Cybersecurity Beyond Tools: Unmasking the Psychological Manipulation

Ajay Prajapati[1], Mrs. Karishma Jain[2]
[1,2]*Department of Computer Science, Patkar Varde College, Goregaon, Mumbai*

Abstract: ***Cybercrime has outgrown mere technicality and has now evolved into a psychological battle exploiting human frailties. The solution needs to be a composite one bringing together technology, education, and psychological insight. The more potential victims are educated about the psychological ploys used by scammers, the more they become a part of the human firewall that could make the cyber world a safe place. Cybersecurity has mostly focused on technical defenses, like software, hardware, and other advanced tools. Still, the other side of the coin, which is psychological manipulation, is equally critical and relatively underrated. This manipulation tactics are the use of human emotions like trust, fear, greed, and curiosity to mislead victims. For instance, children are lured with promises of gaming rewards, teenagers with scams from social media, adults with fake jobs, and the elderly with various frauds. The paper examines how such tactics morph further for specific age groups with real-time examples from India showing their impact. By making known these exploitative techniques, the present study very rightly focuses on the need for integrating psychology into cybersecurity, raising awareness and prevention***.

I. INTRODUCTION

Cybersecurity often refers to protect the systems, networks, and data from cyberattacks. Although the technical defenses are pivotal, they cannot do the job entirely in combating the growing trend of psychologically related cybercrimes. Hackers and scammers are targeting more human weaknesses than technical weaknesses, which creates the weakest link in cybersecurity between humans.

Psychological manipulation, or social engineering, is based on emotions like trust, fear, greed, or curiosity. Analyzing the behavioral patterns of various age groups, cybercriminals design specific scams. This paper will discuss the psychological strategies for targeting specific age groups, from children to the elderly, with real-life examples from India and other countries to tell the impact of these tactics.

II. PSYCHOLOGICAL MANIPULATION IN CYBERCRIMES

A. Children (8-15 Years): The Gaming Lure:

Children in the age group 8-15 are highly into online gaming and are most targeted to scams that provide free in-game currency, rare skins, or discounted items. Scammers use their innocence and greed for reward.

Case Study: 12-year-old Rohan from Sangola, Maharashtra was found at Mumbai Railway Station, he was trying to hide from his neighbors. According to him, he went there to meet his online friend who was 16 years and promised him to give diamonds (Free fire game) Investigations revealed his so called 16-year friend was involved in human trafficking of children. He used to connect with teens from remote areas, lure them and invite to Mumbai. Rohan was saved due to his neighbor's vigilance.

B. Teenagers and Young Adults (16-22 Years): The Social Media and Gambling Trap

Teenagers and young adults are highly active on social media and gambling platforms, making them prime targets for scammers who exploit their desire for quick money and online interactions.

Case Study: In 2022, a 19 year old Delhi college student was one of the victims of a well thought out online gambling fraud. Like his peers he was attracted by the prospect of fast money through the internet. When surfing social media, he found an ad for a gambling app, which had nice graphics and the most audacious claims that one could easily make a lot of money from the application. The ad looked real, with

fake reviews and testimonials of clients allegedly becoming rich through the use of the app.

The student downloaded the app and opened an account because of curiosity and the desire to try his luck. It surprised him when the app displayed what appeared to be a great deal of 'earnings' after he invested as little as ₹500. Having built up a nice balance, he decided to invest more, ₹2,000 and then ₹5,000 in the belief that he could earn even more. The app also sent congratulatory messages which made him think that he was on his way to becoming rich.

one day he tried to withdraw his earnings but, the app refused the transaction. then he contacted the app's customer support, but no respond from there also. For the next few days, his account was completely frozen, and all attempts to access it were unsuccessful. Gradually, the grim reality dawned on him—it was a scam.

The student lost the sum of ₹7,500, which was a considerable amount for him. Besides the financial loss, the experience left him disappointed and betrayed. He later discovered that the app was part of a large scam network on social media targeting young people.

This tale shows how cybercriminals take advantage of people looking for quick money. It highlights the importance of raising awareness among young adults about the risk of online betting websites and how to check apps before using them.

C. Working Adults (23-50 Years): The Professional and Personal Needs Exploitation

This age group is often targeted through job scams, matrimonial fraud, and investment schemes, as scammers prey on their professional and personal aspirations.

Case Study: In the year 2022, Sarah Smith, from Birmingham, she was 34 year old, she was the victim of a cold-blooded sextortion scam that took advantage of her problems and trust. As a single mother who manage work and family, Sarah occasionally used social media and online dating sites to search for a good partner and a possible love interest. On one such platform, she met someone who appeared genuine, kind, and genuinely interested in her life. Sarah and the individual spent weeks talking on the messaging platform, building what she believed was a deep relationship. The scammer, who posed as a considerate and suave partner, gradually gained her trust. Sarah opened up about intimate aspects of her life in their conversation, such as being a single mother, and finally felt comfortable enough to send some private photos when the scammer requested them.

That is when the nightmare began. Then the individual sent her a threatening message, stating that if she did not pay £300 immediately, then her private photos would be sent to her family and friends, they would posted online also. She was very much scared of such public embarrassment and damage to her reputation, Sarah sent the money, hoping to reverse the situation.

And that was not all. After a few days, he demanded another payment in name of money. This time, they threatened her to send even more private information, claiming they had saved copies of their conversation and would expose more private information if she paid them another £500. Sarah was filled with fear and anxiety as she feared that her private life would be exposed before her inner circle.

Unfortunately, extortion was not deterred by this; she was being paid consistently to do more and more for the scammer, and each time he came back with higher demands, and in response, she kept on landing in a vicious cycle of control, tired, and out of pocket.

Then Sarah spoke to a close friend who helped her to report the issue to local police. She then realized that she was one of many victims of an advanced sextortion scam targeting people across the UK. Although it was impossible to trace the scammers, Sarah's experience served to raise awareness of the dangers of online relationships and the very important need to be cautious when sharing private information or photographs online.

Her experience is a sad reminder of the dangers that underpin the digital age and serves to emphasize the need to learn to identify and report these scams. Her experience also serves to emphasize that individuals should seek assistance and not suffer in silence, for no one should have to endure such agonies alone.

D. Elderly (50+ Years): The Trust and Dependency Deception

Elderly individuals are often targeted by scams involving fake government schemes, pension benefits, or health insurance.

Case Study: In 2023, one of the heartbreaing scams that really made rounds was the "grandparent scam" against an elderly woman named Margaret Brown. Margaret Brown was a 76 years old widow living alone with her grandchildren visiting her quite often, making them doting grand parents in close touch with their family members. When she received one dreadful afternoon call that threw her into a panic is what this story tells us.

The caller, speaking with urgency and distress, said, "Grandma, it's me! I'm in trouble. I had an accident and need money to get out of it. Please don't tell anyone—it's embarrassing." The voice sounded shaky, and the scammer cleverly avoided giving too many identifying details by saying they were injured and having a bad connection. Confused but concerned, Margaret believed she was speaking to her 22-year-old grandson, Jake.

The scammer shared some personal information about Margaret's family to make the story convincing—details they likely gathered from Jake's social media posts or public profiles. They mentioned Jake's college, his recent trip abroad, and even the pet dog he often talked about. That level of detail made Margaret completely trust the caller.

The rogue then demanded that he needed £5,000 immediately to pay for "legal fees" regarding the accident. They gave Margaret instructions on specifically transferring the money into a bank account, assuring her that all would be okay once the payment was made. Worried about her grandson's safety and coupled with weight of the situation, Margaret went straight to her local bank and made the transfer without a moment of hesitation.

Hours later, Margaret was still rattled as she called her daughter to report on what had occurred. Her astonishment turned to relief as she learned Jake was perfectly fine, safe in the house and blissfully ignorant of the drama. Realizing that she was duped into that, she became even more shaken-not so much by losing a couple hundred but also about emotional manipulation.

Margaret reported to the authorities that she had recently experienced a kind of scam and they told her this was being termed as the "grandparent scam" whereby a scammer, taking advantage of the aged persons' love and concern towards their family, obtains money. There is only a slight hope for recovering that amount since a scammer keeps accounts that can never be tracked.

Margaret's experience calls for continued watchfulness in even seemingly time-sensitive and emotive situations. She has learned to share the experience with many of her acquaintances, to cross-check all such calls and not to respond under duress or pressure from anyone. Speaking out boldly on her experience, she has empowered the rest not to fall victim to such scammers.

III. PERSONAL EXPERIENCES COLLECTED FROM VICTIMS

Psychological strategies are employed by cybercriminals to exploit vulnerabilities in individuals of all ages. The following are examples of victims:

A. Prince Kumar (Age 15): The Gaming Scam:

At the age of thirteen, Prince Kumar frequently played the popular online game BGMI. During a match, he encountered a random player who was showing off expensive in-game skins. After playing a few matches together, the player promised Prince 10,000 in-game currency (UC) for just ₹1,000, a fraction of its actual cost. Tempted by the offer, Prince used Google Pay to send money he borrowed from a friend’s brother. However, he was disappointed when the scammer vanished after receiving the payment, leaving him without the promised UC.

B. Shiv (Age 20): The Gambling Trap:

He was a common person like us, he use to bet on Dream11 player and often look for advice on gambling apps. He came across a YouTuber who claimed to provide "winning teams" for games, guaranteeing large profits. The YouTuber advised Shiv to invest ₹200 in a gambling app, promising a ₹1,000 return. Despite already facing financial losses from gaming, Shiv decided to take the risk and recover money from it . After he deposited the money, the YouTuber blocked all communication, and also kicked him out from the telegram group from which he got the application link and at the end the scammer took advantage of shiv's situation and scammed him.

C. Rohit (Age 24): The Internship Fraud:

Rohit, in his final year of a Bachelor of Science in Computer Science, he was desperately searching for

an internship. He joined a WhatsApp group that shared job openings and the admin who called him self as a professionalist from IT background, demanded to pay ₹4,000 for a "paid internship" that promised valuable experience and a job offer after attending a Google Meet session. Afterward, he received fake offer letters from well-known companies. Once he made the payment, all communication ceased, and Rohit realized he had been deceived.

D. Priya Sharma (Age 29): The Matrimonial Scam:
Priya Sharma, a marketing expert, signed up for a marriage-matching service. A man claiming to be an NRI living in the UK contacted her. After establishing a connection online over several weeks, he told Priya that he was sending her expensive gifts, including electronics and jewelry. Then after few time, she received a call from someone purporting to be a customs agent, who asked for ₹50,000 to clear the parcel. After transferring the funds, Priya discovered it was all a scam. There was no gift send and the custom officer who called her was also a part of the scammer group.

E. Ramesh Gupta (Age 62): The Pension Fraud:
Ramesh Gupta was a retired bank worker, he got a call one day from someone claiming himself as a pension office official. He was sounding professional and alerted him to about an error in his pension account that required immediate attention. The fraudster requested a minor service fee and banking information for verification, claiming he could fix the problem. Ramesh gave the caller his bank account information since he trusted them. Within few times through many transactions, ₹1.5 lakhs were withdrawn. He noticed unapproved withdrawals from his bank that he realized the scam.

VI. THE RISING THREAT OF SOCIAL ENGINEERING

A Data-Driven Perspective:
Social Engineering Attacks in India:
i) 60% of reported cybercrimes in India is a part of social engineering attacks. (Source: CERT-In Annual Report 2024)

International Trends in Social Engineering Attacks:
i) In 2024, 32% of data breaches globally was ransomware extortion. (Source: Secure Frame Cybersecurity Report 2024)
ii) The percentage of ransomware victims paid ransom grew from 6.9% in 2023 to projected 16.3% in 2024. (Source: Secure Frame Cybersecurity Report 2024)

Economic and Psychological Impact:
i) Phishing-related fraud has cost the world more than $55 billion in 2023. (Source: ABA Banking Journal, 2023)
ii) More than 70% of all victims suffer from stress, anxiety, or loss of trust in digital platforms. (Source: ABA Banking Journal, 2023)

V. GOVERNMENT REGULATIONS AND LAWS COMBATING SOCIAL ENGINEERING THREATS

1. Information Technology Act, 2000 (IT Act):
i) Penalizes unauthorized access, identity theft, and cyber fraud.
ii) Section 66D criminalizes online impersonation.
iii) Section 72 protects digital privacy by penalizing data misuse.

2. Indian Penal Code (IPC) Amendments for Cybercrime:
i) Section 419 criminalizes identity-based fraud.
ii) Section 420 targets online scams and financial deception.

3. Cyber Surakshit Bharat Initiative:
i) A government program aimed at enhancing cybersecurity awareness and providing ethical hacking training.

V. FUTURE STRATEGIES FOR COMBATING SOCIAL ENGINEERING ATTACKS

1. Behavioral Cybersecurity Solutions:
i) AI security solutions monitor an individual's conduct to identify abnormal and fraud-like behavior.
ii) Banking and digital platforms automatically alert against any suspicious behavior.

Real World Application: Anti-Fraud AI:
Anti-Fraud AI is a sophisticated application that prevents and detects cyber threats by constantly

monitoring user interaction on the device and the network. It recognizes unusual behavioral patterns, access attempts arising from questionable grounds, and exposure to vulnerabilities, thus issuing alerts to the user in real-time. This AI-based platform provides an added layer of defense in cybersecurity that marries technological defenses with behavioral analytics.

2. National Awareness and Digital Literacy Programs:
i) To make cybersecurity a subject in the school curriculum.
ii) Establishing a senior citizen's helpline for cybersecurity.

3. Changes to Laws and Policies:
i) Imposing severe sentencing on cyber offenses involving psychological manipulation.
ii) Establishing fast-track courts specifically dedicated to cybercrime cases for quicker delivery of justice.

IV. CONCLUSION

These days, cybercrime is this psychological battlefield wherein human weaknesses are exploited, beyond being a technical concern. When addressing these, one needs to understand that coming from an amalgamation of technology, education, and psychological perspectives is invaluable. Therefore, an understanding of the psychological tricks operated by scammers and the education of potential victims will empower that human firewall, thus making cyberspace safer.

REFERENCE

[1] CERT-In Annual Report 2024. Available: https://www.cert-in.org.in/
[2] "Gaming Scams on the Rise: Protecting Children in India, "Times of India",2023.
[3] "The Psychology of Cybercrime," Cybersecurity Journal,2022.
[4] "Elderly Financial Fraud Cases in India," Economic Times, 2021.
[5] Reuters, 2024
[6] Secure Frame Cybersecurity Report 2024
[7] ABA Banking Journal, 2023

Books:
[1] Dark Psychology in Cybersecurity: Defending Against Psychological Manipulation'
[2] 'The Psychology of Fraud, Persuasion and Scam Techniques' by Martina Dove
[3] 'Hacker Mindset: Psychological Tactics and Strategies for Mastering Social Engineering'
[4] 'Scammer's Mind: Discover the Secrets of Scammers and Protect Yourself' by Aamir Afaq Khan