Computer Fraud and Security
ISSN (online): 1873-7056

Hacking Human Beings? Addressing the Latent Danger of Social Engineering in the Indian Banking System

Prof. Rajbir Singh[1], Dr. Satpal[2], Garima Dahiya[3]

[1]Professor (Dept. of Management Studies from Deenbandhu Chhotu Ram University of Science & Technology, Murthal, Sonipat)

[2]Associate Professor (Dept. of Management Studies from Deenbandhu Chhotu Ram University of Science & Technology, Murthal, Sonipat)

[3]Research Scholar (Pursuing PhD in Dept. of Management Studies from Deenbandhu Chhotu Ram University of Science & Technology, Murthal, Sonipat)

Abstract

Digital communication technology has enabled faster and more convenient human-to-human contact. Personal and sensitive information might be exposed online due to inadequate security measures on social networks and services. Malicious users can easily breach communication networks through social engineering assaults due to their vulnerability. These assaults target individuals or organizations by fooling them into revealing personal information, including PINs, account numbers, and passwords. The widespread use of digital payment methods has led to an increase in transactions and information sharing via electronic media. This has led to hackers who use illegal tactics to gain cash. In the age of globalization, social engineering is a common form of deception that is intricately linked to numerous instances of unfair behavior. Social engineering is dangerous to network security because it exploits people's trust. Curtailing this danger presents a serious security. This study investigates social engineering as a significant cybersecurity issue, exploiting human contact to defeat security mechanisms and obtain access to computer systems or networks. It should be seen as research that detects social engineering hazards and aims to encompass all the facets of a given crime, besides giving an introduction to prevailing cyber threats and emerging dangers of social engineering in the purview of Indian banking. The paper also delves into the most prevalent forms of social engineering cyberattacks that often target humans, who are seen as the weakest links in the organization. The study gives striking details of the global regulatory environment of cybersecurity and concludes with ways to mitigate the risk of social engineering upon unsuspecting institutions.

Keywords: Social Engineering, Technology integration in banks, Cyberattack, Forms, Traits, Mitigation, Global Practices

1. INTRODUCTION

Since the inception of electronic banking, some dishonest people have tried to get past its security measures to steal customers' data. Hence, data security has become a crucial concern as the world evolves and becomes more interconnected through technological advances and developments. Computer-related or cybercrime has become a more widespread and significant threat to people, society, and the economy. The proliferation of internet-enabled banking systems has led to a surge in security risks for consumers and institutions. One of the primary challenges of contemporary banking businesses is the management of information assets. The social engineer's greatest asset is human nature. Humans are naturally inclined to trust one another and enjoy serving those in need. To accomplish their intent, the attacker must first build trust with the target to gain personal information, such as account number or password. Social engineering refers to the strategy used by hackers to get banking customers' financial and personal information. It exploits a flaw in human behaviour and takes advantage of a person's gullibility.

Recently, financial services have become a threat to information security. An information system's integrity must be built to secure its privacy, reliability, and accessibility. Given the contemporary global economy's information-intensive characteristics, which are fuelled by the advent of the Internet and the Web, it's obvious that information security is becoming a bigger concern for most firms (Mitnick & Simon, 2009). In contrast to the traditional risks, social engineering hazards are mostly the result of human action and have received less scrutiny lately. Social engineering poses dangers and

vulnerabilities, so implementing information security defenses in the banking sector requires a holistic approach. The information security solutions market currently exists for the technological aspect of thwarting conventional safety threats.

Subject matter experts generally agree that sincere but negligent employees, specialists, merchants, and other partners pose as much danger to a company's privacy as anonymous attackers from outside. 90% of effective assaults or incidents are due to human faults or behavior (Kelly, 2017). Valuable lessons are sometimes credited with social engineering, a combination of electronic, tangible, and behavioral trickery to dupe people into giving proprietary corporate or sensitive data that can be fraudulently abused. Social engineering is a form of attack that employs interpersonal communication to persuade people to violate conventional safety standards, processes, and guidelines to gain control over networks, servers, or physical locations for monetary or other purposes.

Cybersecurity inertia, which occurs when management fails to identify, plan, and fund appropriate cybersecurity measures, regularly tests, scans, updates, maintains, and backs up systems, computer programs, and storage media, and adequately trains staff to recognize and report cyberattacks and pretexting overtures, is frequently blamed on both public and private organizations. The human element is held accountable for security's weakest point because of its cultural, societal, and behavioral flaws. (Angwin, 2014; Garrett & Danziger, 2008). Even if social engineering approaches have changed, the effectiveness of these assaults still depends on security measures, contemporary preemptive technologies, and the availability of qualified individuals in organizations who can handle sensitive data. (Smith, *et al.* 2013).

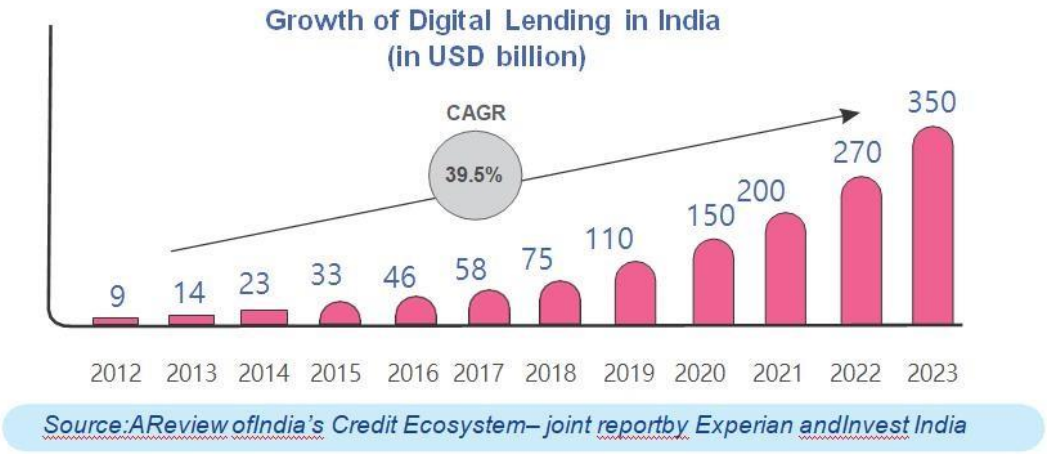
Using innovative and engaging training, and awareness campaigns, organizations hope to provide staff members with the most recent preventive techniques for avoiding social engineering threats. The measures that have been undertaken encompass the implementation of legislative and regulatory frameworks, training materials, and instruction on the safety precautions that need to be done both before and after attacks. Organizations should emphasize the worth of ongoing vigilance by hosting timely information security awareness campaigns alongside regular training. When it comes to defending an organization's interests from socially engineered attacks, employees are the most crucial factor. To secure their data, organizations choose to conduct information security awareness programs. (Aldawood *et al.* 2018). In all, 1714 and 135 phishing attacks were recorded until April 2022 and 2023, respectively. Within 24 to 48 hours, all phishing websites were removed in collaboration with the relevant service providers (Sinha, 2023).

1.1 INTEGRATION OF TECHNOLOGY IN INDIAN BANKS

The current environment has undergone tremendous transformation in the past decade. These accelerated transformations are evident in the banking and insurance industry as well. With the introduction of Internet technology, especially after 1995 banking organizations started to use such applications not only in banking operations but also in areas related to customer service. Many empirical research initiatives have been carried out on technological developments in the banking sector.

The Indian banking sector has thrived by introducing digital channels such as Internet banking, mobile banking, and Unified Payment Interfaces to provide 24/7 customer service. The sector is always evolving to offer consumers the best possible digital services. The Reserve Bank of India (RBI) and the Indian Banks Association formed the National Payments Corporation of India (NPCI) in 2008 to provide comprehensive assistance to all retail banking delivery channels (NPCI 2020).

An increase in the use of digital banking is opening doors for dishonest people to commit crimes. Fraudsters can more easily breach digital channels for financial gain than they can with traditional brick-and-mortar channels. Social engineering is the primary method to commit cybercrimes by infiltrating and infecting computer systems. Cybersecurity specialists refer to "social engineering" as attacks that manipulate humans to divulge sensitive information in digital networks. The most significant threat actors who could endanger organizations are disgruntled or inadequately trained personnel. An employee's carelessness or ignorance in responding to a phishing email could allow hackers to get access to the company's network. The primary cause of this is the lack of knowledge about the latest assault strategies used by social engineers. (Logsign 2020).



Source:AReview ofIndia's Credit Ecosystem– joint reportby Experian andInvest India

1.1.1 *MAJOR CYBER ATTACKS IN INDIAN BANKS*

According to information obtained from the Reserve Bank of India (RBI) through a Right to Information (RTI) application filed by Moneycontrol, Indian banks have seen a concerning surge in fraudulent activities, with a staggering Rs 5.3 lakh crore in frauds reported in the last ten years (2013-14 to 2022-23). The numbers show a concerning trend, with both, private and public sector banks reporting a total of 4,62,733 fraud cases throughout the year. Maharashtra has the most reported scams, followed by Delhi, Haryana, Tamil Nadu, and Uttar Pradesh.

Experts link the increase in fraud to the rising use of digital banking services. Customers are increasingly relying on bank applications for a variety of services, resulting in a rise in fraud complaints.

Description	Amount
Total amount of bank frauds (2013-14 to 2022-23)	Rs 5.3 lakh crore
Total number of fraud cases reported	4,62,733
Fraud cases through cards and Internet banking (FY23)	6,659
Total fraud cases reported (FY23)	13,530
Fraud cases through cards and the Internet (FY22)	3,596
Total fraud cases reported (FY22)	9,097
Fraud cases through cards and the Internet (FY21)	2,545
Total fraud cases reported (FY21)	7,338

Assaults and the possibility of deception (phishing) and data breaches pose problems for the growing use of online banking (Dam and Deshpande 2020). According to the Verizon 2020 Data Breach Investigations Report (Rashid 2020), phishing is the leading threat actor linked to breaches. With a 393 percent rise in attacks over the previous year, the financial and insurance industry had the greatest number of phishing attempts (India ranks third globally for phishing attacks behind the US, UK: Report, 2024).

Overview of notable cyberattacks in Indian banks

- **Heist in Cosmos Bank:** In August 2018, an exceedingly sophisticated cyberattack stole Rs 94 crores from the Pune branch of Cosmos Bank**.** By getting into the main server, the hackers transferred the cash to a bank located in Hong Kong. Furthermore, the hackers were able to access the ATM server and gather data regarding many VISA and Rupay debit cards. The bank and the account holders were unaware that money was being transferred as a result of the attack on the switching system, which connects the payment gateway to the centralized system.

According to the global cybercrime case study, 14,000 transactions involving 450 cards were made in 28 different countries. Across the country, 2,800 transactions using 400 cards were made.

- **Citibank Call Center Fraud:** A few former workers of MPhasiS Ltd, MsourcE's BPO division, conned US Citibank customers out of around Rs 1.5 crores. It was one of those cybercrime situations where several issues were brought up, including the significance of "data protection." It is clear that "Unauthorised Access" to the consumers' "Electronic Account Space" was used to commit the crime. As such, it falls under the category of "Cyber Crimes".
- **SIM Swap Fraud**: Two Navi Mumbai guys were taken into custody in August 2018 on suspicion of cybercrime. Through illegal means, they were able to access the SIM card credentials of numerous individuals, and they proceeded with fraudulent activities, including the transfer of money from their banking accounts. These con artists stole people's personal information and then blocked their SIM cards with fake documents so they could use them for online banking. It was their responsibility to transfer 4 crore Rupees from numerous accounts. They even attempted to break into several firms' accounts.
- **ATM System Hacked in Kolkata**: Almost 20 lakh rupees were taken out of several bank accounts in July 2018 after fraudsters gained access to Canara Bank ATM servers through hacking. Over fifty people were identified as victims, and it was thought that they possessed the account information of over 300 ATM customers in India. The hackers performed a minimum transaction of INR 10,000 and a maximum transaction of INR 40,000 per account by using ATM skimming devices to acquire debit cardholder information**.**
- **Attack on Union Bank of India:** In July 2017, there was another catastrophic cyberattack that sent shockwaves around the world. The Union Bank of India, one of the largest banks in India, was the target of the attack. An employee's opening of an email attachment set off the attack. There was a virus in this email attachment. It made it possible for the hackers to access the bank's network and make use of its data. An email from the central bank was faked in the attachment. The employee disregarded the information and trusted the email, which led to the start of a virus attack that gave hackers access to the bank's data and the theft of Union Bank's SWIFT (Social Worldwide Interbank Financial Telecommunication) access credentials. International transactions use SWIFT.
- **BharatPay Hacked:** A serious data breach at the Indian electronic financial services business BharatPay in August 2022 resulted in the exposure of around 37,000 customers' personal data and transaction details. Hackers have gained access to user identities, hashed passwords, mobile numbers, UPI IDs, and business email addresses of employees of insurance and banking companies in India. The problem was discovered on August 13 by XVigil, CloudSEK's threat intelligence division. It was found that a cybercrime website had obtained access to BharatPay's core database, which included transaction data from August 2022 to February 2018 as well as bank balances and personal information of consumers.

Human errors have caused significant losses at the bank level, as revealed by root cause analysis. Unknowingly providing information or clicking on unknown links might allow attackers to access a bank's internal network or customer accounts. Data breaches and attacks typically entail phishing attempts to gain password details

2. OBJECTIVE OF THE STUDY

1. To study the phenomenon of social engineering.
2. To analyze the types of social engineering attacks.
3. To suggest preventive measures to combat online social engineering attacks.
4. To analyze the global best practices in cyber security.

3. SOCIAL ENGINEERING

Nowadays, the most popular method for infiltrating and infecting computer networks and information technology (IT) assets to do cybercrimes is through the use of social engineering techniques (Abraham and Chengalur-Smith, 2010, 183). It stresses the "human factor" in cybercrimes. Social engineering is the practice of coercing others into disclosing private information. Phishing is the most prevalent kind of attack, wherein unsuspecting users are tricked into clicking on a fake link, enabling hackers to infiltrate the system and install malware. As a result, social engineering attacks mix technical exploitation with social interactions, making it challenging for cybersecurity specialists in organizations and government departments to design efficient solutions. At the Mobile World Congress in Barcelona, a senior executive from cloud

communications company Tanla Platforms stated that approximately 30 crore people in India are susceptible to phishing attempts, of which 5 lakhs might become victims of con artists (Awasthi, 2023).

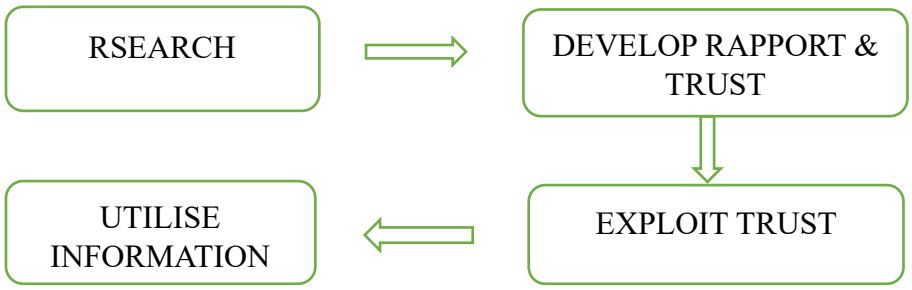
Currently, social engineering assaults pose the greatest risk to cyberspace. They are detectable, but not preventable. Social engineers use people to obtain confidential information that can be sold on the dark internet and black market, or used for specific objectives. It is a widely held belief that scammers mainly target the unsuspecting and that personal information is what they want. Nonetheless, organizational data can also be retrieved through social engineering techniques. Workers who are not taught to reply to scammer inquiries could endanger companies.

Fraudsters use characteristics of human behavior to induce employees to share confidential information. This includes:

- **Want to be courteous**: Professionals are trained to be polite and helpful to clients, especially those in client-facing roles, but in order to respond as soon as possible, they sometimes overlook the significance of double-checking information requests. This led to unauthorized information exchange.
- **Tendency to believe:** Fraudsters perform extensive background research to create situations that build confidence with their victims. This includes providing genuine information about the subject to gain his or her trust and reduce suspicion.
- **Human desires:** Many successful social engineering assaults have been rooted in the greed of individuals, in which the subject is promised something desirable in exchange for confidential information. Greed and unlimited human desires can hamper judgment temporarily and turn the target into a puppet in the hands of the criminals.
- **Desire to avoid unethical practices:** Creating fables about tax defaults, non-payment of fines, and so on is a common way to fool people into giving up their confidential information, as citizens are often weary of handling government authorities such as the tax department, municipal corporation, and police.

3.1 SOCIAL ENGINEERING ATTACK CYCLE

Social engineering follows a consistent sequence with similar stages. The typical assault pattern consists of four steps: (1) collecting data about the victim, (2) maintaining a connection with them, (3) carrying out the attack, and (4) leaving no trace. Kevin Mitnick created a cyberattack cycle at the beginning of the 2000s. The cycle is separated into four phases: investigation, creating rapport and trust, leveraging trust, and using information.



Source: Mouton et al. (2014).

The Research stage is the initial stage of an attack, and it is primarily concerned with target monitoring, gathering data on the intended victim to plan the attack tactic. The next phase is the trust stage, which involves building rapport with the subject by pretending to be someone they know, showing a desire to help, or taking on a position of authority to acquire inside information (Lohani 2019). Mitnick refers to the third stage as the exploitation. Various approaches are utilized to induce the victim's desired mental state, from which exploitation might occur. The details can be recovered once the target is experiencing the right emotions. The information is used to fulfill the attacker's goal in the last stage of the attack procedure (Mouton et al. 2014).

3.1.1 *ASPECTS OF ATTACKS UTILISING SOCIAL ENGINEERING*

Attackers using social engineering concentrate on the predator's use of confidence and persuasion. Victims of these attacks are inclined to act in the attacker's desired manner. The majority of attacks will trick the target into acting in these ways:

- **Emotional manipulation**: In interactions, attackers benefit from elevated feelings. People with high emotional states are more likely to act erratically or dangerously. The following feelings are equally effective in persuading the target: Anger, shame, dread, enthusiasm, interest, and grief.
- **Emergency**: Critical opportunities are another tactical weapon in an attacker's arsenal. The person may be motivated to compromise the sensitive information requiring rapid treatment. Alternatively, an individual may be lured to a prize or reward if they act immediately. Either strategy overpowers critical thinking skills.
- **Trustworthiness:** Reliability is essential and crucial in an attempt at social engineering. The attacker would eventually try to obtain trust in this circumstance. Attackers have enough information about the victim to fabricate a plausible story that is unlikely to cause suspicion.

These features do have certain caveats. Attackers may use simpler social engineering methods to obtain vital information. A perpetrator might, for instance, use the food court at an office building to "shoulder surf" people using laptops. This may expose many login details and passwords without distributing malicious malware or fraudulent emails.

3.1.1.1 FORMS OF SOCIAL ENGINEERING ATTACKS

Social engineering attacks are of two types: man-based and technology-based attacks.

Human-based assaults include a scenario when the attacker physically interacts with the target to obtain crucial information for exploiting it. These assailants are capable of hitting multiple targets at once. Software-driven assaults use laptops, desktops, and cell phones among other devices to obtain confidential data from their targets. They can take advantage of lots of individuals quickly.

1. **Man-based Attacks**

Human-based attacks target individuals' emotions, including thoughts, feelings, behavioral responses, and pleasure/displeasure. A deception tactic known as "social engineering" takes advantage of people's emotions to access confidential information. The word "engineering" describes the scientific understanding of design procedures, apparatus, or buildings. Techniques and technology are used to exploit emotional patterns.

- **Shoulder surfing**
  The direct observation techniques, including peering over someone's shoulder, to obtain private information, is known as "shoulder surfing." It is quite simple to stand next to someone and watch them complete a form, enter a password at an automated teller machine, pay for anything with a credit/debit card, or pay using UPI to collect data in busy places. Shoulder surfing can also be practiced using binoculars or other equipment that improves vision. When an individual is on the phone addressing confidential matters and a colleague is seated next to him, eavesdropping and taking notes is a manifestation of shoulder surfing.
- **Tailgating Attacks**
  Tailgating attacks, piggybacking, or physical access involve accessing a place or facility by following a person who has security clearance to that place. It allows criminals to access unauthorized buildings without permission. For instance, attackers might ask a target to hold the entrance unlocked as they forgot their RFID (radio-frequency identification) card or workplace Identity card. Additionally, they can use a loaned system or cell phone to carry out illicit acts like using spyware. (Xiangyu et al. 2017).
- **Baiting Attacks.**
  In Baiting assaults, scammers ask people to click a link to receive goodies for free. These attacks, like Trojan horses, use insecure computer components like storage media or USB drives to spread virus-infected files to

victims in public places. The USB drive functions as a real-world Trojan horse and infects system resources when victims plug it into their desktop computers.

- **Pretexting Attacks**
  Pretexting assaults involve creating fictitious scenarios to get a target's critical data. They are based on excuses that make the victim believe the person committing the crime. Criminals use public resources such as phone books, websites, and conferences for assault. The pretext might be a proposal to complete a task or obtain employment, a request for private information, helping an acquaintance obtain access to confidential information, or hitting a jackpot.
- **Quid Pro Quo Attacks**
  It translates as "a favor for a favor," and in the context of phishing, it refers to the exchange of confidential data for a reward or other consideration. The attack happens after enticing an individual about something valuable that requires little investment on the part of a person, and then the attacker simply steals data.
- **Dumpster Diving**
  It is the act of digging through trash or recycling cans for objects that can be repurposed or reused. It can also mean looking for important information that could be utilized in cyber assaults.
- **Rubber Hose**
  In cryptography, rubber hose, in contrast to technical cryptanalytic attack, cryptanalysis is a euphemism for extracting cryptographic secrets (for example, the password to an encrypted file) from a person through compulsion or torture—such as pounding that person with a rubber hose, hence the name.
- **Vishing**
  A vishing attack or a voice phishing attack is a type of cybercrime in which a fraudster utilizes the phone to deceive someone into disclosing personal information such as financial credentials or passwords. A vishing attack aims to get confidential information that can be utilized for identity theft, monetary gain, or hacking of an account.
- **Impersonation**
  An impersonation attack is a sort of cybercrime in which a criminal impersonates a familiar individual or institution to seize sensitive information or cash. Hackers utilize social engineering techniques to assume an ID, either by hacking an account or by creating the same account, and then urge unsuspecting targets to perform acts such as paying dues, sharing a file, or clicking a link.
- **Eavesdropping**
  This attack involves hacking, intercepting, deleting, or altering data sent between two devices. Eavesdropping, also known as sniffing or snooping, uses unsecured network communication to steal data between systems.

2. Technology-based Cyberattacks

- **Phishing**
  To trick the victim into disclosing confidential data and other assets, attackers pretend to be from credible organizations or persons. India had 79 million phishing attacks in 2023, according to a recent study by Zscaler, a cloud security business with its headquarters located in California. According to the report, the United States ranks first among the top nations targeted by phishing attacks in 2023. India is in third place while the UK is in second place (Sharma, 2023). Phishing attacks can happen in the following ways:

  Spam phishing: Also known as mass phishing, it involves a huge attack that targets a large number of users with unsolicited emails. These emails are not personal and aim to engage any unwary victim.
  Spear phishing: Spear Phishing, also known as whaling, exploits confidential information to target specific people. Cybercriminals can use a "whaling attack" to act as a senior employee or another important person within an organization and target them directly to steal money, valuables, and critical data, or gain access to computer systems for illegal reasons.
  SMS phishing (smishing): It uses fake texts or messages that trick people into downloading malicious software or a virus via a bogus email address, phone number, or a fake website link.
  Search engine phishing: It involves placing links to bogus or fake websites at the top of search engine results using legitimate optimization strategies. These may be in the form of sponsored advertisements or legitimate websites containing fake web links.

URL phishing: URL phishing links lure victims to fake and bogus websites. These links are frequently forwarded by emails, mobile phone texts, social media messaging, and online advertisements. Attackers hide links within hyperlinked text by employing link-shortening methods or fraudulently spelled URLs.

In-session phishing: Pop-up ads and web links during login might occasionally create frequent disruptions during regular web browsing. For example, when browsing, one may encounter bogus or fake login pop-ups for the web pages.

Email phishing: It is the most popular sort of phishing, as it uses spam email infused with bogus web links, virus-infected files, and malware attachments to urge and lure the target to respond or follow up in another way.

Angler phishing occurs on social media when a cybercriminal impersonates a reputable company's customer service representatives. To access the confidential information of the victim, attackers intercept exchanges with a brand to hijack and redirect the conversation into a private chat, eventually leading to a leak of sensitive information.

- **DNS spoofing and cache poisoning attacks**
  When a legitimate URL is entered, DNS spoofing directs browsers and servers to malicious and fraudulent websites. Once a URL has been compromised by this technique, the reroute will continue until the compromised machines remove the erroneous routing information. Attacks using DNS cache poisoning infect legitimate URLs with routing directives that point to fraudulent websites.
- **Fake Software Attacks**
  Fake website attacks occur by making victims believe and trust that the given website or software is original and trusted. The unsuspected target enters login details into the bogus website, giving access to hackers of all the sensitive data that is used to retrieve online bank accounts and other accounts. One such danger is the tab nabbing attack, which consists of a counterfeit domain and webpages that mimic the login interface of a well-known website that the target frequently visits, such as Facebook, Instagram, Twitter, or online banking, to name a few (De Ryck, 2013).

4. MITIGATION OF SOCIAL ENGINEERING ATTACKS

Digital India has increased the use of cashless transactions and digital currencies. It is crucial to implement comprehensive security measures to protect data and privacy. Banks collect a large amount of clients' data, including name, address, phone number, PAN, Aadhar, and identity proof. The most concerning aspect of cybersecurity is humans. Negligent personnel can breach even the strongest security procedures and systems, with disastrous results for the company. It is more difficult to ensure social engineering remediation than hardware security (Hadnagy, 2011). According to Hadnagy (2011), traditional and perpetual defensive security involves investing in intrusion detection, firewalls, antimalware, antivirus, and other security technologies. Unfortunately, there are no software tools and ways that can protect humans from social engineering attacks.

Samani and McFarland (2014) identify three types of mitigation measures to reduce the chances of social engineering attacks. They are people, processes, and technology. They are as follows:

People

- Personnel should be aware and informed of policies and have clear escalation channels for any requests that exceed their authority.
- To gradually enlighten staff, every organization should implement a security awareness and training program. Staff should be trained by using tools like the McAfee Phishing Quiz that illustrate specific strategies and ways used in cyberattacks.
- Give employees the courage to challenge even seemingly benign requests. To prevent tailgating, challenge individuals who seek to enter offices.
- Even seemingly benign information, like phone numbers, might be utilized to conduct an assault.
- Punishing individual employees who were duped and attacked will make all employees less inclined to disclose information when faced with a similar scenario.

Process

- After detecting suspicious activities, workers should report the contact in detail. This facilitates investigations.
- When employees encounter a dangerous web website, utilize a block page to explain why they can't proceed. Reflecting on previous actions can help detect potential sources of assault.
- Organizations should consider their communication with customers. Whenever a customer is not entitled to access any information, the organization should inform and confirm it. PayPal provides tips to assist users in identifying authentic emails. "A genuine and original email from PayPal will never request bank account details, or debit/credit card information. We never ask for your complete name, account password, PIN, OTPs, or answers to PayPal security questions by email or text"
- Give front-line employees and workers a clear reporting channel or structure so they can report any concerns about potentially counterfeit messaging.
- Regularly assess staff vulnerability to social engineering assaults across numerous communication channels. This can help to measure the success of training and other educational programs.

Technology

- Record phone calls for federal and state eavesdropping regulations for investigation purposes.
- Send questionable calls to a monitored number for verification.
- Delete fake emails and texts that contain malware, both known and unknown.
- Block harmful websites and identify viruses while accessing the internet.
- Using multifactor authentication can make it more difficult for attackers to steal users' authentication credentials, but it does not eliminate the possibility of social engineering.

Effective security rules and procedures require regular implementation by personnel. They provide norms and guidance to reduce the danger of social engineering assaults. These regulations are particularly important for preventing and identifying social engineering assaults. It's critical to understand that security procedures and regulations change over time. Policies must be updated to reflect changing corporate needs, emerging security technologies, and evolving vulnerabilities.

Knowledge is a true power. Hence, education can be used as a defense strategy against most social engineering attacks (Hadnagy, 2011). Education and training programs are essential for preventing social engineering attacks. These should encompass safety procedures, policies, practices, and planning to prevent social engineering assaults. To create a successful training and awareness program, it is important to identify the root cause of vulnerability and threats.

To avoid becoming a target of social engineering, employees should slow down the pace, research for original details, avoid unwanted requests for financial data or passwords, be cautious in downloading, reject help offers from unknown sources, set spam filters, avoid clicking on links, recognize fake offers, and use secure computing devices. Security via education requires a mission statement rather than just a catchphrase.

4.1 DATA PRIVACY IN BANKS

A cybersecurity framework that should be used at all banking levels has been released by the RBI. Still, it's crucial to comply in spirit. Occasionally, low funding and top management's lack of cybersecurity experience make compliance challenging. Top management awareness and participation are essential for putting cybersecurity safeguards in place in banks. A comprehensive security approach with top-to-bottom protection ought to be employed to mitigate the risks associated with social engineering. An organization's main priorities should be preventive security measures, which include education, technical controls, access restrictions, and security policies.

At the bank branch level, stringent internal controls must be put in place to ensure adherence to cybersecurity policies and processes. Workers ought to receive regular training on the latest methods of social engineering. Vendors also need to be aware of security rules and attack methods. For services that are outsourced, a properly executed non-disclosure agreement is required to protect confidential information. Phishing drills are a useful technique to gauge users' awareness and response levels. It is an aggressive technique whereby known operatives craft attack scenarios and purposefully send phishing emails to employees pretending they are legitimate. This method helps determine the degree of system vulnerability by attempting to access privileged data using the same strategies employed by social engineers. These exercises ought to be regularly held by banks to strengthen employees. Suspicious activities can be detected with the aid of fraud control techniques and

tools, hence lowering customer-end fraud. The data can be analyzed using data mining techniques to find questionable behavior patterns (Mishra et al., 2019).

5. GLOBAL BEST PRACTICES IN CYBER SECURITY

According to the International Telecommunication Union's June 29, 2021, report of the Global Cybersecurity Index 2020, India has risen 37 spots to take the tenth spot as the world's best nation. India now ranks fourth in the Asia Pacific area, demonstrating its commitment to cybersecurity.

GCI assessments evaluate cyber security effectiveness across five parameters: legal, technological, organizational, capacity development, and cooperation. The performance is combined to create an overall score.

According to (Sinha, 2023), Global Best Practices for Tackling Fraud are:

- The United Kingdom has implemented a Contingent Reimbursement Model Code for Authorised Push Payment (APP) scammers, which aims to compensate victims of fraud in situations where the bank or payment gateway is deemed at fault, provided that the consumer has complied with the Code's requirements. Currently, in other parts 59 of the world, customer education is widely resorted to avert such frauds and no code exists. This may be another area where “codes” for customers may be formed by regulators.
- Within its mandate, the Single Supervisory Mechanism (SSM) of the European Central Bank (Euro Area Central Bank) generates a cyber-risk profile for every bank. There is a particular element to its method for conducting on-site inspections. For managers who are not present on-site, it also offers analytical devices.
- Authorities are heading towards a testing approach for evaluating cyber-risk resilience and vulnerability that is intelligence-led or threat-informed. An intelligence-led paradigm assesses a bank's cyber-risk resilience and vulnerability past the scope of a modeled cyberattack. The quality of the intelligence obtained and the banks' detection and response capabilities are then evaluated to determine whether or not the banks' degree of information security corresponds with the digital risk they encounter. Examples include the CBEST Threat Intelligence-Led Assessments in the UK, the intelligence-led Cyber-attack Simulation Testing Framework from the Hong Kong Monetary Authority, and the TIBER (Threat Intelligence-Based Ethical Red Teaming) Framework from the Netherlands Bank.
- For every financial institution or just a subset, regulatory instruments to evaluate cyber-risk strengths and weaknesses can be optional. Banks can voluntarily utilize the Cyber-security Assessment Tool (CAT) from the Federal Financial Institutions Examination Council (FFIEC) and the Cyber-security Framework (CSF) from the US National Institute of Standards and Technology (NIST) to evaluate their digital risk.
- It appears managers from different regions actively share customs, yet greater coordination and cooperation between managers is possible.

Global Best Practices	Indian Context
Authorized Push Payment (APP) Frauds in the UK within the ambit of Contingent Reimbursement Model Code: Compensation of victims of fraud in any scenario where the bank or payment gateway is deemed at fault, provided that the client satisfies the code's requirements.	The UK is one of the few countries to adopt such a code.
The Single Supervisory Mechanism (SSM) of the European Central Bank (Euro Area Central Bank) has a specific component in its approach for physical inspections for cyber threat assessment of banks.	The first component of the European Banking Union is the Single Supervisory Mechanism (SSM), which is the regulatory and legislative structure that grants the European Central Bank (ECB) oversight over Ebanks of the EU.

	RBI has a comprehensive Cyber Security Framework for Banks. However, “cyber risk profiling” is not categorically mentioned in that framework.
Authorities are moving towards an evaluation strategy for evaluating security risks, resilience and vulnerability that is intelligence-led or threat-informed. For instance, the Hong Kong Monetary Authority's iCAST (Intelligence-led Cyber-attack Simulation Testing) Framework.	Though RBI’s Cyber Security Framework for Banks, dated 2nd June 2016, has provision for only testing.
Regulatory measures can evaluate cyber-risk resilience and vulnerability required for every financial institution or only a subset of them, such as the Cyber Security Framework (CSF) developed by the US National Institute of Standards and Technology (NIST).	As per RBI’s Cyber Security Framework for Banks dated 2nd June 2016, there is a need for a Board-approved Cyber-security Policy

6. CONCLUSION

In daily life, people abuse their "disease to please" and their inability to say "no" more often. Cybersecurity has been greatly impacted by social engineering, and it might not be long before someone targets staff members at your company. Physicians, psychologists, and therapists frequently employ manipulation to get their patients to conduct beneficial acts. But social engineers also make extensive use of all sorts of persuasion and manipulation. Finding a solution for a technological issue is simpler than finding a solution for people's ignorance.

The ability of the internet to distribute emails widely and the prevalence of social engineering means that it's critical to recognize the telltale signs of a scam. It is also critical to comprehend the three sorts of controls—people, process, and technology - employed to reduce the danger of social engineering. For an organization's security, security technology and policies are crucial, and when they are paired with the right training, it is the best way to reduce social engineering.

Social engineering assaults are increasing in tandem with the expansion of digital banking practices. Despite banks' understanding of cybersecurity, it is insufficient to stop fraudsters from their schemes. Constant awareness-raising efforts and consideration for security policy are crucial. Users must first understand what information is secret or delicate and why it should not be shared with outside parties. Likewise, they ought to be informed of the consequences of sharing data. To raise awareness and prevent repetition, banks should post information regarding cyber incidents, the unfortunate events that led to them, and the reasons behind them on public forums. Fighting social engineering attack techniques and cybercrime requires cooperation from the government, bankers, and regular people. Everyone's dedication to this initiative will get the nation closer to averting losses and increasing customer confidence in digital banking.

Since there are constantly new dangers and weaknesses to be aware of, the worry arising from social engineering is more like an unending "journey" than a "destination by itself."

REFERENCES

1. Aldawood, H., Skinner, G. A. (2018). Critical Appraisal of Contemporary Cyber Security Social Engineering Solutions: Measures, Policies, Tools and Applications. In Proceedings of the IEEE 26th International Conference on Systems Engineering, Sydney, Australia.
2. Angwin, J. (2014). Dragnet Nation: A quest for privacy, security, and freedom in a world of relentless surveillance. New York: Times Books.
3. Awasthi, R. (2023, March 3). Around 5 lakh people potentially fall victim to phishing scams in India: report. The Economic Times.

4. Dam, L., and Deshpande K (2020): "Relationship Between Demographic Variables and Awareness of Cybersecurity Threats: An Empirical Analysis", The Orissa Journal of Commerce, Vol. 41, No. II, pp 112-122
5. De Ryck, P.; Nikiforakis, N.; Desmet, L.; Joosen, W. Tabshots: Client-side detection of tabnabbing attacks. In Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, Hangzhou, China, 8–10 May 2013.
6. Garrett, R. K., & Danziger, J. N. (2008). On cyberslacking: Workplace status and personal Internet use at work. Cyberpsychology & Behavior, 11(3), 287-292.
7. Hadnagy, C. (2011) Social Engineering: The Art of Human Hacking, Indianapolis:Wiley. http://sin.thecthulhu.com/library/security/social_engineering/The_Art_of_Human_ Hacking.pdf
8. India ranks third globally for phishing attacks after US, UK: Report. (2024, August 25). Business Standard.
9. Kelly, R. (2017, March). 90% of Cyberattacks are caused by human error or behavior. Chief Executive Online.
10. Lohani, S. (2019): "Social Engineering: Hacking into Humans", International Journal of Advanced Studies of Scientific Research, Vol. 4, No.1.
11. Mishra, R., Lavanya S, Likitha, V. S., Sree, B. B and Mukesh K. (2019): "Analysing Human Behaviour for Financial Fraud Detection", International Journal of Emerging Technologies and Innovative Research Vol. 6, No.3, pp 384–388.
12. Mitnick, K. D., & Simon, W. L. (2009). The art of intrusion: the real stories behind the exploits of hackers, intruders, and deceivers. John Wiley & Sons.
13. Mouton, F., Malan, M. M., Leenen, L., and Venter, H. S. (2014): "Social Engineering Attack Framework", Information Security for South Africa, Johannesburg, South Africa, 2014, pp. 1-9, https://doi.org/10.1109/ISSA.2014.6950510
14. Rashid, F. Y. (2020): 8-Types-of-Phishing-Attacks-and-how-to-Identify-them, 24 November, https:/www.csoonline.com/article/3234716/8-types-of-phishing-attacks-andhow-to-identify-them.html
15. Sharma, D. (2023, Apr 30). India recorded over 79 million phishing attacks in 2023, new study suggests. India Today.
16. Sinha, J. (2023). Cyber Security and Rising Incidence of Cyber/White Collar Crimes. Fifty-Ninth Report, Seventeenth Lok Sabha, Standing Committee on Finance.
17. Smith, A., Papadaki, M.& Furnell, S.M. (2013). Improving awareness of social engineering attacks. In IFIP Advances in Information and Communication Technology, 406, 249–256.
18. Xiangyu, L.; Qiuyang, L.; Chandel, S. Social engineering and Insider threats. In Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Nanjing, China, 12–14 October 2017; pp. 25–34