Spring 2023

The Concept of Social Engineering and Cybercrime in the Digital Age

Chaitanya Reddy Eleti

The Concept of Social Engineering and Cybercrime in the Digital Age

By

Chaitanya Reddy Eleti

B. Tech, St. Martin's Engineering College, 2020

THESIS

Submitted in partial fulfilment of requirements.

For the Degree of Master of Science,

with a Major in Information Technology

Governors State University

University Park, IL 60484

2023

Table of Contents

Abstract

The increased implementation of digitalization which has come to rise has also raised concerns in terms of privacy and security of the data. Data leaks and stealing of privacy are some of the common practices which have grown over the years. Social engineering majorly depends on the normal human instincts for trusting in stealing personal as well as corporate information which can be implemented for committing the cybercrimes further. The attackers can use social engineering for convincing an employee for divulging the passwords of the company. Hence, there is a need to understand the fact of how social engineering can as well as cybercrime have evolved over the year. Based on this the work aimed to review the social engineering concepts as well as cybercrimes in this digital world. The concepts will be understood better with the use of literature that is focused on the topic of social engineering as well as cybercrimes. Using a literature review the secondary data will be collected based on this literature.

Introduction

Background

The age of digitalization has brought revolutionary changes in the manner in which persons and organizations interrelate with one another. The usage of the internet and another kind of digitalized techniques have made the easiest for communication, sharing of information, and the conducting of transactions of organizations. As the digitalized universe became more complicated and integrated with the life of daily routine, there are several techniques in which the concept of cybercrimes can impact people. The attack on the workplace is uncompromising, and most of the attacking members are the criminals of the cyber that have the capability of the occupied the person or the problems and exploiting their inabilities. All these attackers make the social engineering (SE) concept their most dominating attacking technique. The hacker has shifted from the computerized exploitable strike to the more personal attack that is taking benefit of the mistakes. The issue of SE helps cybercriminals induce the faculties to develop susceptibility, contaminate the structure, transfer funds, and the stealing of authorization. Cybercrime is a big mistake for the economy, one's protection, and also most of the public in a generalized manner as it is the first source of terror (Alghamdi, 2020).

The methods of SE use the technique of the emotional for the creation of the betrayal. Most of the workers are becoming the main aim of the social engineer and their crime. Most of the other people had said the basic step in any malpractice is the gaining of data in an unauthorized manner. As soon as the end user takes the data in use which is available to the hacker, then this will create a danger for the computer system of the company. This then turned into the third attack on the major aim of the system controlling programming of the company in which the transportation, finance, or the data of the DB is revealed. The attack on SE is not only making basic but also becoming more progressive and complicated. The attacker comes up with more tricks to fool the organization team. In such kind of situations, the companies required modern and comprehensive cyber safety social planning keys so that they can face any misleading activity of the cyber attackers. SE is the skill to manipulate others in the form of disrupted private information or taking action that is beneficial to the traducer and cybercrimes on the second hand is any type of suspect task that includes the usage of the internet or the computerized system (Aldawood & Skinner, 2019).

Information security is the fastest-growing discipline. There are various choices at current for the protection of the hardware and the application that is against the outside and the inside harmful attacks on the information system but there is the shortest research on the softest components or the human-made elements in data safety. It is the catching-all word for the widest choices of threats. The various type of the working is carried out with the help of the relationship between human beings. At this time, the socialized engineer takes the usage of the facilities and the platform that created the bottom work for the complicated social engineer attacking for obtaining admission into the information structure and the various other places. The usage of conversation technology, the advancement of the technique, and the interest in both the public and the private sets had made the situation very complicated. It is suitable for determining the stage of deep penetration in the instance of the social engineer that includes the concept of SE in cyber safety.

This documentation helps in discussing increased execution of the digital era that helps in increasing the issues related to the privacy and the security of the information. The leaking of data or the stealing of information is much common process that grows in certain yrs. These attackers make use of social media engineering for the workers to divulge the passkeys of the organization for the understanding of the facts of the concept of the social engineer with the misconduct in the digitalized world.

The title is SE and Cybercrimes in the digital age where SE can destroy the method used by human mistakes exploit for the gaining of personal access or the information that has the most value in the cybercrime for the person hack scam that leads to the lure unethical human.

Aim

This research aims to understand the concept of SE and cybercrime in the digital age.

Objectives

- To understand SE and cybercrime.
- To understand the impact of cybercrime in the digital age.
- To understand various reasons for cybercrime and their impact
- To understand the social impact of cybercrime

Problem Domain

The attacks of SE go into one or more stages. The criminal first of all search the main victim for gathering data on the background of the details, like the main point of the entrance and the weakest safety protocol that is required for proceeding with the attacks. Then the hacker put forward the gaining the belief of the sufferer and gives some encouragement for the basic action that can steal the safety approach like the revealing of the sensational data or the grant of the obtainment to the crucial source. These attacks come in various formats like pretexting, phishing, and baiting. All this focus on the person thing of the structure quite a bit then destructing the computerized weakness (Salahdine & Kaabouch, 2019).

Cybercrime on the other aspect passes from the different wrongdoings that are carried out in cyberspace. They make use of the internet and other digitalized technique for committing a crime like hacking, identification stealing, and phishing. This can lead to a loss in the finance, damage the goodwill of the organization, and can even harm the persons (Almutairi & Alghamdi, 2022).

Rationale

The issue of SE and cybercrime in the digitalized age is essential as it describes the requirement of one person and the organization to the watchful and energetic in the protection of the details and the structure. The use of the internet has made it easiest for cybercriminals the conducting activity and techniques are making more significant. As there is the pervasiveness of the misleads and the attack of the social engineer has become more pronounced in the pandemic the covid-19. With the transformation to remote work and the dependency on social platforms, people and organizations are becoming more unsafe to these threats. So there is a requirement to expand the realization and the learning on the measures of cyber safety for the mitigation of the danger that is linked with this ultimatum.

Literature Review

Social Engineering and Cybercrime

In the digital age, SE and cybercrime have become two major concerns in the realm of information security. Cybercriminals use various techniques to manipulate individuals or organizations into providing confidential information or executing malicious software. SE is a term used to describe a psychological manipulation that aims to exploit human behavior for personal gain. SE is a strategy used by cybercriminals to gain access to sensitive information by exploiting human behavior. According to the Conteh (2021), SE relies on the manipulation of individuals by using techniques such as pretexting, phishing, and baiting. Pretexting involves the use of a fake identity to gain access to information or systems. Baiting involves offering a reward or benefit to trick an individual into divulging sensitive information or installing malicious software. Quid pro quo involves the exchange of something of value for sensitive information. Cybercriminals use a combination of tactics to gain access to information or systems, and once they have access, they can use the information for financial gain or other malicious purposes.

As per the Abu Hweidi et al., (2023), Identity theft involves the use of personal information to impersonate someone else for financial gain. Cybercrime is a constantly evolving field, and cybercriminals are becoming more sophisticated in their tactics. The use of machine learning and artificial intelligence is also making it easier for cybercriminals to launch attacks. SE is often used as a tactic to launch cybercrime attacks. SE can also be used to launch other forms of cybercrime, such as malware attacks. A baiting attack may involve offering a free USB drive that contains malware. When an unsuspecting victim inserts the USB drive into their computer, the malware is installed, and the cybercriminal gains access to the victim's system.

The manner of conversation, work and the conduction of the organization has gone through essential changes in the digitalized area. These changes had been giving new choices for acquiring personalized information on the positive aspects of the physiological and the behavioral tendency in the persons. In the current years, SE, a kind of cyber spank that involves the trick to the person into the disclosure of personal data, had grow in the popularised format.

Impact of Cybercrime in the Digital Age

Cybercrime has become a pervasive threat in the digital age, affecting individuals, businesses, and governments worldwide. Cybercrime can take various forms, such as hacking, phishing, malware, ransomware, and identity theft.

Impact on Individuals

In the same context Alghamdi (2020), discuss that cybercrime has a significant impact on individuals. Identity theft is one of the most prevalent forms of cybercrime and can cause financial, emotional, and reputational harm. When an individual's personal information is stolen, it can be used to open fraudulent accounts, make unauthorized purchases, or apply for loans. Victims of identity theft may spend countless hours and resources trying to rectify the damage caused by the cybercrime. Phishing attacks can also have a significant impact on individuals. Victims of phishing attacks may unwittingly provide login credentials or other sensitive information, which can be used to commit identity theft or other forms of cybercrime.

Impact on Businesses

In the business context Johnson et al., (2020) discuss that cybercrime has a significant impact on businesses. Cybercriminals often target businesses to gain access to sensitive information or systems. A data breach can cause significant financial, legal, and reputational harm to a business. Businesses that suffer a data breach may be subject to lawsuits, fines, and other legal consequences. Ransomware attacks are another significant threat to businesses. A ransomware attack can cause significant disruption to a business's operations and may result in the loss of critical data.

Impact on Governments

Cybercrime also has a significant impact on governments. As per the Carter (2019), cybercriminals often target government agencies to gain access to sensitive information or systems. A cyberattack on a government agency can compromise national security, disrupt essential services, or cause significant financial harm. Governments may also be subject to legal and diplomatic consequences if a cyberattack is traced back to another country. Cybercrime can also pose a threat to democratic processes. For example, there have been instances of foreign interference in elections through the use of social media bots and the dissemination of fake news. This type of cybercrime can undermine public trust in democratic processes and institutions. Cybercrime can also compromise national security and democratic processes, leading to a loss of public trust in institutions. Cybercrime is a significant threat in the digital age that requires ongoing attention and investment in information security.

Various Reasons for Cybercrime and Their Impact

Cybercrime has become a pervasive threat in the digital age, affecting individuals, businesses, and governments worldwide. Cybercrime can take various forms, such as hacking, phishing, malware, ransomware, and identity theft. This literature review aims to explore the various reasons for cybercrime and their impact.

Reasons for Cybercrime:

Koto (2020) express the one of the most common reasons for cybercrime is financial gain. Cybercriminals may target individuals, businesses, or governments to steal money, credit card information, or other financial data. Cybercrime can also be motivated by political agendas. Governments or political groups may engage in cybercrime to steal sensitive information, disrupt essential services, or interfere with democratic processes. Cybercrime can be used as a tool of espionage or to undermine the stability of a country or region. Cybercrime can also be motivated by personal vendettas. Individuals may engage in cybercrime to harass, intimidate, or embarrass others. Cybercrime can take various forms, such as cyberbullying, doxing, or revenge porn. Cybercrime can also be motivated by ideological beliefs. Hacktivist groups may engage in cybercrime to promote a particular social or political agenda. For example, Anonymous, a well-known hacktivist group, has targeted various governments, corporations, and organizations to protest against perceived injustices. Cybercrime can also be motivated by malicious intent. Some cybercriminals may engage in cybercrime simply for the thrill of it. These individuals may engage in hacking or other forms of cybercrime to test their skills or to satisfy their curiosity.

Impact of Cybercrime:

Cybercrime can cause significant financial losses to individuals, businesses, and governments. When financial data is stolen, it can lead to unauthorized purchases, fraudulent loans, or other forms of financial harm. According to the Oluwatoyin et al., (2020), businesses that suffer a data breach may lose customer trust and revenue. Governments may also experience financial losses due to the cost of investigating and responding to cybercrime. Cybercrime can also have legal consequences. Individuals or organizations that engage in cybercrime may be subject to lawsuits, fines, and other legal consequences. Governments may also be subject to diplomatic or legal consequences if a cyberattack is traced back to another country. Cybercrime can also cause reputational harm to individuals, businesses, and governments. When sensitive

information is stolen, it can harm an individual or organization's reputation and lead to a loss of trust from customers or constituents.

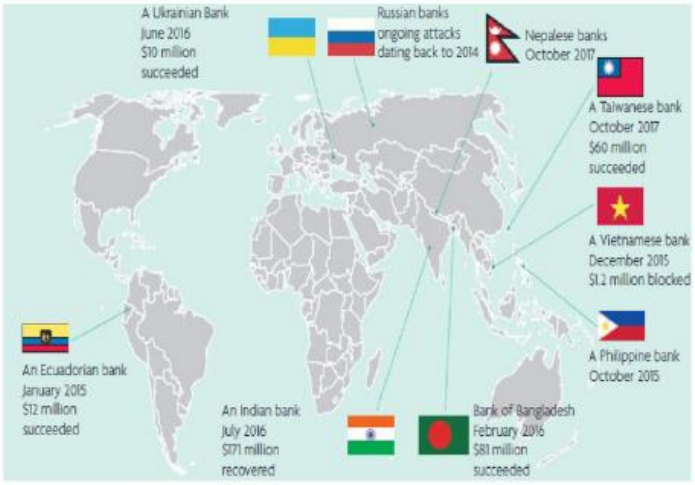

Figure 1 Some Cyber-attacks in Different Countries

Source: (Oluwatoyin et al., 2020).

Figure 1 shows the cyber-attacks in the banking sector. Cybercrime can also pose a threat to national security. Cyberattacks on critical infrastructure, such as energy or transportation systems, can lead to significant disruptions and harm to the economy. Cyberattacks on government agencies can compromise national security and lead to diplomatic or military consequences. Cybercrime can also cause emotional distress to individuals who are victimized. Victims of cybercrime may experience anxiety, depression, or other forms of emotional harm. The emotional impact of cybercrime can be particularly severe in cases of cyberbullying, or other forms of online harassment.

The Social Impact of Cybercrime

Cybercrime has become a pervasive threat in the digital age, affecting individuals, businesses, and governments worldwide. While the financial and legal impacts of cybercrime are well-documented, the social impacts of cybercrime are often overlooked. Monteith et al., (2021), analyzed that cybercrime can erode trust between individuals, businesses, and governments. When sensitive information is stolen or leaked, it can harm an individual or organization's reputation and lead to a loss of trust from customers or constituents. The loss of trust can have a long-lasting impact on relationships and can be difficult to repair. Cybercrime can also have significant impacts on privacy. When personal data is stolen or leaked, it can lead to a loss of privacy and an invasion of personal space. Victims of cybercrime may feel violated, exposed,

and vulnerable, leading to feelings of anxiety and distress. Cybercrime can also lead to social isolation. When individuals become victims of cybercrime, they may become fearful of using technology or engaging with others online. This can lead to feelings of loneliness and social isolation, as individuals may become disconnected from friends and family who primarily communicate online. Cybercrime can also lead to stigmatization. Victims of cybercrime, particularly those who have experienced cyberbullying, doxing, or revenge porn, may feel ashamed and embarrassed. This can lead to a sense of social stigma, as individuals may feel that they have been judged or labeled unfairly. Cybercrime can also have significant impacts on mental health. Victims of cybercrime may experience anxiety, depression, or other forms of emotional harm. The emotional impact of cybercrime can be particularly severe in cases of cyberbullying, revenge porn, or other forms of online harassment.

Apau & Koranteng (2020) discuss in the paper that cybercrime can also contribute to the digital divide. When individuals become victims of cybercrime, they may become fearful of using technology or engaging with others online. This can lead to a widening gap between those who feel comfortable using technology and those who do not, further marginalizing already vulnerable populations. Cybercrime can also impact cybersecurity culture. When individuals or organizations become victims of cybercrime, they may become more aware of the need for cybersecurity measures. This can lead to a more robust cybersecurity culture, as individuals and organizations take steps to protect themselves and others online. Cybercrime has significant social impacts, affecting trust, privacy, social isolation, stigmatization, mental health, the digital divide, and cybersecurity culture. These impacts are often overlooked in discussions of cybercrime, but they are no less important than the financial and legal impacts. As the threat of cybercrime continues to grow, it is important to consider the social impacts and take steps to mitigate them.

The exploitation of the person's emotions like the fearless, greediness, and curiosity is the harmful perspective of the socialized engineer phycology. It is complicated to be more skillful at defending against attacks of cyber. The strongest passcode and two-factorized authentication are all approaches for the protection of one.

Research Framework

It is the corrected structure of the research assignment planning. With the help of the research layout, one can easily describe the complicated sections of the investigation. It will also permit us to bring with the related question of the research and their objectives. For the development of the research, there should be a team working in the organization or the group. These all people may involve localized authority, contractors, voluntary grouping, and the affected singles (Chun Tiem et al., 2019). First of all, the topic is selected for the research, by selecting the research topic, the goal and objective are determined, which will be helpful in conducting the research in a specific way. Based on the aims and objectives, research questions were formulated which are helpful in conducting the literature review. Thorough review of academic literature, including peer-reviewed papers, books, and reports, will be used as the study technique. Electronic resources such as JSTOR, ScienceDirect, and Google Scholar will be used for the searching of data. In the search phrases some specific keywords will be used to search for the articles and paper such as "social engineering," "cybercrime," "digital age," "phishing," "spear-phishing," "vishing," and "smishing." The important themes that arise from the literature review will be recognized, and the data will be classified based on these topics. The concepts covered will include the notion of SE and the link between SE and cybercrime, the many forms of SE assaults, the effects of SE attacks, and ways for limiting the risks of SE attacks was analyzed through the research papers.

This framework is described with the help and use of the research onion. It is the layout that will help in the creation of a robust research methodology, this will help the investigator in making the sequence of decisions that will help in allowing the organized research. It involves six different layers namely philosophy, the approach of research, strategy, choices, time horizons, and the procedure and techniques.

Research philosophy: There are various types of philosophies including positivism, interpretivism, pragmatism, and realism. This research had taken use of the positivist philosophy. It is related to the actual skill that is gained with the help of monitoring.

Research approach: There are two approaches – inductive and deductive. This investigation used the inductive method as the research is conducted on the bases of the research questions.

Research strategy: This investigation has taken use of the grounded theory and the literature review. It is the step-by-step planning of the act that provides the direction to the investigator's thinking procedure. It will help the investigator in conducting the investigation in a sequenced

manner on time. the main aim is to organize the main elements of the conduction like the research topic, area, main focus, the designing, and the final research methodology.

Research choices: This investigation used the mono method. It will only use one type of data and this has used qualitative research. In this research data is collected with the help of literature review.

Time horizons: There are two kinds of horizons- longitudinal and cross-sectional. This research used the cross-sectional time horizons. It is the constant point of the timing in the upcoming section in which the various procedures will be measured or to be assumable at the end.

Techniques and procedures: These are the centralized part of the research. In this research, the secondary data collection method has been used in which there is the use of articles, journals, and related authors' books. Along with that, there is the use of thematic analysis which is the method for the analysis of qualitative information that includes the reading with the data and the patterns (Jansen, 2021).

Future Research Agenda

The long-time investigation purpose is the sequence of the intense or the plan programming measurement and the tools of the research that are created to address an investigation of the aim (Loureiro et al., 2021). As technology keeps on evolving at a fast pace, there will be cybercrimes.

The concept of cybercriminals and SE in the digitalized age is the ever evolve and crucial matter that required a flow researching. As the technique will grow in an advancing manner then the technique also goes on increasing. With the use of ai and the ml algorithms continuing to growable, the investigator was required to search the risks and the harmfulness linked with the techniques. This will involve the exploitation of artificial intelligence and machine learning, concepts.

The criminals or the hackers use various tricks and even the older solution of hacking. Artificial intelligence goes in both manners in cyberspace. It can both be considered a blessing and even a curse. As with the coming of the IoT device, they had predicted the commitment of a greater number of cyber-attacks. The use of AI and the IoT makes it easiest to hack things (Eira, 2019). If any kind of device is connected in an online manner, then it will carry risk also. As well as there is the target of the harmful account that is accessed with the help of phishing mail and texting, the concept of social media will be used for the delivery of the phishing. As compared

with the previous year, the number of cyber criminals is predicted to rise by 20% at the end of 2023 (*UK Cyber Security and Cyber Crime Statistics in 2023*, 2023).

Conclusion

The issue of SE and cybercrime in the digitalized age is important in understanding the requirement for the increasing amount of the measure of cybersecurity. As there is more evolution of technology, cyber hackers will search the new manner for exploiting the sensitivity. Learning the various kinds of SE and cybercrime hacking is crucial in the development of an effective preventive strategy and the mitigation of the hazards that are linked with the danger. All the persons and the organization should be proactive in the protection of the system and the information by the execution of accurate safety policies and should be attentive in their online mode tasks. The measurement of the study review for the crucial appraisal is measured on the concept of the technique being used, the results, and the conclusion for the identification of the limitation that is posed by the adoption of the various policies and their apparatus. There were several measures had been taken for controlling SE attack that involves education, learning, and increases awareness among the workers. The development and adoption of evolving data security measures build the overall workplace safety culture. A policy like compulsory assent, not an allowable plugin, and the manner for treating and disposing of the hard data minimize the chance of the information breach and the leak of the organization's information. The concept of cybercrime is obtained fastest in both developed country and the one that is developing. Most cyber hacks case goes through unreported due to the fear of humiliation. Computerized crimes are not taken as the goal in most of the country. For the effective combating of cybercrime, there is the requirement of the readjustment of rules of hacking and the formalization all over the world. The crimes are different in various countries. The identification and categorization of the crimes that are computerized must be adopted by all the counties all over the globe. Accordingly, with less usage of common thinking and logic, there can be a stoppage of cybercrime to happen. In the all over, it can be said that cyber-attack is the harmful element to one privacy or any kind of thing.

References

Abu, & Eleyan, D. (2023). Social Engineering Attack concepts, frameworks, and Awareness: A Systematic Literature Review. *International Journal of Computing and Digital Systems*. https://doi.org/2210-142X

Aldawood, H., & Skinner, G. (2019). Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal. *Geoffrey Skinner International Journal of Security (IJS)*, *10*, 1. https://f.hubspotusercontent30.net/hubfs/8156085/WhitePaper%20-%20IJS%20-%20Contemporary%20Cyber%20Security%20Social%20Engineering%20Solutions%5B1%5D.pdf

Alghamdi, M. I. (2020). A descriptive study on the impact of cybercrime and possible measures to curtail its spread worldwide. International Journal of Engineering Research and Technology, 9, 731-5. https://www.academia.edu/download/63825161/a-descriptive-study-on-the-impact-IJERTV9IS06056520200704-31501-1be537a.pdf

Almutairi, B. S., & Alghamdi, A. (2022). The Role of Social Engineering in Cybersecurity and Its Impact. *Journal of Information Security*, *13*(04), 363–379. https://doi.org/10.4236/jis.2022.134020

Apau, R., & Koranteng, F. N. (2019). Impact of cybercrime and trust on the use of e-commerce technologies: An application of the theory of planned behavior. International Journal of Cyber Criminology, 13(2). https://www.researchgate.net/profile/Richard-Apau/publication/339941462_Impact_of_Cybercrime_and_Trust_on_the_Use_of_E-Commerce_Technologies_An_Application_of_the_Theory_of_Planned_Behavior/links/5e6e3adda6fdccf994cb8ef6/Impact-of-Cybercrime-and-Trust-on-the-Use-of-E-Commerce-Technologies-An-Application-of-the-Theory-of-Planned-Behavior.pdf

Carter, W.A., (2019). Ensuring Data Security Against Lawful and Unlawful Threats in the Digital Age. Washington, DC: Center for Strategic & International Studies (CSIS). Retrieved July, 30, p.2022.https://www.jstor.org/stable/pdf/resrep37518.pdf

Chun Tie, Y., Birks, M., & Francis, K. (2019). Grounded theory research: A design framework for novice researchers. SAGE open medicine, 7, 2050312118822927. https://journals.sagepub.com/doi/pdf/10.1177/2050312118822927

Conteh, N.Y., (2021). The dynamics of social engineering and cybercrime in the digital age. In Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention (pp. 144-149). IGI Global.https://www.igi-global.com/chapter/the-dynamics-of-social-engineering-and-cybercrime-in-the-digital-age/282231

Eira, A. (2019, October 21). While world governments have their hands full dealing with COVID-19 pandemic, shady cyberheist operators a. Financesonline.com; FinancesOnline.com. https://financesonline.com/cybercrime-trends/#:~:text=With%20the%20advent%20of%20IoT,the%20risk%20of%20getting%20hacked.

Jansen, D. (2021, January 26). Saunders' Research Onion Explained (+ Examples) - Grad Coach. Grad Coach. https://gradcoach.com/saunders-research-onion/

Johnson, D., Faulkner, E., Meredith, G., & Wilson, T. J. (2020). Police Functional Adaptation to the Digital or Post Digital Age: Discussions with Cybercrime Experts. *The Journal of Criminal Law, 84*(5), 427–450. https://doi.org/10.1177/0022018320952559

Koto, I., (2021). Cyber Crime According to the ITE Law. International Journal Reglement & Society (IJRS), 2(2), pp.103-110.http://jurnal.bundamediagrup.co.id/index.php/ijrs/article/view/124

Loureiro, S. M. C., Guerreiro, J., & Tussyadiah, I. (2021). Artificial intelligence in business: State of the art and future research agenda. Journal of business research, 129, 911-926.https://www.sciencedirect.com/science/article/pii/S0148296320307451

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports*, *23*(4). https://doi.org/10.1007/s11920-021-01228-w

Oluwatoyin Esther Akinbowale, Heinz Eckart Klingelhöfer, & Mulatu Fekadu Zerihun. (2020, June 16). *Analysis of cyber-crime effects on the banking sector using the balance score card: a survey of literature*. ResearchGate; Emerald. https://www.researchgate.net/publication/342298927_Analysis_of_cyber-crime_effects_on_the_banking_sector_using_the_balance_score_card_a_survey_of_literature

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 89. https://www.mdpi.com/438626

UK Cyber Security and Cyber Crime Statistics in 2023. (2023). Comparitech.com. https://www.comparitech.com/blog/information-security/uk-cyber-security-statistics/