International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 11 | Nov - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Outcomes of Social Engineering: Understanding Cybercriminals' Exploitation of Human Psychology

Dr. Kiran Kumar M, Shruthi M, Sathwick N, Prathap S

Assistant Professor, MBA Student- Finance, MBA Student- Finance, MBA Student- Finance

Kiranm287@gmail.com, shruthi_m23@cms.ac.in, sathwick_n23@cms.ac.in, prathap_s23@cms.ac.in

Faculty of Management Studies, CMS B School, Jain (Deemed-to-be university), Bangalore.

ABSTRACT

This study explores the growing threat of social engineering attacks in India, examining how cybercriminals exploit human psychology to gain unauthorized access to sensitive information and systems. Analyzing data on compromised accounts, financial losses, and cybersecurity training adoption from 2014 to 2024, the research uncovers alarming trends - a steady rise in compromised accounts, strong correlations between account compromises and financial impacts, and a reactive, yet insufficient, response from organizations through increased training programs. The findings highlight the urgent need for a multi-faceted approach that combines technological safeguards with robust employee awareness initiatives to mitigate the human vulnerabilities exploited by social engineering tactics. Implications for policymakers, businesses, and individuals in India emphasize the critical importance of proactive cybersecurity measures to address this evolving threat landscape.

Keywords:

Social engineering, Cybercrime, Compromised accounts, Financial losses, Cybersecurity training, Human vulnerabilities

INTRODUCTION

Cybersecurity has traditionally focused on protecting networks and systems against technological threats such as viruses, malware, and hacker attacks. But social engineering, where attackers take advantage of people's weaknesses rather than technological one is a growing source of worry. In order to fool people into disclosing private information or allowing illegal access, social engineering assaults use psychological manipulation techniques like deceit, urgency, fear, and trust.

The fact that these attacks get past even the most sophisticated technical protections highlights how important human aspects are to cybersecurity. This paper's main research topic is: How can cybercriminals use social engineering techniques to alter people's psyche in order to take advantage of weaknesses, compromise data, and break into systems.

Background

Driven by rising internet use, digital transactions, and greater reliance on online platforms, India has seen a stunning surge in cybercrimes over the past ten years. Among these crimes, social engineering attacks have become among the most common since hackers take advantage of human nature to control people into revealing private information or providing illegal system access. Phishing, impersonation, and pretexting among other tactics have caused significant data breaches in many different fields and financial losses.

Even although cybersecurity policies are becoming more and more popular, the human factor is still a major problem since many people fall for these dishonest strategies. With an eye on compromised accounts, financial losses, and the function of cybersecurity training programs in lowering these risks, this study seeks to investigate the emergence of social engineering assaults in India. Through data analysis spanning the past ten years, the study aims to evaluate how well awareness-raising campaigns and training help to reduce the effects of social engineering on people and businesses in India.

Significance

The significance of this study lies in its ability to shed light on the growing impact of social engineering attacks in India, a country that has seen a rapid increase in cybercrime incidents in recent years. As highlighted by Panda & Sharma (2021) and Chakraborty & Paul (2020), social engineering tactics have become a key method for cybercriminals to exploit human psychology, making traditional cybersecurity measures inadequate. The financial and data losses from these attacks, as discussed by Ghosh & Sen (2021) and Verma & Rathi (2022), underscore the need for effective countermeasures. By examining the role of cybersecurity training, as noted by Dey & Gupta (2023) and Sharma & Kumar (2023), this research aims to evaluate how such programs can reduce vulnerabilities and mitigate the increasing threat posed by social engineering. This study’s findings are crucial for policymakers, businesses, and individuals to develop better prevention strategies and cybersecurity frameworks.

Problem Statement

The purpose of this study is to investigate the ways in which cybercriminals use social engineering techniques to abuse human psychology in order to carry out cyberattacks in India. Specifically, the study investigates the increasing patterns of compromised accounts and financial losses, as well as the role that cybersecurity training programs have in mitigating these risks. The purpose of this paper is to investigate the impact that social engineering has had on cybersecurity by analyzing data from the past ten years. The paper focuses on the psychological vulnerabilities that make individuals and organizations susceptible to manipulation, and it evaluates the effectiveness of training adoption in reducing such risks.

LITERATURE REVIEW

Social engineering attacks are emerging as a formidable threat to network security in India, bypassing traditional technical defenses by targeting the human psyche. Cybercriminals leverage psychological vulnerabilities, manipulating individuals into unwittingly compromising systems. Panda and Sharma (2021) highlight how these attacks exploit the lack of cybersecurity awareness, especially within the Indian context, where cultural and societal factors amplify risks. Chakraborty and Paul (2020) underscore the surge in phishing schemes, emphasizing how these attacks play on users' trust and urgency. Organizations, too, face significant challenges, as Kumar and Verma (2021) point out, with insufficient employee training leaving businesses exposed. Similarly, Dey and Gupta (2023) illustrate the positive impact of cybersecurity programs in reducing these threats, yet reveal the gaps that persist in creating robust defenses.

The stakes are particularly high in sensitive sectors like banking and government, as reviewed by Srinivasan and Patil (2022), where human error can lead to catastrophic breaches. The COVID-19 pandemic further escalated the issue, driving reliance on digital platforms, as Verma and Rathi (2022) explain in their study of phishing trends. Singh and Sharma (2019) bring attention to case studies of scams, such as fake job offers and lottery fraud, showcasing the emotional manipulation tactics used by attackers. However, hope lies in strategic training and awareness initiatives, as explored by Sharma and Kumar (2023), who advocate for tailored programs in the IT sector to address these unique risks. Through a blend of research and solutions, the evolving landscape of social engineering demands a concerted focus on human behavior, awareness, and proactive cybersecurity practices to fortify India's defenses against these covert cyber threats.

OBJECTIVES OF THE STUDY

1. To investigate the financial impact of social engineering attacks using reported data on financial losses over the years.
2. To examine the correlation between training adoption rates and the cyberattack incidents.
3. To assess the role of human error in the success of social engineering attacks and potential prevention strategies.

THE INTERPLAY OF HUMAN ERROR AND CYBERCRIME TACTICS

Cybercriminals exploit human psychology and human errors through sophisticated strategies that manipulate innate cognitive biases and habitual behaviors. These tactics, commonly referred to as social engineering, rely on deceiving individuals rather than bypassing technological safeguards, making them both subtle and effective.

1. Making Use of Cognitive Biases

Cognitive biases that affect judgment are a natural tendency of humans. Attacks by cybercriminals are planned to take advantage of these weaknesses:

Authority Bias: To get compliance or action, many phishing scams pose as legitimate people or institutions (such as banks, employers, or law enforcement).

Scarcity and Urgency: Scammers use messages that promise limited-time deals or severe penalties to instill a sense of urgency in their victims, leading them to behave rashly.

Trust and Familiarity: To carry out spear phishing or business email compromise (BEC) attacks, cybercriminals pose as reliable contacts or businesses.

Curiosity and Greed: Users are drawn to click on dangerous links or download infected files by emails or advertisements that promise exclusive information, free gifts, or financial rewards.

2. Taking Advantage of Human Error

One of cybersecurity's weakest points is still human mistake. Cybercriminals take advantage of errors like:

Weak Password Practices: A lot of people select simple, easily guessed passwords or reuse them.

Clicking on Phishing Links: Users are vulnerable to phishing attempts when they neglect to carefully examine email sender addresses, URLs, or attachments.

Lack of Awareness: A lot of people and workers are not properly trained to recognize dangers, which increases their vulnerability to social engineering.

Mishandling Sensitive Information: Attackers can take advantage of weaknesses when devices are misplaced, passwords are shared, or networks are unprotected.

RESEARCH METHODOLOGY

1. Data Collection

The research utilizes secondary data from government reports (MeitY), industry publications (Grant Thornton Bharat, Business Standard), academic journals, and news articles to analyze trends in social engineering attacks, cybersecurity practices, and financial losses in India.

2. Tools Used

Microsoft Excel is used for Correlation, Year on year growth percentage, and Descriptive Statistics to identify patterns and relationships between all the four variables.

3. Type of Data

The data is secondary, comprising quantitative data on cybercrimes, financial losses, and training adoption, along with qualitative insights from case studies and expert analyses of social engineering tactics.

4. Limitations of the Data

The research is limited by potential inaccuracies in secondary data, underreporting of cybercrimes, data gaps, and the rapid evolution of cyber threats that may not be fully captured in existing sources.

5. Scope of the Research

The study focuses on the growing prevalence of social engineering attacks in India, analyzing trends from 2014-2024, the role of cybersecurity training, and financial impacts within Indian organizations and individuals.

DATA ANALYSIS:

This data presents a yearly overview of cybercrime trends in India from 2014 to 2024. It includes the number of accounts compromised, reported attacks, financial losses (in Crores), and the training adoption rate (%) for cybersecurity awareness across organizations.

Year	Accounts Compromised (Approx.)	Number of Attacks (Reported)	Financial Loss (₹ Cr.)	Training Adoption Rate (%)
2014	12,000,000	49,000	500	5
2015	13,500,000	56,000	700	8
2016	16,000,000	65,000	1,000	12
2017	20,000,000	79,000	1,500	15
2018	25,000,000	95,000	2,000	18
2019	30,000,000	120,000	2,800	22
2020	40,000,000	240,000	3,500	25
2021	50,000,000	452,000	4,200	30
2022	60,000,000	967,000	5,500	35
2023	75,000,000	1,556,000	7,000	40
2024	85,000,000	1,800,000	8,000	45

Source: https://www.meity.gov.in/

Year-on-year Growth

Year	Accounts Compromised	YoY Growth (%)
2014	12,000,000	
2015	13,500,000	12.5
2016	16,000,000	118.5185274
2017	20,000,000	125
2018	25,000,000	124.99995
2019	30,000,000	119.991944
2020	40,000,000	133.3265867
2021	50,000,000	124.9444775
2022	60,000,000	119.999978
2023	75,000,000	124.9999963
2024	85,000,000	113.3333333

This data shows a steady rise in the number of accounts compromised in India from 2014 to 2024. Each year, the number of compromised accounts grows, with significant jumps in 2016 and 2020, indicating that cyber threats have been steadily increasing over time.

Descriptive Statistics

Accounts Compromised (Approx.)		*Number of Attacks (Reported)*		*Financial Loss (₹ Cr.)*		*Training Adoption Rate (%)*	
Mean	38772727.27	Mean	498090.9091	Mean	3336.364	Mean	23.18182
Standard Error	7699280.851	Standard Error	194667.9436	Standard Error	777.674	Standard Error	3.965346
Median	30000000	Median	120000	Median	2800	Median	22
Mode	#N/A	Mode	#N/A	Mode	#N/A	Mode	#N/A
Standard Deviation	25535625.74	Standard Deviation	645640.5276	Standard Deviation	2579.253	Standard Deviation	13.15156
Sample Variance	6.52068E+14	Sample Variance	4.16852E+11	Sample Variance	6652545	Sample Variance	172.9636
Kurtosis	-0.775576618	Kurtosis	0.44394348	Kurtosis	-0.71536	Kurtosis	-1.03188
Skewness	0.73598947	Skewness	1.373791708	Skewness	0.703435	Skewness	0.296617
Range	73000000	Range	1751000	Range	7500	Range	40
Minimum	12000000	Minimum	49000	Minimum	500	Minimum	5
Maximum	85000000	Maximum	1800000	Maximum	8000	Maximum	45
Sum	426500000	Sum	5479000	Sum	36700	Sum	255
Count	11	Count	11	Count	11	Count	11
Confidence Level(95.0%)	17155066.8	Confidence Level(95.0%)	433747.2084	Confidence Level(95.0%)	1732.766	Confidence Level(95.0%)	8.835341

This table provides a statistical overview of key variables related to cybercrime and cybersecurity training, offering insights into their average values, spread, and distribution, which can be useful for understanding trends and variability in the data.

- Accounts Compromised: On average, around 38.77 million accounts were compromised each year.
- Number of Attacks Reported: On average, there were 498,090 reported attacks each year.
- Financial Loss: The average financial loss due to cybercrimes is ₹3,336.36 Crores annually.
- Training Adoption Rate: On average, 23.18% of organizations adopted cybersecurity training each year.

Correlation

This correlation matrix shows the relationships between the four variables: year, accounts compromised, number of attacks, financial loss, and training adoption rate.

Correlation					
	year	*accounts compromised*	*number of attacks*	*financial loss*	*training adoption rate*
year	1				
accounts compromised	0.965851718	1			
number of attacks	0.857030493	0.954842021	1		
financial loss	0.97142831	0.998272994	0.951326919	1	
training adoption rate	0.994983739	0.984998627	0.90258119	0.988842314	1

This table sheds light on the increasing frequency of cybercrimes as well as the expanding impact that they have over the course of time. The year and the number of accounts that have been compromised have a high positive connection of 0.97, which suggests that there has been a consistent increase in the number of cybercrime events. The link between compromised accounts, attacks (0.95), and financial losses (0.99) demonstrates that hits that are more frequent and sophisticated lead to higher account breaches and severe monetary damage. This increase is mirrored in the relationship between compromised accounts and attacks. The consequences of cybercrime are becoming increasingly severe for both persons and companies, as evidenced by these trends.

The high connections between training adoption and measures such as financial loss (0.99), compromised accounts (0.98), and attack frequency (0.90) demonstrate that enterprises are gradually embracing cybersecurity training programs as a response to the growing threat of cyberattacks. According to these studies, a reactive approach to mitigating cyber risks is being used, in which the financial and operational toll of breaches is driving investments in employee knowledge

and preparedness. Over the course of time, the adoption of training has steadily increased (by 0.99 percent with each passing year), which reflects a realization of the significance of training in addressing the expanding cyber threat scenario.

RESULTS

The high correlation coefficient of 0.97 between year and compromised accounts suggests that this trend is substantially linear. This means that as time goes on, the number of accounts that have been hacked increases at a faster and faster rate.

As the number of accounts that have been infiltrated has increased exponentially, the financial repercussions have also increased, going from ₹500 crores in 2014 to an estimated ₹1,800 crores over the course of 2024. This indicates that fraudsters are able to take advantage of large-scale account hacks in order to inflict huge monetary damages on victims.

It is interesting to note that the data also reveals a significant connection (0.98) between compromised accounts and the rate of acceptance of cybersecurity training. This suggests that firms have reacted to the increasing frequency of cyberattacks by increasing their investments in employee awareness and education initiatives in order to keep up with the trend.

On the other hand, the fact that the number of compromised accounts and financial losses has been steadily increasing implies that the training efforts that have been made up to this point have not been sufficient to fully neutralize the human vulnerabilities that are subject to social engineering strategies.

IMPLICATIONS FOR THE FUTURE

1. Employees should be empowered to recognize and reject psychological manipulation tactics used by cybercriminals, and training should focus on providing them with this ability.

2. The use of advanced identity validation methods such as biometric verification, multi-factor authentication, and other such techniques can be of assistance in preventing successful account takeovers.

3. Enhanced collaboration between the government, law enforcement, and the private sector has the potential to enhance the sharing of threat intelligence, facilitate a more rapid reaction to emerging cyber dangers, and facilitate the development of comprehensive national cybersecurity strategy.

4. Organizations should prioritize proactive defenses like as security monitoring, vulnerability assessments, and threat detection in order to keep ahead of emerging attack methods. This is in contrast to reactive defenses, which would involve reacting to incidents.

5. Increasing the number of cybercrime occurrences that are reported and disclosed can provide better visibility into the scope and nature of the problem, which can lead to more efficient policymaking and resource allocation.

6. Empowering individuals to better protect themselves can be accomplished by educating the general public on safe internet practices, recognizing social engineering strategies, and reporting suspected cybercrimes.

CONCLUSION

The disturbing growth in attempts at social engineering that take advantage of human vulnerabilities is the driving force behind the expanding cybercrime threat in India, which is depicted in this report in a way that is particularly concerning. The fact that there is a strong association between compromised accounts, financial losses, and the adoption of cybersecurity training highlights the fact that these cyber risks are closely intertwined with human psychology and behavior. In order to effectively alleviate this difficulty, a multi-pronged approach is required. This approach should combine thorough staff awareness and education initiatives with robust technology safeguards. It is possible for India to strive toward improving its overall cybersecurity posture and reducing the severe financial and data repercussions of these emerging social engineering assaults. This may be accomplished by providing companies and individuals with the ability to recognize and reject the manipulative tactics used by cybercriminals.

REFERENCES

1. Bhat, R., & Joshi, K. (2020). Understanding human vulnerabilities in cybersecurity: A case study of Indian financial institutions. *Cybersecurity and Risk Management Journal*.
2. Business Standard. (2024). Reports detailed financial losses due to cybercrimes in 2024 and comparative statistics over the years, showing the rising impact of phishing, investment scams, and other digital fraud. *BIZNEWS INDIA*.
3. Chakraborty, R., & Paul, M. (2020). Cybercrime in India: The rise of social engineering attacks. *Journal of Information Security & Cyber Laws*.
4. Dey, D., & Gupta, A. (2023). Impact of cybersecurity training on social engineering attacks in Indian organizations. *Journal of Information Technology & Security*.
5. Ghosh, S., & Sen, P. (2021). Cybercrime and social engineering: An Indian perspective. *International Journal of Cybersecurity and Digital Forensics*.
6. Grant Thornton Bharat. (2024). Financial and cyber fraud report. Highlights trends in financial frauds and training adoption rates within Indian organizations, emphasizing vulnerabilities in cyber defense post-pandemic. *GRANT THORNTON BHARAT*.
7. International Journal of Science and Research Archive. (2024). Insights into cybercrime trends in India over the last decade. *SCIRES ARCHIVE*.
8. Kumar, S., & Verma, M. (2021). A study on cybersecurity practices in Indian organizations: Focusing on social engineering risks. *Journal of Cybersecurity and Policy*.
9. Ministry of Electronics and Information Technology (MeitY). (2023). Annual report on cybercrime trends in India, including data on phishing and social engineering attacks. *Government of India*.
10. Panda, R., & Sharma, D. (2021). Cybersecurity challenges in India: An analysis of human factors in social engineering attacks. *Indian Journal of Cyber Security*.

11. Reddy, M., & Naidu, N. (2021). Training adoption and its role in reducing cybersecurity risks in Indian corporations. *Indian Journal of Information Security*.
12. Sharma, R., & Sinha, S. (2021). Cybercrime in India: The rise of financial fraud and social engineering. *Journal of Digital Forensics and Investigations*.
13. Singh, H., & Sharma, P. (2019). Cybercrime and the human factor: Case studies of social engineering in India. *Indian Journal of Cybercrime Studies*.
14. Soni, A., & Kumar, P. (2022). Psychological manipulation in Indian cybercrime: A study of social engineering attacks. *International Journal of Cyber Crime & Security*.
15. Srinivasan, A., & Patil, K. (2022). Social engineering attacks: A review of cybercrime trends in India. *Indian Journal of Computer Science and Engineering*.
16. The Times of India. (2023). "India sees rise in cybercrimes as digital adoption grows; experts warn about social engineering risks." *The Times of India*.
17. Verma, P., & Joshi, V. (2022). The role of awareness programs in reducing social engineering attacks in Indian enterprises. *Journal of Cyber Risk Assessment in India*.
18. Verma, S., & Rathi, P. (2022). The evolution of phishing attacks in India: A social engineering analysis. *Cyber Defense and Information Security Journal*.