IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

The Psychology of Cyber Fraud: How Scammers Use AI to Exploit Human Behaviour

Arunesh Bal, Student, Lotus Valley International School Noida (India).

Abstract

Cybercrime has taken a more destructive direction, due to the introduction of Artificial intelligence (AI) and machine learning. Cybercriminals can now access tools that have the ability to mimic human behaviour and create schemes which are highly convincing. The aim of this research is to get into the intricate interplay between psychology and technology, when it comes to cybercrime. This study also aims to highlight the underlying mechanisms that drive scamming schemes in the digital landscape, by evaluating how scammers make use of AI for manipulation of emotions and human cognition. In conclusion, it can be said that fraudulent schemes have become more sophisticated with the convergence of human behaviour with technological advancements. The intersection of psychology and cyber fraud has made the environment more complex and vulnerable. Artificial intelligence and machine learning have enabled cybercriminals to personalise their tactics and switch from the traditional rudimentary attacks, to highly targeted ones, which have the capability to exploit the victims on the basis of cognitive biases and emotional vulnerabilities.

Keywords: Cyber Fraud, Human Behaviour, AI, Psychology, Cybercriminals, Cognitive Biases, Emotional Vulnerabilities

Background of the Research

With the evolution of technology, cybercrime has also seen a significant transformation. Earlier, cybercrime was limited to less complex scams like phishing, malware distribution, etc., which exploited the existing vulnerabilities in the internet systems (Button & Cross, 2017). However, in the recent times, cybercrime has taken a more destructive direction, due to the introduction of Artificial intelligence (AI) and machine learning (Hidayati et al., 2021). Cybercriminals can now access tools that have the ability to mimic human behavior and create schemes which are highly convincing. According to Yamin et al. (2021), cybercrime has seen a paradigmatic shift, as now, the fraudulent schemes are being carried out by using psychological manipulation. In addition to that, AI has added to the impact of cybercrime by allowing cybercriminals to personalize their approaches, automate the processes, and operate with scalability. The evolution of cybercrime from rudimentary attacks to highly sophisticated attacks with advanced technology, is becoming a challenge in the context of cybersecurity measures (Blauth et al., 2022).

Blauth and Li (2020) mention that an increase in the incidence of cyber fraud is becoming a cause of worry for individuals, businesses, and governments, at a global level. AI is being used to carry out more sophisticated cyber frauds. According to Yamini et. al (2021), AI-powered algorithms give scammers the ability to create targeted scams that are highly convincing, as they are now able to analyse large amounts of data, and identify behavioural patterns in humans. AI also offers automation and personalisation, which gives an advantage to the scammers, making it easy for them to create scams that are hard to distinguish from genuine schemes. This has given an unprecedented leverage to the fraudsters to exploit psychological vulnerabilities. It amplifies the impact of their fraudulent activities. Blauth et al. (2022) suggests that comprehensive and adaptive strategies are required to tackle cybercrime and its detrimental effects, because AI's integration with the tactics used for cybercrime has fortified its overall impact.

Cyber fraud exploits cognitive biases and emotional vulnerabilities of humans, in order to deceive them. It operates at the intersection of technology and human psychology. (Attrill-Smith & Wesson, 2020). Attrill-Smith and Wesson (2020) states that a key aspect of cybercrime is manipulation. Cognitive biases are the ingrained tendencies in human cognition, which are exploited to carry out cybercrime. For example, authority bias is exploited by the cybercriminals, as it impacts the tendency to trust and comply with figures of authority. Cybercriminals may pretend to be representatives of reputable organisations in order to deceive the victims into giving out private information, or even making financial transactions. Moreover, cybercriminals take advantage of the social proof, exploiting the tendency of humans to follow other people and whatever they do (Matveev et al., 2021). Cybercriminals fabricate social endorsements, and sometimes, even create false narratives of widespread participation in fraud schemes, in order to trick people into believing that their scheme is legit. Scarcity bias is also exploited in a similar way. Fraudsters create a situation of scarcity or urgency in order to compel victims into making quick decisions without critical thinking (Attrill-Smith & Wesson, 2020).

Matveev et al. (2021) mentions that cybercriminals also try to manipulate emotional triggers, beyond cognitive biases, in order to control the victims. They use fear to force individuals into compliance as they use tactics like threatening legal consequences, and loss of sensitive information or personal data. Cyber fraudsters also use Greed to exploit their victims as it is a highly powerful emotional trigger. They tend to promise unrealistic rewards or financial windfalls, which entices the victims into taking part in their scamming schemes. They may also use urgency, which creates a sense of crisis or imminent loss. This makes victims make irrational decisions as urgency clouds the ability use critical thinking in any situation (Matveev et al., 2021; Attrill-Smith & Wesson, 2020).

According to Firdaus et al. (2022), cyber fraud not only causes financial losses to an individual, but it also leaves them psychological distressed. As mentioned earlier, fraudsters generally exploit different psychological vulnerabilities in order to manipulate people into believing in their fake schemes. Individuals feel betrayed, ashamed, and embarrassed after falling into such schemes, which leaves them in distress. Shang et al. (2022) noticed that a very common emotional response to falling victim to a cyber fraud is the sense of violation. Individuals who fall for these schemes feel violated as they realise that they have been manipulated and their personal information is being compromised because of their clouded judgement and irrational decision making. This undermines the confidence of individuals to trust their own ability to use digital advancements and technology, safely.

Cybercrime can also cause victims to have emotional trauma, especially in situations where the victims face huge financial losses or in the cases of stolen identities (Borwell et al., 2022). Bada & Nurse (2020) believes that falling victim to a cyber fraud can have a long lasting psychological impact that leads to high anxiety, depression, and sometimes even post-traumatic stress disorder (PTSD). Victims tend to constantly worry about the future and the fact that they might fall into such a trap again, and they persistently live in fear and mistrust. They also feel apprehensive about making online transactions. As per Shang et al. (2022), cybercrime can also be associated with social and interpersonal consequences. It is because the victims tend to feel embarrassed about the fact that they have been scammed, and they are ashamed to admit it. The psychological toll cybercrime takes on an individual roots from him/her reluctance to seek help or talk about the experience with others. Due to this, the individuals start feeling isolated and lonely.

Cyber fraud not only impacts emotions of an individual, but it also may impact his/her financial well-being and sense of security (Borwell et al., 2022). It is hard to recover from a cybercrime, financially. This may lead to increased stress and stress and uncertainty about their financial stability. Bada and Nurse (2020) believe that falling victim to a fraud adds a sense of vulnerability in the minds of individuals that may undermine their confidence to protect themselves online. This increases anxiety and hyper-vigilance.

According to Matveev et al. (2021), and Attrill-Smith & Wesson (2020), cybercrime operates on the intersection of psychology and technology. As fraudsters continue to integrate AI in their practices and continue to exploit human vulnerabilities, it becomes more important to combat fraud activities. Using a multifaceted approach to address the psychological as well as the technological aspects of the problem is necessary. In order to develop effective measures and strategies to mitigate the impact of cyber fraud, is it important to understand the psychology of cyber fraudsters. Moreover, by understanding the overall psychological impact of cybercrime on the victims, helps in developing effective rehabilitation strategies that allows victims to cope with anxiety, depression, and PTSD. Individuals can avoid being scammed by understanding and recognising the common psychological tactics that cyber fraudsters use to scam people. Cybersecurity professionals can design AI-driven defence mechanisms by understanding the common tactics used by scammers. Such mechanisms can have the ability to detect sophisticated fraud, and thwart it, in real-time. The aim of this research is to get into the intricate interplay between psychology and technology, when it comes to cybercrime. This study also aims to highlight the underlying mechanisms that drive scamming schemes in the digital landscape, by evaluating how scammers make use of AI for manipulation of emotions and human cognition.

Use of AI by the Cybercriminals

Cybercriminals employ a diverse array of technologies to execute their malicious activities, leveraging both traditional and advanced methods to exploit vulnerabilities in systems and networks. One of the most prevalent technologies is malware, which includes viruses, worms, Trojans, ransomware, and spyware (Velasco, 2022). Guembe et al. (2022) opined that these malicious software programs are designed to infiltrate and damage computers, steal data, and disrupt services. Ransomware, for example, encrypts a victim's data and demands payment for the decryption key, causing significant financial and operational damage to individuals and organizations. For instance, the infamous WannaCry ransomware attack in 2017 spread rapidly across the globe, exploiting a vulnerability in Windows operating systems to encrypt files and demand ransom payments in Bitcoin. This attack affected over 200,000 computers in 150 countries, causing significant disruption to businesses, healthcare services, and government agencies (Kaloudi, 2020). Advanced malware often utilizes sophisticated evasion techniques to bypass security measures, such as polymorphism, which alters the code with each infection to avoid detection by antivirus software.

According to Zouave et al. (2020), viruses are malicious code that attaches itself to legitimate programs and files, spreading from one system to another when the infected file is executed. Worms, on the other hand, are self-replicating programs that spread independently of host files, often exploiting vulnerabilities in network security to propagate. Trojans masquerade as legitimate software but carry a malicious payload that is activated once the software is installed. Ransomware, one of the most financially damaging forms of malware, encrypts a victim's data and demands payment for the decryption key, often causing significant disruption and financial loss (Velasco, 2022). Spyware, as the name suggests, covertly monitors and collects information about a user's activities without their knowledge or consent. The case of the Equifax data breach in 2017, where personal data of 147 million people was compromised due to an unpatched vulnerability, highlights the devastating impact of such malware (Vaithianathasamy, 2019).

Phishing is another widely used technique, where cybercriminals use deceptive emails, messages, and websites to trick individuals into divulging sensitive information such as usernames, passwords, and credit card numbers. These attacks have become increasingly sophisticated, employing social engineering tactics to appear legitimate and trustworthy. In 2016, the Democratic National Committee (DNC) suffered a major breach due to a spear-phishing attack that compromised email accounts, influencing the US presidential election (Nadeem et al., 2023). Spear-phishing, a more targeted version, involves personalized messages to specific individuals or organizations, increasing the likelihood of success. This targeted approach increases the chances of compromising high-value targets, such as corporate executives or government officials, and gaining access to sensitive information or systems. The attack on John Podesta, Hillary Clinton's campaign chairman, during the 2016 US presidential campaign, is a notable example of a successful spear-phishing attack that led to significant political fallout (Nadeem et al., 2023). Cybercriminals often use phishing kits, pre-packaged tools that make it easy to create and deploy phishing campaigns without requiring extensive technical knowledge.

Botnets, networks of compromised computers controlled remotely by cybercriminals, are a powerful tool for conducting large-scale attacks. These networks can be used to launch Distributed Denial of Service (DDoS) attacks, overwhelming a target with traffic and causing service disruptions (Kaur et al., 2019). Botnets also facilitate spamming, data theft, and the distribution of other malware. The Mirai botnet attack in 2016, which targeted DNS provider Dyn, caused widespread internet outages, affecting major websites like Twitter, Netflix, and Reddit (Sripriyanka & Mahendran, 2021). The rise of Internet of Things (IoT) devices has expanded the potential for botnets, as many IoT devices lack robust security measures, making them easy targets for cybercriminals to exploit and incorporate into their networks. Once infected, these devices can be incorporated into a botnet and used to amplify attacks or facilitate other malicious activities. The large number of IoT devices globally provides a vast pool of potential targets for cybercriminals, exacerbating the threat posed by botnets (Velasco, 2022).

Exploiting vulnerabilities in software and hardware is another common tactic used by cybercriminals. Zero-day exploits, which take advantage of previously unknown vulnerabilities, are particularly dangerous because they provide no time for developers to patch the flaw before it is used in an attack (Pureti, 2022). Cybercriminals often trade these exploits on underground markets, where they can fetch high prices. Regular software updates and security patches are critical in defending against these types of attacks, but the rapid pace of technological advancement means that new vulnerabilities are continually being discovered and exploited. The 2017 Equifax breach was a result of a zero-day exploit in Apache Struts, a widely used software framework (Thakur, 2024).

Cryptojacking is a relatively recent phenomenon where cybercriminals hijack the processing power of computers to mine cryptocurrencies without the owner's knowledge or consent. This type of attack is often executed through malicious scripts embedded in websites or delivered via malware. When a victim visits an infected website or installs compromised software, the cryptojacking script begins to mine cryptocurrency, consuming the victim's processing power and electricity (Sriman et al., 2023). The rise in the value of cryptocurrencies has made cryptojacking an attractive option for cybercriminals seeking to profit from their activities. Unlike other forms of cybercrime, cryptojacking is less noticeable to victims, as it often results in performance degradation rather than immediate financial loss (Sriman et al., 2023). In 2018, Tesla's cloud computing environment was compromised by cryptojackers who exploited a vulnerability to install cryptocurrency mining software, demonstrating the potential scale of such attacks.

The dark web provides a marketplace for cybercriminals to buy and sell illicit goods and services, including stolen data, hacking tools, and exploit kits. Using technologies like Tor (The Onion Router) to anonymize their activities, cybercriminals can operate with a degree of impunity, making it challenging for law enforcement to track and apprehend them (Guembe et al., 2022). The dark web's ecosystem supports a thriving underground economy, where cybercriminals can collaborate, share information, and refine their techniques. This clandestine network plays a crucial role in the perpetuation of cybercrime, offering a safe haven for those looking to engage in illegal activities (Velasco, 2022).

Cyberpsychology

Human behaviour and the digital domain are intertwined in a complex manner. This leads to the emergence of cyberpsychology. The convergency of psychology and cybercrime is a significant field that attracts the researchers. Today’s environment is highly interconnected, which makes the motivations, techniques, and consequences of the actions of cyber fraudsters, ever-changing (Ancis, 2020). In this section, psychological underpinnings of cybercrime are explored and examined. It also identifies and analyses the factors influencing thoughts and behaviours of fraudsters as well as the victims.

Cyberpsychology combines psychology and technology in order to understand the complex relationship between the human mind and the digital world. It is an emerging concept (Kirwan, 2016). It is important to understand how people interact with technology, how online actions affect psychological, and the typology of cybercrime, in order to navigate through the complexities of the digital landscape.

Primarily, the concept of Cyberpsychology investigates how technology impacts human behaviour, cognition, and emotions. Cyberpsychology explores how people make interactions with the digital world. It focuses on the ever-changing dynamic between technology and humans (Norman, 2017). Cyberpsychology is a significant concept that understands the changes in human experiences in a time where technology dominates the world. It helps in understanding the benefits as well as drawbacks of technology. Cyberpsychology explores how human thoughts, emotions, and behaviours, are affected by technology. It understands the psychological effects of social media usage on the cognitions of human, and its impact on virtual reality.

Cyberpsychology also studies how technology impacts mental health. In today’s interconnected world, technology has drastically transformed the way we interact with others and understand our own identity. Cyberpsychology helps in examining and implementing strategies for addressing major issues like online harassment, cyberbullying and internet addiction. Attrill-Smith et al. (2019) argue that it is important to understand the psychological effects of an excessive screen time, the stress of keeping up with an online identity, and the impact of online comparison on an individual’s mind. Cybersociologists understand these complexities in order to find solutions that can reduce harmful effects of technology on the mental health of individuals.

Psychology of Cybercriminals

Cybercriminals commit crimes due to several reasons, and why they do it can be understood by applying various psychological theories related to the human behaviour, cognition, and motivation. Using these theories, we can understand the underlying mechanisms that make people commit cybercrimes. Rational Choice Theory, Strain Theory, Social Learning Theory, and the Theory of Planned Behaviour are some of the key theories in this regard.

Rational Choice Theory: This theory suggests that individuals tend to make decisions by weighing the potential risks as well as benefits of their actions. Fraudsters are rational actors who deliberately engage in illegal activities as they feel that the potential benefits outweigh the risks (Mohammed et al., 2020). Cybercrime is an attractive option as there are less immediate consequences due to the anonymity factor and lower detection risk in the cyberspace (Stalans & Donner, 2018). For example, a fraudster may believe that the financial gain that can be extracted from stealing sensitive information from an individual is more beneficial due to the relatively low risk of being caught. The decision-making process of fraudsters is driven by this cost-benefit analysis. These individuals consider the rewards and the perceived risks. This helps in getting a better understanding of cybercriminal behaviour.

Strain Theory: This theory is developed by Robert K. Merton. It suggests that individuals can commit crime due to societal pressures. They might experience a disconnect between their goals, and the means available to them for achieving their goals, therefore, they tend to perform illegal activities to cope up with the pressure (Hay & Ray, 2020). For instance, individuals who come from disadvantaged backgrounds can turn to cyber fraud in order to extract financial gains from it. It can help them gain financial stability and the social status that may be otherwise attainable. They resort to illegal means as they believe that using the right means will get them nowhere. Such social pressure can drive cybercriminal behaviour as it allows individuals to achieve their goals, easily and quickly.

Social Learning Theory: This theory was proposed by Albert Bandura. It emphasises that people observe others and imitate them, especially if they have role models (Kirwan, 2016). This suggests that cybercriminals may be influenced by peers, online communities, or subcultures that support illegal activities, and glorify hacking. The cybercriminal subculture generally shares hacks and techniques along with the success stories, which can influence people to use these techniques and commit cybercrime (Whitty, 2016). Social approval, recognition, and the success of peers, can motivate individuals into committing cyber fraud. In this theory, the role of social environments and interactions in shaping behaviour associated to crimes, is highlighted.

Theory of Planned Behaviour: This theory was formulated by Icek Ajzen. It proposes that a person's intention to perform an activity is generally influenced by his/her attitude toward the behaviour, subjective norms, and perceived behavioural control. According to Sanne & Wiese (2018), in context of cybercrime, we can say that if a person's attitude towards hacking is seeing it as a challenge, or seeing it as a means to accomplish something and gain respect, the person is more likelihood to do it. An important role is played by subjective norms, or the perceived social pressure, in influencing people to commit cyber fraud. People are more likely to commit a cyber fraud if they believe that their peer group approves of it (Aiken et al., 2024). Perceived behavioural control can also help in determining whether a person makes an attempt to commit cybercrime. People who believe in their technical skills and their ability to successfully carry out cybercrime are more likely to commit fraud.

Psychodynamic Theory: This theory originates from work of Sigmund Freud. It is based on exploring how behaviours are shaped by unconscious motives, early childhood experiences, and internal conflicts (Balick, 2018). Unresolved psychological issues like a keen desire for power and control, can shape the behaviour for cybercrime (Spitaletta & Hopkins, 2021). For example, successfully hacking and manipulating digital systems can give a sense of control to the hackers, that they cannot exert in other aspects of their everyday lives. Their need to control and validation can drive them to commit cybercrime, as they perceive it as a compensation for their internal conflicts.

General Strain Theory: This theory was suggested by Robert Agnew's. It is an expansion of the traditional strain theory as it identifies three types of strain that can shape criminal behaviour- failure to achieve positively valued goals, removal of positively valued stimuli, and the presence of negative stimuli (Hay & Ray, 2020). Strains that root from financial difficulties, loss of employment, or interpersonal conflicts, tend to frustrate people and can drive cybercriminal behaviour through desperation (Stalans & Donner, 2018). They tend to engage in cybercrime and use it as a coping mechanism to gain a sense of achievement or control and get rid of their negative emotions.

Moral Disengagement Theory: This theory is derived by Albert Bandura's, emerging from the concept of moral disengagement. It explains how individuals justify their unethical behaviour. Cybercriminals may justify their behaviour by using various mechanisms of moral disengagement (Zhao & Yu, 2021). These mechanisms include dehumanizing their victims, diffusing responsibility, or minimizing the harm that their actions cause. According to Stalans and Donner (2018) cybercriminals can completely disengage from the moral implications that their actions have, by seeing the victims as faceless entities or mere data points. They can also distance themselves from all the consequences, which makes them continue their illegal activities, without feely guilty.

The psychological theories mentioned above have helped in developing a comprehensive framework, in order to understand the reasons why individuals commit cyber fraud. The interplay of cognitive, emotional, social, and environmental factors in influencing people to commit crime is highlighted in these theories. They also offer valuable insights into the motivations that drive cybercriminals and their psychological profiles. More effective theories and strategies for prevention of cybercrime can be developed by applying these theories. Such strategies can also be effective in addressing the complexities of cybercrime.

The Psychological Profiles of Cybercriminals

Cybercriminals come from diverse backgrounds and have different motivations that drive their behaviour. Therefore, understanding their psychological profiles is highly complex. There are a few common psychological underpinnings of cybercriminals that can be understood from a few specific personality traits and characteristics. High intelligence levels, lack of empathy, narcissism, low risk aversion, and addictive behaviour are a few of these traits (Attrill-Smith et al., 2019; Whitty, 2016; Stalans & Donner, 2018). Effective strategies can be developed by understanding the above-mentioned traits, which will help in effectively combating cybercrime.

Many cybercriminals have a common and notable trait- High levels of intelligence. Technical skills and a sound cognitive ability is required to navigate through the complex systems, and identify and exploit vulnerabilities (Bansod et al., 2022). A deeper understanding of technology and computer systems is required, beyond academic intelligence. Cybercriminals have a good hold on coding, and network structures. They stay ahead of the security measures by thinking creatively and strategically, before developing fraud schemes. They have high intellectual capabilities that enable them to adapt to advanced technologies, which helps them in countering cybersecurity measures (Bada & Nurse, 2023). This makes them a serious threat in the digital world. Having high intelligence is a concerning misuse of potential in this regard. These individuals can use their capabilities for positive contributions to society, but instead, they are using it for negative purposes.

Cybercriminals also tend to have a lack of empathy. They highly disregard the consequences that their actions can have on their victims. They perceive their criminal acts as abstract or victimless crimes. They also believe that their victims are faceless creatures (Bada & Nurse, 2021). A sense of detachment can lead to diminishing moral responsibility in the minds of these criminals. Internet offers anonymity and distance in the digital landscape, enabling cybercriminals to further desensitise to the suffering of their victims. It is important to understand their lack of empathy because it enables them to commit crimes and engage in frauds that can have adverse effects on others.

The psychological profiles of cybercriminals are also driven by narcissism and ego. Individuals desire recognition and validation, and in order to get that, they perform activities that showcase their abilities, even if they are illegal. For example, they take pride in their hacking skills and seek validation from the cybercriminal community (Zuhri, 2017). A quest for validation can multiply in different forms, be it gloating about successful hacking activities, seeking notoriety, or even leaving signatures on their exploits as success marks. This helps cybercriminals feed their self-image and ego, along with giving them financial gains. Narcissistic traits can make them dare to perform activities that exploit people in adverse ways, in order to get higher recognition and status in the cybercriminal community.

Another trait that most cybercriminals have is low risk aversion. Cybercrime takes place on a digital end where anonymity and distance are maintained. This reduces the immediate consequences, making it an attractive option for criminals (Phillips et al., 2022). Traditional crimes, on the other hand, have higher risk of physical apprehension, and prosecution. Therefore, cyber fraudsters hide their identities and locations, by leveraging the digital and remote environment. They perceive cybercrime to be a safer option to engage in illegal activities. Cybercrime has a lower risk and higher potential return, which makes it an attractive option for people who are influenced into showing cybercriminal behaviour and commit fraud.

In addition to that, Addictive behaviour is also a common psychological aspect of cybercriminals. They get a sense of thrill and challenge by beaching systems and deriving sensitive information, which is unattainable otherwise. It gives them a dopamine rush, similar to the feeling that a person experiences in other addictive behaviours (Gupta & Mata-Toledo, 2016). The desire to continue engaging in such activities is driven by success. After carrying out a cyber fraud successfully, cybercriminals tend to seek out new challenges and go for bigger targets. This is an addictive cycle which reinforces cybercriminal behaviour and drives a person to exploit more victims.

In order to address cybercriminal behaviour from its roots, it is necessary to understand the component of addiction. This will help in developing effective strategies to prevent recidivism. Psychological profiles of cybercriminals are also influenced by various socio-economic and environmental factors, to some extent. Individuals who come from a disadvantaged background, may commit cyber fraud for gaining financial stability, or as a means to let out their social frustration. Hacking and cybercrime created a subculture that has built a community of people who glorify cyber exploits like hacking. This gives a sense of belonging to individuals who felt marginalised at some point in their lives. Such a culture can influence people into committing cybercrime.

The multifaceted nature of the motivations and behaviours of cybercriminals underlines their psychological profile. A few traits like High intelligence, lack of empathy, narcissism, low risk aversion, and addictive tendencies, drive individuals towards committing fraud (March, 2022; Miftari et al., 2022; Perenc, 2022). Understanding the psychological factors associated with cybercriminals through a multi-pronged approach is necessary for addressing these characteristics. The approach must include education, intervention, and effective cybersecurity measures. Better strategies and methods can be adopted to mitigate cyberthreats, by deeply understanding the psychological makeup of cybercriminals.

Psychology of the Cybercrime Victims

Many theories exist in the literature that explain human behaviour, cognition and vulnerability. These theories can be studied in order to understand and explain why people fall victim to cybercrimes. They highlight the underlying mechanisms that influence people to believe the tactics used by cybercriminals. Social Engineering Theory, the Theory of Cognitive Biases, the Theory of Planned Behavior, and the Dual-Process Theory are the main theories that can be studied in this context.

Social Engineering Theory: This theory discusses how fraudsters exploit human behaviour and psychology, in order to influence people into falling victim to their schemes and revealing sensitive information or acting out abruptly without thinking. Cybercriminals tend to use various techniques like phishing, pretexting, and baiting to commit cyber fraud (Hatfield, 2018). These techniques tend to create a situation where urgency and fear take over, making individuals more likely to act hastily without properly analysing the situation and making decisions after thorough considerations. For example, if an individual comes across a phishing email that seems legit as it is sent from a trusted source, warning about a threat to the person's account, the individual is more likely to click on the links provided in the email or add the personal information it requires to take further steps. Humans tend to trust authority figures, and social engineering takes advantage of this human tendency, in order to make people fall prey to cybercriminal activity.

Theory of Cognitive Biases: This theory helps in understanding how systematic errors in thinking are responsible for making people fall victim to fraud schemes. Various cognitive biases like authority bias, availability heuristic, and confirmation bias, tend to impact the decision-making process of a human (Bada & Nurse, 2021). Authority bias enables people to trust authoritative organisations and comply with any requests from such organisations. The request could be made through email from a banking institution or any government agency. This makes people more susceptible to cybercrime as it leads to an overestimation of the likelihood of events (Kirwan, 2016). Individuals tend to overestimate the events on the basis of their recent experiences or readily available information. In the context of Confirmation bias, individuals tend to believe any information that confirms their beliefs or desires. For example, falling victim to a financial scheme that promises a big amount. Cognitive biases tend to impair the judgment ability of individuals and make them more vulnerable to cybercrime.

Theory of Planned Behaviour: This theory was formulated by Icek Ajzen. It suggests that an individual's engagement in a situation depends on his/her attitudes towards the situation, subjective norms, and perceived behavioural control. This theory explains that if a person has a positive attitude towards an offer that seems highly beneficial, or is "too-good-to-be-true", he/she is more likely to take advantage of such an offer due to the perceived social approval (Sanne & Wiese, 2018). This makes the person believe that he/she has control over the situation. These elements are exploited by cyber fraudsters for creating messages that can easily influence an individual in a situation, due to the perceived social norms and attitude towards that situation.

Dual-Process Theory: This theory explains how individuals make decisions after processing certain information. It includes two systems. System 1 includes intuitive and automatic thinking, and System 2 includes analytical and deliberate thinking. Fraudsters generally exploit the System 1 thinking, as it is fast, automatic, and emotional (Pienta et al., 2016). For example, Phishing schemes mainly exploit individuals by creating a sense of urgency, making them respond quickly as the created situation appeals to emotions such as fear or greed. This is not the case with System 2 thinking, where thinking is slower and more rational (Lillie, 2017). Individuals tend to rely on intuitive judgments in situations of urgency, and instead of scrutinizing the validity of the requests made in schemes, they fall victim to them. Sometimes, people who are highly aware and knowledgeable also fall victim to cybercrime. This can be explained by better understanding the interplay between the two cognitive systems.

In conclusion, different theories like Social Engineering Theory, the Theory of Cognitive Biases, the Theory of Planned Behavior, and Dual-Process Theory, which are mainly based on psychology, help in understanding why people fall victim to cybercrime. Human behavior, cognitive processes, and emotional responses are three important aspects that can help in understanding why individuals become vulnerable to cybercrime. These theories can be used in theoretical frameworks in order to come up with educational and preventive measures. This will help in increasing the overall awareness about cyber threats, and ways to not fall victim to cybercrimes, leading to protection against these scams.

Psychological Impact of Cybercrime on its Victims

Victims generally face psychological consequences after they get deceived by cybercriminals. Falling victim to cybercrime impacts an individual's mental health and emotional well-being. An immediate consequence of being a victim is heightened anxiety and stress levels. The victims feel discomfort realizing that their personal boundaries have been violated (Harley et al., 2018). They also feel constantly uncertain about using digital means as they fear the risks of online lurking. According to Parsons (2019), the chronic anxiety caused to the victims can affect their overall psychological health. This results in sleep disturbances, heightened irritability, and an ongoing sense of vulnerability. The feeling of always being on the verge of another cyberattack can be overwhelming, leading to a feeling of being unsafe in online as well as offline environments. People can also feel distracted from their daily life, which can diminish their quality of life, as they will start feeling stuck in a relentless cycle of stress and anxiety.

Distrust is another psychological aspect that comes with falling victim to a cybercriminal activity. In order to have healthy interactions, it is important to trust people. However, victims tend to become suspicious about everything and show wariness towards other individuals and online (Van de Weijer & Leukfeldt, 2017). Having a feeling of distrust in everything can hinder their ability to form as well as maintain relationships, as they may always suspect that they are being deceived or harmed. It not only affects online relationships and interaction, but also extends its impact on offline relationships. Victims might withdraw in a social context by isolating themselves. They might end up avoiding online engagements and offline social engagements, with the fear of being harmed again. This social withdrawal leads to a sense of feeling alone and depressed. A victim cannot recover in such an environment.

Another significant psychological consequence of cybercrime is the violation of digital privacy. Victims tend to feel violated and vulnerable, when their personal information is stolen or exposed. This highly affects the perception of an individual about the diminishing boundaries between the virtual and tangible worlds, and raises concerns for privacy and safety. Some victims also may end up feeling like they're constantly being watched or targeted (Sincek et al., 2017). This results in heightened paranoia, and they might lose control over their daily life. Emotional distress arises from a sense of intrusion, and it can highly affect the normal functionality of a person. Individuals may also start doubting digital technologies and be reluctant to use them as they will always fear invasion of privacy. Use of digital technologies is necessary in the modern world, especially when it comes to online banking, shopping, and communication, therefore, it is necessary to avoid distrust in these technologies.

The psychological impact seen in the victims of identity theft is even more severe as it triggers a deep-rooted identity crisis. Such victims have to reclaim their own identity and build it again in both online and offline worlds. This process brings up a lot of emotional challenges. Victims might also start feeling helpless as they lose control of their own identity (Vakhitova et al., 2022). The impact of identity theft is emotionally draining because of the fact that victims have to go through various legal and bureaucratic challenges to restore their own identity. They also lack clear support and guidance to navigate through the processes. Individuals might also feel sad and withdraw from social interactions due to the fear of being attacked repeatedly. Their retraction can affect online as well as offline communications, which results in an increased mental burden and more isolation. Cybercrime impacts its victims in many ways; however, according to Sánchez-Hernández et al. (2024) these psychological aspects make the impact worse. Therefore, it is imported to provide comprehensive support to the victims, and understand the need for intervention, in order to contribute in their recovery. This can help the victims in regaining a sense of security and well-being.

Conclusion

In conclusion, it can be said that fraudulent schemes have become more sophisticated with the convergence of human behaviour with technological advancements. The intersection of psychology and cyber fraud has made the environment more complex and vulnerable. Artificial intelligence and machine learning have enabled cybercriminals to personalise their tactics and switch from the traditional rudimentary attacks, to highly targeted ones, which have the capability to exploit the victims on the basis of cognitive biases and emotional vulnerabilities. AI is being leveraged into creating schemes that are hard to differentiate from legitimate schemes. It is because AI allows the scammers to personalise and automate their deceptive tactics. Understanding the psychological mechanisms that drive cybercriminals as well as the victims, is important. Without a comprehensive understanding, it can be difficult to address the manipulative tactics used in cyber frauds. Cybersecurity professionals will be able to develop more effective cybersecurity measures to protect people from these attacks and help in mitigating the overall impact of cybercrime.

The victims of cybercrime also face emotional and mental distress, beyond the financial losses they suffer. It becomes a root cause for their heightened anxiety, stress, a pervasive sense of vulnerability, and psychological issues like depression, or even PTSD. Individuals also tend to feel less confident in using online platforms as they start distrusting technology. This distrust also deteriorates their ability to communicate with others, and reflects in their relationships, leading to social withdrawal and isolation. In order to develop effective strategies for the rehabilitation and recovery of victims, understanding these psychological effects becomes necessary. Victims can recover better from such a situation if they are provided with comprehensive support, including counseling and educational programs. It helps them overcome their trauma and regain the trust in technologies, in order to start using digital platforms again, with confidence. A multifaceted approach must be adopted to address the technological and psychological aspects of cybercrime, which will help in safeguarding people and organizations from the detrimental effects of cybercrime.

Reduce the Cybercrime Incidences

On the basis of a thorough analysis of psychological aspects cybercriminals and cyber-victims, authorities and cybersecurity professionals can develop and implement several strategies which will help in reducing the incidences of cybercrime.

The recommendations mentioned below are focussed on addressing the already existing psychological mechanisms that influence individuals to commit cybercrime and enhance the resilience of potential victims.

1. Enhanced Cybersecurity Education and Awareness Programs: implementation of comprehensive cybersecurity awareness programs to educate people about the psychological tactics used by cybercriminals is necessary. These programs must educate people about the commonly used techniques, cognitive biases, and the importance of scepticism in online interactions. Individuals can become less likely to fall victim to cybercrime by understanding the manipulation tactics used by cybercriminals. The significance of critical thinking and cautious online behaviour can be reinforced through regular training sessions, workshops, and public awareness campaigns.

2. Promoting Digital Literacy and Critical Thinking: It is important to improve the digital literacy among people in order to help them navigate through the digital landscape in a safe manner. Authorities should promote digital literacy initiatives that teach users how to identify phishing attempts, recognize suspicious online behaviour, and verify the authenticity of online communications. Additionally, fostering critical thinking skills can help individuals assess the credibility of information and resist cognitive biases. Educational institutions should integrate digital literacy and critical thinking into their curricula, ensuring that future generations are better equipped to handle cyber threats.

3. Enhancing Psychological Support and Counselling Services: Recognizing the psychological impact of cybercrime on victims, authorities should provide access to psychological support and counselling services. These services can help victims cope with the emotional aftermath of cybercrime, such as anxiety, stress, and loss of trust. By offering timely psychological support, authorities can aid in the recovery process and reduce the long-term psychological effects on victims. Additionally, providing resources and support groups for cybercrime victims can foster a sense of community and shared experience, further aiding in recovery.

4. Strengthening Legal Frameworks and Enforcement: Authorities should review and strengthen legal frameworks to ensure they adequately address the evolving nature of cybercrime. This includes enacting stringent penalties for cybercriminals to deter potential offenders. Enhanced collaboration between law enforcement agencies, both domestically and internationally, is essential for effectively combating cybercrime. Authorities should also invest in training law enforcement personnel to better understand the psychological profiles of cybercriminals and employ specialized investigative techniques.

5. Enhancing Online Community Moderation and Monitoring: Authorities should work with online platforms to enhance community moderation and monitoring practices. This involves detecting and mitigating harmful behaviours, such as cyberbullying, fraud, and other malicious activities. By creating safer online environments, authorities can reduce the psychological impact on victims and deter cybercriminals. Implementing robust reporting mechanisms and ensuring swift action against offenders can foster a culture of accountability and safety in digital spaces. Promotion of digital literacy needs to be done by the authorities in order to teach users how to identify scams like phishing, and suspicious online behaviour. They should also be taught how to verify the authenticity of online communications. Individuals can improve their critical thinking skills to resist cognitive biases by taking these workshops and get a better understanding of how to assess the credibility of information. The curriculum of educational institutions must also have digital literacy and critical thinking in order to make sure that students are better equipped to deal with cyber threats and attacks.

3. Enhancing Psychological Support and Counselling Services: The authorities should recognise the adverse impact cybercrime has on the victims in psychological terms, and provide psychological support and counselling services. Such services can help the victims in recovering from the trauma and emotional aftermath of a cyberattack. Victims find it hard to deal with their heightened anxiety, stress, and loss of trust. Authorities can aid their recovery by offering them timely psychological support, and even reduce the long-term effects on the affected individuals. In addition to that, authorities can also provide resources and support groups for the victims. This will make them feel like they belong to a community with shared experiences, further helping them recover from the trauma.

4. Strengthening Legal Frameworks and Enforcement: legal frameworks must be evaluated and strengthened in order to ensure that cybercriminals are strictly penalised. An improved collaboration between domestic as well as international law enforcement agencies is necessary to deal with cybercrime in an effective way. Law enforcement personnel should also be trained well in order to understand the psychological profiles of cybercriminals in a better manner. Investing in their training will help the personnel in employing specialized investigation techniques.

5. Enhancing Online Community Moderation and Monitoring: Community moderation should be enhanced along with monitoring different practices. Authorities can make moderation more effective by working with online platforms. This involves the detection and mitigation of behaviours that may cause harm to people or organisations. These behaviours include cyberbullying, fraud, and other malicious activities. Authorities can help in reducing the overall impact of cybercrime on the psychology of a victim, by creating safer online environments. Authorities can foster a culture of accountability where robust reporting mechanisms are implemented and quick action against offenders is taken to create a safer digital world.

References

Aiken, M. P., Davidson, J. C., Walrave, M., Ponnet, K. S., Phillips, K., & Farr, R. R. (2024). Intention to Hack? Applying the Theory of Planned Behaviour to Youth Criminal Hacking. *Forensic Sciences*, *4*(1), 24-41.

Ancis, J. R. (2020). The age of cyberpsychology: An overview. American Psychological Association. Technology, Mind, and Behavior. Pp. 1-6.

Attrill-Smith, A., & Wesson, C. (2020). The psychology of cybercrime. *The Palgrave handbook of international cybercrime and cyberdeviance*, 653-678.

Attrill-Smith, A., Fullwood, C., Keep, M., & Kuss, D. J. (2019). *The Oxford handbook of cyberpsychology*. Oxford University Press.

Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. In *Emerging cyber threats and cognitive vulnerabilities* (pp. 73-92). Academic Press.

Bada, M., & Nurse, J. R. (2021). Profiling the cybercriminal: A systematic review of research. In *2021 international conference on cyber situational awareness, data analytics and assessment (CyberSA)* (pp. 1-8). IEEE.

Bada, M., & Nurse, J. R. (2023). Exploring Cybercriminal Activities, Behaviors, and Profiles. In *Applied Cognitive Science and Technology: Implications of Interactions Between Human Cognition and Technology* (pp. 109-120). Singapore: Springer Nature Singapore.

Balick, A. (2018). *The psychodynamics of social networking: Connected-up instantaneous culture and the self*. Routledge.

Bansod, N., Kamble, D. B., Mishra, R., & Kuliha, M. (2022). Forecasting the Traits of Cyber Criminals Based on Case Studies. In *Dark Web Pattern Recognition and Crime Analysis Using Machine Intelligence* (pp. 220-234). IGI Global.

Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. *Ieee Access*, *10*, 77110-77122.

Borwell, J., Jansen, J., & Stol, W. (2022). The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory. *Social Science Computer Review*, *40*(4), 933-954.

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Routledge.

Cross, C. (2022). Using artificial intelligence (AI) and deepfakes to deceive victims: the need to rethink current romance fraud prevention messaging. *Crime Prevention and Community Safety*, *24*(1), 30-41.

Firdaus, R., Xue, Y., Gang, L., & Sibt e Ali, M. (2022). Artificial intelligence and human psychology in online transaction fraud. *Frontiers in Psychology*, *13*, 947234.

Garcia, N. (2018). *The use of criminal profiling in cybercrime investigations* (Doctoral dissertation, Utica College).

Goutam, R. K., & Verma, D. K. (2015). Top five cyber frauds. *International Journal of Computer Applications*, *119*(7).

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of ai-driven cyber attacks: A review. *Applied Artificial Intelligence*, *36*(1), 2037254.

Gupta, P., & Mata-Toledo, R. A. (2016). Cybercrime: In Disguise Crimes. *Journal of Information Systems & Operations Management*, *10*(1).

Harley, D., Morgan, J., & Frith, H. (2018). *Cyberpsychology as everyday digital experience across the lifespan*. Springer.

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, *73*, 102-113.

Hay, C., & Ray, K. (2020). General strain theory and cybercrime. *The Palgrave handbook of international cybercrime and cyberdeviance*, 583-600.

Hidayati, A. N., Riadi, I., Ramadhani, E., & Al Amany, S. U. (2021). Development of conceptual framework for cyber fraud investigation. *Register*, *7*(2), 125-135.

Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR)*, *53*(1), 1-34.

Kaur, C.J., Bhandari, A., & Behal, S. (2019). Distributed denial of service attacks: a threat or challenge. *New Review of Information Networking*, *24*(1), 31-103.

Kemp, S., Miró-Llinares, F., & Moneva, A. (2020). The dark figure and the cyber fraud rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research*, *26*(3), 293-312.

Kirwan, G. (2016). Introduction to cyberpsychology. In *An introduction to cyberpsychology* (pp. 2-14). Routledge.

Lillie, M. E. (2017). *Think before you click: The effects of systematic processing on phishing susceptibility* (Doctoral dissertation).

March, E. (2022). Psychopathy: Cybercrime and cyber abuse. In *Psychopathy and Criminal Behavior* (pp. 423-444). Academic Press.

Matveev, V., Khrypko, S., Nykytchenko, O., Stefanova, N., Ishchuk, A., Ishchuk, O., & Bondar, T. (2021). Cybercrime in the Economic Space: Psychological Motivation and Semantic-Terminological Specifics. *IJCSNS International Journal of Computer Science and Network Security*, *21*(11), 135-142.

Miftari, A., Luma-Osmani, S., & Idrizi, F. (2022). Analysis of cybercriminals and where they fall on the spectrum of crime. In *2022 International Conference on Data Analytics for Business and Industry (ICDABI)* (pp. 287-291). IEEE.

Mohammed, A. M., Benson, V., & Saridakis, G. (2020). Understanding the relationship between cybercrime and human behavior through criminological theories and social networking sites. In *Encyclopedia of Criminal Activities and the Deep Web* (pp. 979-989). IGI Global.

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology*, *12*, 561011.

Nadeem, M., Zahra, S., Abbasi, M., Arshad, A., Riaz, S., & Ahmed, W. (2023). Phishing Attack, Its Detections and Prevention Techniques. *International Journal of Wireless Security and Networks*, *1*(2), 13-25p.

Norman, K. L. (2017). *Cyberpsychology: An introduction to human-computer interaction*. Cambridge university press.

Parsons, T. D. (2019). *Ethical challenges in digital psychology and cyberpsychology*. Cambridge University Press.

Perenc, L. (2022). Psychopathic personality disorder and cybercriminality: an outline of the issue. *Current Issues in Personality Psychology*, *10*(4), 253.

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic sciences*, *2*(2), 379-398.

Pienta, D., Sun, H., & Thatcher, J. (2016). Habitual and misplaced trust: the role of the dark side of trust between individual users and cybersecurity systems.

Pureti, N. (2022). Zero-Day Exploits: Understanding the Most Dangerous Cyber Threats. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 70-97.

Sánchez-Hernández, M. D., Herrera, M. C., & Expósito, F. (2024). Perception of cyberdating abuse from the victims' perspective: effect of the type of suffered behavior and gender. *Current Psychology*, 1-14.

Sanne, P. N., & Wiese, M. (2018). The theory of planned behaviour and user engagement applied to Facebook advertising. *South African Journal of Information Management*, *20*(1), 1-10.

Shang, Y., Wu, Z., Du, X., Jiang, Y., Ma, B., & Chi, M. (2022). The psychology of the internet fraud victimization of older adults: A systematic review. *Frontiers in psychology*, *13*, 912242.

Sincek, D., Duvnjak, I., & Milic, M. (2017). Psychological outcomes of cyber-violence on victims, perpetrators and perpetrators/victims. *Hrvatska revija za rehabilitacijska istraživanja*, *53*(2), 98-110.

Spitaletta, J. A., & Hopkins, J. (2021). Cyberpsychology: Adapting a Special Operations Model for Cyber Operations. White Paper- *Strategic Multilayer Assessment*. Pp 1-22.

Sriman, B., Kumar, S. G., Dhanushram, S., Balaji, K., & Priyan, P. A. (2023, November). A Systematic Study About Crypto Jacking. In *2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE)* (pp. 1-7). IEEE.

Sripriyanka, G., & Mahendran, A. (2021, December). Mirai Botnet Attacks on IoT Applications: Challenges and Controls. In *International Conference on Information Systems and Management Science* (pp. 49-67). Cham: Springer International Publishing.

Stalans, L. J., & Donner, C. M. (2018). Explaining why cybercrime occurs: Criminological and psychological theories. *Cyber criminology*, 25-45.

Thakur, M. (2024). Cyber security threats and countermeasures in digital age. *Journal of Applied Science and Education (JASE)*, *4*(1), 1-20.

Vaithianathasamy, S. (2019). AI vs AI: fraudsters turn defensive technology into an attack tool. *Computer Fraud & Security*, *2019*(8), 6-8.

Vakhitova, Z. I., Alston-Knox, C. L., Reeves, E., & Mawby, R. I. (2022). Explaining victim impact from cyber abuse: An exploratory mixed methods analysis. *Deviant Behavior*, *43*(10), 1153-1172.

Van de Weijer, S. G., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407-412.

Velasco, C. (2022, May). Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. In *ERA Forum* (Vol. 23, No. 1, pp. 109-126). Berlin/Heidelberg: Springer Berlin Heidelberg.

Whitty, M. T. (2016). *Cyberpsychology: The study of individuals, society and digital technologies*. John Wiley & Sons.

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277-292.

Yamin, M. M., Ullah, M., Ullah, H., & Katt, B. (2021). Weaponized AI for cyber-attacks. *Journal of Information Security and Applications*, *57*, 102722.

Zhao, L., & Yu, J. (2021). A meta-analytic review of moral disengagement and cyberbullying. *Frontiers in Psychology*, *12*, 681299.

Zouave, E., Bruce, M., Colde, K., Jaitner, M., Rodhe, I., & Gustafsson, T. (2020). Artificially intelligent cyberattacks. *Stockholm: Totalförsvarets forskningsinstitut FOI [Online] Available: https://whttps://www. statsvet. uu. se/digitalAssets/769/c_769530-l_3-k_rapport-foi-vt20. pdf [Accessed: Sep. 28, 2022]*.

Zuhri, F. (2017). The Profile of a Cybercriminal. *Digital Forensic Magazine.* Available on: http://digitalforensicsmagazine.com/blogs/wp-content/uploads/2017/05/The-Profile-of-Cybercriminal. pdf.