Eurasian Journal of Analytical Chemistry
ISSN: 1306-3057 OPEN ACCESS 2018 13 (SP): 390-400

Social Engineering Attacks in Online Banking- Analysis of Trends and Prevention

S. Iswarya, Dr.S. Preetha

Received 08 November 2018 ▪ Revised: 30 November 2018 ▪ Accepted: 06 December 2018

Abstract: Proliferation of digital mode of payment has replicated in more transaction and information sharing through electronic media. This has given rise to the hackers who resort illicit means to amaze wealth. Social engineering is a recent hazard which is widespread across the globe. In India, the prevalence of social engineering is very extensive with the increasing digitalization of financial transactions. It is imperative that the trends are to be analysed and suitable mitigation techniques to be suggested to prevent this evil.

This paper aims at first identifying which psychological traits on online users are more vulnerable, secondly, the most used medium of attack. Finally, to suggest the best possible control measure's for Social engineering attack.

Keywords: Social Engineering Attacks, Attackers' Medium, Psychological Traits, Online Banking Theft, Linkage of Personal Information, Debit card Hacking, and Credit Card Hacking.

INTRODUCTION

In this era of digitalizing India, Social Engineering attacks have been growing along-side. The psychological persuasion of an individual/group to fulfil the hacker's task through a user-friendly medium (internet, mobile networks etc.) can be termed as social engineering attacks. A large population of India about 450million are internet users, where the personal information can be hacked easily using the social forum. The most exhaustively used social media network are Facebook followed by you-tube and what app. are accessed by a social engineering attack. In general, attackers send fraudulent communication (medium) that request us to fill their personal credibility A statistical survey has measured that there are about thousand unique phishing emails sent to the users daily **(Paul Black, Iqbal Gondal, Robert Layton, 2017).** Priority of targeting is the financial industry, i.e. the hackers impersonate themselves as a banker. The motives behind these social engineering attacks are amazing of money from a person's account, collect the credentials.

The medium trusted by common man are email, SMS, Messaging app (Instagram, WhatsApp etc...), Facebook, Yahoo, Messenger or Skype, Push Notification direct to the Company's app to share information or to get engaged. Incidentally, these are the common medium used by hackers to attack the targets. In this scenario, we will broadly analyze the most common used attackers' medium and the psychological traits to gain individuals financial information. The usage and growth of the internet has added the growth of social engineering attacks.

OBJECTIVES

The objectives of this study are:

1) To understand the social engineering attacks prevalent among the individuals (general public).
2) To analyze the influence of psychological ploys of social engineering attacks on individuals.
3) To infer the most used medium by the hacker.
4) To suggest individuals preventive measures from online social engineering attackers.

REVIEW OF LITERATURE

Review of literature is done for Social engineering attack- psychological traits, Cyber-attacks in online financial transactions, most vulnerable mediums of attacks and the prevention measure taken about these attacks.

S. Iswarya, Research Scholar, School of Management Studies, VISTAS, Chennai.
Dr.S. Preetha, Professor, School of Management Studies, VISTAS, Chennai.

A) Review of Literature on Cyber-attacks in Online Financial Transactions

The digitalization has engaged and improved the usage online financial transaction. When the credentials are online there are Trojan and malware which attack the banking transaction leading to financial loss. A destructive chain based taxonomy for financial striving cyber-attack was proposed and studied, A stagewise operational classification is done to enable security practitioners on Trojans detection and strategies to mitigate malware. (**Dennis Kiwia, Ali Dehghantanha, Kim-Kwang Raymond Choo, Jim Slaughter, 2017).** A survey of seven banking malware families and its coherent, variants and relationships were identified. A static analysis technique has been deployed to automatically identify the malware behavior (**Paul Black, Iqbal Gondal, Robert Layton, 2017).** A descriptive and exploratory research on the major security issues in internet banking and addressed Biometrics as a key solution (**Amtul Fatima 2018).**

B) Review of Literature on Psychological Traits of Social Engineering Attacks

In an organization, the keys of the kingdom are with the employee. The employee is the target of the social engineering attacks. Mitigating the risk is always followed by phases and slow but SE attacks alarms are high. The adequate protection can only be a combination of physical security, logical (technical) security and administrative security. Policies, awareness, and education can only be effective if it is understood by all employees **(Berti, John, 2003).** There are pervasive threats for information in organizational context. The research investigates the factors for a successful social engineering attack are from **Allen Mayers(1990)** Commitment, **Gendall (2005)** for trust and **Lindsey and Weatherly, Miller and Mc. Donald's (1999)** for obedience to authority and reactance/resistance. The result shows that all three types of commitments were found prominent in social engineering attacks at organizations (**Michael Workman 2007).** The psychology of hacking which is in existence from pre – Internet era has not been explored. The larger methodologies and hackers techniques and shared and discussed **Steve Gold (2010).**

On an individual person, the social engineering attack trends are based **on** psychological strategies (curiosity, empathy, fear, greed, and excitement) and also classifies the target groups (college students, corporate executives, Countries, religious group and sects). And the measures to minimize are attackers. **(Sherly Abraham, Indushobha Chengalur-Smith 2010).** The effectiveness of legal framework influence in security concern is measured in e-banking. The review measures implemented by the Romania's government to deal with the concerns on trust and security factor. (**Liliana Mihaela Moga, Khalil Md Nor, Michaela Neculita and Naser Khani (2012)**. Social Engineering is made of Laws, codes, and Norms on the member, behavior aspects. There is a adherence to social marketing used as a tool to succeed in Social engineering (**Ann-Marie Kennedy and Andrew Parsons, 2014).** An experimental validation performance of habit formation and moral formation theories were analyzed which proved to set the path to security culture, the earned shape of the path can be modified based on the environment (**Shari Lawrence Pfleeger, M.Angela Sasse and Adrian Furnham. 2014).** The relations among existing principles of influence **(Cialdini),** psychological triggers **(Gragg)** and principles of scams **(Stajano et al,)** are studied and a list of principles for persuasion of social engineering attack. They found by analyzing largely used phishing emails collected **(Ana Ferreira, Lynne Coventry, and Gabriele Lenzini, 2015)**

The factors that influence the adoption of internet banking in rural areas as compatibility, trial ability and environmental variables like the awareness, security quotient. Security and complexity of online banking were identified as major factors to be vulnerable to these attacks (**Ramavhona, T & Mokwena, S (2016).** The effectiveness of priming and warning is investigated in a sample of shopping customers. The findings of the study conclude, the disclosure rate of personal information like email were 79%, bank account information 43.5 %, and past shopping details were 92%. This indicates the adverse effect of warning were found (**M. Junger, L.Montoya, F-J.Overink (2016)**. The persuasion of social engineering extracted from books behind the breach in information security is discussed. The meta-analysis of persuasion principles is identified as authority, conformity, reciprocity, commitment, liking, scarcity, and commitment. Case to case analysis on the social influence of persuasion is analyzed which exploit the human elements (**Jan-Willem Hendrik Bullee, Lorena Montoya, Wolter Pieters, Marianne Junger, Pieter Hartel, 2017**).

The conceptual framework of social engineering evolution from the 1960s and their link with the present cybersecurity issues are defined**.** Social engineering is defined as the individual's behavior and its solicitation in the era of epistemic asymmetry, technocratic dominance, and teleological replacement. He also describes the various ages of social engineering and its antecedent from politics (**Joseph M Hatfield, 2017).** The online (internet) abuses at the workplace are also focussed. The perceived benefit, Behavior,

intention to comply with the Internet Usage policy and their personal characteristics are the factors influencing these kinds of abuses and social engineering **attacks (Han Li, Xin (Robert) Luo, Jie Zhang, Rahindra Sarthy, 2018).**

Vulnerable Mediums of Social Engineering Attacks

Social engineering mostly refers to psychological human exploitation but it recently requires a medium to reach their target. Today's digitalization and the penetration of internet connecting the people fill the gaps between the hacker and the targets. The security issues associated with web-based financial services in are analyzed and better ways to ensure the adoption of financial services in the internet community is recommended. The interest levels of human elements with electronic-based financial transactions are also examined **Zakaria I. Saleh, Frank Dacaro (2003).** On the historical analysis of attacks, phishing attacks are most vulnerable and there is a motivation laid behind each attack. The spear phishing of targeting the individual or a group of individuals in an organization is so challenging. The different stages of phishing attacks, TCP session hijacks, HTTP session hijack, DNS phishing attacks mechanism and taxonomy of phishing detection approaches are framed and analyzed to prevent ourselves from these attacks (**B.B.Gupta, Aakanksha Tewari, Ankit Kumar Jain, Dharma P Agrawal., (2016)**. There is ignorance techno-social engineering of humans. The periodic usage of online (Internet) ends up with the effect of techno-social engineering of humans resulting in nudging humans to react like machines. There is an existence of emotional contagion and it is found to deploy by Facebook (Social Networking Sites SNS). Emotional contagion leads extend towards social contagion and becomes a powerful nudge through social networking (**Brett Frischmann 2016).**

Social engineering attacks through Social networking Sites especially Facebook is used as a medium. The perception-based level analysis is used to evaluate susceptibility to Social Engineering victimization at the organizational level. The perception-based level are classified as Perceived sincerity (number of friends, Common friends, number of post, common beliefs and real name), Perceive Competence (Qualification, celebrity and wealth), Perceived attraction (good looks and good writing skills), and Perceived worthiness (Authority, sexual compatibility and reciprocity) (**Abdullah Algarni, Yue Xu and Taizan Chan, 2017**). The organizations are more vulnerable to social engineering attacks through their online presence in social media. The employees are matched from their social media presence like Google plus, Facebook, Twitter, Linkedin, Web. A decision tree program is derived to understand the vulnerability of the employee (**Matthew Edwards, Robert Larson, Benjamin Green, Awais Rashid, 2017).**

Smart mobiles are the smarter in this information era. The consumer behavioral intention towards mobile banking adoption is analyzed at three stages. The results exhibit positive adaptability of mobile banking with is a threat to security for an individual (**Mahmud Akhter Shareef, Abdullah Baabdullah, Shantanu Dutta, Vinod Kumar, Yogesh K Dwivedi,2018)**. Phishing attempts where measured for the individual by classifying them based on their dark traits. Dark traits are psychopathy, Machiavellianism, Narcissism. The analysis could not predict the effectiveness of their phishing emails. The individuals who are high in psychopathy are more prone to phishing (**Shelby R. Curtis, Prashanth Rajivan, Daniel N.Jones, Cleotilde Gonzalez, 2018).** The most vulnerable phishing techniques challenging the organization are the email-based attacks. Around two-thirds of the non- IT security workforces state that they never see any email threat other than their spams.

The take-offs of a survey among the workforce reveal that 64 % phishing happens through email threat. This threat is successful to the hackers as the organizations rely on secure email Gateways (SEGs) model to protect their email. Today's technological advancement of cloud-based infrastructure is not very efficient with this model and requires a much more evolved model to be in phase (**Lorita Ba, 2018).**

Review of Literature on SE Prevention Techniques

Social Engineering attack prevention cant is accurately measured as it involved the human psychology. The defensive information policy has been proposed to overcome such attacks. The defensive policy includes awareness and illustrations on Attack methods, Communication Mode, Information Issues, and Reporting. Only a good information policy establishment can prevent us from social engineering attacks (**Samuel T.C.Thompson, 2004).** The risk is mainly associated with information sharing. There are no straight hard rules/codes to control social engineering but awareness, educating, training, reporting every small security issues, and controls over physical and logical access can mitigate to a larger extent (**Gary Hinson, 2008).** In social engineering an approach, the attackers to surpass the technical controls by human element in an organization. He addresses the issue of social engineering in organization perspective and mitigation measures as policymaking, awareness and training programs (**Scott**

D.Applegate, Major 2009). The social engineering attacks via email to the banks/organization pretending as their own customer/ employee and the six essential steps that can be taken to prevent ourselves from such attacks. Awareness on major changes in the email received, Using second factor authentication, forward the mail instead of using replying the same mail, delete your spam, free webmail shouldn't be used and use digital signature- encrypted as it is difficult to be hacked (**Jason Riddle, "6 steps to thwart email social engineering attacks", 2014).**

Authentication methods can be to make social engineering hackers tuff to hack the credentials. Four of them were implemented and eight more were recommended for online banking. Authentication is an essential research area in the field of information security (**Sven** Kiljan**, Harald Vranken, Marko van Eekelen 2016**). We can also go for advanced methods in authentication, like the second level of authentication of credentials like the google use mobile verification systems to authenticate. Although with human error (trust, curiosity etc...) social engineering attackers have obtained the full/partial credentials, the second level authentication attack known as Verification code forwarding Attack (VCFA) begins. The author mainly focusses on designing better verification messages and reduction of social engineering to steal verification codes (**Hossein Siadati, Toan Ng-uyen, Payas Gupta, Markus Jakobsson, Nasir Memon, 2016).** An empirical analysis was carried for intentions of organization employees towards social engineering attacks. The organizational factors and individual factors are taken into account. The results of analysis where the attitude towards resisting the social engineering attack was associated with their intention to resist (**Waldo R. Flores, Mathias Ekstedt, 2016).** Understanding these attack are more important. To make the employees understand and result for a long time a game was proposed to the players on how social engineering attackers function. Through the game, the employees can understand the social engineering attacks in an entertaining way which shall last longer for the receiver (**Kristian Beckers, Sebastian Pape Veronika Fries 2016).**

The examination of self-protective mechanism against social engineering attacks. The psychological principles of social engineering attacks are (i) Authority, (ii) Social Proof, (iii) Liking, similarity, and deception,(iv) Commitment, reciprocation and consistency, and (v) Distraction. This article is more of a subjective approach and lacks experimental evidence. Awareness of security program is advised as the strategies to eradicate these attacks (**Peter Schaab, Kristian Beckers and Sebastian Pape 2017).** Human-as-a-Security-Sensor through Cogni-Sense in organizations is formulated. The results strongly prove the active need for a Cogni-Sense to prevent from cyber hygiene and active cyber threat detection and reporting at organization levels **(Ryan Heartfield, George Loukas 2018).**

From the broader literature review, we understand that the social engineering attacks have been researched pertaining to information security of organizations. Social engineering attacks from an individual perspective in online banking are identified as the gap and an empirical analysis to understand the most vulnerable medium and the psychological ploys used by the hackers towards the individual/ general public.

RESEARCH METHODOLOGY

We analyze the psychological ploys of social engineering tactics across the set of individuals who use online baking service.

The psychological ploys are identified as curiosity, empathy, excitement, fear, and greed **(Sherly Abraham and InduSobha Chengalur-Smith, 2010).** We have adopted a descriptive research design to analyze the pattern of online bankers and their vulnerability towards Social engineering attacks through different medium and psychological ploys.

Data collection were done through convenient sampling from 129 respondents. Primary data were collected using questionnaire among the online banking customers. Reliability test shared a Cronbach Alpha value is 0.900, hence the items are proved to be reliable. SPSS 20 is used for the analysis. The tools used for analysis are Karl Pearson's Correlation, One-way ANOVA, Friedman Test, and Regression.

Review of literature helps in identifying the variables. We have adopted 5-point Likert scale to estimate measure each item. We have evaluated our construct using reliability test and factor analysis. The total number of items are 55, classified under each constructs as Social Engineering Attacks (3 items), Psychological traits (26 items) which are sub-divided in Fear (6 items), Greed (6 items), Curiosity (4items), Empathy (4 items) and Excitement (6 items), Medium of attacks (13 items), sub-divided as email (3 items), social media (4items), laptop (3 items and mobile (3 items). Online banking usage (5 items). The frequency of credit and debit card usage (2 items) and demographic variables (5 items) which includes the Age, Gender, Qualification, Occupation and household income.

The following hypothesis was tested:

Hypothesis 1

Age of the individual has no influence on the psychological ploy-Fear which leads to Social Engineering Attack

Hypothesis 2

Age of the individual has no influence on the psychological ploy-Greed which lead to Social Engineering attacks

Hypothesis 3

Gender has no influence on the psychological ploy-Curiosity which leads to Social Engineering attacks

Hypothesis 4

Income has no influence on the Psychological ploy-Greed which leads to Social Engineering attacks.

Hypothesis 5

The association between online banking and psychological traits of Social Engineering positive.

Hypothesis 6

The relationship between emails (Medium) with Psychological traits of Social Engineering are positive

RESULTS AND DISCUSSIONS

Table 5.1: Demographic Profile of the Respondents

Sample Characteristics	Category	Frequency	Percentage
AGE	18-25 YRS	34	26
	26-35 YRS	65	50
	36-55 YRS	26	20
	ABV 55 YRS	4	3
GENDER	MALE	60	46
	FEMALE	69	53
QUALIFICATION	10/12TH	2	1
	GRADUATE	41	32
	POST GRADUATE	67	52
	ABOVE	19	15
OCCUPATION	PROFESSIONAL	64	50
	SERVICE(PVT/GOVT)	39	30
	HOMEMAKER	20	15
	STUDENT	6	4
INCOME P.A	120K-360K	32	25
	360K-720K	48	37
	720K-108K	32	25
	MORE THAN 108K	17	13

We have around 50% of the respondent between the age group of 26-35 who are the most users of the internet. The male and female proportions are almost equal. 52% of our respondents are postgraduates and professionals, the respondent's monthly incomes are proportionally distributed.

Statistical Analysis

Table 5.2: Influence of Age on Fear towards social Engineering attacks

Descriptive- Age and Fear								
FEAR	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
18 yrs-25yrs	33	7.4848	2.78524	.48485	6.4972	8.4725	6.00	16.00
26yrs-35yrs	66	9.8788	4.03643	.49685	8.8865	10.8711	6.00	21.00
36yrs-55yrs	26	9.4615	3.62470	.71086	7.9975	10.9256	6.00	20.00
above 55 yrs	4	7.5000	1.73205	.86603	4.7439	10.2561	6.00	10.00
Total	129	9.1085	3.73380	.32874	8.4581	9.7590	6.00	21.00

ANOVA- Age and Fear					
FEAR					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	139.746	3	46.582	3.540	.017
Within Groups	1644.734	125	13.158		
Total	1784.481	128			

The result shows that there exists a significant difference between age group and Fear as F= 3.540 and p<0.05. The null hypothesis is rejected and the post-hoc test is performed.

Post Hoc Tests

Multiple Comparisons- Age and Fear						
FEAR Tukey HSD						
(I) Age	(J) Age	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
18 yrs-25yrs	26yrs-35yrs	-2.39394*	.77336	.013	-4.4077	-.3802
	36yrs-55yrs	-1.97669	.95121	.166	-4.4536	.5002
	above 55 yrs	-.01515	1.92047	1.000	-5.0159	4.9856
26yrs-35yrs	18 yrs-25yrs	2.39394*	.77336	.013	.3802	4.4077
	36yrs-55yrs	.41725	.83990	.960	-1.7698	2.6043
	above 55 yrs	2.37879	1.86784	.581	-2.4849	7.2425
36yrs-55yrs	18 yrs-25yrs	1.97669	.95121	.166	-.5002	4.4536
	26yrs-35yrs	-.41725	.83990	.960	-2.6043	1.7698
	above 55 yrs	1.96154	1.94821	.746	-3.1115	7.0346
above 55 yrs	18 yrs-25yrs	.01515	1.92047	1.000	-4.9856	5.0159
	26yrs-35yrs	-2.37879	1.86784	.581	-7.2425	2.4849
	36yrs-55yrs	-1.96154	1.94821	.746	-7.0346	3.1115
*. The mean difference is significant at the 0.05 level.						

A turkey post hoc test revealed that the Fear factor with age was statistically significant, i.e. Age has an influence on fear factor. But the Age group 18-25yrs (9.87±4.04 min, p=0.013), where p <0.05, proves influence on fear factor. Other age groups don't have an influence on fear.

Table 5.3: Influence of Age on Greed factor towards social Engineering attacks

Descriptives- Age and Greed								
GREED	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
AGE					Lower Bound	Upper Bound		
18 yrs-25yrs	33	7.2424	2.7045	.47080	6.2834	8.2014	6	17
26yrs-35yrs	66	8.4697	3.8639	.47562	7.5198	9.4196	6	24
36yrs-55yrs	26	7.8462	2.1296	.41766	6.9860	8.7063	6	12
above 55 yrs	4	6.0000	.0000	.00000	6.0000	6.0000	6	6
Total	129	7.9535	3.2688	.28781	7.3840	8.5230	6	24

ANOVA- Age and Greed					
GREED					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	49.836	3	16.612	1.576	.199
Within Groups	1317.885	125	10.543		
Total	1367.721	128			

The result shows that there is no statistically significant difference between Age groups and Greed as determined by one way ANOVA (F(3,125)=1.576, p=0.199). There is no influence of age groups difference on greed factor of social engineering attack as the p >0.05. Hence, age does not influence the greed fact of social engineering attacks.

Table 5.4: Influence of Gender on Curiosity factor towards social Engineering attacks

Descriptives- Gender and Curiosity								
CURIOSITY								
	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Male	59	5.9322	2.63180	.34263	5.2464	6.6181	4.00	14.00
Female	70	5.2143	2.07045	.24747	4.7206	5.7080	4.00	15.00
Total	129	5.5426	2.36183	.20795	5.1312	5.9541	4.00	15.00

ANOVA- Gender and Curiosity					
CURIOSITY					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	16.501	1	16.501	3.004	.085
Within Groups	697.515	127	5.492		
Total	714.016	128			

The result shows that there is no statistically significant difference between gender and Curiosity as determined by one way ANOVA (F(1,127)=3.004, p=0.085). There is no influence of gender on greed factor of social engineering attack as the p >0.05, Both male and female respondents are equally influenced and have the same amount of curiosity while transacting online.

Table 5.5: Influence of Income on Greed factor towards social Engineering attacks

Descriptives- Income and Greed								
GREED								
	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
120k-360k	32	7.4375	2.48787	.43980	6.5405	8.3345	6.00	17.00
360k-720k	48	7.7708	3.37853	.48765	6.7898	8.7519	6.00	24.00
720k-1080k	32	8.2500	3.58311	.63341	6.9581	9.5419	6.00	24.00
more than 1080k	17	8.8824	3.65517	.88651	7.0030	10.7617	6.00	16.00
Total	129	7.9535	3.26884	.28781	7.3840	8.5230	6.00	24.00

ANOVA- Income and Greed					
GREED					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	27.602	3	9.201	.858	.465
Within Groups	1340.119	125	10.721		
Total	1367.721	128			

The result shows that there is no statistically significant difference between Income and Greed as determined by one way ANOVA (F(3,125)=0.858, p=0.465). There is no influence of Income on greed factor of social engineering attack as the p >0.05. Hence the null hypothesis is accepted. Irrespective of their income level, all the respondents are greedy while they engage in online financial transactions.

Table 5.6: Relationship between the type of usage (online banking) and psychological factors leading to social engineering attacks

Correlations							
		usage	EXCITEMENT	EMPATHY	GREED	FEAR	CURIOSITY
Type of usage	Pearson Correlation	1	.259**	-.131	.243**	.152	.288**
	Sig. (2-tailed)		.003	.140	.006	.086	.001
	N	129	129	129	129	129	129
EXCITMENT	Pearson Correlation	.259**	1	.188*	.739**	.513**	.671**
	Sig. (2-tailed)	.003		.033	.000	.000	.000
	N	129	129	129	129	129	129
EMPATHY	Pearson Correlation	-.131	.188*	1	.235**	-.030	.067
	Sig. (2-tailed)	.140	.033		.007	.734	.453
	N	129	129	129	129	129	129
GREED	Pearson Correlation	.243**	.739**	.235**	1	.694**	.669**
	Sig. (2-tailed)	.006	.000	.007		.000	.000
	N	129	129	129	129	129	129
FEAR	Pearson Correlation	.152	.513**	-.030	.694**	1	.542**
	Sig. (2-tailed)	.086	.000	.734	.000		.000
	N	129	129	129	129	129	129
CURIOSITY	Pearson Correlation	.288**	.671**	.067	.669**	.542**	1
	Sig. (2-tailed)	.001	.000	.453	.000	.000	
	N	129	129	129	129	129	129
**. Correlation is significant at the 0.01 level (2-tailed).							
*. Correlation is significant at the 0.05 level (2-tailed).							

From the table, we infer that there exists a correlation between the Usages of online banking with excitement, greed, curiosity (null hypothesis rejected p<0.05). Alternatively, there exists no correlation between Usage of online banking with Empathy, Fear. There exist a correlation of Excitement and Greed with all the other psychological traits and usage of online banking. There is a strong positive correlation between Greed and Excitement factors with 55% significance, Fear and Greed factor with 48% significance and Curiosity and Greed factor with 45% significance.

Therefore, we can conclude that there exists a relationship between the usage of online banking and psychological factors leading to social engineering attacks.

TO FIND THE MOST VULNERABLE MEDIUM OF USAGE BY THE ATTACKERS

Friedman Test

Ranks		
	Mean Rank	Rank
mobile	2.40	2
laptop	3.06	4
Email	1.57	1
social medium	2.97	3
Test Statistics		
N	129	
Chi-Square	120.614	
df	3	
Asymp. Sig.	.000	
a. Friedman Test		

From the table above, we infer that most vulnerable medium for attackers is Email followed by mobile, social media and laptops.

The Relationship between Emails (Medium) of Online Banking on Psychological Traits

Model Summary									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.445[a]	.198	.192	10.66685	.198	31.408	1	127	.000
a. Predictors: (Constant), EMAIL									

ANOVA						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	3573.635	1	3573.635	31.408	.000[b]
	Residual	14450.288	127	113.782		
	Total	18023.922	128			
a. Dependent Variable: PSYCHOLOGICAL TRAITS						
b. Predictors: (Constant), EMAIL						

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	23.806	2.665		8.933	.000
	EMAIL	2.522	.450	.445	5.604	.000
a. Dependent Variable: PSYCHOLOGICAL TRAITS						

The linear regression is established between the most vulnerable medium email and its influence on the psychological trait. 20% of the email medium is proved to predict the psychological trait leading to social engineering.

Psychological Traits= 23.806 +2.5 (Email)

DISCUSSION

The Age group 18-25 year are more vulnerable to the fear trait of Social Engineering attacks. The Age group above 25 years are not influenced by fear trait. Greed trait is more vulnerable psychological traits which are influenced across all ages. Curiosity is also vulnerable to Social engineering attack across gender. [28], [12]

The usage of online banking services is highly relative to the individual user's psychological ploys with is influenced by the hackers for a successful social engineering attack. [2], [11],[27] and [38]. On deriving the contribution of the medium of usage of the individual and the types of online banking usage towards psychological traits. The medium of usage has the maximum influence. The psychological ploys are addressed on the medium like email, Social media (Facebook, Linkedin), mobile, pc). [25],[3],[24],[7],[22] and[20].

Also, the medium of online banking usage contributes directly to social engineering attacks, the types of usage are not considered. Any type of online usage requires a medium to accomplish. Hence the medium of online usage is of importance while measuring the social engineering attacks. [28],[3],[19],[15],[1] and[25] On ranking, the most vulnerable or the prioritized medium of a social medium attacker are email or the phishing technique or spear phishing technique [25],[3],[24],[28],[33],[19] and [15]. The second most vulnerable mobile [20] and [12].

The social engineering attack awareness is largely implemented in organization for the information security purpose [30], [13], [31], [15], [36], [12], [37], [17], [26] and [29]. An individual's social engineering attack preventions are not spoken up largely till date. The digitalization and smart mobiles have increased and imparted the knowledge to use online banking services, but the awareness of social engineering attacker is not spread. Due to this lag, the individual's largely non-IT individuals share their

credentials and are highly vulnerable. Awareness programs from the respective bankers, through online forum etc, has to be initiated to reduce these hazards.

CONCLUSION

The growth of social engineering attacks causing risk to the human life rate has been increasing day by day. The attack starts with information gathering and developing the relationship and exploitation of the relationship. From the study, we clearly infer that the most vulnerable medium of usage by the attacker is the email (phishing). The psychological traits of social engineering most vulnerable are greed (44%) and excitement (42%) followed by curiosity (35%), fear (11%) and empathy (7%) are more used by the attacker to reach their target individuals to establish their relationship. Awareness spreading, following bank policy and authentication of all unknown mail, is required before responding. Awareness through all medium of the attackers would prevent us from these attacks to a larger extent.

REFERENCES

[1] Abdullah Algarni, Yue Xu and Taizan Chan, "*An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook*", European Journal of Information System, 2017

[2] Amtul Fatima, *"E-Banking security issues-Is there a solution in Biometrics?"*Journal of Internet Banking and Commerce.2018

[3] Ana Ferreira, Lynne Coventry and Gabriele Lenzini, "*Principles of Persuasion in Social Engineering and their use in phishing*", Springer International Publishing Switzerland. PP- 36-47. 2015

[4] Ann-Marie Kennedy and Andrew Parsons, "*Social Engineering and social marketing: Why is one "good" and the other "bad"*? Journal of Social Marketing, Vol 4 No 3. 2014

[5] B.B.Gupta, Aakanksha Tewari, Ankit Kumar Jain, Dharma P Agrawal., "*Fighting against phishing attacks: state of the art an future challenges"*, The Natural Computing Applications Forum, Springer, 2016,

[6] Berti, John, "*Social engineering: The forgotten risk*", Canadian HR Reporter, Jul 14, 2003 Pg 16, 2003

[7] Brett Frischmann, "*Thoughts on Techno-Social Engineering of humans and the Freedom to be off (or free from Such Engineering)"*, Theoretical Inquiries in law, Vol 17, Pg 535-561, 2016

[8] Dennis Kiwia, Ali Dehghantanha, Kim-Kwang Raymond Choo, Jim Slaughter, "*A Cyber Kill chain based taxonomy of banking Trojans for evolutionary computational intelligence*", Journal of Computational Science, 2017

[9] Diksha Goel, Ankit Kumar Jain, "*Mobile phishing attacks and defense mechanisms: State of art and open research challenges*", Computers and Security.2017

[10] Francois Mouton, Louise Leenen, H.S.Venter, *"Social engineering attack examples, templates and scenarios"*, Computers and Security, 2016

[11] Han Li, Xin (Robert)Luo, Jie Zhang, Rahindra Sarthy, "*Self –Control, Organizational context, and rational choice in Internet abuses at work*", Information & Management. Vol 55 PP 358-367.2018

[12] Hossein Siadati, Toan Ng-uyen, Payas Gupta, Markus Jakobsson, Nasir Memon, "*Mind your SMSes: Mitigating Social Engineering in Second Factor Authentication*.", Computers and Security,2016

[13] Gary Hinson, "*Social Engineering Techniques, Risks and Controls*", EDPACS: The EDP Audit, Control and Security Newsletter Vol 37:4-5, Pp 32-46, 2008

[14] Jan-Willem Hendrik Bullee, Lorena Montoya, Wolter Pieters, Marianne Junger, Pieter Hartel, "*On the Anatomy of social engineering attacks- A literature-based dissection of successful attacks*". Wiley, P1-26, 2017

[15] Jason Riddle, *"6 steps to thwart email social engineering attacks*", LBMC Managed Security Services, online article: http://www.bankingexchange.com/news-feed/item/4912-6-steps-to-thwart-email-social-engineering-attacks, 2014

[16] Joseph M Hatfield, "*Social Engineering in cybersecurity- the evolution of a concept",* Computers and Security.Pg 1-24, 2017

[17] Kristian Beckers, Sebastian Pape Veronika Fries, "*HATCH: Hack and Trick Capricious Humans- A serious Game on Social Engineering*"., Proceedings of British HCL 2016 Conference fusion, Bournemouth, UK, P1-3,2016

[18] Liliana Mihaela Moga, Khalil Md Nor, Michaela Neculita and Naser Khani, "*Trust and Security in E-banking adoption in Romania*", Communications of the IBIMA, Vol 2012(2012), Pg 10, 2012

[19] Lorita Ba, "*The biggest Email Security Challenge facing organizations today",* SECURITY, "SecurityMagazine.com, 2018

[20] Mahmud Akhter Shareef, Abdullah Baabdullah, Shantanu Dutta, Vinod Kumar, Yogesh K Dwivedi, "*Consumer adoption of mobile banking services: An empirical examination of factors according to adoption stages",* Journal of Retailing and Consumer Services, vol 43 Pg- 54-67, 2018

[21] Mario Silic, Andrea Back, "*The dark side of social networking sites: Understanding phishing risks"*, Computers in Human Behaviour, Pg 35-43, 2016

[22] Matthew Edwards, Robert Larson, Benjamin Green, Awais Rashid, "*Panning for gold: Automatically analyzing online social engineering surface*", Computers and security Vol 69, PP-18-34, 2017

[23] Michael Workman, "*Gaining Access with Social Engineering: An Empirical Study of the Threat"*, Information System Security, P 315-331,2007

[24] M.Junger, L.Montoya, F-J.Overink, "*Priming and warnings are not effective to prevent social engineering attacks*", Computers in Human Behavior, Vol 66, Pg 75-87, 2016

[25] Paul Black, Iqbal Gondal, Robert Layton*, "A survey of similarities in banking malware behaviors"*, Computers and Security, 2017

[26] Peter Schaab, Kristian Beckers, and Sebastian Pape, "*Social engineering defense mechanisms and counteracting training strategies*", Information & Computer Security Vol 25 No.2, Pp- 206-222, 2017

[27] Ramavhona, T & Mokwena, S., "*Factors influencing Internet banking adoption in South African rural areas*", South African Journal of Information Management. Vol 18(2), 2016

[28] Russell A Jackson, "Social Engineering- Pulling Strings", Internal Auditor Magazine, August 2018 issue. Pg.34- 39,2018

[29] Ryan Heartfield, George Loukas, "*Detecting semantic social engineering attacks with the weakest link: implementation and empirical evaluation of a human-as-a-security-sensor framework",* Computers and Security. 2018

[30] Samuel T.C.Thompson, "*Policies to Protect Information Systems: Building Barriers to Intrusion from Social Engineering Attacks*", Library&Archival Security, Vol. 19(1), PP 3-14, 2004

[31] Scott D.Applegate, Major, "*Social Engineering: Hacking the Wetware!*", Information Security Journal: A Global Perspective, Vol 18, Pp 40-46, 2009

[32] Shari Lawrence Pfleeger, M.Angela Sasse and Adrian Furnham, *"From Weakest Link to Security Hero: Transforming Staff Security Behavior*", Homeland Security & Emergency Management Vol 11(4), PP- 489-510, 2014

[33] Shelby R. Curtis, Prashanth Rajivan, Daniel N.Jones, Cleotilde Gonzalez, "*Phishing attempts among the dark triad: Patterns of attack and vulnerability"*, Computers in Human Behavior, 2018

[34] Sherly Abraham, Indushobha Chengalur-Smith, "*An overview of social engineering malware: Trends, tactics, and implications*", Technology in Society Vol.32, Pg.183-196, 2010

[35] Steve Gold, Freelance Journalist, *"Social Engineering today: psychology, strategies, and tricks"*, 2010

[36] Sven Kiljan, Harald Vranken, Marko van Eekelen*, "Evaluation of transaction authentication methods for online banking*", Future Generation Computer Systems.2016

[37] Waldo R. Flores, Mathias Ekstedt, "*Shaping intention to resist social engineering through transformational leadership, information security culture and awareness*", Computers and Security. 2016

[38] Zakaria I. Saleh, Frank Dacaro, "*An examination of the internet security and its impact on trust and adoption of online banking*", Doctor of Philosophy thesis, Capella University. 2003.