Unified Payment Interface (UPI) platform: Conniving tool for Social Engineering Attack

Kalyani Deshpande
Research Scholar
Global Business School, and Research Centre
Dr. D.Y. PatilVidyapeeth, (Deemed to be University)
Mumbai-Bangalore highway, Tathawade
Pune

Leena B. Dam
Professor
Sri Balaji University, Pune
Email: leenadam@gmail.com

Abstract

Unified Payment Interface (UPI) is an innovative online banking product in India which has reached heights of popularity within a short span. Growth in UPI has also resulted in higher frequency of data breach. Social engineering attacks were the greatest security risk India faced in the lockdown period. Users of Unified Payment Interface are easily lured for cyber frauds. These frauds are not due to default in the UPI system or interface but are tactics to deceive customers by the way of phishing, vishing, orsmishing. Social engineering attack techniques are plotted to exploit users with the use of significant UPI features like 'Collect Request', 'Virtual Private Address', or 'QR code'.A study was conducted to generate the phishing score of the users with real-time attack simulating caselets. Responses were analyzed to understand the psychological behavior of users while they interact with fraudulent tactics. Most users blindly follow the instructions received through SMS or phone calls and become victim of cyber fraud. Analysis of the data collected from respondents reveals the dark truth that age or profession has no bearing in the behavior of users responding to social engineering attack techniques.

Keywords: UPI, online frauds, phishing, vishing, smishing, UPI handle fraud, QR code fraud, remote app fraud, KYC fraud.

Introduction

UPI (Unified Payment Interface) is developed for the benefit of the common man with simple functionalities after demonetization in 2016. The main aim of launching UPI was to have a single app to link all bank accounts. Different payment methods provided through UPI are 'Send money', 'Collect Money' and 'Scan QR'. The amount can be transferred through virtual address or by account id & IFSC code of beneficiary whereas in 'Collect money' mode beneficiary ask for money by generating 'COLLECT' request. Generating a QR code for the virtual id with a linked Bank account is the safest method since all the details are hidden. Today UPI has become the most popular payment method. Transactions are increasing exponentially that the year 2020 ended with the count above 2 billion. As the number of transactions and usage of UPI is increasing, on the other hand, more and more fraudulent transactions are reported by customers. Since March 2020, India being in lockdown due to COVID 19 people were confined indoors and performed online transactions to meet their everyday requirement. Cybercriminals have grabbed this opportunity to make fraudulent transactions. These transactions are done by deceiving people for fake reasons and forcibly make them obey the instructions of the fraudster. These criminal activities are done by making use of social engineering techniques which mainly includes phishing, vishing and smishing and by exploiting one of the UPI features.

Social engineering is taking the control of the mindset of people to exploit some emotions for obeying the instructions. Emotions can be fear, greed, curiosity, helpfulness. The attacker behaves like a legitimate or authorized person to get required credentials from the customer by the way of phishing, vishing or smishing. Phishing is a technique in which an attacker masquerades as a reputable entity or person in email or other forms of communication.[1] Vishing is a technique of voice phishing when an attacker calls the person behaving as if an authorized person or legitimate caller and instructs the customers to share his credentials or respond to the mail or link provided.[2] Vishers use an internet telephone service (VoIP) to stay anonymous while calling customers. Smishing is becoming an emerging and growing threat in the world of online security. It is a form of phishing when someone tries to trick a user by giving them private information via a text or SMS message.[3] These fake links can be a payment link. Clicking on these links will direct to the UPI payment app installed on phone. Once, the permissions are granted and credentials entered, the amount gets debited from the UPI app instantly. Sometimes these links open a remote app on the user's phone which gives direct access to the criminals to see the activities performed by the users. Later the same credentials are used by them to execute fraudulent transactions. Fraudsters are making use of RBI guidelines to get KYC compliant. Normally a customer gets a phone call or text message to complete the KYC norms of his wallet when he is asked to download an app. This app is usually a remote access app like TeamViewer or AnyDesk.[4] People received calls from fake bank operators who informed them about innovations regarding the protection of their data and steps that each and should every pass to become more secure. At their request, individuals in conversation gave critical data such as CVV2/CVC2 (3 digits on the back of a bank card) and 4 to 6 digits codes that the operator sent on their smart phones to confirm changes applying during the conversation, also in some cases even card pin-codes and lose money (Sokolov & Korzhenko, 2019). The phishers ask to transfer Re 1 to check the status of the e-wallet. While the customer is entering a password or PIN for his e-wallet, the scammers collect details being entered alongside.[5] Getting access to the user's mobile wallet ID and password, the bank account gets linked to the mobile and the wallet gets debited to other accounts using different transactions. Fraudsters are making use of customer's lack of knowledge to COLLECT REQUEST feature of UPI. Hackers send "request money" links to the customer through the UPI app and customers trust for getting money once accepted.[6] The customer waits for receiving money but gets the message that the amount is deducted from their account once he clicks on the link to authorize the transaction. Criminals make use of social media sites like Facebook or Twitter by using the words NPCI, BHIM or names similar to any bank or government organization for getting attention of the customers. These sites may not be authentic. Many tricksters create fake handles to make the customers reveal account details through a fake UPI app. To donate to the Prime minister fund in COVID 19, many fake virtual addresses were generated with a slight change in spelling of authentic VPA pmcares@sbi.[7] Fraudsters are making use of the panic situation of people facing a pandemic situation in this lockdown period to buy life and health insurance online. These fake insurance policies are designed with an attractive low premium and added benefits to fool people.[8] But customers in a hurry to grab the opportunity ployed by fraudsters and loses the money. In another technique, a fake QR code is shared by the fraudster which looks similar to the authentic ones. The link for the QR code is sometimes provided through the SMS or displayed at dependable places like temples, grocery shops, etc. The message asks the user to scan the code, enter an amount, and enter the UPI PIN to receive free cash rewards in the bank account. These QR codes are fake QR linked to the fraudster's Bank accounts. As soon as the customer scans the QR and enters the UPI pin to authorize the transaction, money gets debited from a bank account.[9]

Social engineers have devised new tricks, based on psychological and social traits many users share. These traits include, the desire to be helpful to others, the desire to avoid unpleasant events for ourselves and others, the desire to appear competent in our profession, the desire to trust others, the tendency to accept what others say as being truthful, the desire to advance our own cause and career, the desire to be attractive to those we admire or desire, the desire to believe that those we deal with are honourable (Dougherty, 2011).

Theoretical Framework

The theoretical framework used to model psychological factors on fraud behavior has three elements, viz., Perceived Incentives/Pressures, Perceived Opportunities, and Rationalization of fraudulent behaviour. All three elements of the fraud triangle are influenced by the fraud perpetrators' psychology (Association of Certified Fraud

Examiners). Considering that committing fraud is a human endeavor that involves deception, purposeful intent, the intensity of desire, risk of apprehension, violation of trust, rationalization, etc. (Ramamoorti & Olsen, 2007). In a further study of (Ramamoorti, 2008), he emphasized an important conceptual framework called as "fraud triangle," loosely based on "means, motives, and opportunity." Fraudsters harp on the human emotions identified as Fear, Greed, Panic, Attraction towards discount, Kindness, and Trust to lure people and victimise them.

Do individuals possess the ability to have self-control over these emotions? Are they digitally literate to not trust the appealing call made by the fraudster? Are the users of UPI certainly carried away by the 'ease of use' of this technology that they believe anyone and everyone? User behavior has often been overlooked in previous studies; it can be an important predictor of reducing cyber fraud. In the forthcoming section, we provide an examination of the level of user awareness when faced with the impending situation of a prospective threat.

Literature Review

The introduction of Unified Interface Payment (UPI) services has opened a new payment channel to the user. Users across all age groups have accepted UPI as its 'Perceived Usefulness' and 'Perceived ease of use' is high. The features of UPI motivates the respondents of service sectors to adopt the tool and UPI Transactions and findings revealed that the respondent has a positive attitude towards the UPI transaction for ushering in a less-cash society in India (Thomas & Chatterjee, 2017).UPI developed m-payment technology by facilitating mobile phone to be used as the main payment device for giving and accepting payments(Neema & Neema, 2016).

UPI opens unique opportunities for businesses to collect payments via unique UPI ID and QR code, where customers are not physically present and payment request can be sent to the customer and customer can pay remotely using mobile phones (Gochhwal, 2017).The design of UPI is made in such a way that APIs (Application Provider Interface) communicate over HTTPS layer checking message security implemented in UPI for trust and non-repudiability. Every message is digitally signed and has a unique message-id for each request response. The studies show that the architecture of UPI is built in a very strong way (Chitrey et al., 2012).It was found that demographic factor except education does not have much impact on the adoption of the UPI. There was no significant difference is perceived by the respondents on the basis of gender age, profession and annual income (K. D. Mishra, 2017).

Hackers have now adopted the alternative method of Social Engineering, exploiting the psychological vulnerability present in people and potential technical vulnerabilities of various technologies (Chitrey et al., 2012). Social engineering is psychological exploitation that scammers use to skillfully manipulate human weaknesses and carry out emotional attacks on innocent people is shown in the study by (Atkins & Huang, 2013). A knowledge framework to check human emotions and behaviour at the time of the fraud is proposed in a study of (R. Mishra et al., 2019). Through the collection of phrases taken from the users from the agent installed on their device gets transferred to a repository for analysis of emotions and behaviour. The conceptual study of (Albladi & Weir, 2020) was used to test user vulnerability to different types of privacy or security hazards associated with the use of social networks. Social engineering bypasses the most sophisticated security tools available by focusing on the weakest link of the security chain that is the human link. Focusing on the human link ensures that no computer security system is immune to social engineering (Mouton et al., 2014).

Several human psychological traits have been used by social engineers to manipulate human as a human is the weakest link in information security. By using these traits, an attacking strategy is laid out to accomplish the attacker's mission whether to gain access or to gather critical information (Zulkurnain et al., 2015). User vulnerability to social engineering can be defined as the set of user attributes that incline that particular user (rather than other individuals) to be a victim of social engineering attacks (Albladi & Weir, 2018).

Need for the study

UPI payment technique is designed with all security measures implemented. Despite that various frauds are getting reported day by day by exploiting one of the features of UPI like fake virtual id, fake QR code, fake payment link or fake collect request. The features of the most popular UPI channel are used to deceive the users. These frauds are not occurring due to the weaknesses present in the system but due to the inbuilt weakness of human behavior. The present research is done to understand social engineering techniques and human behaviour. Understanding customer awareness about such techniques is very important to plan the awareness programs which will result in reducing fraud cases.

Drawing from the aforementioned literature review and theoretical framework, the accompanying objectives and hypotheses were proposed.

Objectives of the study

1.To understand human behaviour traits exposed by attackers in social engineering attacks.

2.To investigate customer awareness about fraudulent tactics in social engineering attacks.

Hypothesis Statements

H1: Phishing risk increases with an increase in age.

H2: There is a positive relationship between work exposure and the level of awareness about phishing techniques.

Research Design

The study was focused on online banking users living in urban area. Primary data collection was done through the survey method. Structured questionnaire was designed to address the objectives of the study. In this randomised empirical study, 540 people who are users of UPI platform were randomly selected. Cluster sampling method was used to collect the data from the samples. Two urban cities in Maharashtra and Karnataka i.e. Pune and Bangalore were chosen for the study to collect sample data.

With reference to the phishing scale developed by NIST (National Institute of Standards and Technology) to check awareness about phishing emails, we designed a phishing scale to check customer awareness about social engineering frauds.[10] Marks were assigned to the correct response chosen by customers and the final score was displayed after taking the phishing test to understand their awareness about these tactics.

In addition to demographics, questions were asked to understand customer's habits towards alertness while using online banking transactions.

The main focus was not to check the use of UPI but to check the human behaviour towards the fraudulent cases which may be posed by attackers to any individual.

Out of the 530 response received, 500 responses were complete in all respect and used for analysis. This gave a response rate of 94%.

Data Analysis and Discussion

Section I of Data Analysis describes the responses received on real time caselets used by fraudsters to connive the gullible users. Section II deals with hypotheses testing to draw conclusion.

The demographic characteristics of the respondents are summarized below:

Table 1: Profile of the respondents

Total responses: 500

Parameters	Categories	Number of Respondents
Age group	18-25 Years	154 (31%)
	25-35 Years	154 (31%)
	35-45 Years	103 (21%)
	45-55 Years	56 (11%)
	Above 55 Years	33 (7%)
Profession		
A.	Working Professionals	250 (50%)
B.	Student	169 (34%)
	Retired	34 (7%)
	Others	47 (9%)

Source: Primary Data

The analysis of the profile indicates that the maximum respondents are below 35 years of age with 31% belonging from the age group 18-25 years and 31% from 25-35 years. The profile also indicates that 50% of the data is collected from working professionals who have more exposure to the external world. The remaining 50% of the data is collected from the people who are having less exposure. This category includes students 34%, retired people7% and other categories 9%that included housewives and people who are not currently working.

Section I

To understand human behaviour traits exposed by attackers in social engineering attacks is the first objective of the study. Real-time scenarios were presented as phishing caselets to the respondents to check their awareness and reaction while selecting one of the options given.

In first caselet users were simulated for KYC verification fake phone call and asked them to select one of the most appropriate action.

Table 2-Response to KYC verification amongst users

Alternatives proposed	Choice of response	Percentage
Follow the instructions to complete the KYC and activate the account	21	4%
Not respond immediately but respond to it later after confirmation from bank	174	35%
Not initiate any action	125	25%
Will delete the link	180	36%

Source: Primary Data

KYC compliance is mandatory in banks for all accounts as per the Prevention of Anti Money LaunderingAct, 2002. Fraudsters are making use of this requirement to fool the people. When people get a call saying their account will be blocked due to incomplete KYC, analysis shows that 4% of people become the direct prey by clicking on the link. Sometimes people confirm with the bank about the KYC drive and if the answer is 'YES', 35% will click on the fraudulent link provided which has no connection with the Bank.

KYC completion and updation in Banks is a continuous process but Banks never call and instruct them to click on the link to complete the KYC formalities to the customers. Either the process needs to be completed at a bank branch or from the link provided on the authentic website of the Bank. The result shows that 39% of people are vulnerable to this type of phishing attack who has the 'FEAR' factor in mind for the disruption in daily banking transaction for blocking of the account

In Caselets2, a very common scenario was presented where the caller informs the user about the winning of the jackpot and asks for a virtual id for receiving the payment. How the user will react to this call is checked with the alternative provided.

Table3- Response for getting awarded in a jackpot as a winner

Alternatives proposed	Choice of response	Percentage
Enter the UPI pin and complete the transaction	9	2%
Set a new UPI pin and confirms the transaction by entering it into the app	11	2%
Register for UPI set a new pin and then inform the UPI address with a pin to the caller.	22	4%
Not take any action	458	92%

Source: Primary Data

Getting a call or mail for the winner for Jackpot is a very common phishing technique. This is a new way where the caller asks for a virtual id to transfer money and sends 'COLLECT REQUEST' on the UPI app. Due to lack of knowledge of UPI features, 8% of people opt for any of the first 3 options above to complete the transaction. It shows that 'GREED' and insufficient knowledge factors of human nature are captured by the attackers to get money.

In caselet 3 an attempt was made to check the human behaviour when they get a call from the insurance company for the attractive insurance scheme specially designed for COVID19.

Table 4- Response in insurance calls

Alternatives proposed	Choice of response	Percentage
You will click on the link and will pay the first premium to get insured from CORONA infection	27	5%
You will find the genuineness of the insurance company on its website and then will click on the link for payment	50	10%
You will check the authenticity of the caller and will make the payment later from other options on the website of the company	125	25%
You will not at all respond to the call and will contact the insurance company if required	298	60%

Source: Primary Data

This is a new technique adopted by fraudsters to capture the 'PANIC' emotion of people in this COVID situation. The analysis shows that 60% of people will not respond to any call and will communicate with the insurance company and 25% agree that they will not make the payment immediately but from authentic options from the company's website. But remaining 15% of people are vulnerable who said, they will click on the link provided for taking insurance with a low premium.

The fourth scenario was to check the user behaviour when they come across any type of heavy discounts and to order for some merchandise.

Table5- Response of customers in the online discount scam.

Alternatives proposed	Choice of response	Percentage
You will click the link to get the discount	20	4%
Not respond immediately but respond to it later after confirmation from the bank	64	13%
Not initiate any action	218	43%
Will delete the link	198	40%

Source: Primary Data

People always get attracted when they hear the word discount. In the first two options, they respond to the fraudulent link and become the prey of the attack. 4 % of people have agreed that they will immediately take the action for not losing the discount opportunity. 13% of people said that they will call the bank for confirmation but Bank does not have any connection with any merchandise company.43% of people will not initiate action but the most correct action of deleting the link will be taken by only 40% of people. But 17% of people carry more risks to get fooled in a hurry of getting more discounts and will lose more money. Human mind get easily tempted to the word DISCOUNT' which is used in this case to usurp money.

The next Caselet was designed to understand user behaviour when they want to make any donations for authentic cause like the prime minister fund for Covid 19.

Table6- Response in donating for good cause

Alternatives proposed	Choice of response	Percentage
You will pay to virtual id starting with pmcares@upi	15	3%
You will pay to virtual id starting with pmcare@sbi	24	5%
You will initiate the transaction from Bhim or other authentic UPI app to donate the amount to prime ministers fund	288	58%
You will double check the authentic virtual id of the prime minister fund and will then make the payment from any UPI app.	173	35%

Source: Primary Data

UPI virtual id is provided in the crisis situation for collecting funds easily. In the COVID situation also Government of India published an official virtual id as pmcares@sbi to get donations in the prime minister fund. This is a very common practice that fraudsters create a virtual id which resembles the authentic id to get money from the people. In this scenario two fraud virtual id's pmcares@upi and pmcare@sbi were given to check the responses of the users. Total 8% people reacted positively donating their amount to the attacker's fund. Human emotion of 'HELPFULLNESS' or 'KINDNESS' is exploited by fraudsters to dupe people. It is clear from this caselet that people are in the hurry in noble cause also like donating to the funds and without any further checking they complete the actions.

A new technique plotted by attackers in this lockdown period was the initiation of refund of the amount and the caller asks for making Re 1 transaction for confirming account details.

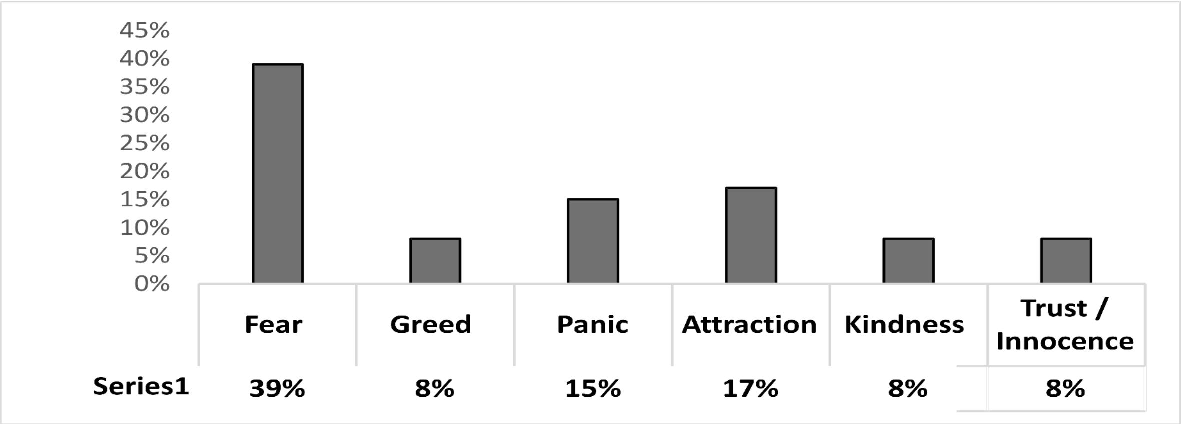
Table7- Response in getting a refund from an unknown source.

Alternatives proposed	Choice of response	Percentage
You will follow the instructions and make a Re 1 transaction as per the instructions of the caller	26	5%
You will provide account details along with OTP generated.	15	3%
You will provide the only account number and IFSC code	168	34%
You will provide only a virtual id for getting a refund	291	58%

Source: Primary Data

In this technique, the caller instructs people to click on the link and further to share the number messaged on their mobile phone after clicking. Normally this number is an OTP to complete 2-factor authentications required for the transaction or sometimes it is 9 digit number which when shared gives remote access to the caller. After getting remote access, the fraudster asks to make a Re 1 transaction where he can find the credentials for later use. Once Re. 1 transaction is complete by the user, the fraudster performs the next transactions from the remote app by using already received credentials. The analysis shows that 8% of people will become the prey of this attack losing their money. Fraudsters exploit 'INNOCENCE' and 'TRUST' factors of the people for listening to any unknown person and to follow the instructions. Data analysis shows that human emotions are captured for executing social engineering attacks. The most vulnerable emotion that is exploited is the 'Fear' followed by the 'Attraction' trait.

Figure1: Various Human Traits exploitation in Social Engineering attack



Source: Primary Data

The statistics show that maximum respondents will be the prey of the attack technique where the FEAR factor is exploited. Attraction towards discounts or free gifts is the next trait commonly exploited by the attacker in developing fraud techniques.

Section II

H1: Phishing risk increases with an increase in age.

To check the second objective of the study, to investigate customer awareness about fraudulent tactics in social engineering attacks, the Hypothesis is checked with appropriate statistical tools.

We calculated spearman's correlation rank to check the awareness level in different age groups.

Table 8 – Age vs phishing risk

Age Group	Spearman's Correlation Rank
18-25 years	5
25-35 years	1
35-45 years	2
45-55 years	3
Above 55 years	4

Source: Primary Data

The result shows that the phishing awareness score in the age group 25to 35 years is highest and decreasing as age moves higher than 35 yrs. The rank shows that awareness is lowest in the age group of 18 to 25 years which is again a human nature of having high curiosity with low maturity level in this age group. Having the highest average score of 68% is also not a good rank when we discuss phishing awareness. To avoid any such financial fraud each one must get 100% marks because having fewer marks means people are unaware of that phishing technique and odds are pronounced to become victim of the attack technique.

Further to check the correlation of Age factor for becoming a prey of phishing attack, the 'F' test technique is used for hypothesis checking.

Table 9: Age and responsiveness to phishing risk

	Score
Mean	65.24
Variance	375.6937876
Observations	500
Df	499
F	257.9405614
P(F<=f) one-tail	0
F Critical one-tail	1.158826595

Source: SPSS Output

As per evidence thrown by the sample in Table 9, we accept H1 as the p-value is less than 0.05. We are 95% confident thatphishing risk is the same for people in all age groups. There is no significant difference in responding to phishing tactics by people in different age groups.The analysis shows that people in all age groups are equally exposed to phishing risks since a small lag in awareness level for fraudulent tactics may result in huge financial loss. Even Spearman's correlation factor shows that awareness levels in different age groups may be different but reacting to any of the phishing techniques is solely dependent on user perception towards attack scenario. An individual can make differentiation among the truthfulness of the scenario and check the authenticity of the initiator. This is only possible when one can have control over their emotions.

H2: There is a positive relationship between work exposure and the level of awareness about phishing techniques.

The additional parameter of work status is checked to understand the possibility of becoming a victim in the attack scenario. To check this hypothesis the respondents were divided into 2 groups having working status in one group and second group consolidated for students, retired persons, and others including housewives and remaining respondents who are not working. An equal number of samples of 250 were present in both groups. F test was used to check the variance between the two groups including students, retired people housewives, and non-working people.

Table 10:Work exposure and awareness about phishing techniques

	The total score of Others category people	*The total score of working professionals*
Mean	62.96	66.92
Observations	250	250
Hypothesized Mean Difference	0	
P(Z<=z) one-tail	0.012394	
z Critical one-tail	1.644854	

Source: SPSS Output

Analysis of the data in Table 10 shows that the work status of the individual has no relationship with the awareness level of an individual about the different phishing tactics. As the p-value is less than 0.05, we are 95% confident that work status does not correlate with becoming a victim of a phishing attack. That means the risk is equal in both categories that are working as well as not working. Users in any category can become prey to a social engineering attack technique.

This hypothesis was designed by considering that the people who are working and have interaction with the outside world must be more aware of attack strategy than the students, retired people or housewives. As per evidence thrown by the sample, we reject H2 and conclude that work status has no relation with getting/not getting exploited by social engineering techniques.

Conclusion

Some form of psychological manipulation is normally involved in Social engineering attacks. Main focus of the attack is to fool users or employees indulging in disclosing confidential or sensitive data. Some forms of human emotions of the victim are exploited to promptly reveal sensitive information. People who exhibit greater trust and are more likely to take risks, and not think about the consequences of their actions, are more likely to fall victim to social engineering (Flores, 2016).

Fraudsters have used UPI as a tool to fool the people. They have made use of the popularity of the UPI channel and its versatile features to plot attack strategy by using the tools like malicious links, fake VPA, fake call or fake SMS to exploit human emotions. The data analysis shows that Fear, Greed, Attraction, Innocence or Kindness can be exploited to reveal sensitive information from the user or sometimes to execute financial transactions. Age or profession does not make more impact on the resilience of the attack. The emotional factor of the individual decides the depth of response to the attack plans. How strong is the emotional factor that will decide the strength of thinking ability? Once the attacker captures user emotions, the next series of actions will be done automatically by the user. It is the initial stage of the attack cycle where a link can be broken between the attacker and user with proper analysis by the user. Control over emotion is the best attack solution in social engineering attack strategies.

It is difficult that every person will come to know about every new tactic used by social engineers. But one can keep control on one emotion while attending any unknown call or sms or making financial transactions to an unknown VPA. It is also important to have up to date knowledge about basic technology and the features of the digital channels before its use. Preventative measures are mostly focused on asking people to be aware and guard against becoming victims through tailored cyber-awareness campaigns(Van De Merwe & Mouton, 2017).To detect Fraud in the e-payment, appropriate security measures can be implemented by monitoring the possible threats during the e-transaction (George & Jacob, 2015).Security awareness training and education is the most important aspect of preventing social engineering attacks and it should be continuous and dynamic(Turner, 2005). Inclusion of future technologies may anticipate possible abuse and work towards baking security by design into the solution development lifecycle (Study, n.d.).

Managerial Implication

Social engineering attacks present a material threat to the security of information systems. Security professionals are only managing the potential effects of a social engineering attack; instead, they should consider such attacks as external threats to the overall information system. Online payment safety is constantly being reinforced by Government laws and regulations backed by next-gen technologies to combat fraud. However, cybercriminals adapt quickly to changing dynamics and come up with new ways to perpetrate fraud. It is the combined responsibility to wake up and fight together against such organized efforts and safeguard the payment ecosystem.

Banks should be more aggressive in implementing preventive controls in the digital banking apps like displaying proper messages in every transaction as alerts, etc. Before registering any customer to the UPI app, a video clip should be mandatorily run to understand functionalities and security features to the users. Banks can share video clips showing new fraudulent tactics and continuously run the same in the branches. UPI blocking facility should be available to customers to freeze the linked account to UPI in case of unauthorized transactions initiated by the fraudster. This is common practice that people under the influence of an attacker through social engineering techniques shares with the information, but their inner voice triggers that 'Something is wrong' when the actuals transaction begins. In this situation, the user should be able to stop further penetration into the account. Banks should take initiative to spread awareness of social engineering attack techniques and preventive measures among their customers by taking special campaigns.

Regulatory authorities like NPCI / RBI should implement more detective controls to identify any security lapses left behind in the app by providers. The need is intense to apply additional detective control in blocking all accounts of the beneficiary in every bank in case of a fraudulent transaction with the help of KYC details. Many times, the amount is transferred to multiple accounts from the beneficiary's account and is withdrawn from the ATMs in multiple locations.

Insurance Companies-As corrective control measure insurance companies can come forward. To transfer or share the risk of losing money of customers, it is recommended that insurance companies can design a scheme with a nominal premium for the saving accounts of the customers. This scheme may be useful in getting some amount back in case of fraud. The premium may be made applicable based on the average balance in an account for the defined period.

Customers should a keep a control on their emotions while addressing to any unknown entity. They should think twice before responding to such fraudulent phisher nets spread in any form by attackers and should check the genuineness.

References:

Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. Human-Centric Computing and Information Sciences, 8(1), 1–24. https://doi.org/10.1186/s13673-018-0128-7

Albladi, S. M., & Weir, G. R. S. (2020). Predicting individuals' vulnerability to social engineering in social networks. Cybersecurity, 3(1). https://doi.org/10.1186/s42400-020-00047-5

Atkins, B., & Huang, W. (2013). A Study of Social Engineering in Online Frauds. Open Journal of Social Sciences, 01(03), 23–32. https://doi.org/10.4236/jss.2013.13004

Chitrey, A., Singh, D., & Singh, V. (2012). A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model. International Journal of Information and Network Security (IJINS), 1(2). https://doi.org/10.11591/ijins.v1i2.426

Dougherty, J. J. (2011). Interested in learning more? ? In sti tu Au th re ns f rig. Style (DeKalb, IL), Security 401.

Flores, W. R. (2016). Shaping Information Security Behaviors Related to Social Engineering Attacks. In PhD Thesis. https://www.diva-portal.org/smash/get/diva2:925493/FULLTEXT02.pdf

George, M. T. K., & Jacob, P. (2015). Fraud detection and mitigation in secure e-payment transaction. International Journal of Scientific & Engineering Research, 6(2). http://www.ijser.org

Gochhwal, R. (2017). Unified Payment Interface—An Advancement in Payment Systems. American Journal of Industrial and Business Management, 07(10), 1174–1191. https://doi.org/10.4236/ajibm.2017.710084

Mishra, K. D. (2017). A Review on Unified Payment Interface [UPI]. International Research Journal of Engineering and Technology(IRJET), 4(6), 5620–5623. https://irjet.net/archives/V4/i6/IRJET-V4I6509.pdf

Mishra, R., Likitha, V. S., & Sree, B. B. (2019). ANALYZING HUMAN BEHAVIOR FOR. 6(3), 384–388.

Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014). Social engineering attack framework. 2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference, February 2018. https://doi.org/10.1109/ISSA.2014.6950510

Neema, K., & Neema, A. (2016). UPI (Unified Payment Interface) – A new technique of Digital Payment? : An Explorative study Ist generation IInd generation III rd Generation. 3(10), 1–10.

Ramamoorti, S. (2008). The Psychology and Sociology of Fraud: Integrating the Behavioral Sciences Component Into Fraud and Forensic Accounting Curricula. Issues in Accounting Education, 23(4), 521–533. https://doi.org/10.2308/iace.2008.23.4.521

Sokolov, V. Y., & Korzhenko, O. Y. (2019). Analysis of Recent Attacks Based on Social Engineering Techniques. ArXiv, 27–29. https://doi.org/10.2139/ssrn.3455471

Study, D. J. (n.d.). Fraud & Risk Management in Digital Payments.pdf.

Thomas, R., & Chatterjee, A. (2017). Unified Payment Interface (UPI): A Catalyst Tool Supporting Digitalization-Utility, Prospects & Issues. International Journal of Innovative Research and Advanced Studies (IJIRAS), 4(2), 192–195. www.ijiras.com

Turner, T. (2005). Social Engineering–Can Organizations Win the Battle? East Carolina University, Greenville, NC.

http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Social+Engineering+–+Can+Organizations+Win+the+Battle?#0

Van De Merwe, J., & Mouton, F. (2017). Mapping the Anatomy of Social Engineering Attacks to the Systems Engineering Life Cycle. Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance, HAISA, 24–40.

Zulkurnain, A. U., Kamal, A., Kamarun, B., Husain, A. Bin, & Chizari, H. (2015). Social Engineering Attack Mitigation. International Journal of Mathematics and Computational Science, 1(4), 188–198. http://www.aiscience.org/journal/ijmcs

Endnotes:

1https://searchsecurity.techtarget.com/definition/phishing

2 https://www.csoonline.com/article/3234716/8-types-of-phishing-attacks-and-how-to-identify-them.html

3 https://us.norton.com/internetsecurity-emerging-threats-what-is-smishing.html

4 https://iamcheated.indianmoney.com/blogs/what-is-paytm-kyc-scam

5 https://www.livemint.com/news/india/do-not-fall-victim-to-new-tactics-used-to-steal-money-through-upi-1561879313342.html

6https://economictimes.indiatimes.com/wealth/save/beware-of-these-6-frauds-while-making-payments-via-upi-amid-lockdown/articleshow/75671798.cms?from=mdr

7https://economictimes.indiatimes.com/industry/banking/finance/banking/cert-in-alerts-people-about-fake-upi-ids-seeking-donations-towards-pm-cares-fund/articleshow/74965804.cms?from=mdr

8https://www.moneycontrol.com/news/business/economy/insurance-fraudsters-try-to-make-the-most-of-coronavirus-lockdown-5465711.html

9 https://blog.phonepe.com/stay-safe-from-qr-code-fraud-cdf9d1ed3aab

10 https://www.nist.gov/news-events/news/2020/09/phish-scale-nist-developed-method-helps-it-staff-see-why-users-click