool.

• While implementing behavior analytics, it should not create interruptions in normal consumer transactions.

• Harsh legislative provisions can discourage fraudsters.

REFERENCES
3. Website about different Internet Banking Fraud http://www.internetbankingfraud.com/