Bachelor of Science with Honours in Computing Science/ Bachelor of Science with Honours in Cyber Security

COURSEWORK No. 1

Module Name : Contemporary Issues in Computing

Module Code : PSB303/603IT

Weighting : 40%

Due Date : 14 APR 2024

SUBMITTED BY

NAME : CHAN JUN QI JULIUS

CU Index No. : 269J87PE

Word Count : 1633

Table of Contents

Table of Figures

1.0 Abstract

The paper looks at three modern computer issues: internet addiction, phishing attempts, and deepfake technologies. These challenges have spread across the digital culture, impacting individuals, companies, and cultural standards.

The research looks at the prevalence and consequences of internet addiction, the strategies used in phishing assaults, and the ethical implications of deepfake technology. Previous studies have emphasized the broad nature of these challenges, but further knowledge and analysis are required.

Key findings of this study include the prevalence of internet addiction, the advance of phishing methods, and the ethical issues underlying deepfake technology. These findings highlight the necessity of addressing these issues and taking steps to prevent their negative effects.

The significance of this paper lies in its capacity to provide insights into laws, practices, and innovations that uphold the moral and responsible use of technology.

This paper contributes to attempts to establish a digital future that prioritizes integrity, security, and social well-being by increasing awareness and knowledge of these existing issues.

s

2.0 Introduction

Have you ever found yourself passively browsing through the internet, unable to pull yourself away from the digital world? Perhaps you've fallen victim to a fraudulent email scam, discovering too late from the implications of a single click. In the digital world we live in today, technology has gradually become part of our daily lives, frequently in unforeseen manners. However, this integration also brings with it a variety of contemporary issues that influence the way our digital world looks.

The computing industry faces a wide range of contemporary issues that have an impact on individuals, corporations, governments, and society as a whole. These challenges range from concerns and ethical issues raised by various technologies.

This paper looks at three major contemporary computing issues: internet addiction, phishing attacks, and deepfake technology of artificial intelligence. It explores into the ethical, business, and societal implications of these issues, which are critical for numerous stakeholders.

This research aims to provide an understanding, foster discussion, and offer a personal perspective on the development of technology that is not only ethically safe but helpful to society as a whole.

Through thorough research and analysis of various resources such as book publications, articles on the internet, and research papers, the goal is to shed light on these critical challenges and pave the way for ethical advancement in technology.

3.0 Contemporary Issues

3.1 Deepfake Technology from Artificial Intelligence (AI)

Deepfake technology has become more common in the emerging field of Artificial Intelligence (AI), raising ethical issues about justice, privacy, autonomy, and societal values. With the use of artificial neural networks, digital media may be modified to produce content that is both completely fake and incredibly lifelike.

Deepfakes can be used to spread fake news, influence elections, introduce highly realistic fake audio evidence in courts, and make fake obscene movies. Each of these applications potentially has a big impact on society, social relationships, democracy, and financial loss. (Bart van der Sloot, 2022)

As per the "2023 State of Deepfakes" report by Homesecurityheroes (2023), a comprehensive analysis of the current state of deepfake technology was conducted. The report draws upon an examination of 95,820 deepfake videos. An estimated 95,820 deepfake videos are accessible online in 2023, a 550% increase from 2019.

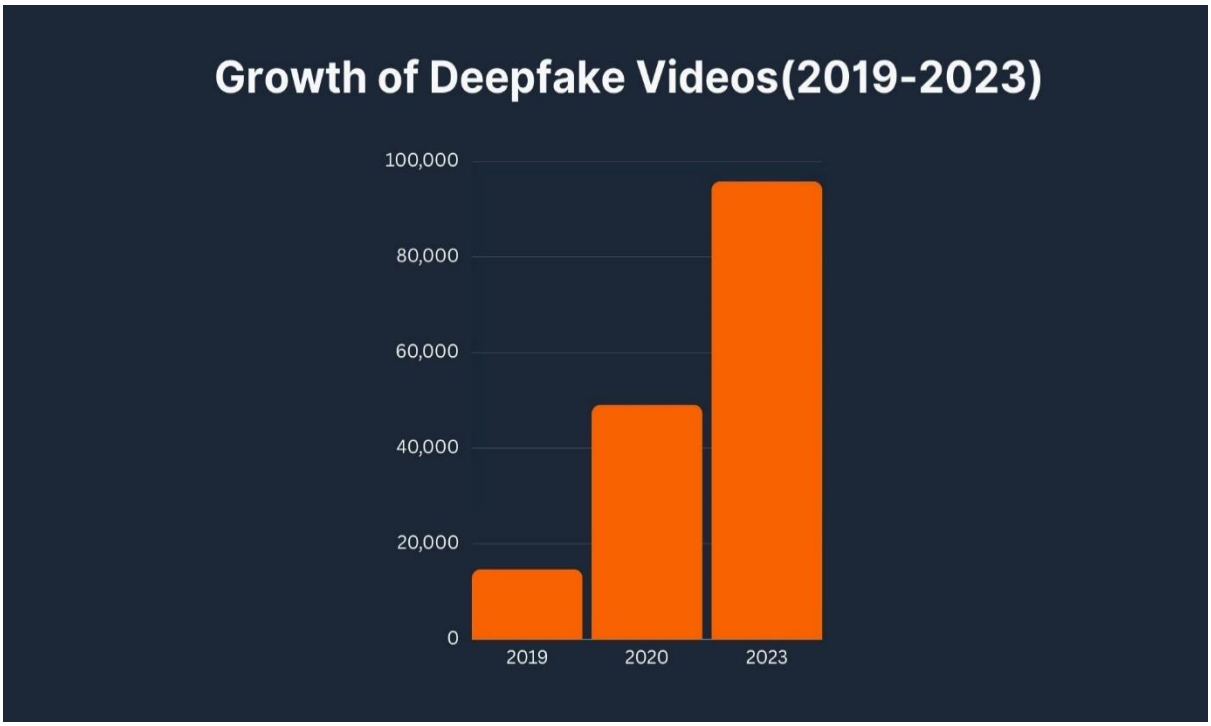

Figure 1: Statistics on Growth of Deepfake Videos (2019 - 2023)
(https://contentdetector.ai/articles/deepfake-statistics)

Technology like this has led to societal issues, particularly for the government. According to recent research, people with strong political interests are more likely to spread false information intentionally and accidentally on social media (Chadwick and Vaccari, 2019).

Additionally, Cybercriminals impersonated a chief executive and demanded a fraudulent payment of €220,000 ($243,000) with the use of artificial intelligence-based software. (Catherine S, 2019). The employee made the

payment believing he was talking to his employer on the phone.

Em Steck (2024) has reported that a robocall posing as President Joe Biden, seeming to be an AI voice, is urging Americans not to cast ballots in the upcoming US general election.

However, Christopher N (2020) has reported that deepfake technology has positively helped an Indian politician to successfully communicate with minorities at home or overseas by delivering messages in any language.

This implies conflicting evidence about the ethical implications of deepfake technology. Positive usage has shown effective interaction in politics and is also used for certain application purposes such as virtual fitting rooms. Therefore, it is important to carefully weigh the hazards and possible benefits of deepfake technology while evaluating its ethical implications.

Collaboration between the government, tech companies, and the media has been actively addressing this issue. While laws are being implemented by the government, journalists should focus on cutting down on fake news and Tech companies should invest in deepfake detection. Ultimately, individuals should always double-check their sources before sharing information.

3.2 Phishing Attacks

Phishing attacks are a kind of cybercrime whereby offenders portray themselves as trustworthy organizations to trick people. Lastdrager (2014) described phishing as an "act of deception whereby impersonation is used to obtain information from a target. Sensitive information includes passwords, credit card numbers, or personal information.

These attacks are often carried out by email, social media, or text messaging, and they frequently use persuasive strategies to deceive victims into clicking dangerous links.

Almost every day, huge organizations make news after falling victim or being impersonated by some sort of phishing, resulting in significant monetary and reputational damages.

The Anti-Phishing Working Group (APWG) observed 1,077,501 phishing attacks in the fourth quarter of 2023. APWG observed almost five million phishing attacks in 2023, the worst year for phishing on record. Notably, the most-targeted industries in 4Q 2023 for such attacks were through social media (APWG, 2023)

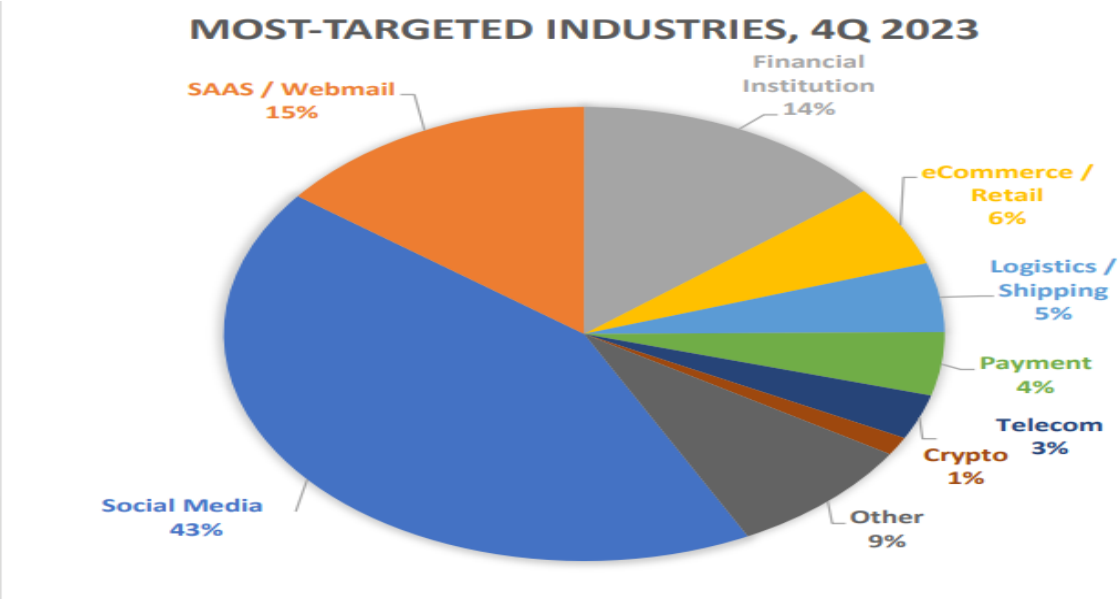

Figure 2: Most Targeted industries for phishing attacks (https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf)

Meta platforms were among the top online channels exploited by scammers which involves false sellers on Meta Marketplace, accounting for nearly half the scam cases, with some $280 million in losses. (Osmond Chia, 2024)

Despite this, Facebook did not implement measures such as safeguard tools to check users against government-issued IDs to provide a secure payment option for Marketplace customers and only offer user guides.

Phishing scams in DBS, a financial institution in Singapore have also been common. Michelle Ching (2024) reported at least 219 victims have fallen for these scams within the first two weeks of January 2024, losing a total of $446,000. The offenders usually use fictional SMS messages to pose as DBS.

Certain implementations have targeted phishing schemes, where Singapore companies that are not part of the whitelist put up by the Infocomm Media Development Authority (IMDA) would have their text messages labelled as "likely scam" on receivers' phones. (Andy Leck, 2023)

However, despite procedures and tools developed by companies to combat phishing scams, the impact of prior victimization by phishing assaults has been investigated in some studies, with the argument that victims learn from their experiences. (Chen et al, 2020).

Furthermore, the occurrence of a monetary loss as a result of responding to a phishing email and not having the amount refunded encourages people to adopt more cautious behaviors in the future, reducing susceptibility to phishing.

3.3 Internet Addiction

The issue of internet addiction has been discussed from multiple perspectives, emphasizing its broad results and importance in modern society. Some individuals spend 40-80 hours per week online, with some sessions lasting up to 20 hours.

Internet addiction has emerged as a result of increasing technology use and draws a similar appearance to other types of addictions. Therefore, in recent years, there has been a growing awareness that using technology every day is often impulsive and thoughtless which distracts attention from other activities. (Aagaard, 2021).

Internet addiction has effects that are comparable to those of other addictions. These issues are related to sleep, mental health, loneliness, anxiety, stress, and depression (Jorgenson, 2016).

While the World Health Organization (WHO) has not yet recognized internet addiction as a disease, certain governments of countries have recognized internet addiction as a public health hazard and professional issue. According to South Korea, the biggest health issue affecting children is internet addiction. Over 26 million people are said to be internet addicts in China. Specialized clinics to treat such addiction are established in China, Taiwan, India, Singapore, and South Korea; in China alone, there are over 300 such clinics.

According to "Technology Addiction: Real World Stats (2024)", individuals aged 13 to 24 have the highest risk of internet addiction, with a prevalence of 73%. Interestingly, Teenagers who spend 5 hours daily on their smartphones are twice as likely to display signs of depression compared to those who spend less time.

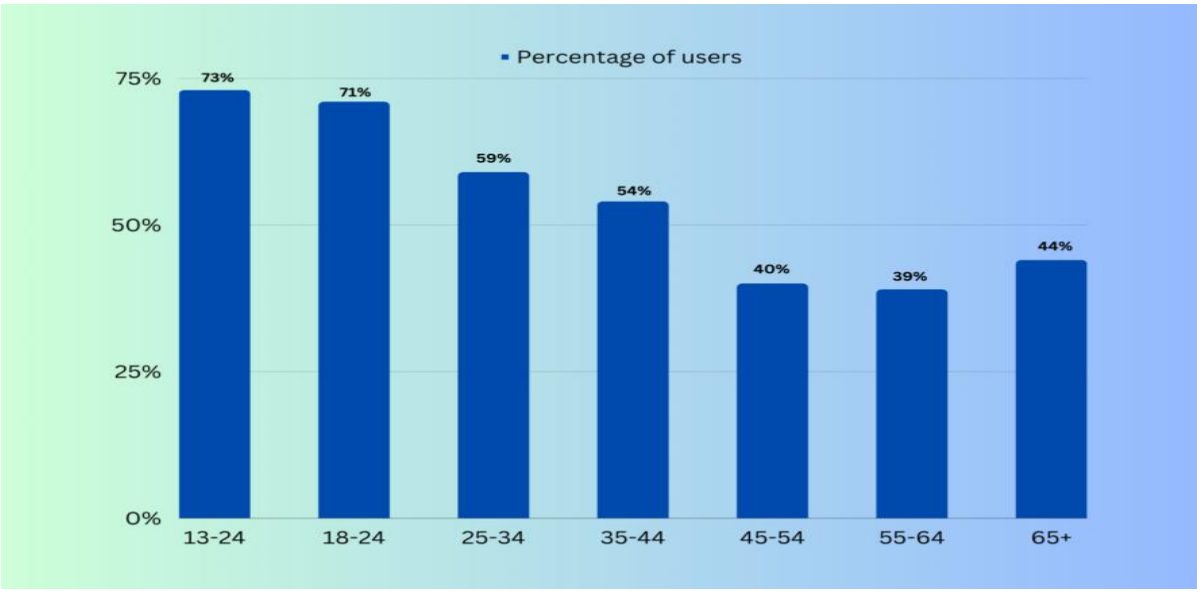

Figure 3: Percentage of Users developing a risk of internet addiction (https://windowsreport.com/technology-addiction-statistics/)

Levounis and Sherer (2021) discuss many types of internet addiction, such as video games, pornography, online gambling, texting, internet browsing, social networking, and shopping. They illustrate patient stories, such as a 25-year-old guy who could not date offline as he valued virtual connections above real ones and a 20-something war veteran who went homeless owing to debt incurred while acquiring virtual items in an online game.

Numerous studies have also demonstrated that internet addiction is a reliable indicator of future risk of alcohol use and cigarette smoking (Chiao et al, 2014).

Kimberly S. Young (1996) developed one of the earliest self-assessment tools for identifying internet addiction, known as the Internet Addiction Test (IAT) which is still used to measure people's levels of internet addiction in clinical and research environments.

However, certain respondents found there is no proof that excessive online usage negatively impacts a person's life over time, unlike drug abuse.

Instead, researchers suggest that a suitable word like "excessive use" is more appropriate and indicates that moderate use is beneficial, whereas either no use at all or extreme use could be harmful. (The Week, 2019)

This implies that there is conflicting evidence supporting the idea of internet addiction. Some experts and researchers agree with the negative consequences of excessive internet usage, but others doubt the necessity of classifying it as an addiction.

Ultimately, individuals are in charge of controlling how much they use the internet and making decisions about their digital lives, especially in cases when parents should be vital in overseeing their kids' online conduct or how individuals would use the internet positively.

4.0 Conclusion

The current difficulties surrounding technology, such as deepfake technology, phishing attempts, and internet addiction, highlight the critical necessity for coordinated efforts to overcome the multiple challenges in our increasingly digital world.

Artificial intelligence-driven deepfake technology raises ethical dilemmas since it may be used to modify digital information, but it also opens doors for creative innovation. For stakeholders to successfully navigate its ethical complexity, collaboration is essential.

In the meanwhile, phishing attempts continue to pose a serious risk, demanding ongoing attentiveness and innovative security measures. Encouraging appropriate usage and digital literacy is essential in order to protect mental health and social well-being in the face of internet addiction, and increasing concern.

Looking ahead, resolving these problems calls for diverse collaboration, innovative technology, and well-informed policy. We may steer toward a future where technology enhances social well-being while limiting threats by promoting discussions and taking proactive measures.

5.0 References

Ahmed, S. (2020) Who inadvertently shares deepfakes? analyzing the role of political interest, cognitive ability, and social network size. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0736585320301672 (Accessed: 07 April 2024).

Chadwick, A. and Vaccari, C. (2019) News sharing on UK social media: Misinformation, disinformation, and correction. Available at: https://repository.lboro.ac.uk/articles/report/News_sharing_on_UK_social_media_misinformation_disinformation_and_correction/9471269 (Accessed: 07 April 2024).

Lastdrager, E.E. (2014) Achieving a consensual definition of phishing based on a systematic review of the literature - crime science, BioMed Central. Available at: https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-014-0009-y (Accessed: 06 April 2024).

Phishing activity trends reports (no date) APWG. Available at: https://apwg.org/trendsreports/ (Accessed: 06 April 2024).

Reddy, R. (2023) 24 deepfake statistics - current trends, growth, and popularity (December 2023), ContentDetector.AI. Available at: https://contentdetector.ai/articles/deepfake-statistics (Accessed: 07 April 2024).

Ribeiro, L. (2023) Which factors predict susceptibility to phishing? an empirical study, Computers & Security. Available at: https://www.sciencedirect.com/science/article/pii/S0167404823004686 (Accessed: 07 April 2024).

Steck, E. and Kaczynski, A. (2024) Fake Joe Biden robocall urges New Hampshire voters not to vote in Tuesday's Democratic primary | CNN politics, CNN. Available at: https://edition.cnn.com/2024/01/22/politics/fake-joe-biden-robocall/index.html (Accessed: 07 April 2024).

Stupp, C. (2019) Fraudsters used AI to mimic CEO's voice in unusual cybercrime case - WSJ. Available at: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 (Accessed: 07 April 2024).

van der Sloot, B. (2022) Deepfakes: Regulatory challenges for the synthetic society. Available at: https://www.sciencedirect.com/science/article/pii/S0267364922000632 (Accessed: 07 April 2024).

2023 State Of Deepfakes: Realities, Threats, And Impact. Available at: https://www.homesecurityheroes.com/state-of-deepfakes/ (Accessed: 07 April 2024).

Chia, O. (2024) Look out for these scams on Facebook, Instagram and WhatsApp, The Straits Times. Available at: https://www.straitstimes.com/singapore/look-out-for-these-scams-on-facebook-instagram-and-whatsapp (Accessed: 06 April 2024).

Chin, M. (2024) Banks don’t send SMS clickable links, police and DBS warn after $446K lost to scams in 2 weeks, The Straits Times. Available at: https://www.straitstimes.com/singapore/banks-do-not-send-customers-sms-clickable-links-police-dbs (Accessed: 06 April 2024).

Jesper, A. (2021) Apa PsycNet, American Psychological Association. Available at: https://psycnet.apa.org/record/2020-24525-001 (Accessed: 07 April 2024).

Leck, A. (2024) Singapore: Implementation of the full SSIR regime, Global Compliance News. Available at: https://www.globalcompliancenews.com/2023/03/19/https-insightplus-bakermckenzie-com-bm-data-technology-singapore-implementation-of-the-full-ssir-regime_03012023/ (Accessed: 07 April 2024).

Bisen, S.S. and Deshpande, Y.M. (2018) Understanding internet addiction: A comprehensive review, Mental Health Review Journal. Available at: https://www.emerald.com/insight/content/doi/10.1108/MHRJ-07-2017-0023/full/html#:~:text=There%20is%20ample%20proof%20that,addictive%20behavior%20like%20cigarette%20smoking (Accessed: 08 April 2024).

Faraci, P. (2013) Internet addiction test (IAT): Which is the best factorial solution?, Journal of medical Internet research. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3806548/ (Accessed: 09 April 2024).

Game Changer? World Health Organization recognises the global impact of addictive technology (no date) Game changer? WHO recognises the global impact of addictive technology - Consumers International. Available at: https://www.consumersinternational.org/news-resources/blog/posts/game-changer-addictive-technology-blog/ (Accessed: 09 April 2024).

Petros, L. and Sherer, J. (2021) Technological Addictions. Available at: https://ebookcentral.proquest.com/lib/coventry/reader.action?docID=6688783&query=technological+addiction (Accessed: 09 April 2024).

Sisodia, S. (2024) Technology addiction: Real world stats & facts for 2024, Windows Report. Available at: https://windowsreport.com/technology-addiction-statistics/ (Accessed: 08 April 2024).

Staff, T.W. (2019) Is internet addiction real?, theweek. Available at: https://theweek.com/99259/is-internet-addiction-real (Accessed: 09 April 2024).