Advances in Consumer Research
https://acr-journal.com/
Volume-3 | Issue-2 | Feb 2026
Original Researcher Article

Consumer Browsing Behaviour and Cyber Threats in Digital Banking

Vinod Kumar Mishra[1], Dr. Shilpi Khandelwal[2]
[1]Research Scholar Faculty of Management Studies Jagannath University, Jaipur
Email ID: vins_mishra@yahoo.com
[2]Professor Faculty of Management Studies Jagannath University, Jaipur
Email ID: shilpi.khandelwal@jagannathuniversity.org

ABSTRACT
Indian banking industry has witnessed a tremendous growth in its digital footprints. Consumers have become accustomed to online banking particularly through mobile apps and Unified Payment Interface (UPI). Digital banking platforms make use of internet for opening accounts, e-KYC, performing online purchases, funds transfer and investments. As the banking services are exposed to internet a robust cyber security framework is required to protect consumer personal information and bank's deposits. While banks are making huge expenditure on technology deployment for cyber security, consumer behaviour also plays a great role in protecting their data and funds in their accounts. The present study analyses consumers' online browsing behaviour and its impact on cyber threats in digital banking sector resulting in cyber-crime. The study also examines impact of browsing behavior on cyber threats. The data for study is collected from 300 individuals who are using online banking apps, IMPS and UPI etc. to collect data structured questionnaire is prepared with multiple choice options, Likert scale etc. Statistical tools used for study include descriptive statistics, one way ANOVA & correlation coefficient. The study indicates that online browsing behaviour of consumer has a significant impact on cyber-crime and cyber threats.
Keywords: Cyber, Digital Banking, Security, Hacking, Ransomware

INTRODUCTION

India is third largest internet consumer after USA & China. Technology is key force behind Indian economic growth. IMF has made a forecast that Indian Economy shall cross USD 5 trillion by 2026-27. Digital development in Indian banking and finance sector has enabled retail payments for day to day purchase requirements of consumers. Whether it is retail payments of groceries, apparels, milk products, fashion or online purchases all are made through digital banking channels like UPI, IMPS, internet banking and cards. Manivel Rajakrishnan and Ramasamy (2023) presented the issues of digital banking in Indian scenario in a conference held at Coimbatore. Internet based banking and financial services have made consumer life easy for funds transfer, purchase and e-commerce activities. The sector is prone to vulnerabilities as well. Unauthorized access of intruders to financial setup for stealing personal & confidential information has increased manifold with the increase in digital footprints. Digital banking framework comprise of bank's IT infrastructure, online applications, service providers, merchants and consumers. An institutional banking setup requires deployment of sophisticated security controls, intrusion detection and prevention systems as per regulatory mandate (Alkadi et. al., 2020). Kandukuri & Yadav (2022) indicated that social engineering tactics are used by attackers for conducting exploits. RBI and banks also run awareness campaigns for educating customers on cyber literacy. Digital banking made banking services reach consumers at their doorstep. Post Covid era consumers digitally literacy has increased. Banks have put in place all security measures to protect consumer confidential data & information. Despite all systems in place consumer come up as weakest & vulnerable link of the Digital banking setup. Consumers are warned over and again not to fell prey to the lucrative offers of the hackers. Social engineering (Patel, 2013 and Duarte N, 2021) tactics are used by the hackers to manage consumer psychology in such a way that they trust them and fell prey to their malafide intentions. Hackers tend to send some message, QR Code or URLs which is intended to get hold of the confidential information of the consumers and gain access to the mobile or laptop of consumers. Ahamed & Mustafa (2019) stressed upon the need for encryption in ATM & QR based transactions. In unsecure systems, once access is obtained a malware may be planted for seeking internet banking credentials to execute financial frauds. Social Engineering techniques are adopted by the fraudsters to make consumers believe that their requests are coming from a trusted source. Actually such URLs and domains are manipulated in such a way that there is a very minute difference and is difficult to identify the genuineness of the source of such mails & links. Cyber fraudsters take advantage of greed, threat and urgency behaviour of the consumer to trap them. Consumer can use ATM Cards, UPI/Mobile/Internet id/password to access accounts through digital awareness (Okereafor, 2021).

Literature Review

The present age bank' businesses are dependent solely on IT. Cyber Security has evolved over a period of time and

accordingly definitions have been provided (Schatz et. al. (2017), Merriam-Webster (2021)). Dekkati et, al. (2022) argued about challenges faced by institutions due to hacking, cyber intrusions, privacy aspects and data losses. Previously business processes were hindered by deploying computer virus, Trojans, worm etc. Later on this trend further developed into cyber-attacks causing massive services restrictions. As a service provider of the banking services it is bank's responsibility to keep customer personal data and financial information safe and secure. Any security breach may result in reputational loss. Security incidents may result in customer unrest and have legal implications as well. Bank periodically sensitize their staff, management, board and customers regarding cyber security issues.

CIA Triad

There is no single creator for this framework. Most common framework for security being followed is known as CIA Security Framework which was used by the war generals. CIA stands for Confidentiality, Integrity and Availability Popescul (2011). He demonstrated CIA with focus on security of knowledge as a human problem and not a technical one. It should be treated as such. Sensitive aspects of knowledge related aspects must be analyzed continuously for improvement and must not be handled in traditional manner as those are not enough. The concept is used in integrated manner since 1998.

Source: https://fortinet.com

In banking sector Confidentiality is to ensure that the customer centric confidential, sensitive and personal information is accessible only to the authorized users, processes and systems. When it comes to managing confidentiality the same is managed by encryption of the data at rest and in transit. By encryption no one except authorized person can access the data. Users are allowed to access the data based on the access controls given to them. Such users also have access to their roles after multifactor authentication. The role based access practices is followed not only by users of the financial information in banks but also the digital banking users while accessing data online or through their mobile applications.

Integrity is to ensure that the data provided for a customer is correct and accurate which cannot be modified without a prior authorization from competent authority. Data integrity also requires warehousing data in such a manner that there is no redundancy which may result in ambiguity. Precision in data & information along with its factual position is another attribute that is required form integrity of data. Trust worthiness and prevention from accidental damage are other key concerns.

Availability of the data requires that the infrastructure which is processing data must be appropriately available at all times whether it is hardware, network, storage or application. Access to data shall be allowed only to the authorised and intended users & customers with proper access of banking services 24 x 7 round the clock. CIA Triad provides a framework for data security. However no one can be absolute about a risk &threat from cyber channel breach. Any vulnerability that may crop in system or a threat incident can pose a risk for the information being stolen and misused.

In practical terms the CIA triad is about the maintaining confidentiality, integrity and accessibility through restricting administrative rights on the systems, access to correct and timely information and availability through all possible channels without any intrusion.

Cyber Crime Statistics & Modus operandi

Along with the digital banking expansion cyber threats have also developed. OTP sharing, ATM card skimming, QR code based frauds have all raised a concern for the government to adop stringent measures Approximately 50% plus crimes pertain to net banking & ATM (Sekhar & Kumar, 2023). With a view to create a safe cyber space Indian Cyber Crime Coordination (I4C) Center has been set up. I4C serves as a common point to identify, regulate and monitor activities of banking, telecom, social media, police department and law enforcement agencies. A dedicated portal national Crime Reporting portal, NCRP (2024) (https://cybercrime.gov.in) has been developed for customers to report their grievances online. A dedicated helpline no. 1930 is also introduced.

NCRP data indicates that cyber-crime has increased 113% during 2021-22 and 60.9% during 2022-23. An online financial fraud of Rs.11269.83 crore is reported during last six months only.

Figure 1: Cybercrime Trends

Source: Indian Cyber Crime Coordination Centre (I4C)

Citizen Financial Cyber Fraud Reporting & Management System (CFCFRMS) statistics indicate that 6000+ online fraudulent complaints are submitted on NCRP on daily basis. Based on these reports approximately 60 crore of rupees are lost daily of which 35% complaints involve an amount of more than Rs.50 lakh.

Financial frauds through local as well international origin are exponentially increasing year on year both. As per the status reported on NCRP portal modus operandi and their approximate contribution is as under:

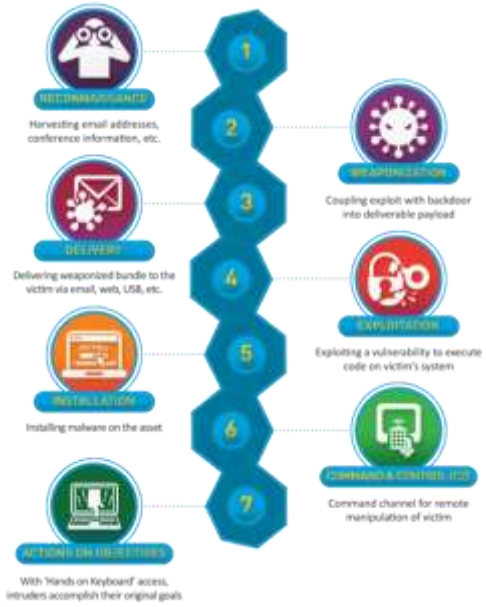
Figure 2: Nature and Extent of Cyber Enabled Financial Frauds - 2023

Source: NCRP Analysis

Cyber Security Threat Landscape

A comparison of economic growth of US & China economy with cyber-crime illustrate that cyber-crime stands at 9.5 trillion dollars against 27.9 trillion dollars of US & 17.7 trillion dollars of China economy. Several cases have been reported in I4C where anonymous and mule accounts have been created for siphoning of funds. Such funds may be used for terrorist funding as well. Unemployed youths are taken into confidence and on pretext of giving jobs they are roped into cyber slavery. They are deported to some other nations and their passports are seized. Yadav & Rao (2015) indicated in his research that there is an increase in the targeted cyber-attacks which have a massive impact on institutional working. A modus operandi that is followed is that of cyber kill chain process. Cyber Kill Chain Process used for targeting bait for financial fraud is indicated as under.

Figure 3: Cyber Kill Chain Process



Source: https://lockheedmartin.com

Any crime that a hacker intends to execute is done with a proper planned approach. This is done by sending some lucrative offer by means of an email, a whastapp message or an image or a video. The user clicks on the above on impression of a trusted source and gets entangled in trap. All required information of customer its mobile, email or any other personal information is harvested using this. Once the hacker gets hold of the system he is able to plant its weapon for generating more crucial information. The malware, Trojan or other harmful components are planted in system. The malware is designed to pop up and run at any pre defined time.

Cyber Security Framework (CSF)

National Institute of Standards and Technology, US (NIST) proposed CSF 2.0 wherein focus is on identification, protection, detection, response & recovery of the system in case of a cyber-security incident. This act as a guiding document to manage risks associated with the cyber security. The focus is on the deployment of baseline controls which may be used for fulfillment of the security objectives. Based on the exposure to risk channel several tiers are proposed for the institutions to identify themselves and deploy controls that are relevant to them. It is not a common solution fitting all approach. It is about assessing where we stand in risk and how many and what controls we deploy to meet our customized risk assessment and requirements. NIST stresses on the requirements of keeping a vigil of the entire IT system right from individual, its rights, IT systems, rights, permission of the IT infrastructure and encryption of transactions.

Figure 4: Creation of Cyber Security Framework Organizational Profile

Source: NIST(2024)

A cyber security framework is proposed by the NABARD vide its circular no. EC No.32/DOS-7/2020 dated 6.2.2020. The important baseline controls that are proposed for a financial institution are highlighted with focus on prevention of attacks (NABARD, 2024).

Figure 5: Baseline Cyber Security and Resilience Requirements

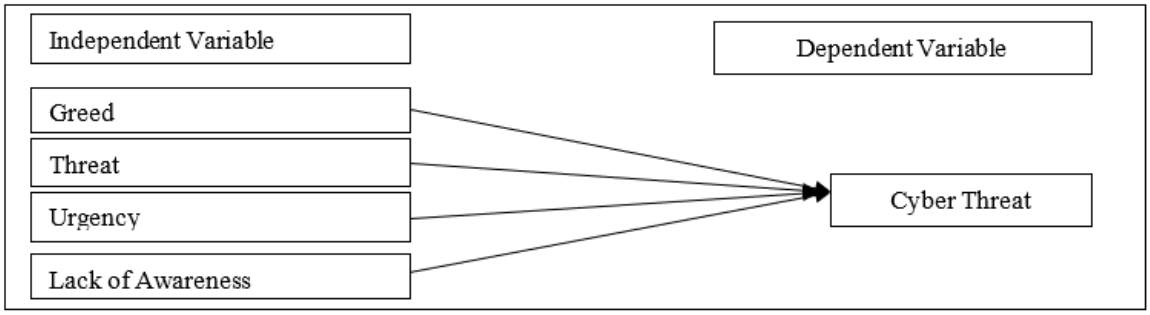
Source: NABARD (2020)

Social Engineering Tactics

Tactics used by the fraudsters to manipulate people in such a way that they are driven to share their personal, confidential and sensitive information to the fraudsters. Such tactics are so used that people trust them to be coming from a genuine source. Most common techniques used are Phishing, Spoofing, Spear phishing, Vishing, Smishing, DoS/DDoS & Man in the Middle. Hackers

generally impersonate the messages to be coming from a genuine source while it is in fact coming from a malafide source. Breda et. al (2027) discussed the shift of cyber security aspects from technical to social aspects. With social media in place, sharing of social profile on internet and transactions happening online these threats cannot be ruled out. Social engineering art is the key for such attacks specially knowledge workers, Krombholz et al. (2014), Muniz (2013), Mitnick & William (2011).

Figure 6: Conceptual Model Showing Relationship between Consumer Browsing Behaviour and Cyber Threats in Digital Banking



Source:Author

Source: Author Research

Objectives of Study.

1. To assess relationship of consumer greed driven browsing and cyber threats in digital banking
2. To assess relationship of consumer threat driven browsing and cyber threats in digital banking
3. To assess relationship of consumer urgency driven browsing behaviour and cyber threats in digital banking
4. To assess relationship of consumer lack of awareness driven browsing behaviour and cyber threats in digital banking

Hypothesis

1. Ho1: There is no significant relationship between consumer greed driven browsing behaviour and cyber threats in digital banking
2. Ho2: There is no significant relationship between consumer threat driven browsing behaviour and cyber threats in digital banking
3. Ho3: There is no significant relationship between consumer urgency driven browsing behaviour and cyber threats in digital banking
4. Ho4: There is no significant relationship between consumer lack of awareness driven browsing behaviour and cyber threats in digital banking

Research Methodology

The present research work is based on primary data collection. The study focuses on consumers who use ATM Cards & digital banking channels for purchases, e-commerce, funds transfers and bill payments. To identify the consumer browsing behaviour that influence cyber threats in digital banking a detailed literature review work is undertaken. A measurement of cyber threats in digital banking is done on basis of four key consumer browsing behavior i.e. greed, threat, urgency & lack of awareness. A Google form with structured questions based on four dimensions of consumer browsing was sent to 300 consumers' who use digital banking services.

Statistical tools like ANOVA, Descriptive Statistics and correlation coefficient are used. The dimensions of behavior are used as independent variables and cyber security is dependent variable.

Table 1: Behaviour Wise Consumer Classification

Browse Behaviour	Respondents	Frequency	Percentage
Greed based click on URL, Scan QR, emails, Whatsapp link etc.	300		
Never click		21	7%
Click Sometime		97	32%
Click Frequently		92	31%
Always		45	15%
Very Frequently		45	15%

Threat based click on URL, Phone, Whastapp, email, courier information etc.	300		
Click any URL without verifying legitimate source		103	34%
Check URL/email source diligently		152	51%
Verify messages source for it's trustworthiness		205	68%
Do not click threat link		14	5%
Urgency based click for saving some child, investment offer, etc.	300		
Click on link		224	75%
Transfer money		191	64%
Share credentials		54	18%
No action		25	8%
Lack of Awareness based click due to ignorance, casual handling etc.	300		
Sharing Phone numbers		129	43%
Sharing OTPs		159	53%
Sharing Locations		109	36%
Sharing Address		181	60%
Sharing Financial Data		40	13%

Source: Field Survey

Results & Analysis

Table 2 : ANOVA summary showing consumer greed driven browsing and cyber threats in digital banking

ANOVA						
Source of Variation	Sum of Squares	df	Mean Square	F Stat	Sig. (P-value)	F crit
Between Groups	14.54667	4	3.636667	24.11504	<0.00001	2.37788
Within Groups	225.4533	1495	0.150805			
Total	240	1499				

Source: Author Analysis

The ANOVA summary describes that the p value is <0.00001. The result is significant at p<0.05. Since p value is less than the standard value 0.05, the null value hypothesis is rejected; which proves that there is a significant relationship between the customer greed driven browsing and cyber threat.

Table 3: Descriptive Statistics of Greed Behaviour

Greed Behaviour - click on unsolicited mails, URL, whatsapp link & QR code promising a refund or cashback	Count	Sum	Variance	Mean	Std Dev.
Never click	300	21	0.065318	0.07	0.2556
Click Sometime	300	97	0.219521	0.3233	0.4685
Click Frequently	300	92	0.213333	0.3067	0.4619

Always	300	45	0.127926	0.15	0.3577
Very Frequently	300	45	0.127926	0.15	0.3577
Greed behaviour				0.2	0.4001

Source: Author Analysis

Consumer which click on unsolicited links on pretext of getting some cashback, refund or for some reward are definitely going to fall in a trap due to their greed behaviour. Out of the five parameters sometime clicking of fraudulent links is most important dimension while never clicking is least.

Table 4: ANOVA summary showing consumer threat driven browsing and cyber threats in digital banking

ANOVA						
Source of Variation	Sum of Squares	df	Mean Square	F Stat	Sig. (P-value)	F crit
Between Groups	65.88333	3	21.96111	118.9093	<0.00001	2.612343
Within Groups	220.8867	1196	0.184688			
Total	286.77	1199				

Source: Author Analysis

The ANOVA summary describes that the p value is <0.00001. The result is significant at p<0.05. Since p value is less than the standard value 0.05, the null value hypothesis is rejected; which proves that there is a significant relationship between the customer threat driven browsing and cyber threat.

Table 5: Descriptive Statistics of Threat Behaviour

Threat Behaviour Response of threat over email or URLs	Count	Sum	Average	Variance	Mean	Std Dev.
Never click	300	21	0.07	0.065318	0.07	0.2556
Click Sometime	300	97	0.323333	0.219521	0.323	0.4685
Click Frequently	300	92	0.306667	0.213333	0.307	0.4619
Always	300	45	0.15	0.127926	0.15	0.3577
Very Frequently	300	45	0.15	0.127926	0.15	0.3577
Threat behaviour					0.395	0.4891

Source: Author Analysis

Consumers may click on the threat related links and fall prey to fraudulent cyber hack or digital arrest. Out of five parameters sometime clicking and never clicking are most important dimensions for decisive factors.

Table 6 : ANOVA summary showing consumer urgency driven browsing and cyber threats in digital banking

ANOVA						
Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	97.29667	3	32.43222	200.6255	<0.00001	2.612343
Within Groups	193.34	1196	0.161656			
Total	290.6367	1199				

Source: Author Analysis

The ANOVA summary describes that the p value is <0.00001. The result is significant at p<0.05. Since p value is less than the standard value 0.05, the null value hypothesis is not accepted. This result indicates a significant relationship between the customer urgency driven browsing and cyber threat.

Table 7: Descriptive Statistics of Urgency Behaviour

Urgency Behaviour – Consumer reaction in urgency situation	Count	Sum	Variance	Mean	Std Dev
Click on link	300	224	0.189788	0.7467	0.4356
Transfer money	300	191	0.232096	0.6367	0.4818
Share credentials	300	54	0.148094	0.18	0.3848
No action	300	25	0.076644	0.0833	0.2768
Urgency Behaviour				0.412	0.4923

Source: Author Analysis

Table 8 : ANOVA summary showing consumer lack of awareness driven browsing and cyber threats in digital banking

ANOVA						
Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	39.264	4	9.816	45.27619	<0.00001	2.37788
Within Groups	324.12	1495	0.216803			
Total	363.384	1499				

Source: Author Analysis

The ANOVA summary describes that the p value is <0.00001. The result is significant at p<0.05. Since p value is less than the standard value 0.05, the null value hypothesis is rejected; which proves that there is a significant relationship between the customer lack of awareness driven browsing and cyber threat.

Table 9: Descriptive Statistics of Lack of Awareness Behaviour

Lack of Awareness Behaviour - Sharing of personal information over social media or internet	Count	Sum	Variance	Mean	Std Dev
Sharing Phone numbers	300	129	0.24592	0.43	0.4959
Sharing OTPs	300	159	0.249933	0.53	0.4999
Sharing Locations	300	109	0.232096	0.3633	0.4818
Sharing Address	300	181	0.240123	0.6033	0.49
Sharing Financial Data	300	40	0.115942	0.1333	0.3405
Lack of Awareness behaviour				0.412	0.4924

Source: Author Analysis

Table 10: Behaviour Wise pattern of consumer

Browsing Behaviour	Mean	SD	F Value	p Value

Greed	0.2	0.4001	24.11504	0.0000
Threat	0.395	0.4891	118.9093	0.0000
Urgency	0.412	0.4923	200.6255	0.0000
Lack of Awareness	0.412	0.4924	45.27619	0.0000

Source: Author Analysis

The above table depicts the mean, standard deviation, F value & p values of customer behaviour and cyber security threats. Table indicates that urgency (0.412) & lack of awareness (0.412) contribute to the maximum mean score in consumer behaviour followed by threat (0.395) and greed (0.2). Urgency & lack of awareness are most important dimensions that contribute to cyber threats while greed contributes the least. Further the greed also contributes the least standard deviation as well. Highest standard deviation is reported by lack of awareness. All dimensions of behaviour report p value less than 0.05 which implies the consumer behaviour contribution to cyber threat activities. F statistics of 200.62 & 0 of p value in urgency is indicative of the demonstration that consumer behaviour determines cyber threats in digital banking.

Table 11: Correlation between the Browsing Behaviour and Cyber Threat

Consumer Behaviour	Correlation Coefficient
Greed	0.143
Threat	0.143
Urgency	0.390
Lack of Awareness	1

Source: Author Analysis

A positive correlation coefficient indicate that consumer behaviour have impact on cyber threat in digital banking system.

Discussion and Recommendations

Current age digital banking technology has equipped consumers to execute financial transactions in online manner. Consumer behaviour in changed environment is of paramount importance. Any slackness on account of handling credentials, clicking unsolicited mails or links, sharing details, getting engaged in digital arrest coop may have drastic impact. Hard earned money of many a person has been duped by cybercriminal using such social engineering tactics. No financial institution can afford to lose money and goodwill of consumers. Banks are committed to follow such cyber security principles as required by regulators in protection of personal data. When executing a system in banks the banks must ensure cyber security principles that the services are rendered in uninterrupted manner and at the same time there is simplicity in design for services availability and defense in depth (with no single point failures, EDR, Network security, VAPT of Infra , patching & reassessment). Least privilege must be used for online users (hardening, remove unnecessary settings, remove unused Ids)

It is mandatory that the customers are made aware of such tactics used by fraudsters. URL and links coming from untrusted sources should not be clicked without proper validation from originating sources. Such drives offering cash for click or refund for clicking a QR code. Any anonymous prompt for making an investment should be abandoned. A control on greed behaviour may be helpful to protect the money kept safe in banks. Similarly any phone call, whatsapp call or email stating any kind of legal action or FIR or pretending engagement into some illegal activity must be taken as an alert. No threat must be entertained in any circumstances as such channels are never used by regulatory setup.

Consumer awareness programs must be done on frequent intervals and through news channels and social media sites that they must ensure not to disclose their personal information to anyone who so ever it may be. Any lack of awareness must not be tested on digital channels and it may be costing very dearer.

Though banks deploy latest technologies to ensure that there are minimal threats, consumers also must ensure that their browsing behaviour is not adding to cyber threats and cyber-attacks.

REFERENCES

1. Ahamed, S. & Mustafa, H. A. (2019). A Secure QR code System for sharing personal confidential information. International conference on computer, communication, chemical, materials and electronic engineering (IC4ME2).
2. Alkadi, O., Mustafa N., Turnbull B & Choo K. K. (2020), A deep block chain framework enabled collaborative intrusion detection for protecting IoT and cloud networks. IEEE Internet things.
3. Breda F., Barbosa H. & Morais T. (2017). Social Engineering And Cyber Security. 10.21125/inted.2017.1008
4. Dekkati S. Thaduri U. R. & Ballamudi V. K. R. (2022), AI and Machine learning for remote suspicious action Detection and Recognition. ABC journal of advance research, Vol. 11(2), pp.97-102.
5. Duarte N. (2021). Social Engineering: The art of attacks. In book: Advanced Research in Technologies, Information, Innovation and Sustainability, First International Conference, ARTIIS 2021, La Libertad, Ecuador, November 25–27, 2021, Proceedings (pp.474-483)
6. Kandukuri S. & Yadav D, (2022). Protecting legitimate and preventing unauthorised access to

confidential information in social engineering. International Journal of research. Vol 11(10).
7. Mitnick K. & Simon W. (2011). The art of deception: controlling the human element of security. John Wiley & Sons.
8. Krombholz K., Hobel H., Donko-Huber M, & Weippl E. (2014), Advanced social engineering attacks. Journal of Information Security and Applications, Vol.22, do:10.1016/j.jisa.2014.09.005
9. Manivel R. and Ramasamy P. (2023). Digital Banking in India. ICSSR sponsored Conference [online] available at https://www.researchgate.net/publication/ accessed 10th Jan 2025.
10. Merriam-Webster (2021), Most trusted dictionary in America.
11. Muniz J. (2013). Web penetration Testing with kali Linux. Packt Publishing. India.
12. NABARD (2020). Comprehensive Cyber Security Framework for Rural Cooperative Banks. [online] available at https://www.nabard.org/auth/writereaddata/tender/E-2020Cir_32_E.pdf accessed 10th Jan 2024
13. National Cyber Crime Reporting Portal (2024) [online] available at https://cybercrime.gov.in accessed 10th Jan 2024.
14. NIST (2024). The NIST Cyber Security Framework (CSF) 2.0. [online] available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf accessed 5th January 2025.
15. Okereafor, K. (2021). Cybersecurity in the COVID-19 Pandemic. New York, CRC Press, pp.125-135.
16. Patel R. S. (2013). Kali Linux Social Engineering. Packt Publishing, India.
17. Popescul D. (2011). The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation. 16th International business information management association conference, pp.1338-1345.
18. Schatz D., Bashroush R. & Wall J. (2017). Towards a more representative defintion of cyber security. Journal of Digital Forensics Security and Law, Vol. 12(2), pp.53-74.
19. Sekhar C. and Kumar M. (2023). An overview of cyber security in digital banking channel. East Asian Journal of multidisciplinary research, Vol. 2(1), pp.43-52.
20. Yadav T. & Rao A. (2015). Technical Aspects of Cyber Kill Chain. 3rd International Symposium on Security in Computing and Communications (SSCC'15): Kochi, India, Vol.536