**Understanding the Psychological Manipulations by Cyber-crime Offenders**

**1Megha Aggarwal (M.Sc. Forensic Psychology, NFSU, Gujarat)**

**ABSTRACT**

A feeling of security is a feeling of being safe and free from worry. Most of the time when we feel secure and comfortable, we reveal all the information we behold in a sudden flash of seconds it does happen with us every time we are on the internet. Cyberspace is that place in the world where we feel the most comfortable and yet it's the most dangerous place in the world. With this growing era of technology, cyberculture, and a world full of cyborgs the first word which comes to our mind when we talk about security is cybersecurity. Until now humans have developed an endless number of firewalls and other cybersecurity systems. What if we take a shift from technologies towards the creation of a human firewall? Digging deeper into a number of cyber frauds we find that most of them are just mere psychological manipulations. If we think technology can solve our security problems, then we don’t understand the problems and we don’t understand the technology".

**Keywords**: Human Firewall, cyberspace, cyberorgs, cybersecurity, cyberculture, Psychological manipulations

**1. Introduction**

Security is both an emotion and a physical reality. And they are not the same thing. There can be a difference between when we feel secure v/s when we are secure. We feel the most secure when we are on the internet with our laptops or mobile phones, but the reality is completely different. Cyberspace is the most vulnerable place in this world. Cyberspace is a place where everyone expresses themselves to the fullest without thinking about being judged or detected thanks to the anonymity feature available in this virtual world. Cyberspace is the world where we pour ourselves out and feel the most comfortable. We trust our online interactions more as compared to our offline interactions and share heaps of information. Online interactions are often based on trust, and the sharing of information and involve a degree of interdependence. High-profile cybersecurity incidents, such as the Ashley Madison website hacking, demonstrate what happens when this trust relationship is breached.

Yet despite the common media depiction, such incidents may not be the result of the archetypal hacker using technological means to get into a system. Instead, cybersecurity attacks are increasingly based primarily on social engineering techniques – the use of psychological manipulation to trick people into disclosing sensitive information or inappropriately granting access to a secure system (Tetra & Vuorinen, 2013). Information security has for a long time been a field of study in computer science, software engineering, and information communications technology. The term ‘information security’ has recently been replaced with the more generic term cybersecurity. The goal of this paper is to show that, in addition to computer science studies, Behavioural sciences focused on user behavior can provide key techniques to help increase cyber security and mitigate the impact of attackers’ social engineering and cognitive hacking methods (i.e., spreading false information)

The increasing digitization of our lives has led to an exponential increase in the amount of personal and sensitive data that is being transmitted and stored digitally. From online banking to social media, we rely heavily on the internet for communication, entertainment, and daily tasks. However, this dependence on technology comes with significant risks, including cyber-attacks and data breaches that can result in financial loss, identity theft, and reputational damage.

While technological advancements have improved cybersecurity measures, cybercriminals are becoming more sophisticated in their tactics and are targeting human vulnerabilities rather than exploiting technical weaknesses. This has led to an increasing focus on the human element of cybersecurity, which involves studying user behavior and developing strategies to address vulnerabilities such as social engineering and cognitive hacking.

Social engineering refers to the use of psychological manipulation to deceive individuals into divulging sensitive information or granting access to secure systems. This can involve tactics such as phishing emails, pretexting, and baiting, where attackers use fake personas or tempting offers to trick users into taking action that compromises their security. Cognitive hacking, on the other hand, involves spreading false information to manipulate an individual's perception of reality, causing them to make decisions that benefit the attacker.

Both social engineering and cognitive hacking rely on exploiting human vulnerabilities, such as trust, curiosity, fear, and urgency. To address these vulnerabilities, it is essential to consider user behavior and apply insights from the behavioral sciences to develop effective cybersecurity strategies.

One key aspect of addressing human vulnerabilities in cybersecurity is education and awareness. Users need to be trained to recognize common social engineering and cognitive hacking tactics and to understand the risks associated with sharing sensitive information online. This can involve awareness campaigns that highlight the importance of cybersecurity and provide tips on how to stay safe online.

Simulation and training programs can also be used to educate users on cybersecurity best practices. By simulating real-world scenarios, users can learn how to recognize and respond to potential threats in a safe and controlled environment. These training programs can be customized to target specific user groups, such as employees, students, or senior citizens, and can be designed to be engaging and interactive to increase participation and retention.

Another key aspect of addressing human vulnerabilities in cybersecurity is the design of secure systems. By considering user behavior and psychology in the design process, systems can be designed to minimize the risk of social engineering and cognitive hacking attacks. For example, multi-factor authentication can be used to reduce the risk of password-based attacks, while user-friendly interfaces can make it easier for users to identify and report suspicious activity.

In addition to education and system design, the behavioral sciences can also be used to develop more effective incident response and mitigation strategies. By understanding how individuals react to cyber-attacks, responders can develop more targeted and effective response plans. For example, by understanding the cognitive biases that can lead to overconfidence or panic, responders can develop strategies to address these biases and ensure that response efforts are effective.

One approach that has shown promise in mitigating the impact of cyber-attacks is gamification. By using game-like elements such as points, badges, and leaderboards, users can be incentivized to adopt more secure behaviors and to report suspicious activity. Gamification can also be used to encourage users to participate in training programs and to create a culture of cybersecurity awareness and vigilance.

While the behavioral sciences have shown promise in improving cybersecurity, there are also challenges associated with their application in this field. One challenge is the need for interdisciplinary collaboration between behavioral scientists, computer scientists, and cybersecurity experts. Developing effective cybersecurity strategies requires a deep understanding of both the technical and human aspects of cybersecurity, and interdisciplinary collaboration is essential to bridge this gap.

Another challenge is the need for ongoing research and innovation. Cybercriminals are constantly evolving their tactics, and cybersecurity strategies must also evolve to stay ahead of these threats.

**2. Cyber Crime**

Cybercrime refers to any illegal activity that involves the use of computer networks or other digital technologies, often to obtain financial gain or cause harm to individuals, businesses, or governments. Cybercrime includes a wide range of activities, from online harassment and identity theft to hacking, malware distribution, and cyber terrorism.

Cyber-terrorism global problem that affects millions of people every year. The rapid growth of the internet and the increasing reliance on digital technologies have created new opportunities for criminals to exploit vulnerabilities in computer networks and systems. As a result, cybercrime has become a major threat to individuals, businesses, and governments around the world.

The most common types of cybercrime include hacking, phishing, malware, and identity theft. Hacking involves gaining unauthorized access to computer systems, networks, or devices to steal or modify data, disrupt services, or cause damage. Phishing is a form of social engineering that uses fraudulent emails, websites, or text messages to trick people into revealing sensitive information, such as passwords or credit card numbers. Malware refers to any type of malicious software, such as viruses, Trojans, or ransomware, that is designed to infect computer systems and cause harm. Identity theft is the theft of personal information, such as Social Security numbers, credit card numbers, or login credentials, for financial gain or other illegal activities

Cybercrime can have serious consequences for its victims, including financial losses, reputational damage, and emotional distress. Businesses may suffer significant financial losses due to cybercrime, including the costs of repairing systems, paying legal fees and compensating customers for any losses or damages caused. Governments may also be targeted by cybercriminals, which can result in the theft of sensitive information or disruptions to critical infrastructure.

The fight against cybercrime requires the cooperation of individuals, businesses, and governments at all levels. One key strategy is to improve cybersecurity by implementing stronger password policies, using encryption to protect sensitive data, and regularly updating software and security systems. Education and awareness programs can also help people to recognize and avoid common cyber threats, such as phishing scams or malicious links.

Governments also play an important role in combating cybercrime by passing laws and regulations that address cyber threats and provide legal frameworks for investigating and prosecuting cybercriminals. International cooperation and information sharing are also critical in fighting cybercrime, as many cybercriminals operate across national borders and jurisdictions.

In conclusion, cybercrime is a growing problem that poses significant risks to individuals, businesses, and governments around the world. The fight against cybercrime requires a multi-faceted approach that involves improving cybersecurity, educating people about common cyber threats, and developing stronger legal frameworks and international cooperation to combat cybercrime. By working together, we can reduce the risks posed by cybercrime and protect the integrity and security of the digital world.

# **2.1 Types of cybercrime**

Cybercrime refers to illegal activities that are committed using the internet or other digital technologies. These crimes can take many forms, and they can have serious consequences for victims, including financial loss, reputational damage, and emotional distress. Here are some of the most common types of cybercrime, along with statistics as per current trends.

**2.1.1 Hacking**

Hacking is one of the most common types of cybercrime. It involves gaining unauthorized access to computer systems, networks, or devices with the intent to steal data, disrupt services, or cause damage. Hackers can use a variety of techniques to gain access to systems, including exploiting software vulnerabilities, stealing login credentials, or using social engineering to trick users into revealing sensitive information.

Stats: According to a study by the Center for Strategic and International Studies, cybercrime costs the global economy up to $600 billion per year, with the majority of losses attributed to hacking.

**2.1.2 Phishing**

Phishing is a form of social engineering that involves using fraudulent emails, websites, or text messages to trick users into revealing sensitive information, such as passwords, credit card numbers, or other personal data. Phishing attacks can be highly sophisticated and can use a variety of tactics, such as creating fake websites that mimic legitimate ones or using fake email addresses that appear to come from trusted sources.

Stats: According to the 2020 Verizon Data Breach Investigations Report, phishing was involved in 22% of all data breaches.

**2.1.3Malware**

Malware refers to any type of malicious software, such as viruses, Trojans, or ransomware that is designed to infect computer systems and cause harm. Malware can be used to steal data, disrupt services, or damage systems. Malware can be spread through email attachments, infected websites, or other means.

Stats: According to a study by the Ponemon Institute, the average cost of a malware attack on a company is $2.4 million.

**2.1.4 Identity Theft**

Identity theft is the theft of personal information, such as Social Security numbers, credit card numbers, or login credentials, for financial gain or other illegal activities. Identity thieves can use this information to open new accounts, make fraudulent purchases, or commit other crimes. Pictorial representation: A person holding up a wallet with a question mark, representing the idea of someone stealing personal information.

Stats: According to the Federal Trade Commission, identity theft was the second most common type of consumer complaint in 2020, accounting for 13% of all complaints.

**2.1.5Cyberbullying**

Cyberbullying refers to the use of digital technologies to harass, intimidate, or embarrass others. Cyberbullying can take many forms, including spreading rumors, posting embarrassing photos or videos, or sending threatening messages.

Pictorial representation: A person sitting at a computer with a sad face, represents the emotional impact of cyberbullying.

Stats: According to a survey by the Cyberbullying Research Center, 36% of teenagers in the United States have experienced cyberbullying.

**2.1.6Cyberstalking**

Cyberstalking is a type of harassment that involves using the internet or other digital technologies to follow or harass someone. Cyberstalks can use a variety of tactics, such as sending threatening messages, tracking someone's location through their phone, or using fake social media accounts to monitor someone's activity.

Here are three case studies of cybercrime involving social engineering:

**2.1.7The Bangladesh Bank Heist:**

In February 2016, hackers stole $81 million from Bangladesh Bank, the central bank of Bangladesh, in one of the largest cyber heists in history. The hackers used social engineering tactics to gain access to the bank's SWIFT payment system, which allowed them to transfer the money to accounts in the Philippines and Sri Lanka. The hackers had gained access to the bank's computer network by sending spear-phishing emails to bank employees. These emails contained malware that allowed the hackers to gain access to the SWIFT credentials of the bank

**2.1.8The Ashley Madison Data Breach:**

In July 2015, Ashley Madison, a dating website for people seeking extramarital affairs, suffered a massive data breach. The personal information of over 30 million users was stolen by a group of hackers known as "The Impact Team". The hackers used social engineering tactics to trick Ashley Madison employees into giving them access to the company's computer network the hackers sent spear-phishing emails to Ashley Madison employees that contained malware, allowing the hackers to gain access to the company's network.

**2.1.9The Twitter Bitcoin Scam:**

In July 2020, hackers took control of high-profile Twitter accounts, including those of Barack Obama, Joe Biden, Elon Musk, and Bill Gates, to promote a Bitcoin scam. The hackers used social engineering tactics to gain access to the Twitter accounts of celebrities and politicians. They sent spear-phishing emails to Twitter employees, posing as colleagues in the IT department, to gain access to the company's internal tools. With these tools, the hackers were able to take control of the accounts and post messages asking followers to send Bitcoin to a specific address.

**3. Jamtara**

Jamtara is a district in Jharkhand, India that has become known for cybercrime. Criminals in the region use a variety of tactics to trick people into giving them money, often by posing as customer service representatives for banks or other companies. They will call people and ask for their bank details, then use that information to transfer money out of their accounts. They also use phishing emails and fake websites to steal personal information.

The police in Jamtara have been working to crack down on these activities, but it's a challenging task. The criminals are often very sophisticated in their tactics, and they can be difficult to track down. Many of them use public phone booths to make calls, making it harder to trace their location. The police have also faced resistance from local politicians, who have been accused of protecting the criminals.

**4. Modus Operandi of Cybercriminals**

The modus operandi of cybercriminals can vary greatly depending on the type of cybercrime they are committing, but there are some common tactics and techniques that are often used. Here are some of the most common ways that cybercriminals operate:

* **Social engineering:** This involves using psychological manipulation to trick people into giving away sensitive information or downloading malicious software. Cybercriminals might pose as a trusted entity, such as a bank or government agency, to gain the victim's trust and persuade them to share their personal information.
* **Malware attacks:** Malware is a type of software designed to infiltrate computer systems and cause harm. Cybercriminals may use phishing emails or social engineering tactics to trick victims into downloading malware onto their devices, which can then be used to steal sensitive information or cause damage to the system.
* **Ransomware:** This involves encrypting a victim's files and demanding payment in exchange for the decryption key. Cybercriminals often use social engineering tactics or phishing emails to spread ransomware, which can cause significant damage to individuals or organizations.
* **DDoS attacks:** A distributed denial-of-service (DDoS) attack involves overwhelming a server or website with traffic to make it unavailable to users. Cybercriminals may use a network of infected devices, known as a botnet, to carry out DDoS attacks.
* **Insider threats:** Insider threats refer to individuals within an organization who use their access to sensitive information or systems for malicious purposes. This can include stealing data, sabotaging systems, or selling confidential information to outside parties

The six principles of influence can be used by cybercriminals to manipulate individuals into providing sensitive information or performing actions that can result in financial loss or identity theft.

The principle of reciprocity is based on the concept that people feel indebted to someone who has done something for them or given them something without expecting a return. Cybercriminals can use this principle by posing as Good Samaritans who offer a way out of an embarrassing or career-ending situation in exchange for access credentials to a fake internal website.

The principle of consensus is when people seek the opinions of others when they are uncertain. Cybercriminals can exploit this principle by posing as charities after a disaster and collecting donations.

The principle of consistency is based on the idea that people like to act in a way that is consistent with their previously held views. Cybercriminals can use this principle by posing as IT managers and requesting access credentials under the pretext of cyber security.

The principle of sympathy is based on the idea that people are more likely to comply with a request from someone who appears sympathetic. Cybercriminals can use their charms to appear sympathetic on the phone and trick individuals into providing sensitive information.

The principle of authority is based on the idea that people are more likely to comply with a request from a high-ranking person. Cybercriminals can exploit this principle by sending fake emails from CEOs or banks, requesting money transfers or information verification.

The principle of scarcity is based on the idea that people are more likely to comply with a request when there is a perceived scarcity of time or resources. Cybercriminals can use this principle by sending phishing emails from tax authorities or other government agencies, requesting quick responses under the threat of fines or account suspension.

Overall, understanding these principles can help individuals protect themselves from cybercrime by being aware of the tactics that cybercriminals use to manipulate them. It is important to verify the authenticity of requests and to never provide sensitive information or perform actions without proper verification.

**5. Literature Review**

Understanding psychological manipulations made by cybercriminals is crucial in the fight against online fraud and scams. Cybercriminals often use various tactics to manipulate their victims into giving up sensitive information or money. One common tactic is phishing, where cybercriminals send fraudulent emails, texts, or social media messages to trick their victims into clicking on malicious links or opening infected attachments. Another tactic is social engineering, where cybercriminals manipulate their victims into divulging personal or sensitive information through human interaction.

Research has shown that cybercriminals use various psychological tactics to make their victims more vulnerable to manipulation. One such tactic is fear. Cybercriminals often use scare tactics to make their victims feel threatened or vulnerable, such as by posing as a government agency and threatening legal action if the victim doesn't comply with their demands. Another tactic is urgency, where cybercriminals create a sense of urgency and pressure their victims to act quickly, such as by posing as a bank and claiming there is fraudulent activity on the victim's account that needs to be resolved immediately.

Cybercriminals also use the principle of reciprocity to manipulate their victims. This principle suggests that people are more likely to give something back when something is given to them first. Cybercriminals often offer something of value, such as a gift or service, in exchange for personal information or money. Once the victim has given up their information or money, the cybercriminal disappears, leaving the victim with nothing.

Another psychological tactic used by cybercriminals is social proof. This principle suggests that people are more likely to do something if they see others doing it too. Cybercriminals often create fake reviews or testimonials to make their scams appear more legitimate and trustworthy. They may also use fake social media profiles or manipulate the number of followers they must create a false sense of popularity.

Furthermore, cybercriminals often use the principle of authority to manipulate their victims. This principle suggests that people are more likely to comply with someone in a position of authority. Cybercriminals may pose as law enforcement officers or other officials to create a sense of authority and intimidate their victims into compliance.

Finally, cyber criminals use the principle of scarcity to manipulate their victims. This principle suggests that people are more likely to act when they believe something is in limited supply. Cybercriminals often create a false sense of scarcity to make their victims act quickly, such as by offering a limited-time deal or claiming there are only a few spots left for service.

In conclusion, understanding psychological manipulations made by cybercriminals is essential in protecting oneself from online fraud and scams. Cybercriminals use various psychological tactics, such as fear, urgency, reciprocity, social proof, authority, and scarcity, to manipulate their victims into giving up sensitive information or money. By being aware of these tactics and staying vigilant, individuals can protect themselves from falling victim to these scams. It is also essential to report any suspicious activity to the appropriate authorities to prevent others from falling victim to these manipulations.

**6.Methodology**  
The study was a qualitative exploration. Victims of cybercrime in the Delhi/ NCR region were interviewed. A purposive sampling technique was employed, with a total of 12 victims of cybercrime recruited to take part in the study. Informed consent was taken from each participant. The transcripts produced were used for the development of codes and themes and thematic analysis was used in this study for further analysis of the statements given by the victims of cybercrime offenses. All the crimes were reported to the police officers before and during this study.

|  |  |  |  |
| --- | --- | --- | --- |
| PARTICIPANT | INCIDENT | CODES | THEME |
| PARTICIPANT 1 | I fell victim to a cyber-attack My Facebook account got hacked and left my personal information exposed and my online privacy compromised. | * Cyberattack * Facebook account hack * Personal information exposure * Online privacy compromise * Blackmail * Password weakness * Two-factor authentication | * Cybersecurity: The importance of strong passwords and two-factor authentication to protect against cyber attacks. * Privacy: The importance of safeguarding personal information and the consequences that can arise when privacy is compromised. * Trauma: The emotional impact of the cyber attack, including feelings of violation, anxiety, and avoidance. * Responsibility: The acknowledgment of the victim's role in the hack by not taking appropriate security measures, such as enabling two-factor authentication and using a strong password. |
| PARTICIPANT 2 | Last year during the covid period my dad wanted to take a loan from some agency. He found an online website and started with the procedure of applying for a loan using that website. | * Loan Scam * Online Fraud * Threat Calls * Payment Refund | * Vulnerability: The text highlights how the victim's financial needs during the COVID period made them vulnerable to the scam. * Deception: The scammers used a professional-looking website and promised refunds to deceive the victim into making multiple payments. * Intimidation: The scammers resorted to threat calls and messaging to intimidate the victim into making more payments and to deter them from reporting the scam to the police. * Financial Loss: The victim ultimately suffered a significant financial loss due to the scam, as the promised refunds were never received. |
| PARTICIPANT 3 | we got a message that we have won a lottery during the covid times. We were really happy because our family was facing a financial crisis. They said that they were calling from some foreign country and we had a lottery for buying a new brand of coffee. | * Lottery scam * Foreign country call * Currency conversion fee * Request for additional payment * Non-refundable payment | * Financial need: The victim's family was facing a financial crisis, making them vulnerable to the scam. * Deception: The scammers used the lure of a lottery win to deceive the victim into paying a currency conversion fee. * False reassurances: The scammers reassured the victim that the currency conversion fee would be refunded, but never did. * Pressure: The scammers pressured the victim into making additional payments to receive a larger amount of money, leading to suspicion of fraud. * Financial loss: The victim ultimately suffered a financial loss due to the scam, as the initial payment was non-refundable. |
| PARTICIPANT 4 | The schemers trapped me as I was a desperate and innocent job-seeker with lucrative monthly salaries. They asked me to make a security deposit to cover the cost of the services provided and then duped me of their money before the start of my work or within a month or two of joining. 2-3 of my friends were  duped of their money either before the assignment started or after a month or two of working | * Job scam * Deception * Exploitation * Financial fraud | * Desperation of employment * Trust in the job provider * Pressure to pay for services * False promises of high salaries * Vulnerability to financial loss |
| PARTICIPANT 5 | I had posted on my social media account a post for buying a second-hand bike. a man claimed to be an army officer and asked me to pay through the Google link. only. I paid him an amount of rs. 60000. and after that, he was nowhere to be found. He broke my trust | * Social media transaction fraud * Impersonation of military personnel * Payment through unauthorized means * Lack of verification of seller's identity * Financial loss | * Social media transaction fraud * Impersonation of military personnel * Payment through unauthorized means * Lack of verification of seller's identity * Financial loss |
| PARTICIPANT 6 | Credit card received for overseas use, one for son sent in a package. Noticed a $950 charge to State Farm Insurance, but no accounts with them. Bank-issued permanent credit, curious about the name on the policy. Lucky to catch it, wonder if would've caught on frequent use | * Credit card fraud * Unauthorized transaction * Tampering with the package * Care package * Temporary credit * Permanent credit * Financial security | * Financial fraud and scams * Importance of monitoring bank accounts and credit cards * Vulnerability of online transactions * Trustworthiness of delivery services * Importance of timely reporting of fraudulent transactions * Protection of personal and financial information |
| PARTICIPANT 7 | A year ago, ad downloaded a free mobile application from Tata Motors. On November 10, he received a phone call from a person who said he was calling from Tata Motors and informed him that his app subscription has ended and he will have to pay Rs 3,528 for the subscription. The complainant said he took the subscription but the application is not working. | * Credit card fraud * Unauthorized transaction * Tampering with package * Care package * Temporary credit * Permanent credit * Financial security | * Phishing scam * Impersonation of a legitimate company or brand * Pressure tactics to make payment * False promises of service or product |
| PARTICIPANT 8 | I fell for a phishing scam where I received an email from what appeared to be my bank asking me to log in to my account to confirm some recent transactions. The email looked legitimate, but when I clicked on the link and entered my information, I unknowingly gave the scammer access to my bank account. The scammer then emptied my account of all funds | * Downloaded free mobile application * Received phone call claiming to be from Tata Motors * Informed about the end of the app subscription * Asked to pay Rs 3,528 for subscription renewal * Took the subscription but the application is not working | * Vulnerability to cybercrime * Deception and manipulation * Financial loss and hardship * Trust and credibility in online communication * Importance of cybersecurity awareness and education * Need for stronger security measures and regulations * Impact of cybercrime on individuals and society as a whole. |
| PARTICIPANT 9 | A small business owner was the victim of a ransomware attack where all of his company's files were encrypted and held for ransom. The attacker demanded a large sum of money in exchange for the decryption key. The business owner was forced to pay the ransom to regain access to his company's files and continue operating. | * Email scam * Social engineering * Identity theft * Financial fraud * Unauthorized access * Cybersecurity breach * Phishing scam | * Vulnerability of small businesses to cyber attacks * Impact of ransomware attacks on business operations and finances * Ethics of paying ransoms to cyber criminals * Importance of implementing cybersecurity measures to prevent attacks * Need for increased awareness and education on cyber threats and scams. |
| PARTICIPANT 10 | A man's identity was stolen when a hacker gained access to his email account and used it to reset the passwords on all of his financial accounts. The hacker then proceeded to drain the man's bank accounts, max out his credit cards, and open new lines of credit in his name. The man was left with thousands of dollars of debt and a damaged credit score. generate codes and themes | * Identity theft * Email account hacking * Password reset scam * Financial account fraud * Bank account draining | * Financial fraud and theft * Personal information protection and security * Password management and security * Credit score and debt management * Cybercrime consequences and impact on victims |
| PARTICIPANT 11 | A woman received a call from someone claiming to be from Microsoft, who informed her that her computer was infected with a virus. The caller then convinced her to allow him remote access to her computer to fix the issue, but instead, he installed malware that allowed him to steal her personal and financial information. | * Social engineering * Tech support scam * Remote access * Malware | * The victim was targeted through a phone call and convinced to give access to her computer * The scammer posed as a legitimate tech support representative from Microsoft * The victim's trust was exploited to install malware on her computer * The scammer was able to steal the victim's sensitive information, potentially leading to further financial harm |
| PARTICIPANT 12 | I was scammed by a fake online shopping website that appeared legitimate. I purchased an expensive item, but never received it. After contacting the website's customer service, I realized it was a fake website and that he had been scammed. | * Fake online shopping website * Deceptive appearance of legitimacy * Non-delivery of the purchased item * Customer service as part of the scam | * Online shopping scams * Deceptive websites and online content * Financial loss due to online fraud * Importance of verifying the legitimacy of websites and sellers |

**7. Data Analysis**

Data were analyzed using inductive thematic analysis, following the steps outlined by (Braun & Clarke, 2006): familiarization with the data; generation of initial codes; searching for and creating themes; reviewing themes; and refining and naming the themes. Inductive thematic analysis is data-driven, meaning that theme development was not restricted by the researcher’s interest in the area (Braun & Clarke, 2006). Another researcher reviewed all transcripts to check for the validity of the analysis. No differences were reported about coding; however, several themes were expanded to include subthemes.

|  |  |  |
| --- | --- | --- |
| **PARTICIPANT** | **CASES** | **PSYCHOLOGICAL TACTICS USED BY THE OFFENDER** |
| PARTICIPANT 1 | I fell victim to a cyber-attack. My Facebook account got hacked and left my personal information exposed and my online privacy compromised. | **Fear**: The offender instilled fear in the victim by threatening to expose their chats. This fear likely motivated the victim to comply with the offender's demands and change their password.  **Guilt:** The offender may have used guilt to make the victim feel responsible for the cyber-attack, emphasizing that the victim's weak password and failure to enable two-factor authentication made the hack possible.  **Intimidation:** The offender used intimidation to exert control over the victim by blackmailing them with their chats. This put the victim in a vulnerable position, as they felt that their reputation and privacy were at stake.  **Deception**: The offender used deception to gain access to the victim's Facebook account, likely by using a phishing scheme or other social engineering tactics. This allowed the offender to take control of the account without the victim's knowledge or consent. |
| PARTICIPANT 2 | last year during the covid period my dad wanted to take a loan from some agency he found an online website and started with the procedure of applying for a loan using that website. | **Building trust:** The professional-looking website and the initial promise of a refund may have been designed to build trust with the victim.  **Consistency and commitment**: By requesting small payments initially and promising refunds, the offender may have been trying to get the victim to commit to the loan application process and increase the amount of money they were willing to pay.  **Fear and intimidation**: The threat of police complaints and messaging relatives could have been a tactic to intimidate the victim into paying the requested amounts.  **Sense of urgency:** The offender may have created a sense of urgency by requesting payments for verification purposes and pressuring the victim to pay quickly before they had time to think through the situation. |
| PARTICIPANT 3 | we got a message that we have won a lottery during the covid times. we were happy because our family was facing a financial crisis | the cybercriminal used the **lure** of a lottery win during a time of **financial crisis** to **manipulate** the victim into paying a large sum of money. They used promises of refunds and **assurances** to gain the victim's **trust** and then continued to demand more money. They may have also used **persuasive language and urgency** to **pressure** the victim into making the initial payment. Overall, the cybercriminal used **social engineering tactics** to manipulate the victim's emotions and decision-making to their advantage. |
| PARTICIPANT 4 | The schemers trapped me as I was a desperate and innocent jobseeker with lucrative monthly salaries. They asked me to make a security deposit to cover the cost of the services provided and then duped me of their money before the start of my work or within a month or two of joining. 2-3 of my friends were duped of their money either before the assignment started or after a month or two of working | * Preying on the victim's desperation: * Offering a sense of security: * Creating a sense of urgency * Appealing to the victim's social |
| PARTICIPANT 5 | I had posted on my social media account a post for buying a second-hand bike. a man claimed to be an army officer and asked me to pay through the Google link. only. I paid him an amount of rs. 60000. and after that, he was nowhere to be found. He broke my trust | * I had posted on my social media account a post about buying a second-hand bike. a man claimed to be an army officer and asked me to pay through the Google link. only. I paid him an amount of rs. 60000. and after that, he was nowhere to be found. He broke my trust |
| PARTICIPANT 6 | Credit card received for overseas use, one for son sent in a package. Noticed a $950 charge to State Farm Insurance, but no accounts with them. Bank-issued permanent credit, curious about the name on the policy. Lucky to catch it, wonder if would've caught on frequent use | * Exploited a lapse in security to gain access to the victim's personal information or intercept the credit card package * Made a small, plausible charge to avoid detection or suspicion * Impersonated a legitimate company like State Farm to appear trustworthy and legitimate * Took advantage of the distance and unfamiliarity of the victim with local businesses and charges |
| PARTICIPANT 7 | A year ago, he downloaded a free mobile application from Tata Motors. On November 10, he received a phone call from a person who said he was calling from Tata Motors and informed him that his app subscription has ended, and he will have to pay Rs 3,528 for the subscription. The complainant said he took the subscription, but the application is not working. | * Impersonating a legitimate company: the offender claimed to be calling from Tata Motors * Creating a sense of urgency: the offender informed the victim that their app subscription had ended and needed to pay immediately * Exploiting fear of losing a service: the offender played on the victim's fear of losing access to the mobile application * Offering a seemingly good deal: the offender offered a subscription at a relatively low cost, which may have seemed like a good deal |
| PARTICIPANT 8 | I fell for a phishing scam where I received an email from what appeared to be my bank asking me to log in to my account to confirm some recent transactions. The email looked legitimate, but when I clicked on the link and entered my information, I unknowingly gave the scammer access to my bank account. The scammer then emptied my account of all funds | * Impersonating a legitimate company * Creating a sense of urgency: * Exploiting fear * Offering a plausible explanation * Using social engineering: |
| PARTICIPANT 9 | A small business owner was the victim of a ransomware attack where all his company's files were encrypted and held for ransom. The attacker demanded a large sum of money in exchange for the decryption key. The business owner was forced to pay the ransom to regain access to his company's files and continue operating. | * Exploiting vulnerability: The attacker likely targeted a small business owner who may not have had the resources or knowledge to adequately protect against cyberattacks. * Creating a sense of urgency: The attacker likely demanded a large sum of money and threatened to permanently delete the encrypted files if the ransom was not paid within a certain timeframe. * Exploiting a vulnerability: attacker targeted weak or easily guessed passwords or lack of two-factor authentication on the man's email account |
| PARTICIPANT 10 | A man's identity was stolen when a hacker gained access to his email account and used it to reset the passwords on all his financial accounts. The hacker then proceeded to drain the man's bank accounts, max out his credit cards, and open new lines of credit in his name. The man was left with thousands of dollars of debt and a damaged credit score. generate codes and themes | * A man's identity was stolen when a hacker gained access to his email account and used it to reset the passwords on all his financial accounts. The hacker then proceeded to drain the man's bank accounts, max out his credit cards, and open new lines of credit in his name. The man was left with thousands of dollars of debt and a damaged credit score. generate codes and themes |
| PARTICIPANT 11 | A woman received a call from someone claiming to be from Microsoft, who informed her that her computer was infected with a virus. The caller then convinced her to allow him remote access to her computer to fix the issue, but instead, he installed malware that allowed him to steal her personal and financial information. | * Exploiting trust: the attacker claimed to be from Microsoft, a well-known and reputable company. * Creating a sense of urgency: the attacker informed the victim that her computer was infected with a virus, creating a sense of urgency to fix the issue as soon as possible. * Offering a seemingly good deal: the attacker may have offered to fix the issue for free or at a relatively low cost, which may have seemed like a good deal. * Exploiting fear of losing data: the attacker may have played on the victim's fear of losing important data on her computer due to the virus. |
| PARTICIPANT 12 | I was scammed by a fake online shopping website that appeared legitimate. I purchased an expensive item, but never received it. After contacting the website's customer service, I realized it was a fake website and that he had been scammed. | * Exploiting trust: The scammer created a fake online shopping website that appeared legitimate, potentially using convincing logos, design elements, and product listings to deceive the victim. * Creating a sense of urgency: The victim may have been motivated to make the purchase quickly due to limited product availability or time-sensitive deals offered on the website. * Offering a good deal: The scammer may have offered the victim a discount or an unbeatable deal on the expensive item, which may have enticed the victim to make a purchase. * Using social proof: The scammer may have used fake customer reviews, ratings, or testimonials on the website to create the impression that other people had successfully purchased and received products from the site. |

**8. Conclusion**

This paper sheds light on the complicated and disturbing strategies used by cyber offenders to influence their prey for malevolent intentions. This study emphasizes the vital need to increase awareness about the hazards presented by these manipulative strategies in the digital realm through an in-depth examination of psychological principles and real-world case studies

This study's findings show that cyber offender use fundamental characteristics of human behavior, such as cognitive biases, emotional triggers, and social engineering, to achieve their malicious goals. Understanding these deceptive strategies is critical for individuals, businesses, and legislators alike in order to increase cybersecurity measures and combat cybercrime successfully.

This study's findings show that cyber offenders use fundamental characteristics of human behavior, such as cognitive biases, emotional triggers, and social engineering, to achieve their malicious goals. Understanding these deceptive strategies is critical for individuals, businesses, and legislators alike in order to increase cybersecurity measures and combat cybercrime successfully.

As we go further into a more connected and digitally driven society, the consequences of psychological manipulation by cyber criminals go beyond financial losses and data breaches. They include the deterioration of confidence in digital interactions, the violation of personal privacy, and the possible exploitation of vulnerable people. As a result, cybersecurity professionals, law enforcement agencies, and lawmakers must work together to develop comprehensive measures to successfully counter these deceptive methods.

In conclusion this study emphasizes the need of cultivating a cybersecurity culture that promotes awareness, alertness, and resilience. We can jointly protect ourselves, our companies, and our digital society from the insidious hazards hiding in cyberspace by recognizing the relevance of psychological manipulation by cyber criminals and adopting proactive actions. Only by educated awareness and collaborative efforts will we be able to strengthen our cyber defences and build a safer, more secure digital world for everybody

**9.References**

1. Das, S., Kim, T.H.J., Dabbish, L., & Hong, J.I (2014). The Effect of Social Influence on Security Sensitivity. In Proc. SOUPS’2014.

2. Das, S., Kramer, A.D.I., Dabbish, L., & Hong, J.I. (2015). The Role of Social Influence in Security Feature Adoption. To appear In Proc. CSCW’2015.

3. Das, S., Kramer, A.D.I., Dabbish, L., & Hong, J.I. (2014). Increasing Security Sensitivity With Social Proof: A Large Scale Experimental Confirmation. In Proc. CCS’2014.

4. Nolan, J.M., et al. Normative Social Influence is Underdetected. Personality and Social Psychology Bulletin 2008; 34; 913. <http://www.csom.umn.edu/assets/118360.pdf>

5. Goldstein, N., Cialdini, R., & Griskevicius, V. (2008). A Room with a Viewpoint: Using Social Norms to Motivate Environmental Conservation in Hotels, J. Consumer Research, 35. <http://www.csom.umn.edu/assets/118359.pdf>

6. Thurston, W. On Proof and Progress in Mathematics. Bulletin of the American Mathematical Society; 30(2); 161-177. <http://arxiv.org/pdf/math/9404236v1.pdf>

7. Stokes, D.E. Pasteur's Quadrant: Basic Science and Technological Innovation. Brookings Institution Press. 1997

8. Ahmed a Mustafa, Abubakar Bello.,et al.( 2018) The role of user behaviour in cybersecurity management. school of psychology, western Sydney Australia .2018 <https://www.frontiersin.org/people/u/15417>

9. Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon* 3:e00346. doi: 10.1016/j.heliyon.2017.e00346

10. Gutzwiller, R. S., Fugate, S., Sawyer, B. D., and Hancock, P. A. (2015). The human factors of cyber network defense. *Paper presented at the In Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Los Angeles, CA.