DRAWN TO CYBERCRIME: PROTECTING AGAINST ONLINE PHISHING SCAMS DURING A CRISIS

SAMUEL C. AULT

Student number: 170260738

Supervisor: Dr. Konstantinos Mersinas

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London.

Royal Holloway, University of London

Information Security Group

Egham, Surrey, TW20 0EX

United Kingdom

Dissertation Project Submission

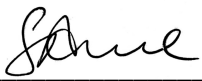
UNIVERSITY OF LONDON - MSc INFORMATION SECURITY

Dissertation Project Title	Drawn to cybercrime: Protecting against online phishing scams during a crisis
Student	Samuel C. Ault
Student Number (SRN)	170260738

ANTI-PLAGIARISM DECLARATION

I declare that this dissertation is all my own work, and that I have acknowledged all quotations from the published or unpublished works of other people.

I declare that I have also read the statement on plagiarism in the General Regulations for Awards at Graduate and Masters Levels for the MSc in Information Security and in accordance with it I submit this project report as my own work.

Signed:  **Date:** 31st March 2022

Samuel C. Ault

Acknowledgements

Firstly, my sincere gratitude to Dr Konstantinos Mersinas, Senior Lecturer, Director of Distance Learning MSc Programme and Dr Peter Komisarczuk, Senior Lecturer, Programme Director, Department of Information Security. The support and guidance you have provided is a testament to the high reputation of Royal Holloway, and it has been an absolute pleasure to take part in the distance learning programme.

With special thanks to Dr Zach Warner, Assistant Professor of Political Science, Purdue University, for your extraordinary expertise and kindness.

To my client leadership team for granting flexibility in my consulting engagement to support my goals in this external area.

To my loving family for always showing such an interest in my work and passions, for always making me believe I can achieve whatever I set out to accomplish in life.

Lastly, but not least, to my wife Rebecca, for your incredible patience and unwavering support in helping me achieve this major life milestone. I promise to support you in everything you set out to do.

Table of Contents

Table of figures

Table of Tables

Executive Summary

The COVID-19 pandemic health crisis has caused major disruption worldwide, creating a unique set of events in our current lifetime. Cybercriminals quickly bombarded the public with pandemic-related phishing scams, which has led to widespread suffering and loss of personal information. Phishing remains a persistent threat and targets human weaknesses by using social engineering techniques to convince victims to hand over their personal information. The disruptive events of the pandemic have further increased susceptibility to these types of cyberattacks.

The ability for human-targeted cyberattacks to cause such an impact may have initially resulted from the global reduction in movement, as travel restrictions came into place and the workplace shifted from the office to the unfamiliar and unpredictable home setting. As people spend more time online, dependency on emails and messages has also increased. By capitalising on the emergent pandemic experience, many fraudsters have become psychological experts, increasingly adopting sophisticated ways of stealing information through these channels.

Sophisticated attacks can often happen through a series of chained events. Phishing becomes a primary attack method that allows fraudsters to collect and steal personal and financial information, building up active target profiles in real-time. By following on with secondary and more devastating social engineering attacks, victims are being deceived and coerced into handing over online banking details or transferring funds, causing significant financial harm.

Financially motivated cybercrime is shifting from the shadows of the dark web and is finding a welcoming audience within the sphere of social media. Emboldened influencers gain reputation and generate revenue through social channels that draw young people to cybercrime. UK cyber scam subculture emerges at the crossroads of the pandemic, where easy money is made online under the protection of the home. These online crimes are non-physical and can occur from any location, with high anonymity. This work aims to provide reader awareness and highlight the enhanced dangers of phishing and online scams in a crisis environment.

Keywords

Cybersecurity, COVID-19, Phishing, Pandemic Factors, Cyber Scam Subculture

Chapter 1 - Introduction

The objective of Chapter 1 is to provide the structure, motivation, and methodology for the project, including the core objectives that this work will achieve.

1.1 Project Motivation

Unsurprisingly, psychological sophistication within the phishing threat landscape is likely to keep growing. In a crisis environment, it is the unfortunate targeting of the most vulnerable individuals, often at the point of them experiencing a sudden loss or when anticipating much-needed financial support. I am interested in identifying how quickly fraudsters have reacted to recent COVID-19 news and announcements, which might reveal more socially organised criminal activity.

It is concerning how much fraud and online scamming go unnoticed and unreported. As the pandemic crisis lengthened, the prolonged events are likely to have had a de-stabilising effect on human behaviour and therefore increased phishing susceptibility. Specific research covered in **Chapter 5** shows the serious matter of personal and financial information captured from phishing attacks, then freely shared and traded on public social media channels with little remorse.

The motivation for this work is to help establish the connection between phishing as primary information capture, to then be distributed through wider criminal social networks, allowing others who are drawn to cybercrime to perform more sophisticated and advanced secondary-stage attacks. These serious and devastating final attacks can cause the most significant personal and financial harm. I am deeply motivated in providing reader awareness to aid in protecting against online phishing scams.

1.2 Contribution

This thesis makes three main contributions. Firstly, by examining phishing evidence during the COVID-19 Omicron variant outbreak, the aim is to create a new visual timeline that builds on the earlier research [1] produced at the start of the pandemic. The aim is to study the reactivity of fraudsters who use pandemic crisis factors to target victims. Secondly, a case study covering the recent BBC Panorama investigation into social media fraudsters, may yield some significant findings and discover how younger people are drawn towards the glamour of cybercrime. Thirdly, by providing new research and analysis of underground public social media channel communications where services, techniques and financial profiles are freely being exchanged, a multi-chain attack theory will be presented.

1.3 Project Outline and Structure

The remainder of this project will be structured into five chapters.

Chapter 2 – Review of the scientific literature provides a comprehensive cybersecurity literature review related to the current crisis environment. I will identify existing research areas to highlight gaps and how I can prepare a new contribution covering the very recent period of the last two years.

Chapter 3 – How attackers target people and human factors during a crisis starts to build out a deeper study to explain how attackers use social engineering techniques and other phishing attack methods within the context of the pandemic. After providing a brief background on human behaviour, I will outline common types of phishing attack methods and techniques, social influence, human-related challenges, and pandemic-related situational factors that have arisen. I will identify various pandemic-related factors and how these have compounded to increase phishing susceptibility.

Chapter 4 – Omicron: A visual timeline of phishing evidence provides a diagram of announcement events and phishing attacks to determine the speed at which attackers can modify phishing content to target victims. This chapter provides a new contribution and builds upon the existing literature covering the initial pandemic period in 2020. I will identify patterns between announcements and phishing evidence, using the classification of elements prepared in **Chapter 3**. I will also highlight how phishing campaigns start as a primary data collection mechanism for attackers to perform more advanced and targeted social engineering attacks.

Chapter 5 – Case Study: Cyber scam subculture explores a case study of the BBC Panorama investigation, *Hunting the Social Media Fraudsters*. I will provide new contributing research uncovering social messaging application channels that have become readily available. I will identify advanced software techniques which perform secondary stage attacks and bypass one-time passcode protections. This chapter also explores how cyber scam subculture has developed to draw young people into a world of cybercrime through social media influence and the prospect of a luxury lifestyle. Finally, I will discuss three key issues from the investigation and provide my recommendations alongside each issue:

- How cyber scam subculture has developed to draw young people into a world of cybercrime through social media influence.
- How failures in removing scam content and fake accounts allow cybercriminals to circumvent controls.
- Whether victims are forgotten as online scamming goes unreported.

Chapter 6 – Conclusions

As a concluding chapter, I will provide a comprehensive summary of the core objectives set out in this project. I will demonstrate how pandemic factors outlined in **Chapter 3** impact human behaviours and increase phishing susceptibility during a crisis. I will then argue that the findings in **Chapter 4** raise important questions about how attackers might group in a herd to quickly target victims using **chained attack** techniques. I will discuss the case study from **Chapter 5** and highlight the challenges that arise from UK cyber scam subculture and how difficult it is to prevent the distribution of material through social media channels. I also suggest that social media companies need to do more to prevent harmful content. In parallel, I highlight how the police and authorities need to modernise and adapt to the new threats that draw young people to cybercrime. In the concluding chapter, I will take an opportunity to summarise my thoughts, followed by limitations in the overall approach to this work. As a final objective and contribution, I will provide five additional recommendations to offer the reader awareness and highlight how to protect against online phishing scams.

1.3.1 Project structure

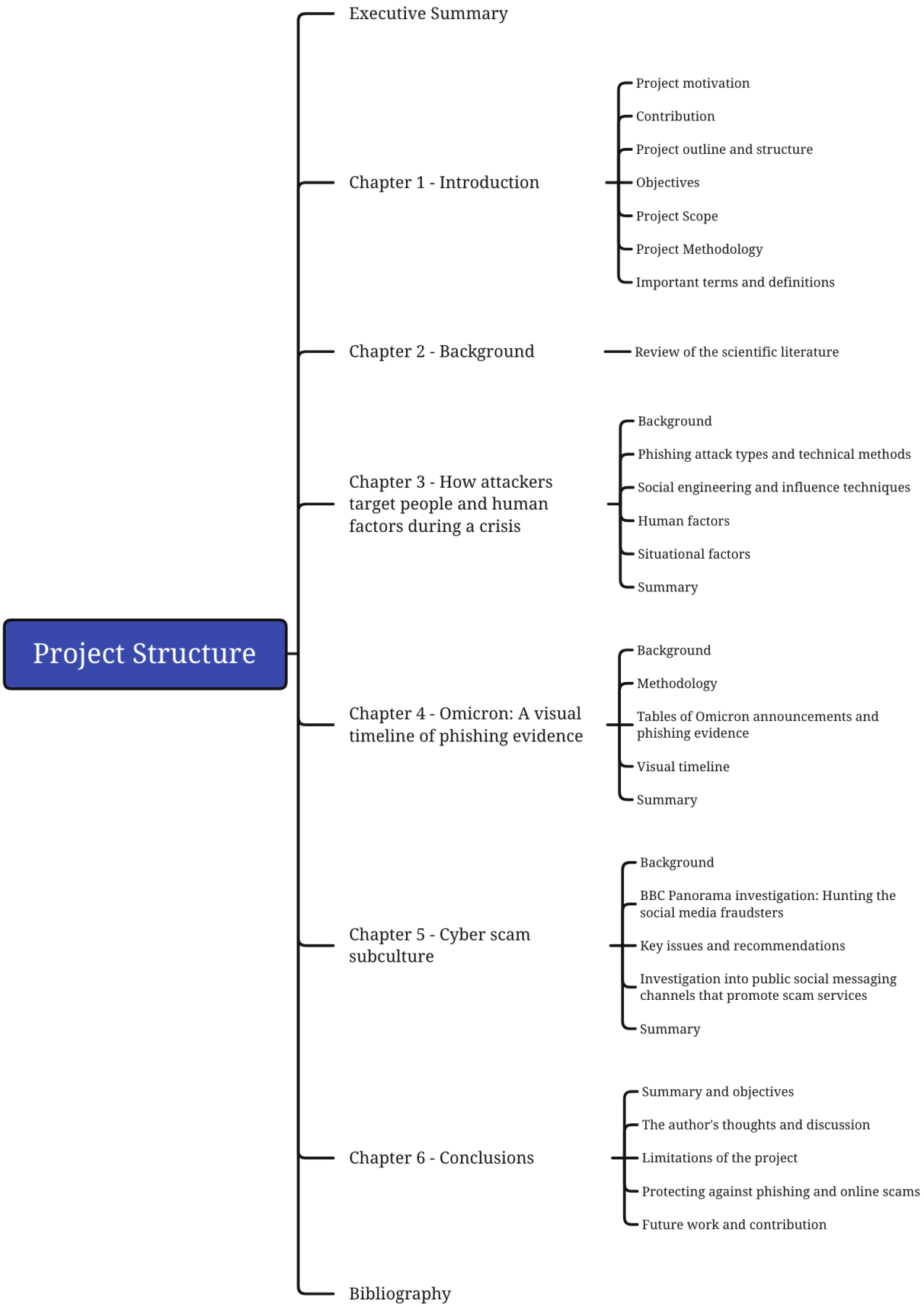


Figure 1 - Project Structure

1.4 Objectives

Table 1 of 11 - Objectives		
Objective	**Description**	**Chapter**
1	Demonstrate how pandemic factors impact human behaviours and increase phishing susceptibility.	Chapter 3
2	Produce a visual timeline of pandemic phishing events, using the emergence of the Omicron variant to evidence how quickly attackers modified phishing campaigns to target victims.	Chapter 4
3	Use a case study to examine the recent BBC Panorama investigation: *Hunting the Social Media Fraudsters* and highlight key issues and recommendations. a) Identify whether there are plausible links between social-influenced cybercrime and a rise in independent actors using pandemic factors to their advantage. b) Provide new research to uncover specialist social messaging channels used to promote online scam activity and demonstrate how easy it is for young people to be drawn to cybercrime. c) Identify evidence of chained attack techniques.	Chapter 5
4	Provide five additional cyber security recommendations to safeguard against phishing threats and online scams.	Chapter 6

Table 1 - Objectives

1.5 Project scope

COVID-19 has been a unique global event, and whilst this has impacted people from all over the world, this work primarily focuses on events in the United Kingdom (UK).

Within the comprehensive scientific literature review in **Chapter 2**, I acknowledge other areas of cybercrime, such as malware and specifically ransomware. I recognise that the latter has become a significant challenge for many organisations during the pandemic health crisis [2]. However, this area will not be the primary focus of this project, and I will leave this to form a future research contribution.

The project focuses primarily on the phishing attack area, which continues to be a highly dominant cybersecurity threat [3]. In **Chapter 3**, I acknowledge business email compromise (BEC). Whilst this is increasingly problematic for organisations, this project is specifically interested in how phishing attacks can quite easily lead to further financial and identity-based fraudulent activity and as part of **chained attack** techniques. Financial fraud is a broad area, and in **Chapter 5**, I attempt to focus on common types of online fraud rather than card-specific fraud. The specific goal is to uncover cyber scam subculture, social media influence, and social messaging applications used to promote and discuss online fraud techniques.

Throughout this work, I aim to keep a consistent approach with terminology. Attackers, fraudsters, scammers, and cybercriminals all mean the same: someone attacking or targeting an individual or organisation to extract sensitive personal, financial information or assets from them. Online fraud, cyber scams, and scamming terms describe financially motivated crimes committed online.

1.6 Project Methodology

I used both the Royal Holloway Online Library[1] and Google Scholar[2] as a core search engine for high-quality and relevant academic material of the following types:

- Research publications
- Books

I used the Google[3] search engine to identify specialist research within the following categories:

- Technical reports, websites and blogs for secondary data gathering
- Online newspaper articles

[1] https://onlinelibrary.london.ac.uk/
[2] https://scholar.google.com/
[3] https://www.google.co.uk/

The primary literature search covers the latest refereed research material available. Several books covering very recent events were unavailable through online library systems and were purchased directly for consideration in this thesis. Websites, security vendor reports and credible online newspaper resources were selected as the supporting evidence around the pandemic, and online fraud is continually evolving. Where possible, I selected newspaper articles of longstanding reputation in the UK, for example, *The BBC*, *The Guardian*, and *The Telegraph*. Website, blog articles, social media and online newspaper resources have been retrieved, which I recognise as non-academic sources. I acknowledge that there is often an advertising element within some security vendor reports, but I accept that the underlying research will have been carried out appropriately.

The nature of this work considers very recent events in the past two years, where the availability of relevant peer-reviewed and well-cited research was initially challenging. During the preparation of this work, significant events occurred, notably the emergence of the Omicron COVID-19 variant. I decided that **Chapter 4** would cover an analysis of immediate threats that evolved rapidly within weeks of the official announcement. During the initial research, it became apparent that there was scarce appropriate content from mainstream national newspaper sources. Regional source articles were selected instead due to their availability, see **Section 4.2.3**. In **Chapter 5**, I decided that I must de-identify all social media messaging application channel research for ethical reasons, see **Section 5.4.1**.

1.6.2 Document styling, formatting, and referencing

The report is structured into chapters and sections to ensure good readability throughout.

The following styling choices have been made:

- **Bold** – Chapters and Sections are highlighted in bold to indicate to the reader where the further discussion takes place. Phrases and headings are highlighted in bold where appropriate to indicate important discussion and summary topics.
- *Italic* – Source titles and specific terms are written in italics.

The IEEE referencing style [4] has been chosen for citing references. This referencing style involves a numerical system for indicating citation numbers inside square brackets, next to each passage or quote. The source page number will also be indicated where a direct quotation has been used. A complete list of corresponding references is available in the Bibliography section at the end of this thesis. Where necessary, footnotes will be highlighted next to the text and then listed at the bottom of the page.

1.7 Important terms and definitions

APP – Authorised Push Payment

BEC – Business Email Compromise

BIN – Bank Information Number

CVV – Card Verification Value

CEO – Chief Operating Officer

CIA Triad – Confidentiality, Integrity, Availability

COVID-19 – Coronavirus disease 2019 (see SARS-CoV-2)

DCMS – Digital, Culture, Media, and Sport

DHSC – Department of Health and Social Care

FBI – Federal Bureau of Investigation

GDPR – General Data Protection Regulation

HaaSS – Human-as-a-Security-Sensor

HMRC – Her Majesty's Revenue and Customs

KYC – Know your customer

NCA – National Crime Agency

NHS – National Health Service

NIST – National Institute of Standards and Technology

ONS – Office for National Statistics

OTP – One-Time Password

Omicron – COVID-19 variant, classified as the B.1.1.529 variant

PCR – Polymerase Chain Reaction, referring to COVID-19 testing

SARS-CoV-2 – Severe Acute Respiratory Syndrome Coronavirus 2

SMS – Short Message Service, referring to a text message

URL – Uniform Resource Locator, referring to an internet web address

VPN – Virtual Private Network

WHO – World Health Organisation

2FA – Two-Factor Authentication

Chapter 2 - Background

Whilst there is a delay in available research covering the latest events, there is a rich opportunity to build on the scientific research published shortly after the initial COVID-19 announcement in March 2020 [1] [5] [6] [7]. However, it is unlikely that this immediate research could have predicted that the pandemic would extend for two years, nor consider the prolonged impact of the pandemic on human behaviours. The emergence of the Omicron variant and subsequent announcements are likely to have triggered similar responses to the start of the pandemic, increasing overall susceptibility to phishing attacks as the crisis returned.

As this environment has evolved so dramatically, this review of the scientific literature aims to provide a comprehensive background to cover cybercrime, a crisis environment, the impact of COVID-19 on cybersecurity, online fraud, pandemic distraction, and human weakness.

2.1 Review of the Scientific Literature

2.1.1 Cybercrime

The global cost of cybercrime is likely to reach $6 trillion annually in 2021 [8], increasing to $10.5 trillion annually by 2025 [9]. Cybercrime describes "*crimes committed using computers and the Internet*" [10, p. 2]. Though cybercrime is now a widely used term, there is little agreement on how to define it. Schinder and Cross in [10] use the traditional crime triangle to liken motive, means and opportunity as a correlation to cybercrime, with the victim or target being people or the computer. In this case, the computer can either commit the crime, be the target of the crime or be used incidentally in the crime. Another model [11] draws between "crimes against the device", where the confidentiality, integrity and availability (CIA triad) of a device is compromised, and "crimes using the device", where a victim is targeted.

According to the two 2013 Home Office reports on cybercrime offences [12] [13], distinctions are drawn between pure "cyber-dependent" and traditional "cyber-enabled" crimes. Within this literature review, I will refer to the model in **Figure 2**, which eloquently indicates the various sub-categories of "cyber-dependent" and "cyber-enabled" crime.

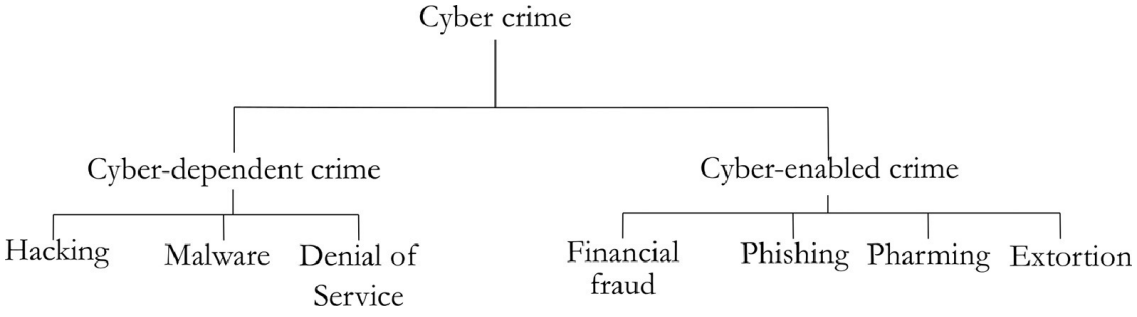


Figure 2 – Cyber-dependent and cyber-enabled crime [12, p. 5]

2.1.2 Cyber-dependent crime: Malware

Malware, meaning malicious software, has evolved dramatically in the past decade and much since the earlier work from Denning [14] on the classification of computer viruses. Primarily due to advancing levels of code sophistication [15] [16] and the use of new transmission and evasion methods, such as timing and network-based techniques [17]. AI-driven malware uses deep-learning algorithms to perform more effective attacks and may soon become widespread [18]. Artificial intelligence could create many new problems, such as being applied to create more targeted and convincing social engineering threats via phishing or be used to evade existing malware detection measures that look for more traditional programming signatures.

Some common examples of malware are viruses, trojans, worms, spyware, and ransomware. Discussions on computer virus Trojan horses date back to the 1960s [14], where Denning describes this type of malicious software as one of the most common ways of invisibly introducing a computer virus into a system. Attack chains have now become more sophisticated [19], where multiple malware types, such as Trojans and ransomware, are combined. **Figure 3** shows how **chained attacks** allow multiple stages of lateral movement through a system or network to circumvent and evade various controls and deliver malicious payloads before a final system-locking ransomware package. I refer to this method in **Chapter 5**, to identify how social media channels enable **chained attacks** to succeed, using phishing and sophisticated online fraud techniques.

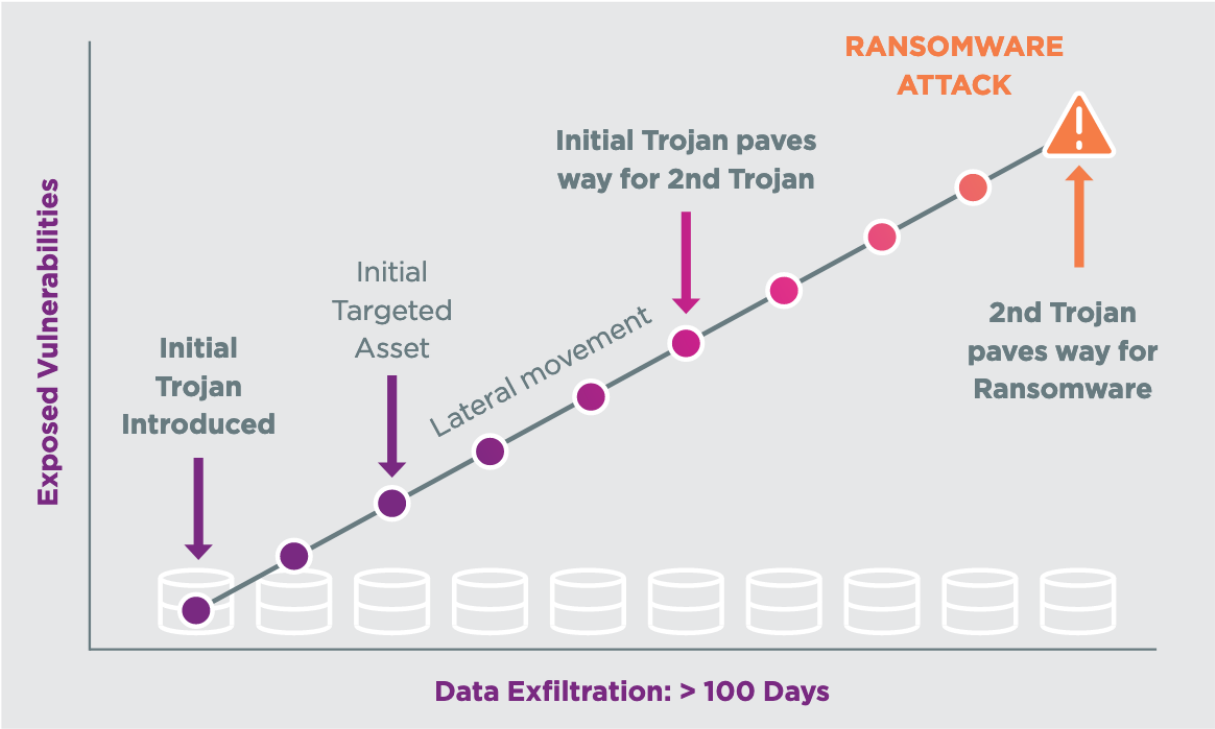


Figure 3 - Sophisticated multi-attack chain scenario showing lateral movement [19, p. 7]

Ransomware aims to intrude into a system undetected before encrypting critical files and then demanding the user for payment or a "ransom", often in the form of cryptocurrencies, to return the system and files to their original state [20]. The latest annual report from the National Cyber Security Centre [21] highlights three times as many ransomware-related attacks during the first quarter of 2021 than in 2019. During the pandemic health crisis, ransomware attacks have created a crisis for hospitals and healthcare organisations across the world and these often started through phishing attacks [2] [22] [23]. **Figure 4** shows that spam phishing emails and weaknesses exploited through social engineering techniques correspond to the highest infection causes. Cybercriminals take advantage of these entry points to increase the overall likelihood of attack success [24].

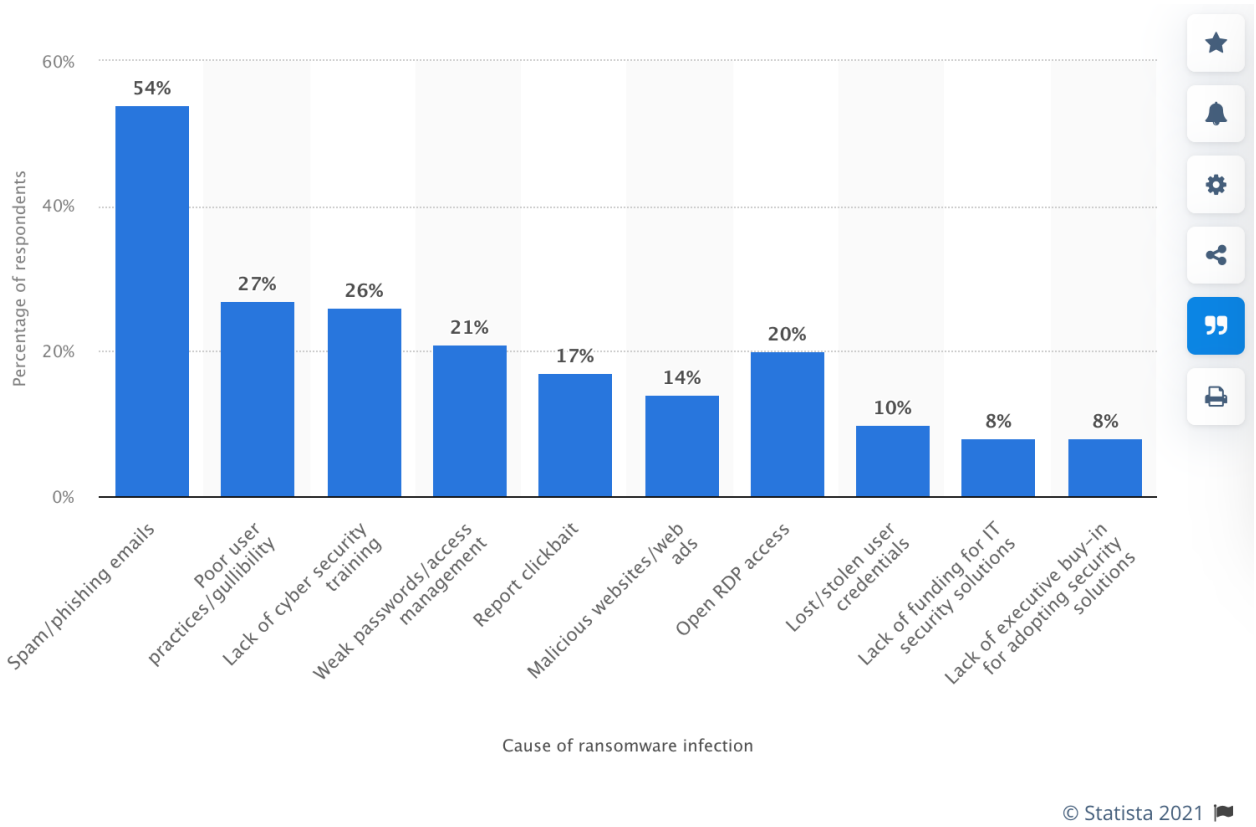


Figure 4 – Common causes of ransomware infection 2021 [24]

This thesis focuses on "cyber-enabled" crimes, primarily through phishing and financial fraud. As cybersecurity threats continue to evolve during the pandemic, phishing frequency also increased, appearing in 36% of breaches and 11% higher than in 2020 [25].

2.1.3 Cyber-enabled crime: Social engineering and phishing

The broader category of social engineering is now being described as "social actions" [25], with phishing and pretexting within the top threat techniques. When attackers combine a technical angle, such as phishing, with persuasive techniques to target human weaknesses, this could be better categorised as a socio-technical approach [26]. Hadnagy in [27] introduces four main phishing attack vectors; smishing, vishing, phishing and

impersonation. However, various technical methods are being utilised across the social engineering attack space [28] [29], some of which I will cover in **Chapter 3**.

As smartphone usage grows worldwide [30], phishing and specifically smishing attacks continue to increase in popularity [31]. Smishing-based attacks are particularly concerning in specific geographic locations, such as South Korea, where mobile device ownership has grown to almost 100% [32]. In the UK, at least 87% of adults in the UK owned smartphones in 2020 [33], with overall dependency and usage increasing since the pandemic started [34]. Attackers are now specifically optimising phishing content for mobile devices [35] to target those who might be distracted when checking new messages and emails in a rush. Canova et al. in [36] agree that there are often challenges identifying the legitimacy of a website URL, especially when using a smaller screen mobile device and that fraudsters look to exploit these techniques.

Hadnagy and Fincher in [3] summarise that phishing has become such a high-profile attack vector because of its relative ease in reaching vast numbers of people and its ability to create urgency and get users to do something quickly without thinking. Their work documents many historical high-profile data breaches that occurred due to phishing. Critically, they mention post-disaster situations, where fraudsters like to take advantage of a crisis environment and "people's desire to help others" [3, p. 19].

2.1.4 A crisis environment

In early 2020, the World Health Organisation (WHO) announced the global outbreak of Severe Acute Respiratory Syndrome Coronavirus 2 (SARS-CoV-2) known as COVID-19, declaring it a pandemic on 11th March 2020 [37]. During the initial COVID-19 crisis, many individuals were easily distracted. Fraudsters quickly began deploying malicious phishing campaigns and websites with **coronavirus-themed keywords** and terms to lure and deceive vulnerable users [38] [39]. Cybercrime is often highly opportunistic and is likely to thrive in a crisis environment [5]. Impersonation and anonymity are easily achievable online [40], where cybercriminals can frequently exploit and trick users into believing they are accessing credible resources. Naidoo in [5] developed a "multi-level influence model", **see Figure 5**, to map pandemic context as situational factors and then towards attack methodologies. The model helps further understand the dynamic process cybercriminals look to follow when targeting victims.

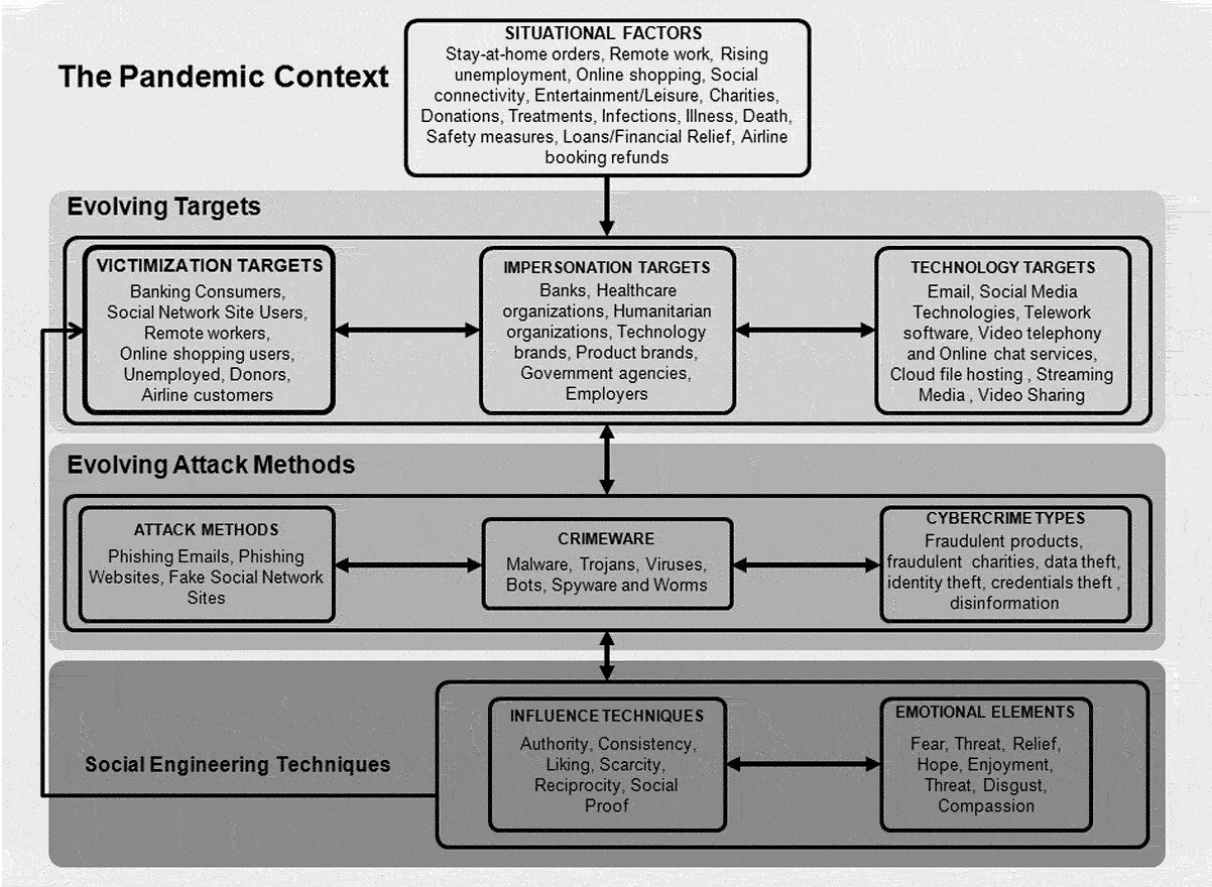


Figure 5 - The pandemic context – a "multi-level influence model" developed by Naidoo [5, p. 316]

The COVID-19 pandemic provided a suitable backdrop for new situational factors to cause an impact, such as homeworking and shifts to online shopping. People spent much more time online [41], as the recommendation was to stay at home [42] [43]. The overwhelming disruption caused by the pandemic is likely to have increased susceptibility to phishing attacks. Naidoo in [5] summarises that information security academics have paid little attention towards linking criminological theories to certain situational factors, and critically that "cybercriminals are resorting to increasingly more devious compliance techniques by integrating greater elements of situational factors into their scam designs." [5, p. 315]. **In Chapter 3, I will aim to contribute to this specific research field by drawing upon the importance of the pandemic-related context brought on by situational factors and the associated opportunities seized by cybercriminals.**

2.1.5 The impact of COVID-19 on cybersecurity

At the beginning of the global pandemic, a staggering number of cybersecurity attacks occurred [44], but as the pandemic lengthened, new waves of sophisticated and opportunistic attacks have continued to surface [45]. Okereafor, in his recent book *Cybersecurity in the COVID-19 pandemic* [46], states the following, "a pandemic on its own neither stops nor promotes cybercrime activities, but can potentially trigger a chain of

abnormal events that could lead to elevated waves of cybercrimes" [46, p. 17]. I will attempt to interpret this point throughout by explaining how prolonged disruption and pandemic-related situational factors can impact human behaviour in a crisis.

Lallie et al. in [1] provide a visual timeline of events, covering the period March-May 2020, **see Figure 6**. This timeline reveals the sheer extent of the UK's problems during the initial pandemic period. In **Chapter 4**, I will extend their initial research to focus specifically on phishing evidence by creating a visual timeline of the disruption caused by the emergence of the COVID-19 Omicron variant. This contribution will track a key objective in this thesis to determine how quickly attackers can modify pandemic-themed phishing content to target unsuspecting victims.

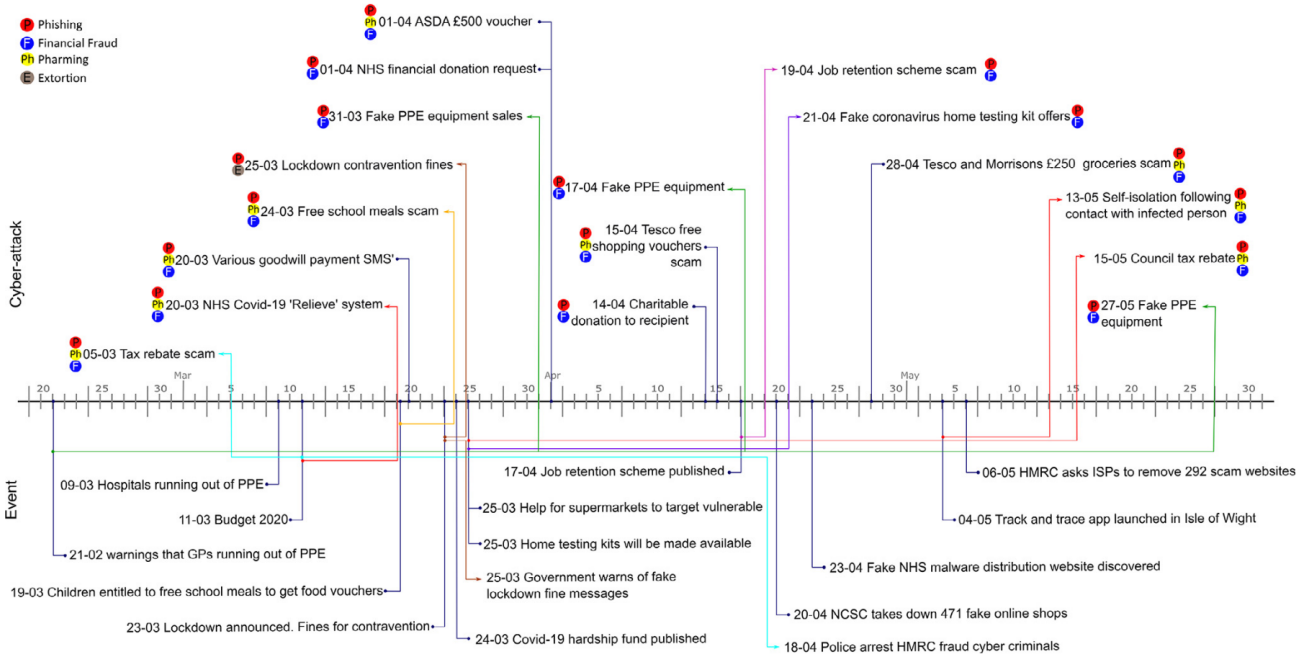


Figure 6 - Timeline of COVID-19 cybersecurity events in the UK [1, p. 9]

Several studies [1] [47] highlighted rapid digital and technological acceleration, further brought on by the COVID-19 pandemic. Organisations and their technology providers had to quickly accelerate to accommodate the increased demand for collaboration tooling and necessary connection bandwidth. However, some companies may have grown trust-dependent on the vendors that provide software and tools [48], leading to the adoption of incorrect risk-based approaches. Cybersecurity risk increased primarily due to the dispersion of users working remotely [49] and the decreased situational awareness that this caused [50]. Okereafor in [46] shows that COVID-19-related cybersecurity incidents aligned tightly to the initial advisories that initiated a global shift to working from home. This work highlighted that no business is immune from cyberattacks, but that employee exposure to pandemic factors did accelerate to make these risks more apparent. Furnell in [6]

considers that organisational "unpreparedness" played a key factor in rising cybersecurity-related incidents. In this research, it became clear that before the pandemic struck, so few employees were regularly working from home, it was unlikely that organisations even needed to consider mitigating the risk. **The primary risk is that employees become more distracted and less vigilant over time due to increasing pandemic-related factors** [50].

Georgiadou et al. in [51] state that readily-deployable finances and technical solutions allowed larger enterprises the flexibility to adapt to intense pandemic-related change within their business environments. However, they argued that prioritising the immediate need to ensure remote access may have inadvertently reduced the focus on overall asset protection. Malecki in [49] indicated that organisations observed a significant number of cyber-attacks during the initial pandemic period, which used advanced social engineering techniques to target weaknesses in the technology supply chain. Okereafor in [46] attempted to highlight that the pandemic period did create an opportunity for organisations to examine their digital assets more carefully. He observed that they became more conscious of cybersecurity due to a significant rise in cybercrime cases, which "ignited the focus" [46, p. 17] and increased global demand for cybersecurity expertise. However, if an organisation cannot prioritise and hire the relevant expertise to protect information and assets within this new operational climate, variance in overall preparedness may continue to exist.

2.1.6 A rise in online fraud

Financially motivated organised criminal groups are often involved in various criminal activities during crisis events [52]. However, some of the earlier pandemic research questioned the direct involvement of such organised groups [53] [54]. Riccardi in [55] suggests a high likelihood that organised crime groups were indirectly involved and targeted COVID-19 related "recovery funds" designed to reach the most vulnerable people during the pandemic period. In the UK, the HM treasury had initially estimated that total exposure to losses from COVID-19 emergency scheme-related opportunistic fraud and error at £15bn [56]. However, more recent announcements from the Office for Budget and Responsibility (OBR) now place this figure closer to £29bn [57]. As it transpires, HMRC now firmly believes that £5.2bn of taxpayers' money has been stolen through opportunistic fraud [58], see **Figure 7**, from the COVID-19 emergency response schemes, such as furlough and £4.9bn of fraudulent loans taken out as part of the business bounce-back loan scheme [59]. These figures suggest that a significant amount of UK COVID-19-related opportunistic fraud has not been prevented by the authorities and the banks facilitating the loans. Online fraud is likely to have been highly lucrative for both organised groups and new individuals during the pandemic.

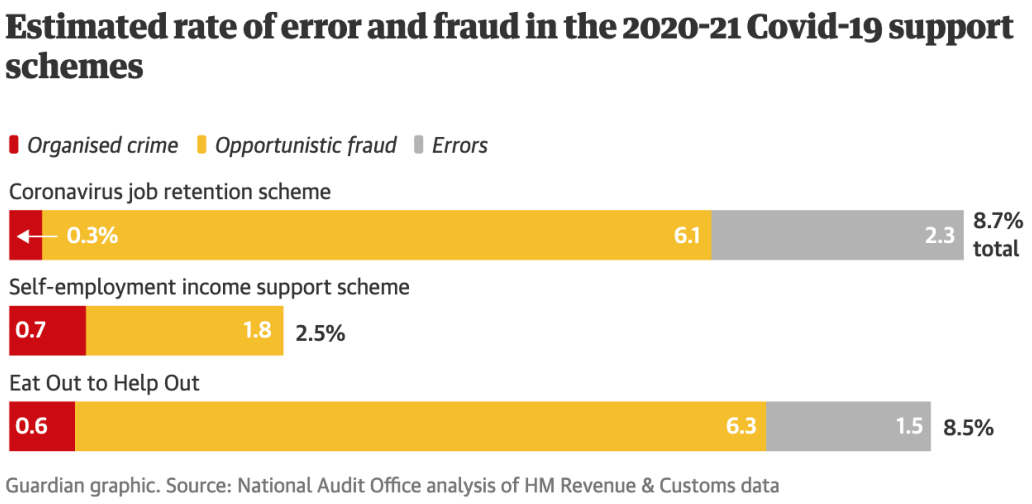


Figure 7 - Estimated rate of error and opportunistic fraud in the 2020-21 COVID-19 support schemes [58]

It is important to look towards other emerging angles, such as **a rise in young people drawn towards cybercrime** [60] and **enticed towards money laundering** [61, p. 56]. Technology can act as an enabling factor, introducing attractive pathways, such as cryptocurrencies [62], which can further interest young people. Whilst larger organised crime groups might also utilise subscription and affiliate programmes [63] to lure participants, boredom [64], unemployment or other unexpected events caused by the pandemic could also contribute to a rise of independent actors looking for financial opportunities. Widely available low-cost boiler-plate phishing toolkits require minimal technical skill and yield much higher rewards than other traditional methods and physical crimes. Ultimately it is highly likely that some individuals may have turned to forms of cybercrime during the pandemic to provide an income, as a recent *BBC Panorama* documentary critically uncovered [65]. Independent threat actors are taking advantage of new opportunities created through the rapidly evolving pandemic attack surface [66] [67]. **Since those already experiencing pandemic factors**, such as constantly changing Government guidance [68], **might also be able to know precisely how to target others and adapt to the disruption**. I will utilise a case study in **Chapter 5** to explore how social media scam influencers depict a life of luxury and, by doing so, draw younger technical individuals towards a world of phishing and cybercrime.

2.1.7 Homeworking and pandemic distraction

In recent years, changes in business models and a more modern workforce have seen the movement of users and devices shift outside of traditional corporate and academic perimeters and outside zones of control [69]. Homeworking within the pandemic climate involved many people rapidly shifting from their traditional working environments to the home, primarily due to various authorities compelling them to do so [46]. The pandemic and subsequent restrictions placed upon people during the crisis meant that workers were even more dispersed and were shifted rapidly to a remote-working setup, which was previously not a common

practice [70]. Cybercriminals quickly took advantage of this through phishing campaigns since people became more easily contactable at home [71]. Lallie et al. [1] suggest that "working at home *en-masse* has realised a level of cyber security concerns and challenges never faced before by industry and citizenry" [1, p. 2]. New working models also mean these threats are unlikely to go away in the short term [72], straining resources and operational output. Further, this could lead to unprepared staff diverting away from their normal operations, which occurred at the UK's Defence training academy [73], causing significant disruption.

Other interesting studies in [74] [75] suggest that several psychological factors become challenged when work duties are performed at home. In work by Savolainen et al. [75], a deep study of Finnish workers during the pandemic shows that increased psychological distress, including "**technostress**", contributed to increased levels of COVID-19-related anxiety notably impacting work performance, overall wellbeing and mental health. This research correlates with Giuntella et al. in [76], which critically highlights the overall impact on individuals' mental health during the COVID-19 pandemic, noting this impact was severe and that those surveyed reported symptoms of depression during the pandemic across broadly all age groups. However, in this crucial area and recent timeline, there is relatively limited research, outside of medical-setting specific research [77] [78], on pandemic-related stress resulting from working at home.

2.1.8 Humans as the strongest link

Much of the existing literature [5] [79] [80] [81] [48] suggests that it is easy for cybercriminals to target and exploit human vulnerabilities and that humans remain the weakest link in cybersecurity matters. It is the notion that "even the strongest technical protection systems can be bypassed if an attacker successfully manipulates the user into divulging a password, opening a malicious e-mail attachment or visiting a compromised website." [28, p. 1]. Heartfield and Loukas in [28] attempt to challenge much of the current thinking by exploring the use of a prototype "Human-as-a-Security-Sensor" (HaaSS) framework. They suggest that humans should be empowered as the "strongest link". The framework aims to use human context within detection mechanisms to notify users of incoming social engineering attacks so that preventative measures can be immediately enabled. Cognitive research from Jensen et al. in [82] starts to explore supplemental "mindfulness" to encourage human-related security awareness and reduce susceptibility to phishing attacks. Overall, this is an exciting area of cognitive research. I believe we will begin to see innovation that looks to strengthen the human element, reducing the stigma around human-centric cybersecurity weakness.

Chapter 3 now examines how attackers look to target human weakness during a crisis. In such a modern crisis environment, new situational factors further increase susceptibility towards devious phishing attack techniques.

Chapter 3 – How attackers target people and human factors during a crisis

The overall objective of this chapter is to focus primarily on phishing attacks to provide examples of how attackers look to target people during a crisis environment. The chapter will begin with a background on human behaviour. **Sections 3.2 - 3.5** provide a detailed cross-section of phishing attack methods, social influence, human and situational factors. Each item within these sections will contain a description and examples, providing pandemic-related context to highlight susceptibility to phishing.

Chapter 3 also acts as preparation for the work in **Chapter 4**, where the items from this chapter are to be correlated against recent COVID-19 announcements and phishing evidence to produce a visual timeline of events.

3.1 Background

Previous disaster events have often led to a rise in cyber-related crime and opportunistic attacks on vulnerable victims [83]. The COVID-19 pandemic has not differed [84] and, as a unique global event, will have impacted and overwhelmed people in many different ways. Coelho et al. in [85] highlight that the COVID-19 pandemic "formed a serious multi-etiological global mental health challenge influencing every aspect of life and disrupting the social fabric." [85, p. 3].

With prolonged exposure to a crisis environment, human responses, such as uncertainty, stress, anxiety, and exhaustion, will have increased the risk of errors in decision-making. Attackers will also have utilised the chaos and disruption to their advantage. Crimando in [50] recognises the significance of human behaviour being of vital interest to attackers since "they know how to manipulate it to achieve their goals" [50, p. 3]. **As attackers adapted during the pandemic, through shared human experience, they undoubtedly became psychological experts** [86].

The psychologist Kurt Lewin in [87] outlines the following heuristic formula **B = *f* (P,E)** to explain what defines human behaviour. In this formula, **human behaviour (B)** is a **function (*f*)** of the relationship between the **person (P)** and the **environment (E)** they find themselves in.

To frame this formula within the scope of this thesis, the person or **"P" factors** indicate the psychological influence techniques, such as authority and scarcity, which attackers aim to exploit against a target. Therefore, the **"E" factors** indicate the pandemic environment, where confusion, stress, and uncertainty flourished as the crisis unfolded. Situational factors, such as rapidly changing Government guidance and long-term working from home routines, also contribute to these **"E" factors**. It is essential to acknowledge that during a prolonged

period of disruption caused by the crisis, which will be two years when this work is published, these **"E" factors** will continually evolve. Cybercriminals know this too, as they adapt within the current environment to use more devious methods, which I will explore through a timeline study of phishing attacks during the recent Omicron COVID-19 variant in **Chapter 4**.

At the cognitive level, several factors can affect susceptibility towards the threat of phishing, such as variability in impulsiveness and different personality traits [88]. Certain cognitive biases can also lead to misjudgement and increased susceptibility [89]. Overconfidence bias occurs when people believe they are less likely to experience something negative than others. Fatalistic thinking is contrary in that people believe there is little they can do about a situation and therefore assume it will happen anyway. In both cases, the outcome is the same. Both stem from the misinterpretation of risk [90], and unpreparedness can increase susceptibility to phishing and cybersecurity threats.

It is important to introduce phishing attack concepts and technical methods next as a starting point. Secondly, I will explore the **person (P) factors**, social influence, and human factors. Finally, I will provide examples of **environmental (E) situational factors** that caused an impact during the pandemic.

3.2 Phishing attack types and technical methods

Phishing attacks, primarily through email, have become a persistent threat group primarily used to steal information from victims [50]. Several phishing variations have been selected for **Table 2** in **Section 3.2.1**, covering common delivery approaches, such as **smishing, vishing, spear-phishing, and whaling**. There are many technical methods available to attackers carrying out phishing attacks; however, I have selected specific techniques for **Table 3** in **Section 3.2.2**, which are likely to have helped by technically enabling phishing attempts to become more successful during the pandemic. I acknowledge that this is by no means an exhaustive list but that it is sufficient to cover the scope of this chapter.

Tables 2 and 3 aim to provide pandemic context to show how various phishing attack methods have targeted victims during this period. As a simple classification method, phishing attack types will be identified in the table using the format P1 to P5 and technical methods using T1 to T7.

3.2.1 Phishing attack types

Table 2 of 11 – Phishing attack types			
ID	**Phishing attack types**	**Description**	**Pandemic context**
P1	**Phishing (email)**	Phishing emails are often sent to recipients indiscriminately and conveniently in bulk, through spoofing techniques, see **Section 3.2.2**, and by impersonating trusted sources. The term phishing is analogous to fishing by using social engineering techniques, such as lures and hooks within a sea of potential victims on the internet.	Fake NHS emails [91] disguised using official logos and urging recipients to act quickly by offering free COVID-19 testing will have triggered fear and urgency responses for those who received these phishing emails. Carefully disguised URLs using NHS keywords and other Typosquatting techniques, see **Section 3.2.2**, trick users into clicking them. Malicious phishing websites and forms then aim to harvest personal and financial information.
P2	**Smishing (sms phishing)**	While phishing uses email as the attack technique, smishing, which combines SMS and phishing, utilises text messages. Sometimes these phishing messages can have a higher response rate than emails [92] and can be easily disguised to include harmful links that appear from a legitimate source.	Fake text messages claiming to come from the NHS [91] with urgent and misleading content will have caused many individuals to panic. If convinced by the short message and believing they had come into close contact with someone who has COVID-19, they may have inadvertently clicked on a malicious link inside the message. See **Figure 9** for an example of a fake NHS text message.
P3	**Vishing (voice phishing)**	Vishing or voice phishing involves voice calls, which can be automated or spoofed by an attacker to create a disguise, see **Section 3.2.2**. These voice attacks aim to use social engineering techniques to extract sensitive information from a target via a conversation or automated calling.	In Vishing evidence reported during the pandemic [93], an elderly individual received a call from someone claiming to be from the NHS. The victim had to pay a small fee to update their NHS COVID pass details. The fraudster might have used the principles of authority and liking by pretending to work for the NHS. Common Vishing attempts can be more successful when spoofing the phone number and using various social engineering techniques to trick the recipient into providing personal and financial information.
P4	**Spear-phishing**	Spear-phishing usually involves precise targets of interest as part of a cleverly coordinated approach to gain access or cause disruption. Often, these types of attacks form part of a	During the pandemic, the hiring and onboarding of new users will have happened in virtual settings, with lots of information exchanged over email. There is evidence [95] of spear-phishing campaigns targeting

		chained approach, or they allow secondary attacks through a compromised initial target. Business email compromise (BEC) attacks are becoming a more popular way to describe the workplace scenario where attackers look to combine various techniques as part of a spear-phishing attack, such as persuasive social engineering, using email spoofing to disguise the origin or by enticing an employee to download a malicious attachment [94]. More advanced spear-phishing attacks will involve detailed research on the target, aiming to compromise a single user. These approaches might also target the technology stack used by an organisation to exploit specific vulnerabilities common to the target.	specific remote-working and return to work scenarios, see **Section 3.5**, to trick individuals with fake COVID-19 workplace protocols. This example is a precise and advanced spear-phishing attack technique. It might have involved detailed research on the location of employees or by collating information from job posting websites to target new starters.
P5	**Whaling**	Whaling attacks aim to target higher-ranking individuals in an organisation, such as members of the executive team. Attackers know that senior individuals usually have access to the most sensitive information or may have elevated credentials and less scrutiny on their accounts, which might be highly desirable. Notably, a whaling attack happened in 2015 at the networking company Ubiquiti. £33m was lost through the fraudulent transfer of funds as a senior staff member was impersonated [96].	CEOs, just like employees, were at home during the pandemic. Outside of the physical setting of the organisation, senior executives may have become more susceptible to targeted whaling attacks. Remote working has meant that these senior individuals became physically distanced from their staff and the protections of an office environment. Some organisations also suffered immensely due to the pandemic disruption, seeing many cyber-attacks occurring during the initial crisis [49]. These events will have likely put a large amount of stress upon senior individuals suddenly running operations remotely, increasing the risk of whaling attempts becoming successful.

Table 2 - Phishing attack types

3.2.2 Phishing technical methods

Table 3 of 11 – Phishing technical methods			
ID	**Technical methods**	**Description**	**Pandemic context**
T1	**Spoofing**	Email spoofing techniques disguise the sender's email address to trick the recipient into believing the message originates from someone they trust. Spoofing tools allow fraudsters to modify and forge email headers to disguise the sender address rendered in the recipient's mail client application [97]. **Section 5.2** highlights the advanced nature of spoofing software and services, which can quickly disguise phone numbers for Vishing and Smishing attacks and run automated calls to steal one-time password codes.	During the pandemic, the Government, NHS, and media outlets issued high-frequency information updates [98]. Phishing attempts could quite easily be mistaken for these official announcements. The ability for fraudsters to technically disguise their phishing campaigns using spoofing techniques is likely to have resulted in users unknowingly divulging their personal and financial information.
T2	**Static phishing kits**	Static phishing kits allow attackers to rapidly customise static content using software and templates. Sometimes referred to as boilerplate kits, these can include pre-built user-interface elements that replicate official Government or health organisation styles.	Fake NHS emails quickly circulated during the pandemic [91], which contained identical fonts, styles and official NHS logos to trick users into believing these were legitimate emails from official health service providers.
T3	**Dynamic phishing kits**	Dynamic phishing kits allow attackers to use more advanced techniques to extract personal information, login credentials and two-factor authentication codes dynamically as part of the phishing content [99].	There is evidence from the NCSC [100] of dynamic phishing kits being used to replicate the UK Government GOV.UK websites during the pandemic, **see Figure 8**. The malicious clones of well-known, trusted websites aim to harvest personal and financial information from a user. These clones may have had a higher chance of success around the period when the UK Government was offering emergency financial support, such as the "Hardship Fund" [101], drawing users who needed financial support to GOV.UK websites.
T4	**Mobile optimised content**	Attackers can better disguise content and malicious URLs by optimising phishing content for smaller screens. Since mobile devices are smaller and portable, it is much more likely that	Many individuals were likely distracted by the situation and changing events during the pandemic. The regular announcements and news reports may have resulted in more frequent activity on mobile

		users will scan and swipe through content quickly and spend less attention than on a fixed desktop device.	devices. However, this may have led to lower focus and attention on the content received on these smaller mobile devices, increasing the phishing success rates. Using Typosquatting techniques, attackers can create very long URL strings that potentially stretch outside of smaller mobile screens, disguising the true nature of these malicious links and increasing the chance of successful clicks.
T5	**Typo-squatting**	Typosquatting or URL hijacking and manipulation refers to several techniques which allow attackers to impersonate existing URL domains. Typosquatting involves subtle misspelling of the malicious domain by mixing, missing, or duplicating similar letters, which might easily fool a target. Alternatively, using the same URL path but choosing a different top-level domain, such as *.org.uk* instead of *.org*, might be enough to convince a target. Convincing keywords, special characters, hyphens, or full stops in the target domain can lengthen a URL outside of device screens to improve the disguise.	There is evidence of Typosquatting techniques [91] used in the fake NHS emails and messages sent to recipients during the pandemic. The URLs within these phishing campaigns cleverly used NHS and COVID-19 related terminology to hide the malicious nature of the URL links. **Figure 10** shows an example of Typosquatting in the following URL: **https://nhs-pcr-testkit.com**. This example contains targeted keywords to convince a recipient. Unfortunately, harmful phishing links can also start to appear in mainstream search engines. By utilising paid advertising techniques, attackers can promote their phishing website URL above other legitimate websites in search rankings [102].
T6	**Malicious QR codes**	QR codes are machine-readable matrix bar codes that allow stored URLs within the QR pattern to be scanned and read by using mobile devices.	During the pandemic, QR codes quickly became a popular and effective way of contact-free URL sharing when individuals became cautious of close contact due to the virus. Physical menus were replaced with QR codes in a restaurant setting to reduce interaction when ordering. NHS systems also used QR codes for vaccination certificates and “track and trace” systems [103]. The challenge with QR codes from a cyber security perspective is that the pattern that users scan is not easily identifiable from one to another. An attacker could generate a physical malicious QR code as part of a multi-layer phishing campaign to direct a target to a malicious website.
T7	**Use of AI**	*Deepfake*, as a term, describes where audio and video content, using AI deep-learning tools and	The Government urged people to stay inside during the pandemic, and organisations shifted rapidly to a

		techniques, is fabricated [104]. Large sample datasets, sometimes gathered through the social reconnaissance activity of a person of interest, are processed to create the artificial *Deepfake* content. To bypass security controls, attackers aim to use this *Deepfake* content as part of targeted spear-phishing and BEC attacks to convince someone they are interacting with a genuine person.	work from home setup. Virtual communication tools replaced physical face-to-face information exchange, which might have allowed *deepfake* phishing attacks to become more successful. Without the in-person verification that workplace settings often provide, spear-phishing attacks using AI deepfake techniques could have succeeded.

Table 3 - Phishing technical methods

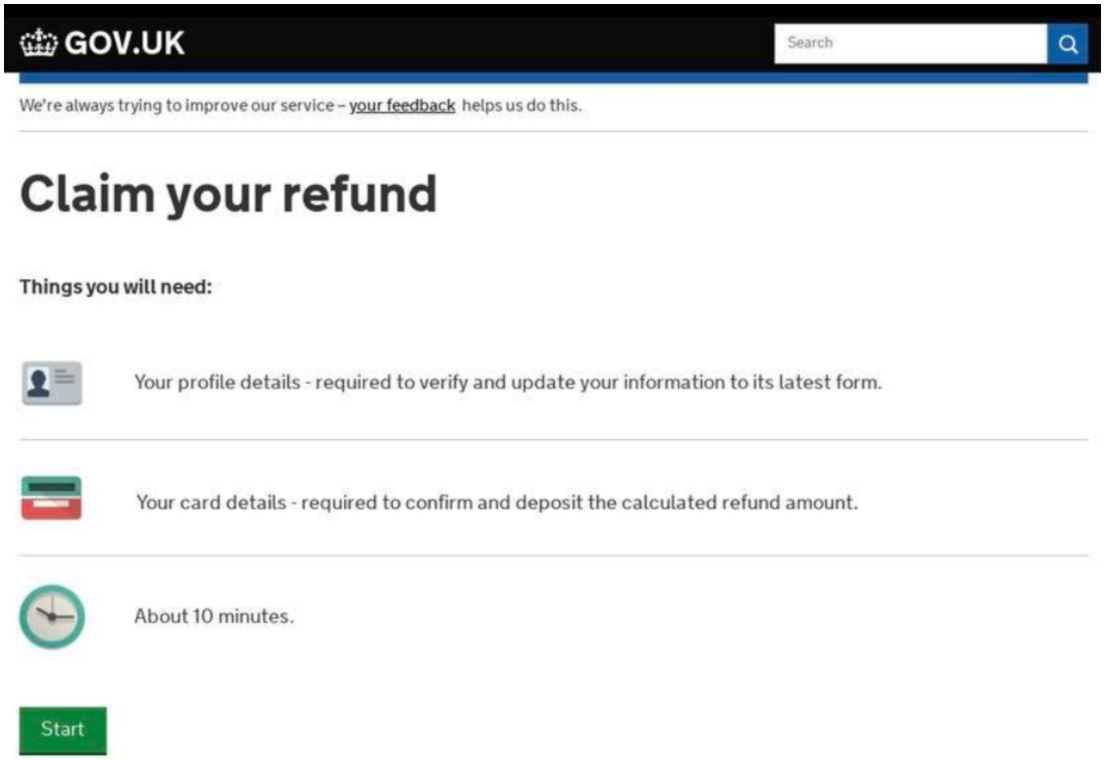


Figure 8 - Example of fake GOV.UK webpage using dynamic phishing kits to clone official elements to steal personal and financial information [100]

3.3 Social engineering and influence techniques

Social engineering tricks allow cybercriminals to lure or convince a target into a vulnerable situation, ultimately and with enough patience, to gain access to their personal information [105]. These social engineering tricks can convince a target to click malicious links or reply to messages. Successful social engineers do so without raising any suspicion and are not always outsiders [106], building trust and likeability since people are more likely to say yes to others they like [107].

In Fogg [108], we know that social engineers aim to target and exploit social and cognitive vulnerabilities through persuasive influencing methods. They do this through nudges and by motivating a target to take an easy action, resulting in a successful response. A target will often unknowingly give up sensitive information since social engineers interfere with the target's emotions, causing them to reveal information, sometimes through misinterpretation of the original message [109].

In his book *Influence: The Psychology of Persuasion* [110], Cialdini identifies "six principles of influence". By exploring these six influence techniques in **Table 4**, the aim is to provide examples where pandemic context will have allowed social engineers to exploit and convince victims to respond to requests via phishing. As a simple classification method, each influence technique will be identified in the table using the format I1 to I6.

Table 4 of 11 – Influence techniques

ID	Influence techniques	Description	Pandemic context
I1	**Reciprocation**	Neurological responses are triggered when we receive something, affecting our decision-making [111]. People often feel obliged to return the favour if offered something first.	Much of the evidence of fake NHS phishing emails and messages seen during the pandemic [112] shows content that offered free testing kits, vaccine appointments and options to update COVID-19 pass information for a small cost. These phishing campaigns will have used the principle of reciprocity to try to offer something free in return for cleverly disguised requests for personal or financial information.
I2	**Commitment and Consistency**	People tend to admire and value commitment, consistency and honesty seen in others. Guadagno and Cialdini in [113] refer to this as the "foot-in-the-door" procedure, whereby someone starts with a small request and then moves onto a second or larger request.	Pandemic phishing campaigns often start with a small request in an email or message, such as stating that a person is now eligible for a COVID-19 pass and that they can apply via a link. **Figure 9 demonstrates the persuasive techniques used**. Once a person clicks on the malicious link, further personal and financial information requests may occur.
I3	**Social proof**	When uncertain about a decision or situation, people often look at others to guide them or for validation. Social media and frequent communication between friends and family can often	As the pandemic unfolded, many essential items, face masks and COVID-19 test kits became out of stock for periods. Stockpiling behaviours developed because of the panic response to certain items being unavailable. It is likely that the uncertainty surrounding the crisis spread through social communication at the time. If people saw others

		trigger these behaviours, which relate to the principle of social proof.	stockpiling items, it was likely that this would have guided their behaviours to attempt to source and stockpile certain items.
I4	**Liking**	People are more likely to say yes to those they like, find attractive, or if the person they are interacting with is similar to them [111]. Strangers can also be more persuasive if they come across as likeable.	At the start of the pandemic, there was a "Clap for Carers" movement, where people celebrated NHS staff by clapping outside their homes each week [114]. In Vishing evidence seen during the pandemic [93], fraudsters targeted vulnerable individuals by pretending to call from the NHS. The principle of liking may have been used to convince a target that they were being called by a hard-working and likeable NHS staff member, offering their help to the community. Fraudsters might have used the pandemic environment and sentiment towards the NHS to start a conversation topic as part of a subtle social engineering attack.
I5	**Authority**	It is human nature to reciprocate and help someone in a position of hierarchy or authority [115]. When we believe we are interacting with someone of authority, we are more likely to follow instructions, and social engineers take advantage of this by impersonating common positions of authority, such as the police, from a bank or someone from the NHS.	In Vishing (voice phishing) social engineering scenarios, see **Section 3.2.1**, authority is a primary persuasive method used to impersonate others and instil fear in a victim [116]. Another common example is when fraudsters use email spoofing and *deepfake* AI techniques, see **Section 3.2.2**, to impersonate a senior person in an organisation, such as a CEO. In this case, they will try to convince an employee to transfer money to them urgently as part of a targeted phishing campaign. These attacks can have a high success rate as individuals believe they are exchanging contact with a senior person in the company, and as they do not wish to lose their job, they follow orders.
I6	**Scarcity**	When we believe something is in short supply, we often want it more. Scarcity can override specific decision-making, as we place a high value on something we believe to be of limited availability. Attackers use scarcity techniques to motivate individuals to act quickly [116].	During the pandemic, certain items were in high demand or became unavailable, for example, face masks and COVID-19 testing kits. Fake NHS health-related phishing email attempts [91] offering free testing kits may have triggered scarcity responses. When these items were in short supply, this may have led to panic responses and clicking unsafe links without thoroughly checking whether these were safe. Fraudsters may have also targeted those working from home with spear-phishing emails, see **Section 3.2.1**, that appear to have come from the organisation or academic

			institution's IT. By crafting an email that explains that an individual's work account will be deactivated in a short period, then by using a malicious link to steal login credentials.

Table 4 - Influence techniques

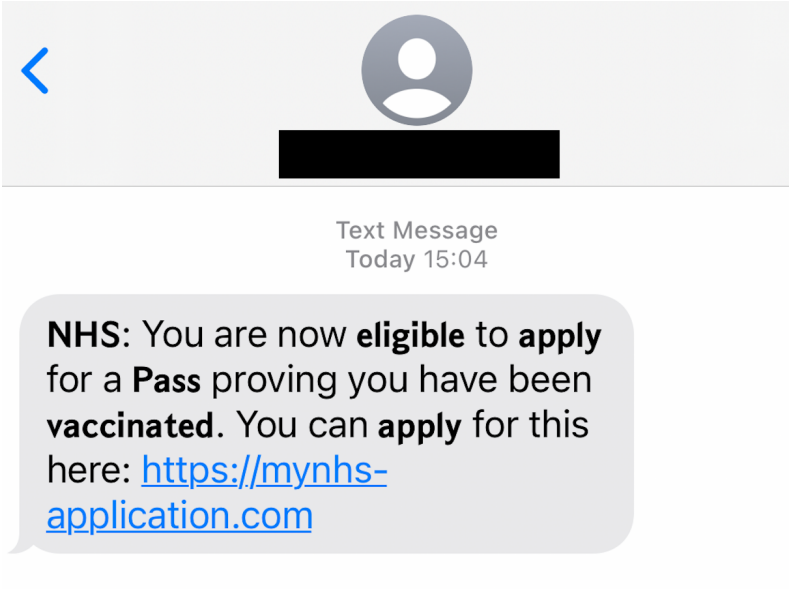


Figure 9 - Example of fake NHS smishing message, showing persuasive techniques (sourced directly as received by the author)

3.4 Human factors

Whenever a human element is involved, an attacker will attempt to target and manipulate a victim through the shared understanding of human behaviours [86]. I have chosen to include the following elements in **Table 5** for their suitability and to provide pandemic context during the crisis. The focus of this table is to highlight human susceptibility to phishing attacks. I acknowledge that this is by no means an exhaustive list of human factors, but some of the most relevant to the scope of this chapter. As a simple classification method, each human factor will be identified in the table using the format H1 to H8.

Table 5 of 11 – Human factors			
ID	**Human Factors**	**Description**	**Pandemic context**
H1	**Emotions**	Emotions and emotional impact play a crucial part in our overall decision making, bias and overall judgment [117]. Incidental emotions, such as our	The pandemic will have triggered emotional responses due to health-related concerns and changing situational factors. These changes have a high likelihood of impacting our overall behaviours and decision-making. Both incidental

		mood, might be experienced as we decide on something but are not related to the decision [118]. Alternatively, a decision can cause integral emotions to surface when considering the implications, possibly from prior experience, resulting in anxiety or regret.	and integral emotions will have amplified during the pandemic, specifically in situational scenarios, see **Section 3.5**, related to the health of our family and friends. Anxieties may have developed, changing decision-making, increasing vulnerability and susceptibility to more convincing phishing threats.
H2	**Fatigue**	Physical and mental fatigue can occur because of stress or tiredness, leading to mistakes in judgement. Fatigue can also develop through repeated situational circumstances that manifest over time, creating a variance in our decision bias.	Fatigue is an important topic within the context of pandemic events. National *lockdowns* and *stay at home* guidance, see **Section 3.5**, may have amplified the symptoms of fatigue, such as exhaustion, frustration or even developed into depression. During a prolonged crisis period, fatigue can cause a reduction of focus, therefore increasing our susceptibility to phishing threats.
H3	**Confusion**	Confusion can often occur due to misinformation or a general misunderstanding of certain information, which during a crisis period presented many challenges. In **Section 3.3**, the principle of Social Proof tells us that we often look to others to guide our decision-making. If this is not possible, confusion can occur if a person is alone.	New Government announcements and emergency measures [119] changed what people could and could not do during the pandemic. According to some critics [120], much of the Government advice during the pandemic has been inconsistent and unclear. However, the spread of false and misleading information [121] has not helped. Ultimately, the overload of information will have led to confusion amongst the public. Vulnerable scenarios caused by the emergency measures and isolation rules would mean those physically alone were more at risk of being confused. If a person cannot verify the legitimacy of the information they receive, they are likely susceptible to fraud or online scams during the pandemic.
H4	**Stress**	When making decisions under stress or pressure, our behaviours are often erratic and different to how we might more calmly address a decision. Stressful situations can lead to inconsistent choices and reactions, differing from behaviours when not placed under pressure.	In phishing evidence [91], fake NHS messages aim to trigger a stress response in a recipient. News surrounding new COVID-19 variants, such as Omicron, may have led to immediate and stressful reactions and increased susceptibility to phishing threats.

H5	**Technostress**	*Technostress* is a term used to describe the resulting distress caused by ineffective coping strategies towards technology use [122].	People spent more time online during the pandemic [41] and needed to interact more with technology. For those less used to technology, *technostress* might explain other behaviours forming, such as frustration, mental exhaustion, or a feeling of technology burnout [75]. *Technostress* factors can increase the risk of errors in decision-making occurring. The pandemic accelerated the use of technology, such as NHS COVID-19 passes and various websites and online forms. Those unfamiliar with technology may have struggled to determine the legitimacy of these websites and become more susceptible to phishing emails and messages.
H6	**Urgency**	When information or a simple request arrives in a time-sensitive or urgent manner, it can be human nature to respond or do something more urgently and reactively. Sometimes, this can result in less care or consideration, such as sharing personal or financial details. In urgent scenarios, less verification of the legitimacy and trustworthiness of a source might occur.	Fraudsters will use urgency techniques to convince a victim to do something by creating a sense of real urgency. The pandemic provided a prime environment for these techniques, **see Figure 10**, where the threat of being in close contact with someone who has the virus might nudge a recipient into clicking a link urgently. Urgent language in phishing messages, such as "you must order a Test Kit," can further enforce a sense of urgency in a recipient.
H7	**Curiosity**	Curiosity or intrigue can sometimes occur through boredom. However, an attractive incentive or something that appears free from cost will usually be enough to pique human interest and curiosity.	Fraudsters often use phishing campaigns with incentives to lure people into exploring something out of curiosity to bypass rational thinking. When travel costs increased due to new entry requirements for different countries, attackers used techniques to steal personal information and card details by offering a free or low-cost COVID-19 testing kit for travel [112].
H8	**Fear**	Fear is a human response to the threat of harm arising from a physical, emotional, or psychological response to a situation. The medium intensity of fear moves responses from nervousness to anxiety and worry, and higher intensity of fear can lead to desperation and panic [123].	Fraudsters capitalised on fear throughout the pandemic, specifically around health concerns and testing for the virus. Smishing text message evidence, see **Figure 10**, shows targeting phishing message evidence, with content that evokes the threat of illness and positive contact with the virus.

Table 5 - Human factors

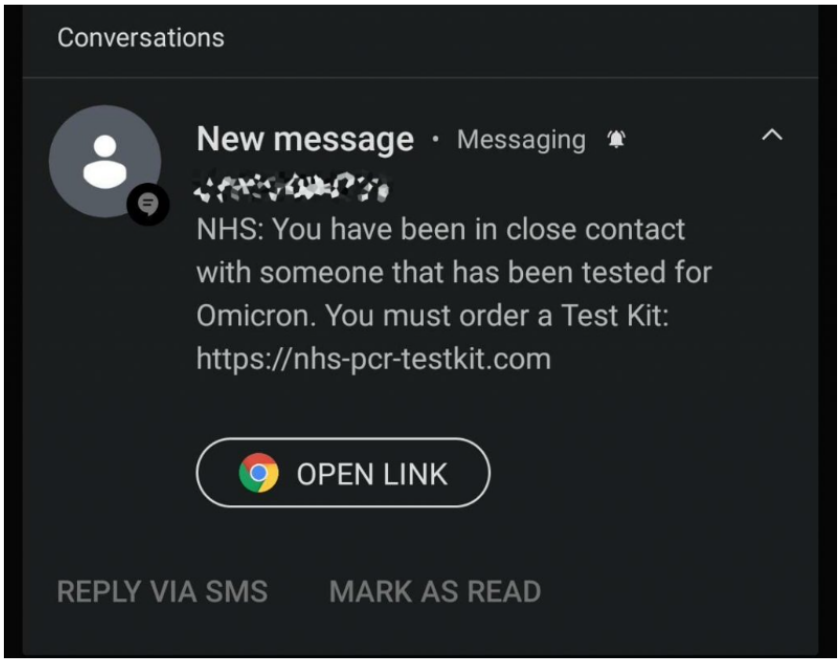


Figure 10 - Example of a fake NHS smishing text message from February 2022 during the time of the Omicron variant wave [91]

3.5 Situational factors

The pandemic created situational circumstances which disrupted the way people responded and behaved. Due to various Government restrictions [98], much of the working population was ordered to stay inside and shifted to full-time homeworking [1].

I have chosen the following situational factors in **Table 6** to explore how a number of these circumstances will have impacted people during the crisis and increased their susceptibility to phishing attacks. As a simple classification method, each situational factor will be identified in the table using the format S1 to S8.

Table 6 of 11 – Situational factors			
ID	**Situational factors**	**Description**	**Pandemic context**
S1	**Lockdown and stay at home orders**	In March 2020, the Government advised all citizens of the UK to stay inside, avoid non-essential contact with others outside of the household and avoid unnecessary travel [98]. At the same time, the DHSC issued *stay at home* and self-isolation orders if any household members developed Coronavirus symptoms [124].	Many individuals are likely to have suffered symptoms of stress, and fatigue when *lockdown* and *stay at home* orders with lifted and then subsequentially re-applied as new COVID-19 variants surfaced. As a result, it is essential to highlight that the overall effect of these restricting orders, further amplified with other situational factors discussed in this section, contributed to heightened COVID-19 anxiety and the emotional

		Government-issued national *lockdowns*, requiring individuals to stay inside and help control the virus, were introduced by law at various points in 2020 and 2021 [125].	disruption of a considerable number of people in the UK and around the world. Targeted phishing campaigns, aimed at tricking and coercing individuals into unwillingly providing personal and financial information, are likely to have had higher success rates due to the Government-issued orders and restrictions.
S2	**Homeworking**	Homeworking took immediate effect due to the advice from the Government to stay inside and remain at home [98]. Organisations quickly shifted to working models, which permitted employees to continue their regular duties from home. Attackers will have been looking to target those unsettled from regular working routines, taking prime advantage of the disruption caused by widespread remote working [51].	As highlighted in **Section 3.4**, *technostress* will have contributed to COVID-19-related anxiety and became linked with homeworking. Studies show that *technostress* can impact work performance [75]. Many individuals are still unlikely to have returned to their regular working routines or even a physical location. The prolonged impact of homeworking is therefore significant as a situational impact. Several other human factors discussed in **Section 3.4**, such as fatigue and stress, are likely to have been amplified by a state of permanent homeworking for almost two years. As more devious pandemic-related phishing campaigns evolved, they will likely to have had a higher success rate because of elevated behavioural responses and as individuals were much more easily contactable at home [71].
S3	**Return to work**	At the beginning of the pandemic, businesses had to close, and some people were placed on temporary furlough schemes [126] or even lost their jobs. As companies hired new staff during the re-opening period, many individuals returned to standard or hybrid working patterns. In a hybrid setup, individuals might attend their employment location on a rotational pattern, for example, two days per week.	Inspired by the disruption to regular working patterns in the pandemic, evidence of phishing campaigns [95] targeted new starters by confusing those returning to employment or a physical work environment. These attacks allowed attackers to steal login credentials and then compromise systems. For those new employees starting in a remote working environment, this may have caught them off guard since the usual protections offered by in-person and office employee onboarding processes may not have been in place.
S4	**Remote teaching and home-schooling**	As schools and academic institutions closed upon the news of the COVID-19 virus spread [127], students and teachers were forced immediately into the new environment of education from home.	Many human factors discussed in **Section 3.4** are likely to have been strained due to the disruption caused by home education requirements during the pandemic. Younger children require regular supervision [128], which may have been inconsistent in a home setting,

		Parents needed to provide educational support for their children but may have had no prior experience. The technology requirements for home education may have presented new financial and technical challenges.	and where adults too were working and distracted. For parents, this is likely to have caused stress, technostress, and fatigue, increasing errors in decision-making. Urgent-themed phishing attempts may have caught many parents and even children off-guard, causing high success rates and loss of sensitive information. From the academic institutions' perspective, increased bandwidth demanded by a rapid shift to new remote applications and video calling software may have put IT departments under considerable pressure. Many existing systems will not have been designed for fully remote scenarios, distracting those responsible for administrating remote-education services and potentially opening the educational organisations up for increased cybersecurity risk. This suggestion from a 2021 NCSC report [129] highlighted increased cybersecurity risk and ransomware attacks targeting schools, colleges and universities in the UK.
S5	**Online shopping and home delivery**	As a result of the pandemic, brick and mortar shops had to close. People spent much more time online, which translated to increased online shopping [42]. Home delivery attempts would therefore have increased, including delivery-based message notifications.	During the pandemic, a common menace has been delivery-related phishing attempts [130]. These phishing messages arrive explaining that a parcel has been missed, with a link to enter personal details to rearrange for a small fee. There could be an argument that people might react with confusion and curiosity since they had not left home. Alternatively, with such an increase in online shopping and home delivery, a person may inadvertently forget many of the items they had ordered, assume this was a legitimate parcel attempt and then fall prey to the phishing message by clicking an unsafe link.
S6	**Quarantine and illness**	Those who were unfortunate to catch the Coronavirus at various pandemic stages will have suffered from varying degrees of illness. The Government also issued travel guidance for all non-domestic UK arrivals [131] with specific restrictions to spend a period in quarantine.	Those who lost family members and friends during the pandemic will have suffered from a wide range of human emotions. These factors could have increased susceptibility to phishing attacks and enabled much higher success rates. Quarantine, whether in a hotel due to country-specific entry requirements or self-isolation at home, may have caused unfamiliar behavioural

			patterns, including fatigue, distraction, and confusion. If a person was suffering illness from the virus itself, this could have caused more severe levels of stress, fatigue, and fear to occur.
S7	**Financial loss**	The pandemic brought immediate disruption, causing the Government to issue *lockdowns* and order citizens to *stay-at-home*. An estimated 7.6 million job losses occurred, around 24% of the UK workforce [132]. As a result, according to the ONS [133], companies stopped hiring. In the lowest income sub-regions of the UK, the vulnerability to job losses was the highest [132].	There is evidence of phishing campaigns [112], as shown in **Figure 12**, that utilise the principle of reciprocation by offering something for free, such as a variant-specific COVID-19 test kit, which may have increased phishing success rates for those struggling financially. **Those who suffered a financial loss may have also been drawn to cybercrime** [60] to provide an income.
S8	**Vulnerability and isolation**	Many isolating situations arose during the pandemic, such as being apart from friends and family members, naturally increasing vulnerability. However, this does not imply that age or demographics determine the vulnerability when referring to situational vulnerability.	News events throughout the pandemic reported a rise in virus cases and deaths, which are likely to have triggered vulnerability or panic responses. Panic would have certainly heightened vulnerability factors, where individuals might have reacted quickly or caught off-guard, resulting in errors in decision-making. Isolation can lead to verification challenges in a particular situation. In an example of a phishing campaign, if an individual cannot verify the actual legitimacy of the email, message, or phone call, they may fall victim to the attack.

Table 6 - Situational factors

In **Table 6**, it is evident that the situational factors that arose during the pandemic health crisis will have impacted human factors. As an opportunity to visualise the relationship between situational factors and differing human factors, I have produced a diagram, see **Figure 11**, to demonstrate how phishing susceptibility can increase due to situational pandemic events and cause an impact on human behaviours.

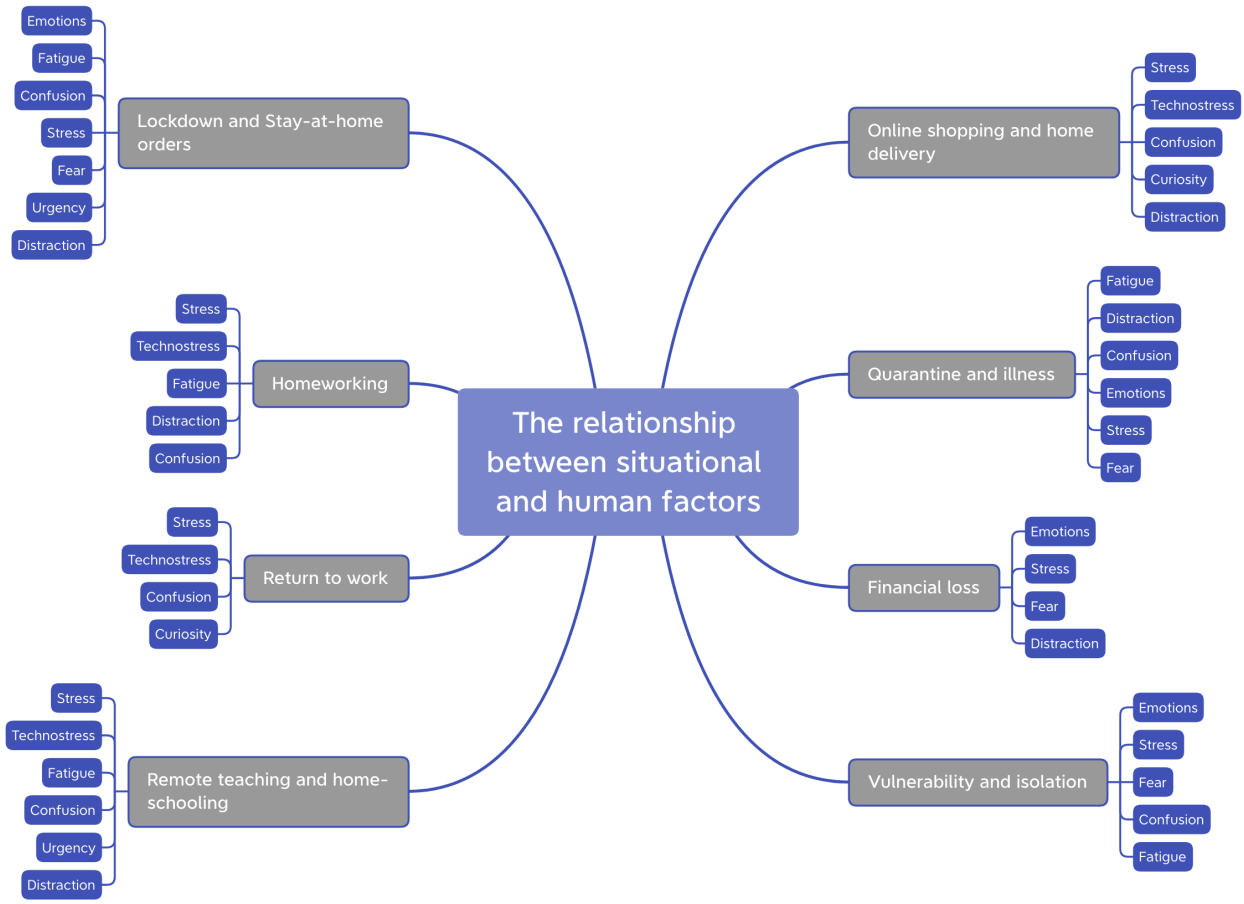


Figure 11 - Diagram to visualise the relationship between situational and human factors (author contribution and visualised from analysis in Table 6)

3.6 Summary

Structuring this chapter using Lewin's heuristic formula **B = *ƒ* (P, E)** [87] helped establish the relationship between the **person (P)** and the **environment (E)**.

Understanding how attackers use persuasive social influence techniques to exploit cognitive vulnerabilities provides one aspect of the **person (P) factors**. Another aspect of the **person (P) factors** is understanding how human elements are manipulated to increase susceptibility to phishing attacks.

The pandemic situational factors in **Table 6** are critical to consider when attempting to understand how **environment (E) factors** combine with the **person (P) factors**. **Environmental situations can be used to an attacker's advantage** by amplifying the disruptive effects that a situation can have on human vulnerabilities. It is also the shared environmental experiences that all people go through during a

crisis. **Through access to these same shared experiences, fraudsters might have become psychological experts and used the pandemic disruption to their advantage**.

Whilst it is essential to identify how attackers target people in a crisis, it is also important to understand how quickly they can do so. I present a visual timeline in **Chapter 4** to show how the Omicron COVID-19 variant helped enable targeted phishing attacks. The attack types, the **person (P)** and **environment (E) factors** detailed in this chapter, also play a core part in classifying the evidence and analysis.

Chapter 4 – Omicron: A visual timeline of phishing evidence

The overall objective of this chapter is to demonstrate how attackers quickly modified phishing content with COVID-19 Omicron-related terminology. Tables of Omicron-related announcements and phishing evidence from December 2021 form the data for a visual timeline diagram of events. **Chapter 3** provided a list of phishing methods, social influences, human factors, and situational factors, with an ID to classify each item. I refer to these to identify whether increased susceptibility to phishing attacks occurred due to Omicron-related factors.

4.1 Background

In November 2021, the World Health Organisation (WHO) announced a new COVID-19 variant of high concern, which was named "Omicron" [134]. As soon as December 2021, Omicron cases were reported in the UK and across the rest of the world [135]. Due to the various international responses to COVID-19, a variance exists between vaccine rollout strategy, approaches, and entry requirements, also highlighting a growing concern around global vaccine inequality [136]. Some countries have launched third and fourth dose booster programmes, where additional doses of COVID-19 vaccines were administered broadly to citizens of all ages, with high supply. However, as of January 2022, only 9.5% of people in low-income countries have received one vaccine dose [137], and in Africa, only 10.09% of people have completed two-dose full vaccination [138].

When the first B.1.1.529 Omicron variant case emerged in South Africa [134], immediate and cautionary travel restrictions came into play. Prior to the announcement, it is likely that people had started to relax as the UK returned to some sense of normality. However, news of the Omicron variant spreading rapidly worldwide and arriving in the UK will have created a return of fear, panic and the urgent need for vaccine boosters and protection due to the high transmissibility of the variant being reported [139]. At the time, the third dose UK booster rollout had not progressed with speed [140], leaving elderly individuals facing more time alone and vulnerable to fraudsters.

4.1.1 The importance of creating a visual timeline for the Omicron variant

The November 2021 WHO announcement of the Omicron variant provides a suitable starting point to investigate phishing evidence during the period immediately afterwards. As with the earlier phase of the pandemic, fraudsters preyed on the fear and uncertainty that surrounded the new Omicron variant [141]. Using a visual timeline will help correlate how quickly targeted phishing evidence appeared alongside announcements. It is also important to evidence the continually shifting focus of phishing campaigns. Finding such evidence of Omicron phishing content, see **Figure 12**, that exploits confusion around changing

restrictions will highlight fraudsters' psychological sophistication and their ability to react immediately to the evolving new variant situation.

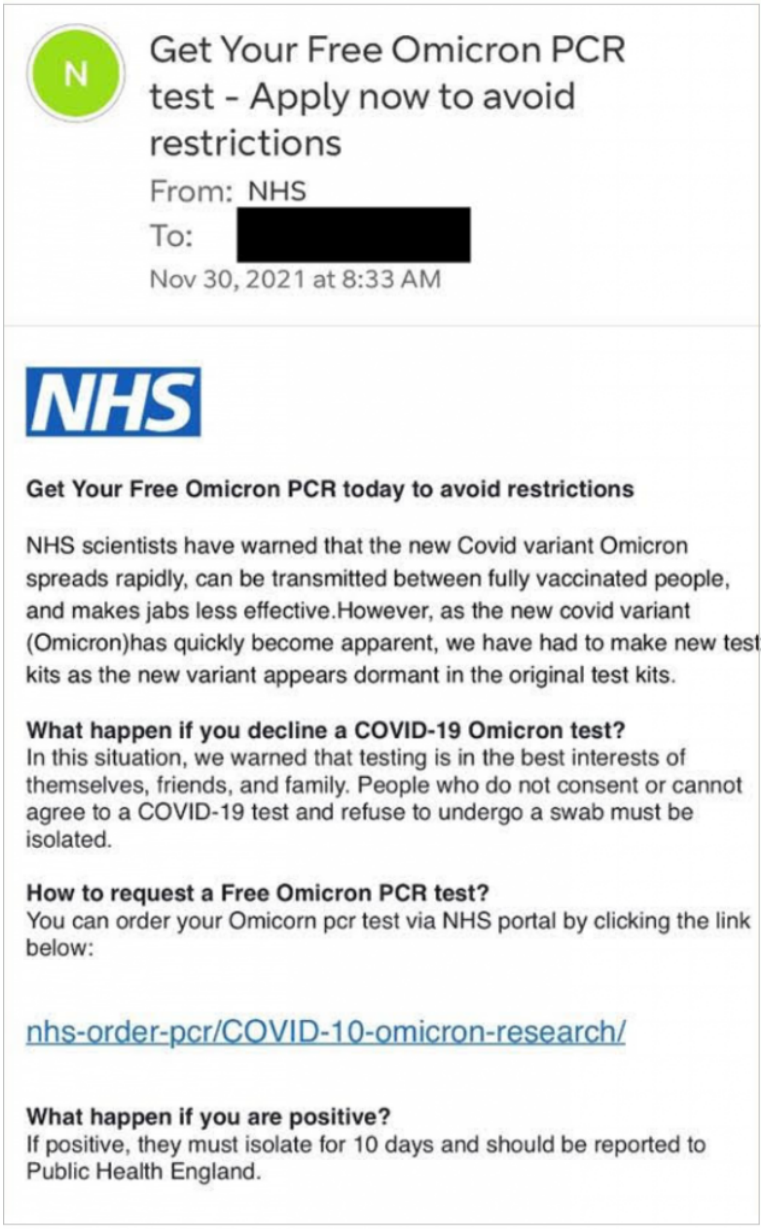


Figure 12 - Omicron variant fake NHS phishing email, showing persuasive and typo-squatting techniques [112]

The findings from this chapter will also bridge into **Chapter 5**, where the aim is to explore how social messaging applications and software tools can allow attackers to perform secondary-stage attacks, with phishing attacks forming the primary data extraction method.

4.2 Methodology

Whilst structured and systematic approaches for classifying cybercrime incidents exist in cybersecurity literature [142], I have decided to retain a tight scope and build upon the original research methodology deployed by Lallie et al. in [1]. In their work, **see Figure 6,** a temporal visualisation was produced to map cybercrime events that occurred during the initial COVID-19 outbreak period in early 2020. Using a streamlined approach will allow the findings to show how attackers can use situational factors to target victims quickly and allow for correlation between COVID-19 Omicron events and phishing evidence.

The approach will be as follows:

- Research and select online source articles within the geographic context of the UK that, on the first level, refer to significant Omicron-related announcements and, on the second level, provide Omicron-related phishing evidence that occurred in December 2021.
- Create the first table to order the announcements by their event date and identify correlating person and **environment (E)** factors by applying the ID references from **Table 7**.
- Create the second table to order the phishing evidence by event date and identify correlating phishing attack types, technical methods, and **person (P)** factors by applying the ID references from **Table 7**.
- Provide a visual timeline combining the announcements and phishing evidence and summarise findings and correlations.

4.2.1 Selection of source articles

This research refers to the COVID-19 variant B.1.1.529 as Omicron and classified by the World Health Organisation in November 2021 [134]. The Google search engine[4], explicitly configured for UK search results, was used to administer the search. Results were filtered using the "news" setting, and a custom date range was applied to refine the results:

- For the Omicron announcement evidence in **Table 8**, the starting date aligns with the WHO announcement on 26th November 2021.
- For the Omicron phishing evidence in **Table 9**, the custom date range chosen was 1st December 2021 to 31st December 2021.

[4] www.google.co.uk

I have decided that the period from 1st December 2021 to 31st December 2021 provides sufficient representation of evidence to provide a visual timeline for the immediate period following the initial Omicron variant announcement. As the scope of the research was limited to UK news articles and reports, several specific English terms and keywords were applied independently and together to yield maximum search engine results. The search strategy included the following keywords: *Omicron*, *phishing*, *covid*, *covid-19*, *variant*, *scam*, *online*, *fraud*, *vulnerable*, *PCR*, *test*, *covid-pass*. An example keyword search using a combined method was "*omicron phishing scam*".

4.2.2 Table and timeline structure

I have chosen to separate key announcements in one table, with evidence of phishing attacks in a second table. Each source article has a reference in both tables, using the IEEE referencing style [4]. The published article date and the corresponding event date follow with a short description. I have chosen to sort both tables by event date since this correctly allows the analysis of the timing between these events and avoid discrepancies in source article publishing. The timeline intends to visualise announcement dates alongside phishing evidence by using the event dates on which these occurred. Structuring the timeline using the first recorded event date on the left and the last recorded event date on the right will allow for a coherent visual timeline. The timeline position will begin in November 2021 and finish at the end of December 2021. To ensure further visual separation, I have decided to show announcements below the central timeline ruler and the phishing evidence above. Dates in the format *dd/mm/yy* will be used, along with a short description for each item. Omicron-related announcements connect to the central timeline ruler in blue, phishing evidence connect in red.

4.2.3 Limitations of the overall approach

The source material chosen for this research included non-academic regional newspaper articles. I would argue that these are appropriate enough to use in this approach since the journalistic intention within the articles appears to be primarily supporting vulnerable individuals within local communities in the UK and preventing them from experiencing online scams. Whilst undertaking the research, it became apparent that many secondary news articles regularly cross-reference phishing events from notable sources. The approach was to carefully prune the search engine results to prevent duplication of research in the tables. The risk otherwise was that this might lead to erroneous visualisation of attack events or indicate more attacks occurred than actual.

Whilst the COVID-19 pandemic has been a global event, I have decided to include research specifically focused on evidence in the UK. However, one instance was included in the table to highlight a phishing attack initially

circulating in the UK, which appears to have circulated in another country, **see ID 8 in Table 9**. The relevance of including this evidence is to highlight the ability for attackers to quickly modify phishing context for different purposes and might highlight broader international intentions of phishing threat actors. **Chapter 5** will further evidence that fraudsters use social messaging apps to increase their global reach.

4.2.4 Table of phishing attack types, technical methods, influence techniques, human factors, and situational factors

Table 7 itemises the attack types, person and environment factors explored in **Chapter 3**. By applying the correlating ID references to Omicron announcements in **Table 8** and Omicron phishing evidence in **Table 9**, a calculation of the frequency these factors were likely to have occurred will follow in each table summary in **Section 4.3**.

Table 7 of 11: Table of phishing attack types, technical methods, influence techniques, human factors, and situational factors

Attack type				**Person (P) factors**				**Environment (E) factors**	
ID	**Phishing attack types**	**ID**	**Technical methods**	**ID**	**Influence techniques**	**ID**	**Human Factors**	**ID**	**Situational Factors**
P1	Phishing (email)	**T1**	Spoofing	**I1**	Reciprocation	**H1**	Emotions	**S1**	Lockdown and stay-at-home orders
P2	Smishing (sms phishing)	**T2**	Static phishing kits	**I2**	Commitment and Consistency	**H2**	Fatigue	**S2**	Homeworking
P3	Vishing (voice phishing)	**T3**	Dynamic phishing kits	**I3**	Social proof	**H3**	Confusion	**S3**	Return to work
P4	Spear-phishing	**T4**	Mobile optimised content	**I4**	Liking	**H4**	Stress	**S4**	Remote teaching and home-schooling
P5	Whaling	**T5**	Typosquatting	**I5**	Authority	**H5**	Technostress	**S5**	Online shopping and home delivery
		T6	QR codes	**I6**	Scarcity	**H6**	Urgency	**S6**	Quarantine and illness
		T7	Use of AI			**H7**	Curiosity	**S7**	Financial loss
						H8	Fear	**S8**	Vulnerability and isolation

Table 7 - Table of phishing attack types, technical methods, influence techniques, human factors, and situational factors (author contribution and collated from IDs in Tables 2-6)

4.3 Tables of Omicron announcements and phishing evidence

4.3.1 Table of Omicron announcements

Table 8 shows evidence of Omicron-related announcements from November to December 2021. The **person (P)** – human factors and **environmental (E)** – situational factors are correlated in **columns 6 and 7** using the item classification from **Table 7**.

Table 8 of 11: Table of Omicron announcements						
ID	**Ref.**	**Article date**	**Event date**	**Description**	**Person (P) human factors**	**Environment (E) factors**
1	[134]	26/11/21	09/11/21	The first known confirmed Omicron infection.	H1, H3–4, H8	S6
2	[134]	26/11/21	24/11/21	The Omicron variant was first reported to the WHO from South Africa and announced.	H1, H3–4, H8	S6
3	[143]	30/11/21	30/11/21	UK Government urges the public to get the booster vaccination.	H1–4, H6, H8	S1, S6, S8
6	[95]	03/12/21	03/12/21	Reports of pandemic distress and Omicron-related anxiety appear.	H1–6, H8	S1, S5–8
9	[144]	08/12/21	08/12/21	The Prime minister confirms England will move to “Plan B” following the rapid spread of the Omicron variant in the UK. Work from home guidance starting on Monday 13th December 2021.	H1–6, H8	S1–2, S4–8
10	[145]	12/12/21	12/12/21	The UK Chief Medical Officers recommends increasing the UK COVID alert level from Level 3 to Level 4. Urgent recommendation for vaccination.	H1–6, H8	S1–2, S4–8
11	[146]	13/12/21	13/12/21	There is widespread reporting of lateral flow testing kits being unavailable.	H1–6, H8	S1–2, S4–8
17	[147]	18/12/21	18/12/21	The Mayor of London declares a “major incident” due to the spread of the Omicron variant within the capital.	H1–6, H8	S1–2, S4–8

Table 8 - Table of Omicron announcements (author contribution, source article references are listed in column 2)

The sampling of Omicron announcements was limited to eight items. The initial approach in **Table 8, column 6**, was to apply the classification of items from **Table 7** to each Omicron announcement. The secondary approach was to review each announcement scenario from the corresponding source article and determine the applied human factors. The final approach calculated each occurrence as a % total from the eight

announcement items. From the eight announcement items collected, the person (P) – human factors potentially impacted are as follows:

- Emotions (100%)
- Fatigue (75%)
- Confusion (100%)
- Stress (100%) and technostress (62.5%)
- Urgency (75%)
- Fear (100%)

Emotional responses, such as confusion, stress, and fear, are likely to have been experienced by individuals when the announcements in **Table 8** occurred. Fatigue responses are likely to have remained higher for those who felt the pandemic might have ended. Omicron-related announcements will have returned a sense of these feelings.

Using the previous calculation method and referring to **Table 8, column 7**, the environment (E) – situational factors which potentially impacted people during this period are as follows:

- Lockdown and stay-at-home orders (75%)
- Homeworking (50%)
- Remote teaching and home-schooling (50%)
- Online shopping and home delivery (62.5%)
- Quarantine and illness (100%)
- Financial loss (62.5%)
- Vulnerability and isolation (75%)

The threat of quarantine, illness and health-related concerns as the new COVID-19 variant was detected ranked highest in the analysis. As new announcements were released, other situational factors started to impact people:

1. The threat of new restrictions, such as recommendations to stay at home, led to vulnerable situations where people might have become isolated.
2. People were likely to have stopped going to shops and restaurants for fear of catching the new variant, increasing the need for online shopping and home deliveries.

3. The new guidance that recommended working from home will have included teaching and potentially home-schooling for children, creating several distractions for parents.

4.4.2 Table of Omicron phishing evidence

Table 9 shows Omicron-related phishing evidence in December 2021. Phishing attack types and technical methods are applied to highlight the attack methods in **column 6**. Social influence techniques are also applied to reference the **person (P)** factors in **column 7,** using the item classification from **Table 7**.

Table 9 of 11: Table of Omicron phishing evidence collected from source articles in December 2021

ID	Ref.	Article date	Event date	Description	Attack types, technical methods	Person (P) influence techniques
4	[148]	02/12/21	30/11/21	Fake NHS email circulating offering free Omicron PCR test. Official NHS logo used. The recipient then diverted to a form asking for full personal details, including their mother's maiden name— requesting delivery payment for £1.24, targeting financial information.	P1 T1, T2-3, T5	I1-3, I5-6
5	[148]	02/12/21	01/12/21	As ID 4, with variation: Second modified fake NHS email with NHS text header instead of a logo, using similar content but reordered, a "Get it now" button is used instead of a link URL.	P1 T1, T2-3, T5	I1-3, I5-6
7	[93]	07/12/21	03/12/21	An elderly resident received a scam phone call from someone claiming to be from the NHS. The person called was asked to update the COVID passport with full personal and banking details - £4.99 requested for the service.	P3 T1	I4-5
8	[149]	06/12/21	06/12/21	U.S. based article, referencing ID-4. Bitdefender report of ID-4 clone repurposed to appear from the Federal Department of Health and Human Services. Recipients urged to book a slot for the Omicron variant test. Fake U.S. phone number provided, asking for full personal and banking details.	P1 T1, T2-3, T5	I1-3, I5-6

12	[150]	13/12/21	13/12/21	Facebook marketplace advert offering fake forged PCR "Fit to Fly" certificates for £40 to circumvent Omicron travel restrictions.	N/A	I3, I6
13	[151]	13/12/21	13/12/21	Fake NHS COVID pass messages 'now eligible to apply for a COVID pass'. Recipients diverted to a form requesting full personal and financial details.	P2 T1, T4-5	I1-2, I5-6
14	[152]	20/12/21	14/12/21	Fake NHS text message, "now eligible for booster" with link URL. Recipients diverted to a form requesting full personal and financial details - delivery payment for £1.99.	P2 T1, T4-5	I1-2, I5-6
15	[152]	20/12/21	14/12/21	Fake NHS email with a reminder to enter financial details before booster vaccination appointment.	P1 T1, T2-3, T5	I1-2, I5
16	[153]	16/12/21	16/12/21	Reports of further fake NHS emails appear, with a similar content format as ID-4, ID-5, diverted to the form that asks for full personal and financial details.	P1 T1, T2-3, T5	I1-3, I5-6
18	[154]	23/12/21	22/12/21	Fake NHS email in conjunction with National Insurance scheme, offering tax refund of £850.34. The claim the offer, recipients diverted to a form requesting full personal and financial details.	P1 T1, T2-3, T5	I1-2, I5-6

Table 9 - Table of Omicron phishing evidence in December 2021 (author contribution, source article references are listed in column 2)

The sampling of phishing evidence was limited to ten items. The initial approach in **Table 9, column 6**, was to apply the classification of items from **Table 7** to each item of phishing evidence. The secondary approach reviewed each phishing scenario from the corresponding source article to determine the attack types and technical methods used. The final approach calculated each occurrence as a % total from the ten phishing evidence items. This data collection is not an indicator of the number of phishing attacks following the initial Omicron announcement. From the ten phishing evidence items collected, the attack methods divide into the following categories, with phishing and smishing attack methods dominating the sample:

- Phishing – email (60%)
- Smishing – text messages (20%)
- Vishing – voice attacks (10%)

- Social media – spam advertising (10%)

The most popular technical methods used were spoofing (90%), Typosquatting (80%) and the use of static/dynamic phishing kits (60%).

When referring to **Table 9, column 7**, the **person (P)** – influence techniques have been calculated as a % total from the ten phishing evidence items. Where multi-layer social influence techniques are utilised as a part of the social engineering strategy, the percentage frequency in the ten samples is as follows:

- Reciprocation (80%)
- Commitment and Consistency (80%)
- Social proof (40%)
- Liking (10%)
- Authority (90%)
- Scarcity (90%)

The entire sample of phishing evidence shows at least two social influence techniques used to target a victim, with 70% of the overall evidence showing four or more of the social influence techniques in use. It is not surprising to see high use of authority since much of the phishing evidence was impersonating the NHS. Scarcity factors seen in almost all evidence will trigger an urgent reaction in a target. Combined with reciprocation, an offer for something in return, these techniques were highly likely to have convinced the recipients into handing over personal and financial information.

4.4 Visual timeline

Using the Omicron announcement and phishing evidence data from **Tables 8 and 9**, I have created a visual timeline, **see Figure 13**, to bring together both sets of evidence and to help provide findings in **Section 4.4.2**.

4.4.1 Timeline diagram

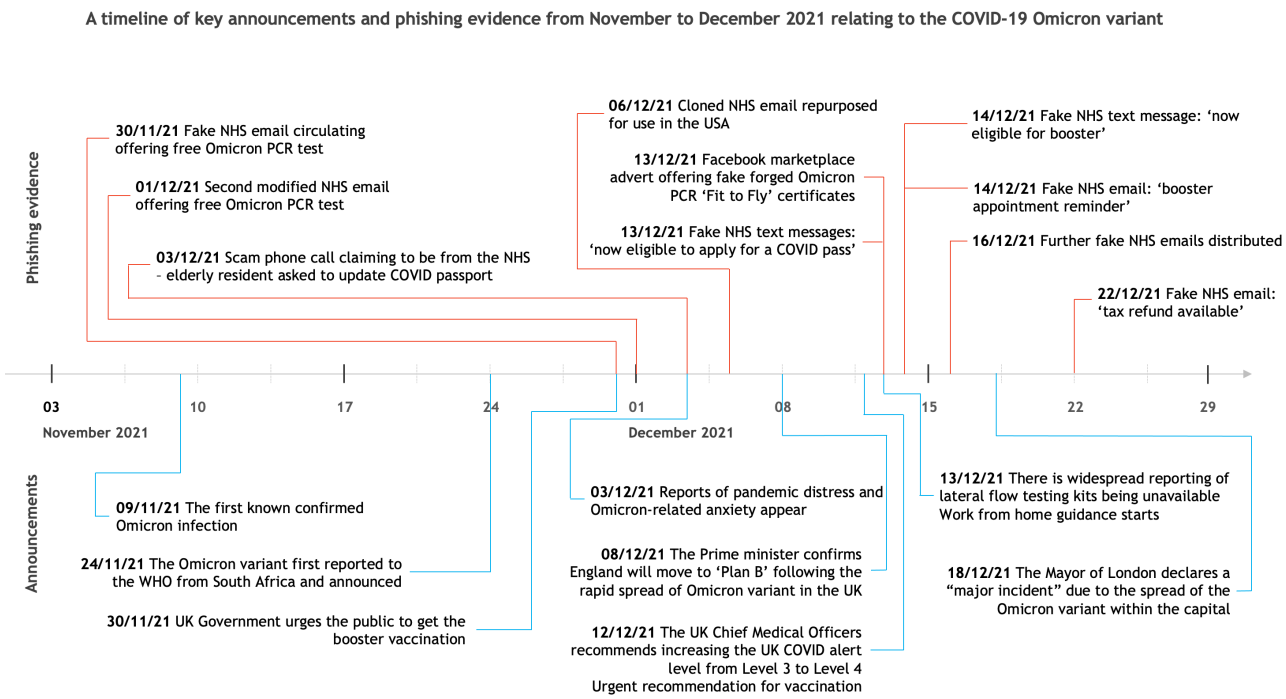


Figure 13 - A visual timeline of key announcements and phishing evidence from November to December 2021 relating to the COVID-19 Omicron variant (author contribution and visualised from data collected in Tables 8 and 9)

4.4.2 Timeline findings

The key findings from the events visualised in **Figure 13** are as follows:

The WHO Omicron announcement on the 24th November 2021 appears to be the main event that triggered a global awareness of the new Omicron variant. Six days later, on the 30th November 2021, the UK Government urged the public to go out and get the booster vaccination. Broader media-driven awareness of the situation likely caused human factors such as stress and panic. On this same day, fake NHS phishing evidence first appeared containing specific Omicron terminology sent to recipients.

I interpret the correlation between these two findings as either:

- **Scenario A** - targeted phishing content was sent on 30th November and prepared over six days between the 24th and 30th November 2021.
- **Scenario B** - alternatively, the UK Government announcement on the 30th sparked an immediate interest in those who were able to distribute Omicron phishing emails on the same day. This plausible

theory would show the rapid ability to pivot and distribute targeted COVID-19 variant-specific phishing campaigns.

There was a spelling mistake, “Omicorn” instead of “Omicron” in the first phishing evidence on the 30th November, implying that the phishing email was rushed and further aligns the suggestion that **Scenario B** occurred. This analysis would reinforce a view that fraudsters might be able to immediately craft Omicron-themed attacks on the day that announcements occur. Multiple other phishing variations appear within a week of the UK Government guidance.

On the 12th December, the COVID alert moved from Level 3 to Level 4. The next day, there was widespread reporting of a shortage in lateral flow COVID-19 testing kits. Immediately, three variations of Omicron phishing and smishing evidence appear by the next day. **These results imply that different message content is either quickly replicated, modified, or newly generated, indicating that multiple individuals or groups are working on this phishing content**. As further announcements and events appeared in December, including the announcement from the London mayor, increased awareness of the Omicron variant will have further caused disruption and increased phishing susceptibility.

4.5 Summary

Fraudsters quickly crafted theme-based phishing attacks in line with announcements due to shared awareness of psychological factors caused by the return of the COVID-19 Omicron variant in December 2021. For victims, these **recent Omicron-related announcements are likely to have triggered returning factors such as fear and anxiety**, resulting in similar experiences to the beginning of the pandemic. High transmissibility and immediate recommendations to stay at home due to uncertainty around the Omicron variant also meant that vulnerable people remained on their own and a target. Therefore, **increased susceptibility to targeted Omicron phishing attacks occurred during this analysis period**.

It is vital to question if this analysis is missing something. There was evidence of incorrect spelling of Omicron. Could it be that a phishing email with this mistake was quickly detected and subsequently published in news articles? **The existing phishing evidence might only be a fraction of the content sent during this period.** More sophisticated and devious phishing emails and messages may not have contained errors and therefore been less detectable. **Vishing threats are even harder to detect since there is less tangible evidence of these attacks, aside from victim reports. Chapter 5** further considers how much online fraud is going unreported or unnoticed, which is becoming a critical issue. **COVID-19 and Omicron-themed phishing attacks may continue**

to evade our attention and become more successful through sophistication, leading to a greater risk of personal and financial information loss.

Chapter 5 investigates the rise of scam culture and is core to the overall thesis that themed phishing forms the primary mechanism ahead of more advanced secondary-stage attacks. It is also likely that the concept for these theme-based phishing attacks appear on social media scam channels, where fraudsters gather. **The speed at which attacks happen might also indicate a "herd approach", where participants design new phishing approaches together in real-time.** In **Section 5.4.3**, there is evidence of gamification and a "herd approach" occurring through underground social media messaging channels, which correlates to the attack speeds which the visual timeline prepared in this chapter shows.

Chapter 5 – Cyber Scam Subculture

The core objective of this chapter is to provide a descriptive case study of the August 2021 BBC Panorama investigation: *Hunting the Social Media Fraudsters*. The aim is to explore a rise in fraudsters using social media platforms and messaging apps that influence and draw young people towards cybercrime and scam subculture. New contributing research in this chapter will explore how public discussion channels on the *Telegram* messaging app promote harmful scam content and aim to attract young people to help them launder money and digital assets online.

5.1 Background

The idea of "subcultures" forming within cybersecurity may have begun with studies on hacker subculture [64] [155]. Cyber scam subculture appears without negative context amongst Nigerian youths [156] to describe the on-trend phenomenon of internet-related scam activity. *Online fraud* is an umbrella term often related to online scam activity, identity theft, online shopping, and e-commerce website fraud [157]. Online fraud cases in the UK have increased [158] and surged during the pandemic [159]. Popular social media platforms and social messaging apps have become a valuable weapon for cybercriminals to promote online activities and services. Scam communities can quickly form within these online social spaces, which furthers the idea of cyber scam subculture.

Social media platforms, such as *Meta* (formally *Facebook*), *Instagram*, *YouTube*, *Snapchat* and *TikTok*, allow users to register and create content within the platforms. Although some basic information is required to sign up to these social media platforms, such as name, email address and telephone number, this information is not cross-verified with identity documents [160]. Harmful content can exist on these platforms and is difficult for content moderators to remove and manage, especially if other users do not report this content. *TikTok* is one of the newer social media platforms to emerge with popularity and has been facing scrutiny over its protection of younger users from witnessing harmful content [161].

Social messaging applications, such as *Telegram*, *Signal* and *WhatsApp*, have increased in popularity due to various privacy-enabling communication features, including end-to-end encryption mechanisms [162]. In an unclassified document from the United States FBI, **see Figure 14**, the ability for federal authorities to access the content and metadata varies dramatically across nine of the most popular social messaging applications [163]. *Telegram* appears to give authorities the least access to metadata compared to other popular social messaging applications, and cybercriminals will be aware of this.

In **Figure 14**, the following lawful access limitations are highlighted for *Telegram*:

- No message content.
- No contact information provided for law enforcement to pursue a court order.
- As per *Telegram's* privacy statement, for confirmed terrorist investigations, *Telegram* may disclose IP address and phone number to relevant authorities.
- Only "Registration Time Data" is available.

Telegram offers the highest levels of anonymity, requiring only the most basic registration and allows users to hide their telephone number and select a pseudo username [164]. Additionally, *Telegram* allows the creation of public and private broadcast channels, where stolen data is often shared and traded, with 1 million harmful channel links posted on the dark web in 2021 [165].

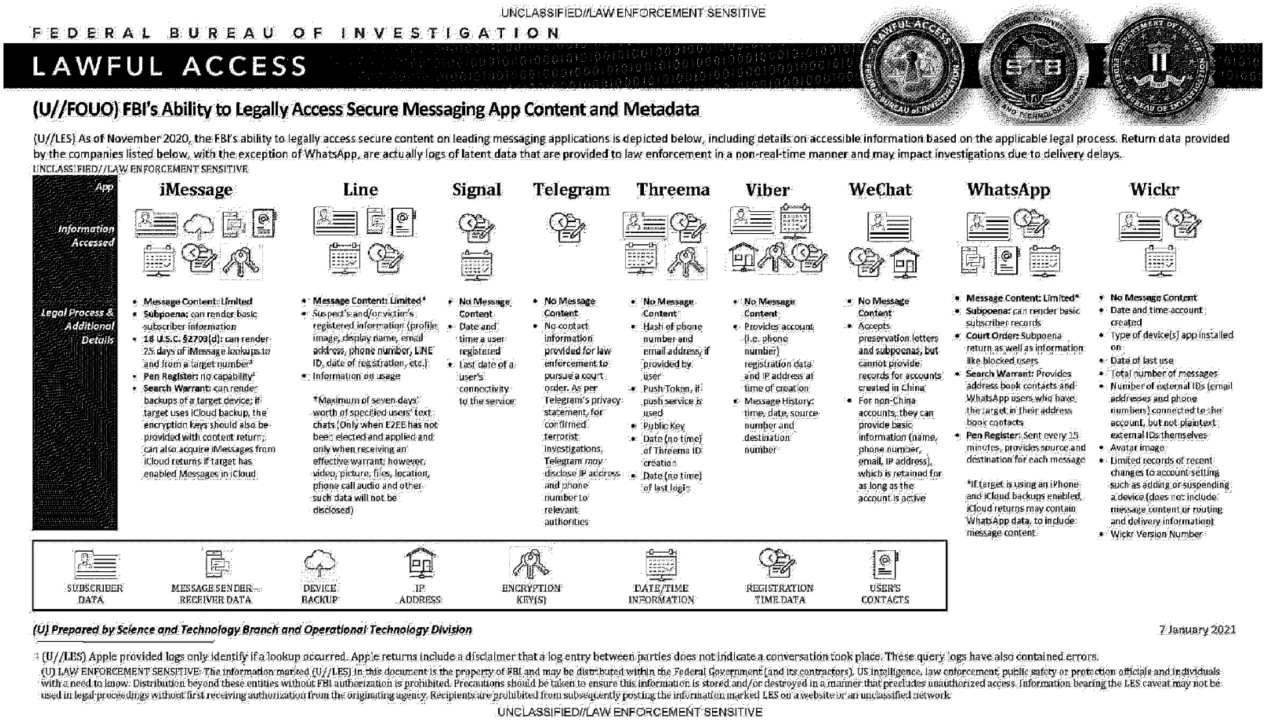


Figure 14 - Unclassified FBI document showing ability to access secure content and metadata for nine popular social messaging apps [163]

5.2 BBC Panorama investigation: Hunting the social media fraudsters

In August 2021, BBC Panorama released an investigative programme, "*Hunting the social media fraudsters*" [65], which exposes an underground world of online fraudsters using social media platforms to promote their online scamming activities. The investigation likened these fraudsters to *social media influencers* whereby new subscribers increase traffic to their content channels, generating advertising income. If reported, influencers quickly create new accounts and direct users towards these account aliases through their other platform

channels. Regular video blogs show a life of luxury, promoting cars, clothing and high-end items purchased. The content exposed appears to be exciting and engaging for young subscribers. School-age teenagers explain that online fraud does not appear as a serious crime because it is normal to see scamming appear on social media and simply as something that young people do online.

The investigation exposed that the social media fraudsters offer tiered packages that provide various guides known as *methods* that allow individuals to commit online fraud easily. The promotion and sale of these *methods* seem to be a highly lucrative model, requiring minimal outlay and advertised at scale through exposure to large social media audiences. It is essential to highlight that this process also helps remove the original cybercriminals from the actual online crimes themselves, allowing them to claim ignorance of the attack chain. These online crimes are non-physical and can occur from any location, with high anonymity. The investigation showed a blurred set of techniques for UK retailers which aim to expose weaknesses in a target system. As online websites try to close loopholes and vulnerabilities, the method documents will likely stay updated with new techniques.

A victim was interviewed as part of the investigation, explaining how a sophisticated phone call resulted in serious financial loss. A fraudster, claiming to be from the victim's bank, had convinced the victim to move all of their money to a new account for safety. Unfortunately, this was a socially engineered authorised push payment (APP) attack, and losses from this form of online fraud totalled £355m in the first half of 2021 [166]. Seemingly the fraudster already had a complete target profile of the victim to aid the attack, extracted through phishing. This scenario was confirmed later in the evidence when the victim explained that they had received a strange text message from Royal Mail about a missed parcel and had entered redelivery information only a day earlier.

Another victim interview explained a detailed social engineering scenario where an attacker extracted a sensitive one-time password code for a banking application. Spoofing software appears to be used to schedule an automated call that tricks a victim into revealing these time-sensitive authentication codes. One-time-password (OTP) spoofing software is highly professional and becoming more readily available online [167] [168]. OTP spoofing software has many hidden malicious features but masquerades primarily as a telephone forwarding service. If a victim inadvertently reveals their time-sensitive one-time password codes through these forms of attacks that use OTP spoofing software, fraudsters can proceed to take over a victim's online bank account.

The investigation shows that social media influencers draw young people to cybercrime, and these social channels act as a gateway. Social influencers also use music videos to promote UK cyber scam subculture, which is a powerful and attractive medium. The BBC Panorama investigation throughout refers to slang expressions but fails to draw a direct conclusion to specific cyber scam subculture developing in the UK. I believe that cyber scam subculture is already flourishing online in the UK and has accelerated due to the pandemic. Young people have easy access to social media with techniques, guides, and channels that can provide a bridge to attract individuals through the glamour of making money online and from the safety of home. Online scamming might also appear acceptable amongst their peer groups the more it appears on social media, and slang expressions could contribute to a shared identity within cyber scam subculture.

Throughout this work, the aim is to highlight that **primary information capture is used to perform a sophisticated secondary-stage attack on a target**. **Chapter 3** previously shows that phishing attacks allow fraudsters to build complete financial profiles through social engineering techniques. **People have been more susceptible to phishing during the pandemic, at the very time when online scam subculture has been rapidly growing in the UK**, as reinforced throughout the BBC Panorama investigation.

5.2.1 Slang expression and cyber scam subculture

There is evidence that new slang expressions and terminology replace the more traditionally-recognised terms, techniques and elements of online fraud [169]. In [156], Ajayi highlights that young Nigerian fraudsters prefer secret slang expressions by creating an anti-language to identify and solidify themselves in society. A crisis of identity can occur in young people as they adapt to adulthood [170], which means there could be an attractiveness towards cyber scam subculture by subscribing to and engaging in scam social media content. In **Section 5.4**, I provide new contributing research into social communication channels that demonstrate UK cyber scam subculture development through informal slang usage in discussions, as individuals use *Telegram* channels to promote online scamming techniques and services.

5.2.2 Table of cyber scam slang terminology

As a reference to guide the reader, in **Table 10**, I have chosen a simple approach to translate a selection of cyber scam subculture slang expressions from the BBC Panorama investigation [65] by providing a brief description and example of potential threats faced.

Table 10 of 11 – Table of cyber scam slang terminology		
Slang term	**Description**	**Threats**
Clicking	"Clicking" refers to the general activity of online scamming, phishing, and credit card fraud.	The term clicking appears to glamourise this activity and to liken the related cybercriminal activity to easy work that can earn someone money. The main threat is that creating a general slang term to describe the activity can attract young people seeking to associate themselves with a trending and popular activity.
Spoofing	"Spoofing" is similar to the email spoofing technique explained in **Section 3.2.2**. More broadly, the terminology refers to masquerading as someone else, for example, a person of authority. Spoofing can also refer to the software technique when manipulating a telephone caller ID to appear as a different or hidden number.	When receiving a message or phone call from an unknown or hidden number, a recipient may be curious to answer their telephone to see who is calling. Advanced attacks can utilise spoofing techniques by masquerading as a legitimate entity. Fraudsters can use software to extract information from a target in an automated call scenario. Alternatively, in a direct call scenario, fraudsters use social engineering techniques to convince a target that they are speaking with a legitimate source, and this is where a more sophisticated attack can occur. When a person believes they are interacting with someone legitimate, they may reveal sensitive information or inadvertently agree to transfer money to the fraudster.
Methods	"Methods" refers to guide documents or scripts which explain step-by-step how to run online scams. These methods include social engineering techniques to give the attacker a psychological edge or provide examples of influence techniques best suited for a given scenario. Methods are sold at various price tiers or as subscriptions and can include targeted approaches for specific banks, online retailers, and platforms.	Fraudsters aim to utilise these documents or scripts for specific approaches, such as reverse-payment fraud techniques for the "Apple Pay" protocol. Purchasers and subscribers can select which type of scenario they want to target and follow instructions to commit the fraudulent activity. Multiple entities may be selling these same methods or variations of the same. Therefore, these instructions and techniques might become accessible to many different individuals, creating a significant risk.
Fullz	"Fullz" refers to collecting a target victim's complete financial and social profile, which can be used or shared online.	The sharing of a victim's complete financial and personal details online, potentially retrieved from a phishing attack, may then be used as part of more sophisticated secondary attacks on a victim. This information is often immediately

		shared online because it is newly retrieved, allowing others to utilise it before a victim knows their information has been made available.
Dumps	"Dumps" refers to sharing either a single or more extensive list of financial information from debit/credit cards, including whole account numbers, expiry dates, and 3- or 4-digit card verification value (CVV) numbers.	Dumps of financial data can be written either singularly or in bulk to fake debit/credit cards. Combining dumped financial data with the social profiling of a target can lead fraudsters to have a complete profile of a target victim to be used in various fraudulent activities.
Drops	"Drops" or drop addresses refer to the address fraudsters send goods to, for example, clothing or electronic items, as part of payment reversal fraud. Fraudsters use drop addresses to prevent their address or location from leaking. Fraudsters actively look to sign up individuals who might be willing to provide their address details for a small percentage fee or some of the delivered goods.	Accomplices are being motivated to help fraudsters circumvent address controls and the tracing efforts of authorities. The risk is that fraudsters find ways to remove themselves from the transaction chain and create a situation where more individuals become involved.
BINs	"BINs" or Bank Identification Numbers refer to the first six digits on a debit/credit card, used to identify the banking institution that the cardholder belongs to.	Fraudsters use the BIN numbers with software to generate the remaining number on a debit/credit card. Usually, they will test the card details to see if the BIN generation is successful by making small transactions before committing more serious card fraud.
Crypto	Cryptocurrencies are digital assets and tokens, such as Bitcoin and Ethereum. Online cryptocurrency exchange platforms allow instant trading of cryptocurrencies with Government-issued currencies. Fraudsters actively seek individuals with existing verified cryptocurrency exchange accounts. For a small percentage fee, often in cryptocurrency, fraudsters will look to launder money or steal cryptocurrency by exchanging and then withdrawing to various subaccounts or a bank account.	Similar to drops, there is an increasing threat that individuals are being drawn to cybercrime by agreeing to offer up their cryptocurrency exchange accounts to be used as part of money laundering activity for a fraudster. While this may appear as an easy way for someone to make money online, it creates a complex situation for authorities who need to trace the movement of stolen cryptocurrency or money through these exchanges. Some cryptocurrency exchanges might be domiciled outside of authorities' jurisdiction, making this process even more challenging. Another threat is the use of cryptocurrency "mixers", such as *Tornado Cash*, which as a decentralised service, aims to obfuscate the digital asset transaction history by breaking the on-chain

		relationship of the asset address under the guise of improving user privacy [171]. **Section 5.4** discusses cryptocurrency exchange accounts used by accomplices or '*digital mules*', showing how individuals are easily motivated to commit cybercrime.
Logs	Logs refer to the banking or cryptocurrency exchange login details shared online by fraudsters.	A common method for extracting account login details is via phishing attack techniques, which I explored in **Chapter 3**. Once these login details are collected, a fraudster will attempt to access a target's bank or cryptocurrency exchange account, where money and digital assets might be stored. In this scenario, the attacker may still need a multi-factor authentication code to log in to a banking or cryptocurrency exchange platform. A secondary stage attack might require more advanced one-time password (OTP) software to trick users into revealing these self-generated authentication codes. Once retrieved, the fraudster will quickly use the OTP code before it expires to log in and pass the multi-factor authentication checks. Fraudsters can then bypass other security controls and take over an account.

Table 10 - Table of cyber scam slang terminology

Table 10 shows how a wide selection of new slang expressions emerge as anti-language further develops in UK cyber scam subculture.

5.3 Key issues and recommendations

I have selected three key issues to explore from the BBC Panorama Investigation and will provide recommendations on the following:

1. Scam subculture is being glamourised to young people, drawing them towards cybercrime.
2. Social media companies are not doing enough to slow an unprecedented rise in fake accounts.
3. Victims of fraud might be forgotten as online scamming becomes normalised.

5.3.1 Scam subculture is being glamourised to young people, drawing them towards cybercrime

Not only is scam subculture being glamourised through social media and influence, but it appears to be becoming socially acceptable to those who follow these channels. Committing fraud online and sharing stolen personal information seems to be normalised amongst younger individuals, and they appear less phased by

the harm that it causes. There is an expectation that victims will get fully reimbursed by their banks. However, victims do not always receive a full refund in these scenarios [172]. Often only a partial amount is returned to the victim at most. Fraudsters who share stolen information are being gratified throughout these social channels by other users in the comment sections and across the channels themselves, earning a reputation, which is leading to a thriving subculture and accelerating a rise in scam activity.

Recent investigations have likened the urgent situation to the "new country lines" [60], comparing online scamming to physical and organised crimes across UK counties relating to drugs and other criminal offences [173]. During the pandemic, travel has been much more complicated, and young people have been at home with access to the internet and perhaps fewer means to earn an income from more traditional working roles. Scamming and committing fraud online are likely to grow because of these situational factors, and it might also be a desirable occupation, especially for young technical people. This form of online robbery can generate large amounts of easy income and be faster and much less detectable than physical crimes. If the police cannot keep up with these modern and digital crimes [174], then a new trend surrounding scam subculture and scam activity will further draw young people into the world of cybercrime.

Recommendations

- The criminal justice system will need to impose harsher sentences to highlight the damage and harm to victims caused by online fraud and cybercrime.
- The related authorities will need to improve online awareness and continue education campaigns, such as the National Crime Agency (NCA) Cyber Choices programme [175], to help target young people to warn about the risks of becoming involved with online scams and cybercrime.
- The police will need to quickly adapt and modernise, both technically and culturally, to understand the situation thoroughly enough to intervene.
- The related authorities, tech and social media companies will need a joined-up approach to tackling online fraud since silo efforts might be less effective.

5.3.2 Social media companies are not doing enough to slow an unprecedented rise in fake accounts.

Social media companies desire users and advertising revenue generated from these users. Therefore, they have removed barriers to user registration. In the third quarter of 2021, fake accounts detected on the *Meta* platform rose from 1.7 to 1.8 billion accounts [176]. High detection rates appear only as a success story. The challenge remains that 1.8 billion fake accounts could enter the social landscape for this platform. Critically, there is limited information on the number of users prevented from signing up to social media platforms.

Systems of reporting are present in all social media platforms, but these do not prevent malicious users from regenerating new account aliases online once a previous account has been closed. Due to the vast amounts of content posted daily, moderation can be slow and relies on users reporting harmful content and fake user accounts. These are reactive measures and not proactive measures. Fake accounts allow users to remain anonymous online, often hiding behind pseudo names. Fraudsters can also quickly communicate their newly generated aliases across their social audience, allowing uninterrupted promotion of their harmful content. The BBC Panorama episode reported that social media companies and the related authorities are playing a "cat and mouse" game and are currently losing the battle [65]. The investigation also critically mentioned that victims' personal information shared online had remained online for a month before eventually being removed. If other users are not shocked by the scam content posted or cannot identify a fake or harmful account themselves, it is unlikely that timely reports will be made for content moderators to take action.

On the 18th of January 2022, the DCMS Parliamentary sub-committee met to discuss *online harms and disinformation* with social media company representatives [177]. The response from *Meta* was surprisingly defiant, citing steps the company had recently made to improve. Other representatives acknowledged but were vague in their responses to the various criticisms from the sub-committee. Countries within the EU fined large tech companies over 1 billion euros in 2021 for failing to comply with GDPR requirements [178]. However, the current penalty measures might be ineffective, considering the social media companies generate huge revenues. A dangerous situation may have developed, which has allowed tech giants to act as they please first and then pay later through fines. Much more needs to be done to hold these companies accountable and ensure that improved reporting mechanisms are in place.

Recommendations

- The Parliamentary sub-committee and related authorities will need a continued effort to ensure regulatory pressure is applied to social media companies, with harsher measures and controls to prevent further abuse:
    - Increase pressure on social media companies by threatening to restrict platform geo-availability unless there are clear safeguards to protect their users.
    - Demand more rigorous measures to prevent new fake accounts from spawning when a previous account is eventually deactivated.
- The related authorities will need to incentivise the reporting and reduction of fake accounts and harmful content.

- Social media companies will need to adopt ID verification to help improve the traceability of cybercriminals. Alternatively, a softer shift towards an ID verified user content model might drive user awareness towards verified content and away from content that is not.

5.3.3 Victims of fraud might be forgotten as online scamming becomes normalised

Victims of fraud in the UK lost more than £850m between 2019-2021 in bank transfer scams, and only 42% of losses appear to be reimbursed [179]. People are likely to think online fraud will never happen to them through overconfidence bias. The concern must be on the financial and mental well-being of victims of fraud. Further, understanding how much online fraud goes unreported for those who do not report a crime. Individuals might blame themselves, be too embarrassed to report the crime, or not know how to report a concern. If a victim reaches their bank, long cases and investigations can occur. In the case of APP fraud, where a fraudster convinces the victim to initiate the payment, sometimes the banks will not be able to reverse payments. Banks often deny responsibility [172] and have started to show warning messages, which shift responsibility to the victim. In 2019, TSB bank launched its "Fraud Refund Guarantee" [180], aimed at protecting innocent customers that have been tricked by a scam, offering a refund of the money lost on the account. Despite this, there are still reports of customers fighting for multiple years to receive compensation [181]. Identity fraud can also cause significant harm to an individual's credit rating, preventing victims from accessing new credit and taking years to resolve.

As a final point, we cannot look at crime data from the police as an indicator since this will only cover reported figures. The September 2021 ONS report [182] showed a 47% increase in *fraud and computer misuse*. This data is invaluable since it includes crime survey data for England and Wales, which gives a much denser indication of victim numbers and highlights how much goes unreported. The consumer group Which? offer several scam protection services [183], including victim support. Importantly, regular surveys and analysis of UK financial data can give a more realistic indication than crime data alone.

Recommendations

- Government officials need to carefully inspect the September 2021 figures from the ONS and include *fraud and computer misuse* crime data in all discussions in Parliament, with the public, and not exclude this critical data or indicate that online crimes in the UK are falling if they are rising [184].
- The UK public needs to be made aware of the threats that online fraud, phishing, and other cybercrimes can have on them, so they can be on high alert. Advertising campaigns and other forms of education and awareness should be well-funded by the Government and related authorities.

- Banking institutions should attempt to align in working groups and share policies. Initiatives, such as the Contingent Reimbursement Model code [185], should be carefully followed to ensure victims get the compensation needed and without blame.
- Banking institutions should continue to look at two-factor payment verification mechanisms, configurable payment limits, or prompts to contact the bank directly to confirm large payments to break the potential attack chain.
- Regulators should continue to apply pressure to phone networks to improve phishing detection and SMS filtering techniques, building upon efforts in 2021 when Ofcom pressured major phone networks to implement technical strategies to reduce scam phone calls in the UK [186].

5.4 Investigation into public social messaging channels that promote scam services

This section aims to contribute new research and investigate how easy it is to find online public channels that can promote online scam services.

I have chosen the *Telegram* messaging application for this investigation since anonymous users can easily set up an account and promote harmful content using public communication channels. *Telegram* has been criticised for not providing effective content moderation [165]. Only limited research is available in this area with specific reference to *Telegram*. What is available refers to clone and fake channels [187], advertising of cryptocurrencies [188] and distribution channels linking more recent cryptocurrency scams with COVID-19 [189]. This investigation will cover the promotion of scam services, sharing personal and financial information and the availability of software that can form sophisticated attacks on a target.

In **Section 5.4.1**, I provide a straightforward methodology to collate publicly available evidence of online scamming services to demonstrate the extent of serious scam-related content shared through the *Telegram* messaging application. In **Section 5.4.2**, the data prepared in table form also includes the number of active subscribers for each sample channel. The research was carried out in January 2022.

5.4.1 Methodology

The approach is as follows:

- Once registered, load *Telegram* to reveal the internal search bar to find public channels.
- Enter the following English search terms: “spoofing”, “scamming”, “clicking”.
- Select five sample public channels from the search list which appear highest on the search results page.

- Access channel data in read-only mode since all data is publicly available in this mode.
- Scroll through the channel messages, collate evidence of message posts and services offered, and then provide details in short bullet form in **Table 11**.
- Collect the number of active subscribers in each sample channel and provide this in **Table 11** in the t-shirt size format **small (S)**, **medium (M)** and **large (L)** using a baseline from the smallest sample channel.
- Evaluate and correlate the findings per channel in a summary section.

Further to the data collection methodology above, a simple method was to scroll through previous messages to identify channel creation dates.

The investigation did not require joining any of the public *Telegram* channels, as this was out of scope and did not prevent data collection. To prevent PII data from being included, I have decided to de-identify the channel names of the source *Telegram* channels, opting to provide a simple numerical reference, as the name is irrelevant to the data analysis. Active subscribers from each channel will be double anonymised using either small (S), medium (M) or large (L) as a format to de-identify the user information within the *Telegram* channels. No other reference to channel subscriber usernames or identifiable detail applies as evidence in the data collection or presentation in **Table 11**. The temporary data collection was used entirely for the analysis in **Sections 5.4.2 – 3** and was immediately destroyed. These steps were taken for ethical considerations and compliance with the Royal Holloway, University of London, research ethics risk checklist.

5.4.2 Table of Telegram channels offering online scam services

The following **Table 11** provides evidence of data collected in January 2021 from five sample *Telegram* channels using the methodology defined in **Section 5.4.1**.

Table 11 of 11 – Table of Telegram channels offering online scam services

Channel ref	Services offered	Channel size (S/M/L)
1	Dedicated announcement channel to promote a spoofing software provider: • Broadcast announcements provide detailed explanations of software use, such as automated features, PIN extraction and global telephone number anonymising techniques. • Various methods and user bypass techniques explain how the software can target victims by tricking them into revealing one-time password codes.	L

	• Social engineering methods aim to convince recipients of a phone call from their banking institution. • Software updates advertise new features added.	
2	Discussion channel offering the following messages and services: • Laundering services, with 45% of the money paid back as an incentive. • Primary targets appear to be European banks. • Requesting individuals with high credit scores who can open bank accounts immediately. • Offering gift cards at half price rates and COVID-19 vaccination passports for sale.	M
3	Discussion channel offering the following messages and services: • Primarily laundering focused and looking for trusted large cashers, individuals with high credit scores and a preference for those using challenger banks (Monzo, Revolut). • Requesting users with active cryptocurrency exchange accounts. • Offering Apple and Android reverse payment methods.	S
4	Discussion channel with a team of 5+ admins, offering the following messages and services: • Offering full active BINs for £25, two for £40, partial BINs posted • Full personal details and bank login details are offered for purchase through direct message. • Direct links to private channels are available on request. • Targeting USA, Canada, UK Bank logins.	L
5	Discussion channel offering the following messages and services: • Requesting drop addresses from users. • Regular posting of full financial profiles to the channel. • Posting images of success stories and luxury goods purchased. • UK & Foreign BINs are available for £25 each. • Requesting active cryptocurrency exchange and TransferWise accounts, with verified ID and deposit history. • Offering methods/lessons on how to target victims for £500.	S

Table 11 - Table of Telegram channels offering online scam services

5.4.3 Table findings

The investigation findings from **Table 11** are as follows:

Channel 1 offers services as a broadcast channel to promote spoofing and one-time password bypassing software. No further communication from subscribers existed in this channel, so I interpret the use of this

channel primarily to announce software updates and new features, which alert the subscribers to changes in the software they have acquired. However, the high active subscriber count shows a likelihood that large numbers of users might have access to the spoofing software and be using this to target victims in sophisticated telephone scams, using social engineering and vishing techniques to trick a target into parting with information and money. Of specific concern is the advanced software features promoted, which aim to automate phone calls to trick recipients into handing over valuable authentication codes that allow fraudsters to access target online bank accounts and other online platforms.

Channel 2 contained many requests for users with high credit scores who could immediately open bank accounts in Europe to move money for a set fee. This *Telegram* discussion channel openly promoted COVID-19 passes to users, similarly noted in **Chapter 4**, where fake Omicron "Fit to Fly" passports are often sold on the Facebook marketplace [150]. The option to buy half-price gift cards was also a significant part of the overall discussion, attracting attention from other users. Externally, many websites allow the purchase of popular gift cards through cryptocurrencies [190]. Therefore, it is highly likely that fraudsters are using laundered or stolen cryptocurrencies to purchase gift cards and then sell these on through the *Telegram* channel. Fraudsters also appear highly motivated to find candidates, or as I interpret as *digital mules*, to help launder money by offering attractive returns.

Channel 3 was a smaller discussion channel, with high-frequency communication and interaction between participants. The primary focus of this discussion channel appeared to be money laundering and the movement of money and cryptocurrencies. Specific conversational evidence showed techniques specific to cryptocurrency exchange platforms and how to utilise privacy-enhanced cryptocurrency through withdrawal and deposit mechanisms. Popular centralised cryptocurrency exchanges, such as *Binance*, have know-your-customer (KYC) requirements [191], which may prevent certain fraudsters from using themselves. However, I interpret the purpose of the discussion channel as a means for enticing *digital mules* for a reasonable fee, and those with fully verified accounts within these cryptocurrency exchanges are highly desirable. These *digital mules* are then rewarded if they can help move money and digital assets through their accounts in small amounts to avoid detection.

Channel 4 had the most significant active subscriber base among the sampled discussion channels. A dedicated team of administrators are also available through the direct-message functionality. This channel seemed to focus on debit/credit card fraud, with card BINs and online bank logins for the USA, Canada, and UK available for sale. Full information dumps were shared, presumably extracted from phishing attacks, and used as secondary-stage and identity-based attacks relating to card fraud. Of specific interest in this channel

was the regular posting from administrators, asking channel subscribers to direct message to gain access to private *Telegram* channel links. Private channel links were out of scope for this investigation, and more extensive communication will likely occur there, which is a concern.

Channel 5 showed harmful content relating to full personal and financial details shared in real-time, similar to **Channel 3**. Messages indicate that the details have been newly extracted through phishing attacks and are available for more immediate and targeted attacks. The dumps, shared in batches of 5-10, contained UK residents and individuals of adult age, notably elderly individuals. Success stories from criminal activity appear on this discussion channel. **Channel 5** had one of the smallest active subscribers range from the sample. However, the communication was frequent, which gives the impression that the channel utilisation is for real-time attack scenarios. Immediate requests for users with available drop addresses and active cryptocurrency exchange accounts are commonplace. Fraudsters communicate step-by-step instructions on how to help launder and move money through these exchanges, including techniques to avoid detection when withdrawing from these exchanges to a bank account.

As an overall point of interest, **Channels 2-5** demonstrate much of the slang expression and anti-language discussed previously in **Section 5.2.2** and **Table 10,** which shows that the cyber scam subculture exists in these discussion channels. Pre-requisite targeted phishing attacks on individuals may have formed hidden stages before discussing and sharing content within the channels. Throughout the exchanges between users in the channels, there appears little thought to the victims of the stolen information. There was high confidence and often a perception that the participants were untraceable and acting in high anonymity. Much of the channel conversations showed excitement. **The activity is gamified** in a way in which channel participants can engage immediately to make themselves money. **As an important observation, users of these channels act together as a herd, the moment new target profile information is shared.** Channel subscribers *tag* and alert each other to highlight active victim profiles in an organised manner. **This evidence also confirms a "chained attack", using the active dump information to go on and then perform secondary stage targeted attacks on a victim using sophisticated online fraud techniques.**

Critically, this investigation reveals that each of the channels sampled has been active for at least one month and show regular communications throughout 2021, without interruption. Within these channels, participants appear to interact as if they are free to do as they please with the stolen personal and financial information, without fear of authorities or a need to present any communication in secret. **The *Telegram* channels also appear to act like organised crime units, where a particular administration hierarchy exists, and the top-level participants remain in control and ultimately remove**

themselves from the immediate activity. I liken the channel participants to ***digital mules***, in which users appear to be **collaborators in organised online crime**. There does not appear to be any evidence that this collaboration exploits participants, but this might occur in private communication. Cybercriminals at the top of the *Telegram* channel chain act as organised administrators, recruiting users through social media influence to help them launder money, crypto assets, or luxury items in return for a percentage fee. The *Telegram* channel evidence shows success stories and the influential suggestion that online scamming can make a participant easy money.

5.5 Summary

The evidence in **Section 5.4** raises serious questions about the potential harm inflicted by the malicious activity going unreported on social channels. Increased **exposure to social media influence, channels, and cyber scam subculture can draw young people towards scamming and cybercrime**. Scam influencers primarily aim to build followers and promote their interests. The secrecy and excitement of scamming, aided by new slang expressions and anti-language, could lead to a shared sense of belonging to groups promoted by these influencers. As highlighted in **Section 5.3**, **Government and police authorities have struggled to contain social media online fraud growth and must modernise**. Without the social media companies' support, the situation will continue to worsen. Several Governments have attempted to block the *Telegram* messaging app [192]. New open-source secure messaging applications will surface to replace these, and cybercriminals will shift toward the most anonymous channels. I believe awareness and education is key to helping slow the spread of these channels, with relentless pressure applied towards social media companies to ensure they restrict access to scam-related content.

It is important to cross-reference previous chapters as part of this summary discussion. In **Chapter 3**, situational factors caused by the COVID-19 pandemic could also have increased subscribers to these social channels. If individuals lost access to their source of income due to the pandemic or have been unable to return to traditional workplace roles, they may be attracted to making easy money online. In **Chapter 4**, I demonstrated the speed and mobility of fraudsters when the Omicron variant surfaced. The evidence collected in **Section 5.4.3** was carried out shortly after this period, in early January 2022. **Active target profile dumps may have been extracted from Omicron-related phishing campaigns during this period**. The evidence in **Section 5.4.3** further demonstrates that **chained attack techniques are in use** and is of significant concern. **Due to Omicron-related situational factors, higher phishing susceptibility may directly increase attack success rates, causing personal and financial harm**.

A final observation from the previous **Chapter 4** is that the Omicron phishing evidence showed that UK NHS phishing emails were modified for use in the USA, indicating the global nature of activity across these social channels. With the pandemic being a global event, fraudsters are likely working together across borders for any source of income. Phishing and scamming ideas might have been stolen and contextualised for maximum geographical impact. The *Telegram* channel investigation in **Section 5.4** also demonstrated communication cross-over and services offered across multiple regions, including North America and Europe, highlighting the broader threat scale. The pandemic has shifted more people online and reduced movement significantly. **The online world of scamming, enhanced by pandemic events, seemingly has no physical barriers compared to traditional or physical crimes.**

6. Conclusions

This concluding chapter is a final opportunity to bring together all of the themes from **Chapters 3 - 5**. **Section 6.1** provides a detailed review of the project objectives to establish how these have been achieved. **Section 6.2** then provides a list of the author's thoughts, whilst **Section 6.3** highlights some of the limitations in this work. **Section 6.4** provides five additional recommendations to guide the reader in awareness of how to protect against online phishing scams. Finally, **Section 6.5** provides an opportunity to discuss future work and technical contributions.

6.1 Summary and objectives

Investigating whether phishing susceptibility increased during the pandemic is an important cause. Using the recent events of the Omicron variant to produce a visual timeline has shown how quickly attackers can modify phishing campaigns. Linking criminological theories with pandemic-related situational factors also significantly contributes to the discussion within this modern crisis environment. **However, these perspectives alone may create limited outcomes**. Therefore, it is essential to understand how the pandemic accelerated a rise in online cybercrime, how individuals are drawn to cybercrime, and **whether phishing attacks are just the first stage before more sophisticated attack techniques occur**.

A rise in cyber scam subculture, including the use of social media influence and channels to coordinate and gamify fraudulent activity, shows the depth of secondary stage attack sophistication. Ultimately these avenues lead to serious personal and financial harm for a target victim. Many victims may suggest that they were unsure how it could even happen to them. Understanding the true scale of attacks that go unreported and how challenging this is for various authorities to monitor and prevent is a question that will remain with me. The crisis environment surrounding the pandemic extended for two years, and the next unknown crisis will surely follow. Without the full support of social media companies and authorities to better moderate and protect, cybercriminals will continue without fear, restriction, or prosecution.

6.1.1 Objectives

The first objective was to **demonstrate how pandemic factors impact human behaviours and increase phishing susceptibility**. I used **Chapter 3** to explore how attackers target people during a crisis. I chose to use Lewin's heuristic formula **B = *f* (P, E)** [87] to explain what defines human behaviour, where human **behaviour (B)** is a **function (*f*)** of the relationship between the **person (P)** and the **environment (E)**. This formula was helpful since it provided structure for the chapter in the following way:

- Firstly, **Section 3.2** introduced phishing attack types and technical methods to provide a full background into the pandemic phishing attack landscape.
- Secondly, **Section 3.3-4** explored the **person (P) factors**, using Cialdini's "six principles of influence" [107] and a selection of human factors to demonstrate how **attackers target people disrupted by the pandemic, using social engineering techniques to increase phishing susceptibility**.
- Finally, **Section 3.5** explored the **environmental (E) factors**, demonstrating how **certain situations during the pandemic increased phishing susceptibility**.

In **Chapter 3**, I asserted that **fraudsters, through shared experiences, might become psychological experts and used the pandemic disruption to their advantage**. I also used a basic ID system to classify each topic item to help correlate these to COVID-19 events captured in **Chapter 4**.

The second objective was to **produce a visual timeline of pandemic phishing events, using the emergence of the Omicron variant to evidence how quickly attackers modified phishing campaigns to target victims**. I used **Chapter 4** to define a methodology for researching Omicron announcements and phishing evidence. I mapped the topic item IDs from **Chapter 3** to provide a high-level analysis of the frequency in which **person (P)** and **environmental (E) factors** occurred. This analysis revealed a **significant overall impact across all selected factors**, as each new Omicron announcement was released, climaxing at the end of the data collection period in December 2021. The evidence in **Chapter 4** further reinforced the assertion in **Chapter 3** that **fraudsters used psychological sophistication and the pandemic disruption to their advantage.**

The analysis of the findings from the visual timeline in **Section 4.4.2** shows that **attackers quickly mobilised to construct new phishing threats as COVID-19 Omicron announcements were communicated**. However, the phishing evidence collected will only present a fraction of the content sent during this period. **More sophisticated and devious phishing emails and messages would have been less detectable and not appeared in the research, which raises questions about how much phishing content is going unreported**. Findings in **Chapter 4** also raise important questions about how attackers might be grouping together in a herd to target victims and use **chained attack** techniques. In **Chapter 5**, I demonstrated evidence of **chained attacks** forming through public social media channels closely following the research period.

The third objective was to use a case study to examine the recent BBC Panorama investigation: *Hunting the Social Media Fraudsters* and highlight key issues and recommendations. **The case study in Chapter 5 demonstrates that social media influenced cybercrime exists in the UK, with multiple examples of how independent actors are drawn to cybercrime**.

In **Section 5.3**, I outlined three areas from the case study for discussion and provided my recommendations:

- Online scamming appears to be an attractive way to earn easy money online. I highlight challenges with the emerging cyber scam culture and how authorities must modernise and adapt. The police may have abundant experience handling traditional crimes but will need to invest heavily in technical and cultural strategies to combat online crime culture amongst young people. **It is no longer physical crimes that are carried out across UK county lines. It is crimes that are carried out online and from the safety of the home**.
- Social media companies are hungry for new users, therefore have removed registration barriers and do not appear to be acting proactively. I argue that social media companies must do much more to prevent fake accounts and harmful scam content from appearing on their websites and communication applications. Poor content moderation and weaknesses in reporting tools allow new fraudulent accounts to be created, and loyal subscribers soon pivot. **Harsher regulatory measures and controls must be applied to social media companies to prevent social media fraudsters from causing harm**.
- Victims of fraud appear to go unnoticed, and banks are shifting responsibility onto these victims. The case study in **Chapter 5** highlighted how online scamming appears normalised amongst young people. There are assumptions made by those that commit the crimes that banks will refund victims of fraud. However, this is often not the case. Authorities need to carefully inspect fraud survey data to ensure they are not miscalculating official crime figures, which may only show a fraction of reported cases. **To fully understand the true scale of the problem, accurate victim numbers must first be identified, with rapid measures implemented to reduce further harm**.

It was also necessary within the **third objective** to dive deeper into **three sub-objectives**:

a) Identify whether there are plausible links between social media influenced cybercrime and a rise in independent actors using pandemic factors to their advantage.

Section 5.4 provides evidence of *Telegram* channel users interacting, sharing harmful content, scam techniques and dumps of complete personal and financial information profiles. **Figures 8 – 10, 12** show genuine phishing examples of how attackers use pandemic factors to their advantage. Whilst it is difficult to identify precisely whether specific pandemic factors were taken advantage of in these social channels, there was evidence of COVID-19 passes being advertised. The *Telegram* investigation in **Section 5.4** was carried out

in January 2022, shortly after the worldwide emergence of the Omicron variant. Therefore, **there is a high likelihood that sensitive information was captured from pandemic-themed phishing campaigns and shared through social media during this time**. Omicron phishing evidence captured in **Chapter 4** helps demonstrate a theory that fraudsters will have used pandemic factors to their advantage to extract sensitive information from victims and then further utilise social media channels to share these target profiles with others.

b) Provide new research to uncover specialist social messaging channels used to promote online scam activity and demonstrate how easy it is for young people to be drawn to cybercrime.

In **Section 5.4**, I investigated the *Telegram* social messaging app, analysing messages within public channels to reveal scam services and communication. By sampling five individual Telegram channels, I demonstrate evidence of sophisticated online fraud techniques used to deceive victims. The data collection methodology identifies how easy it is to locate these harmful public channels. The evidence from **Section 5.4** also validated claims from the BBC Panorama Investigation that slang expressions are in use. In **Sections 5.2.1 – 2**, I provide a detailed reference for the reader to explain how **UK cyber scam culture emerges using slang and anti-language** that can be an attractive way to communicate and bind identity, **drawing young people to cybercrime**.

c) **Identify evidence of chained attack techniques.**

In **Section 5.4.3**, a specific analysis from *Telegram* **Channel 5** shows that users on these channels are working together to share active dumped personal and financial information profiles. **I uncovered real-time communications discussing chained attack techniques.** Messages exchanged imply that active information profiles are ready for immediate secondary stage targeting. This evidence confirms that **primary phishing attacks first capture active victim profiles. The next stage in the chain is to perform secondary stage attacks, such as spoofed phone calls, through automated software. These sophisticated online fraud techniques allow an attacker to successfully deceive a victim, which can result in serious financial harm.**

6.2 The author's thoughts and discussion

Section 6.2 is an opportunity to summarise my thoughts after producing this piece of work, and I believe that this final analysis demonstrates the following points:

- The COVID-19 pandemic health crisis has caused major disruption worldwide, creating a unique set of events in our current lifetime.

- When people were distracted and stressed during the pandemic, fraudsters were more likely to have had a higher chance of successfully turning a target into a victim.
- Phishing is a straightforward attack method and can be quickly modified to deliver devious campaigns that trick users into revealing sensitive information.
- Phishing susceptibility has increased, and fraudsters have become more psychologically sophisticated through the shared experience of the pandemic.
- Complete financial profiles extracted from phishing can be used for sophisticated secondary stage attacks. These attacks are becoming more accessible through widely available OTP spoofing software.
- Pandemic situational factors, such as home working or financial loss, lead to disruption and contribute to increased phishing susceptibility.
- From the evidence in **Chapter 5**, there is dangerous growth of socially influenced cybercrime, where scam channels, subscription services, scam technique documents and software for spoofing and sending phishing emails are freely available on the public internet.
- UK cyber scam subculture has emerged during the pandemic and appears to be thriving on social media, with anti-language and slang expressions growing in popularity.
- **Young people are easily drawn to cybercrime**, and this is a complex issue:
    - On the one hand, we have a large portion of the population shifted quickly to some form of homeworking or, at a minimum, spent more time at home and online.
    - Specific types of jobs may no longer exist due to the pandemic, which means individuals need to look for new sources of income.
    - Boredom and more time spent online can also contribute to individuals investigating new social spaces online.
    - The BBC Panorama investigation highlights that young people are involved. However, there could be just as many adults involved, not only from the UK. Online scamming could be administered from abroad to target individuals in the UK, which is highly plausible.
- As in organised crime, where money mules are used to carry out laundering and criminal tasks through the chain of command [193], ***digital mules* emerge** in the same format online. The evidence in **Section 5.4.3 demonstrates** that this happens within *Telegram* channels, where administrative hierarchy exists to coerce new users into fraudulent activity.
- The coordinated activity of searching for users with active cryptocurrency exchange accounts allows channel administrators to avoid detection and launder proceeds from scams without directly committing online crimes.
- Online cybercrime and sophisticated attempts to defraud victims are on the rise. There may be many cases of fraud that go unreported to the police, skewing official figures and indicators. The ONS [182]

and Which? surveys [183] provide a better indication of the scale since these will survey individuals who may not have reported crimes to the police.

- Social media companies and authorities must work harder to protect users, and significant public awareness efforts are needed to highlight the dangers of phishing and online scams.

6.3 Limitations of the project

Focusing so much on the context of the pandemic period was the primary concern as I set out to prepare this work in late 2021. However, as the events surrounding the Omicron variant returned such a sense of disruption in December 2021, I felt it was entirely appropriate to consider the impact of the pandemic from an extended nature. As the global health crisis extended for two years, it became essential to recognise the prolonged impact this has had on human behaviours.

It was necessary to define the project scope to events that occurred and have relevance in the UK, to ensure focus throughout. However, it could be argued that this project and the intentions set out in it are entirely applicable for a global readership.

A limitation of this project might be the vast scale of **Chapter 3** which explored how attackers target people in a crisis. The phishing threat group is broad, and the targeting of human vulnerabilities can occur in many ways. Whilst it might have been more concise to focus on a smaller sample of topics in **Tables 2 – 6**, each element was necessary to provide the reader with coverage and appropriate awareness.

Initially, I had intended to focus specifically on phishing. However, in **Chapter 5**, my curiosity uncovered the emerging social media elements. Since cybercriminals desire sensitive information to perform more serious secondary attacks, I felt it was imperative to develop a thesis that considered the entire chained attack cycle. Specifically, how dumped phishing data is used to build active target profiles to share with others in real-time. It was here that I began to find evidence that young people are drawn towards cybercrime through social influence and cyber scam culture. I acknowledge the overall length of this project, but it felt necessary to ensure a thorough exploratory piece of work covered all angles of this emerging topic.

6.4 Protecting against phishing and online scams

As a final opportunity to improve awareness, **Section 6.4** aims to provide five additional recommendations to help the reader protect against phishing and online scams:

1. **Sign up to the Which? Scam Alert Service**[5] **campaign website** [194]. This resource provides a regular email newsletter highlighting new trends in online scams. The newsletter includes tips to help protect against fake messages and avoid being targeted online.
2. **Visit the Take Five**[6] **campaign website** [195]. This resource provides fraud protection information with the following "**Stop, Challenge, Protect**" guidance:
   - **Stop:** Pause to think carefully about the current situation.
   - **Challenge:** First, question if this could be a scam. It is okay to reject and ignore any request.
   - **Protect:** Use the number on your bank card to contact your bank directly if you believe you may have been involved in a scam.
3. **Enable Two-Factor Authentication (2FA) for each email account and all online website accounts supporting this feature**. SMS text message-based authentication is weaker than authentication apps such as Authy [196] and Google Authenticator [197]. These applications can be installed on your smartphone device and allow you to generate a thirty-second authentication code for each online platform session. Two-factor authentication provides an additional layer of security and provides some assurance that unlawful access will not be permitted even if your password has been compromised.
4. **Modern smartphones can restrict unknown phone calls** unless a known number is stored in your address book. It is advisable to enable this caller protection feature to prevent unknown callers. Attackers will also take advantage of the small screen size on smartphone devices to conceal malicious links. **If in doubt, check a suspect email or message on another device, or show it to somebody else**.
5. **If you receive a phone call, email, or message from someone appearing to be your bank or organisation you trust, simply hang up and do not respond to any digital communication**. Call your bank directly, using the number printed on the back of your bank card and ask to speak to an advisor. Do not give out authentication or one-time passwords to anyone, as these will never be requested.

6.5 Future work and contribution

This work has primarily been explorative, and to enhance it in the future, I have provided some technical areas in which this research could contribute additional value in this field:

- Technical research could be carried out based on the research, setting up a honey pot to examine the footprint of COVID-19-related phishing emails.

[5] https://campaigns.which.co.uk/scam-alert-service/

[6] https://www.takefive-stopfraud.org.uk

- Following the BBC Panorama investigation, a deeper dive into the OTP spoofing software investigated might add new value. Technical analysis could then be provided to the relevant cybercrime agencies by interrogating feature sets and investigating weaknesses or vulnerabilities.
- Further technical work to support the investigation into *Telegram* messaging channels:
    - Develop a tool to detect and report these channels automatically. The tool would crawl new channel variations and auto-report and auto-post to community moderated channels for reporting purposes.
    - Automated analysis to understand new slang expressions and anti-language to help authorities decipher messaging.
    - Design a model to interrogate participant location and age groups within the channels.

Bibliography

[1] H. S. Lallie *et al.*, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Comput. Secur.*, vol. 105, p. 102248, Jun. 2021, doi: 10.1016/j.cose.2021.102248.

[2] Interpol, "Cybercriminals targetting critical healthcare institutions with ransomware," 2020. Accessed: Nov. 28, 2021. [Online]. Available: https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware.

[3] M. Hadnagy, Christopher;Fincher, *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails | Christopher Hadnagy, Michele Fincher | download*. John Wiley & Sons, Ltd, 2015.

[4] I. Periodicals, "Ieee Reference Guide - How To Reference," 2018. Accessed: Jan. 29, 2022. [Online]. Available: https://ieeeauthorcenter.ieee.org/wp-content/uploads/IEEE-Reference-Guide.pdf.

[5] R. Naidoo, "A multi-level influence model of COVID-19 themed cybercrime," *https://doi.org/10.1080/0960085X.2020.1771222*, vol. 29, no. 3, pp. 306–321, May 2020, doi: 10.1080/0960085X.2020.1771222.

[6] S. Furnell and J. N. Shah, "Home working and cyber security – an outbreak of unpreparedness?," *Comput. Fraud Secur.*, vol. 2020, no. 8, pp. 6–12, 2020, doi: 10.1016/S1361-3723(20)30084-1.

[7] B. Pranggono and A. Arabo, " COVID -19 pandemic cybersecurity issues ," *Internet Technol. Lett.*, vol. 4, no. 2, p. e247, Mar. 2021, doi: 10.1002/itl2.247.

[8] R. Herjavec, "The 2020 Official Annual Cybercrime Report - Herjavec Group," 2020. Accessed: Nov. 14, 2021. [Online]. Available: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/.

[9] S. Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," 2020. Accessed: Nov. 14, 2021. [Online]. Available: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

[10] D. L. Schinder and M. Cross, *Scene of the Cybercrime - Debra Littlejohn Shinder, Michael Cross*. 2008.

[11] J. R. C. Nurse, "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit," in *The Oxford Handbook of Cyberpsychology*, Oxford University Press, 2019, pp. 662–690.

[12] H. Office Science, "Cyber crime: A review of the evidence Research Report - Chapter 1: Cyber-dependent crimes," vol. Chapter 1, 2013.

[13] H. Office Science, "Cyber crime: A review of the evidence Research Report - Chapter 2: Cyber-enabled crimes - fraud and theft," vol. Chapter 2, 2013.

[14] P. J. Denning, *Computer Viruses*. 1988.

[15] G. Suarez-Tangil, J. E. Tapiador, P. Peris-Lopez, and J. Blasco, "Dendroid: A text mining approach to analyzing and classifying code structures in Android malware families," *Expert Syst. Appl.*, vol. 41, no. 4, pp. 1104–1117, Mar. 2014, doi: 10.1016/J.ESWA.2013.07.106.

[16] S. Sibi Chakkaravarthy, D. Sangeetha, and V. Vaidehi, "A Survey on malware analysis and mitigation techniques," *Comput. Sci. Rev.*, vol. 32, pp. 1–23, May 2019, doi: 10.1016/J.COSREV.2019.01.002.

[17] T. Dargahi, A. Dehghantanha, P. N. Bahrami, M. Conti, G. Bianchi, and L. Benedetto, "A Cyber-Kill-Chain based taxonomy of crypto-ransomware features," *J. Comput. Virol. Hacking Tech.*, vol. 15, no. 4, pp. 277–305, Dec. 2019, doi: 10.1007/S11416-019-00338-7/TABLES/5.

[18] "AI-powered malware… theory or fact?," *Bullguard*, 2021. https://www.bullguard.com/blog/2021/02/ai-powered-malware-theory-or-fact (accessed Dec. 07, 2021).

[19] S. Security, "Report | Tear up the cybersecurity rule book," 2020. Accessed: Nov. 21, 2021. [Online]. Available: https://lp.skyboxsecurity.com/WICD-2020-11-VTM-POV_Asset.html.

[20] S. Song, B. Kim, and S. Lee, "The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform," *Mob. Inf. Syst.*, vol. 2016, 2016, doi: 10.1155/2016/2946735.

[21] National Cyber Security Centre, "Annual Review 2021 Making the UK the safest place to live and work online," 2020.

[22] NCSC, "Cyber warning issued for key healthcare organisations in... - NCSC.GOV.UK," 2020. Accessed: Nov. 28, 2021. [Online]. Available: https://www.ncsc.gov.uk/news/warning-issued-uk-usa-healthcare-organisations.

[23] J. Stubbs and C. Bing, "Exclusive: Iran-linked hackers recently targeted coronavirus drugmaker Gilead - sources," 2020. Accessed: Nov. 28, 2021. [Online]. Available: https://www.reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex-idUSKBN22K2EV.

[24] Johnson Joseph, "Leading cause of ransomware infection 2020 | Statista," *Statista*, 2021. https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/ (accessed Nov. 21, 2021).

[25] Verizon, "Verizon: 2021 Data Breach Investigations Report," 2021. doi: 10.1016/s1361-3723(21)00061-0.

[26] F. Breda, H. Barbosa, and T. Morais, "Social Engineering and Cyber Security," *INTED2017 Proc.*, vol. 1, pp. 4204–4211, 2017, doi: 10.21125/inted.2017.1008.

[27] C. Hadnagy, *Social Engineering: The Science of Human Hacking | Christopher Hadnagy | 2nd Edition*, vol. 18, no. 4. 2018.

[28] R. Heartfield and G. Loukas, "Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework," *Comput. Secur.*, vol. 76, pp. 101–127, 2018, doi: 10.1016/j.cose.2018.02.020.

[29] T. Moore and R. Clayton, "Discovering phishing dropboxes using email metadata," *eCrime Res. Summit, eCrime*, 2012, doi: 10.1109/ECRIME.2012.6489515.

[30] K. Taylor and L. Silver, "Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally," 2019. Accessed: Dec. 06, 2021. [Online]. Available: https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/.

[31] E. Nix, "Stop, Think, Call: Avoiding scams on WhatsApp | by Emily Nix | Nov, 2021," 2021. Accessed: Dec. 06, 2021. [Online]. Available: https://wearecitizensadvice.org.uk/stop-think-call-avoiding-scams-on-whatsapp-d878e8819148.

[32] Y.-J. L. J. Choi, "The change in the methods of smishing in south-korea after the onset of covid-19," 2021. Accessed: Dec. 06, 2021. [Online]. Available: https://www.proquest.com/docview/2585993326?pq-origsite=gscholar&fromopenview=true.

[33] "Outstanding Smartphone Usage Statistics UK Edition [2021]." Accessed: Dec. 06, 2021. [Online]. Available: https://cybercrew.uk/blog/smartphone-usage-statistics-uk/.

[34] M. E. David and J. A. Roberts, "Smartphone use during the COVID-19 pandemic: Social versus physical distancing,"

Int. J. Environ. Res. Public Health, vol. 18, no. 3, pp. 1–8, Feb. 2021, doi: 10.3390/IJERPH18031034.

[35] *Mobile Users Prove More Susceptible to Phishing Attacks*. 2020.

[36] G. Canova *et al.*, "Learn to Spot Phishing URLs with the Android NoPhish App," *IFIP Adv. Inf. Commun. Technol.*, vol. 453, pp. 87–100, 2015, doi: 10.1007/978-3-319-18500-2_8.

[37] WHO, "WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020," 2020. Accessed: Dec. 13, 2021. [Online]. Available: https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020.

[38] Interpol, "COVID-19 Cyberthreats," 2020. Accessed: Nov. 21, 2021. [Online]. Available: https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats.

[39] S. Lloyd, "ICANN - Registrations Related to COVID-19: 18 Months of Data," *ICANN*, 2021. https://www.icann.org/en/system/files/files/octo-028-09nov21-en.pdf (accessed Nov. 14, 2021).

[40] D. W. Jolley, "If You Only Knew the Power of the Dark Web! Finding Intellectual If You Only Knew the Power of the Dark Web! Finding Intellectual Freedom, Privacy, and Anonymity Online Freedom, Privacy, and Anonymity Online," *Digit. Commons @ Gardner Webb Univ.*, 2021, Accessed: Dec. 13, 2021. [Online]. Available: https://digitalcommons.gardner-webb.edu/doverlibfacpub/18.

[41] Ofcom, "UK's internet use surges to record levels - Ofcom," 2020. Accessed: Nov. 29, 2021. [Online]. Available: https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2020/uk-internet-use-surges.

[42] "Pandemic accelerated UK's shift online, says Ofcom - BBC News," 2021. Accessed: Dec. 09, 2021. [Online]. Available: https://www.bbc.co.uk/news/technology-57383998.

[43] M. Auer and M. D. Griffiths, "Gambling Before and During the COVID-19 Pandemic Among Online Casino Gamblers: An Empirical Study Using Behavioral Tracking Data," *Int. J. Ment. Health Addict.*, pp. 1–11, Feb. 2021, doi: 10.1007/S11469-020-00462-2/FIGURES/5.

[44] Geneva, "WHO reports fivefold increase in cyber attacks, urges vigilance," 2020. Accessed: Oct. 31, 2021. [Online]. Available: https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance.

[45] "Warning over NHS Covid Pass scams as criminals target bank accounts | InYourArea News." Accessed: Oct. 31, 2021. [Online]. Available: https://www.inyourarea.co.uk/news/warning-over-nhs-covid-pass-scams-as-criminals-target-bank-accounts/.

[46] K. Okereafor, *Cybersecurity in the COVID-19 Pandemic*. CRC Press, 2021.

[47] A. Mihailović, J. C. Smolović, I. Radević, N. Rašović, and N. Martinović, "COVID-19 and Beyond: Employee Perceptions of the Efficiency of Teleworking and Its Cybersecurity Implications," *Sustain. 2021, Vol. 13, Page 6750*, vol. 13, no. 12, p. 6750, Jun. 2021, doi: 10.3390/SU13126750.

[48] C. Boulton, "Humans are (still) the weakest cybersecurity link," *Cio.Com*, 2017, Accessed: Nov. 21, 2021. [Online]. Available: https://www.proquest.com/docview/1889632656?pq-origsite=summon&accountid=14565.

[49] F. Malecki, "Overcoming the security risks of remote working," *Comput. Fraud Secur.*, vol. 2020, no. 7, pp. 10–12, Jul. 2020, doi: 10.1016/S1361-3723(20)30074-9.

[50] S. Crimando, "A Perfect Storm for Social Engineering: Anticipating the Human Element in Post-Pandemic Cybersecurity," 2021. [Online]. Available: https://abnormalsecurity.com/resources/human-element-post-

pandemic-cybersecurity.

[51] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Working from home during COVID-19 crisis: a cyber security culture assessment survey," *Secur. J.*, pp. 1–20, Feb. 2021, doi: 10.1057/s41284-021-00286-2.

[52] B. Akhgar, A. Staniforth, and F. Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook*. 2014.

[53] R. Bruce *et al.*, "Policy Enforcement in the Presence of Organized Crime: Evidence from Rio de Janeiro *," 2021, Accessed: Nov. 21, 2021. [Online]. Available: https://ssrn.com/abstract=3678840.

[54] M. Dellasega and J. Vorrath, "A Gangster's Paradise? - Stiftung Wissenschaft und Politik," 2020, Accessed: Nov. 21, 2021. [Online]. Available: https://www.swp-berlin.org/10.18449/2020C66/.

[55] M. Riccardi, "View of Organised Crime Infiltration of the COVID-19 Economy," *Transcrime – Jt. Res. Cent. Transnatl. Crime, Univ. Cattol. del Sacro Cuore*, 2021, Accessed: Nov. 21, 2021. [Online]. Available: https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/488/358.

[56] "Covid-19: Bounce Back Loan Scheme - Public Accounts Committee - House of Commons," 2020. Accessed: Jan. 30, 2022. [Online]. Available: https://publications.parliament.uk/pa/cm5801/cmselect/cmpubacc/687/68703.htm#_idTextAnchor000 AND https://www.nao.org.uk/wp-content/uploads/2020/10/Investigation-into-the-Bounce-Back-Loan-Scheme-Summary.pdf.

[57] D. Thomas and S. Morris, "'A giant bonfire of taxpayers' money': fraud and the UK pandemic loan scheme | Financial Times," 2022. Accessed: Jan. 30, 2022. [Online]. Available: https://www.ft.com/content/41d5fe0a-7b46-4dd7-96e3-710977dff81c.

[58] R. Neate, "Over £5.5bn of Covid support funds lost to fraud or error," 2021. Accessed: Mar. 28, 2022. [Online]. Available: https://www.theguardian.com/world/2021/nov/04/over-55bn-of-covid-support-funds-lost-to-or-error.

[59] J. Elgot, P. Walker, and R. Neate, "Minister quits in Lords over government handling of Covid loans fraud," 2022. Accessed: Jan. 30, 2022. [Online]. Available: https://www.theguardian.com/politics/2022/jan/24/minister-resigns-in-protest-at-handling-of-fraudulent-covid-loans.

[60] D. Cohen, "The new county lines? Teenagers drawn into world of cybercrime scams | The Independent," 2021. Accessed: Jan. 10, 2022. [Online]. Available: https://www.independent.co.uk/news/uk/crime/online-scamming-new-county-lines-b1945459.html.

[61] "National Strategic Assessment of Serious and Organised Crime 2020," *Natl. Crime Agency*, no. May, 2020.

[62] M. Aiken, J. Davidson, and P. Amann, "Youth Pathways into Cybercrime," 2016, Accessed: Mar. 28, 2022. [Online]. Available: https://www.researchgate.net/publication/309563967.

[63] M. Hopkins and A. Dehghantanha, "Exploit Kits: The production line of the Cybercrime economy?," *2015 2nd Int. Conf. Inf. Secur. Cyber Forensics, InfoSec 2015*, pp. 23–27, Mar. 2016, doi: 10.1109/INFOSEC.2015.7435501.

[64] B. Collier, R. Clayton, A. Hutchings, and D. Thomas, "Cybercrime is (often) boring: Infrastructure and alienation in a deviant subculture," *Br. J. Criminol.*, vol. 61, pp. 1407–1423, 2021, doi: 10.1093/bjc/azab026.

[65] K. Okpattah, "BBC One - Panorama, Hunting the Social Media Fraudsters," 2021. Accessed: Jan. 27, 2022. [Online]. Available: https://www.bbc.co.uk/programmes/m000ywtq.

[66] *Cyber Threats in Physical Security*. 2021.

[67] CISA, "COVID-19 Exploited by Malicious Cyber Actors," 2020. Accessed: Dec. 14, 2021. [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/aa20-099a.

[68] "UK coronavirus (COVID-19) alert level increased from Level 3 to Level 4 - GOV.UK," 2021. Accessed: Dec. 13, 2021. [Online]. Available: https://www.gov.uk/government/news/uk-coronavirus-covid-19-alert-level-increased-from-level-3-to-level-4.

[69] *Zero Trust Security | Akamai*. 2018.

[70] B. Wang, Y. Liu, J. Qian, and S. K. Parker, "Achieving Effective Remote Working During the COVID-19 Pandemic: A Work Design Perspective," *Appl. Psychol. AN Int. Rev.*, vol. 2021, no. 1, pp. 16–59, 2020, doi: 10.1111/apps.12290.

[71] "The definitive overview of payment industry fraud," *UK Financ.*, 2021.

[72] S. Fadilpašić, "Many CISOs still feel unprepared to deal with cyberattacks | ITProPortal," 2021. Accessed: Jan. 05, 2022. [Online]. Available: https://www.itproportal.com/news/many-cisos-still-feel-unprepared-to-deal-with-cyberattacks/.

[73] "Cyber-attack on UK's Defence Academy caused 'significant' damage | Ministry of Defence | The Guardian," 2022. Accessed: Jan. 05, 2022. [Online]. Available: https://www.theguardian.com/uk-news/2022/jan/02/cyber-attack-on-uks-defence-academy-caused-significant-damage.

[74] J. I. Dingel and B. Neiman, "How many jobs can be done at home?," *J. Public Econ.*, vol. 189, p. 104235, Sep. 2020, doi: 10.1016/J.JPUBECO.2020.104235.

[75] I. Savolainen, R. Oksa, N. Savela, M. Celuch, and A. Oksanen, "COVID-19 Anxiety-A Longitudinal Survey Study of Psychological and Situational Risks among Finnish Workers," *Int. J. Environ. Res. Public Heal. Artic.*, 2021, doi: 10.3390/ijerph18020794.

[76] O. Giuntella, K. Hyde, S. Saccardo, and S. Sadoff, "Lifestyle and mental health disruptions during COVID-19," *Proc. Natl. Acad. Sci.*, vol. 118, no. 9, Mar. 2021, doi: 10.1073/PNAS.2016632118.

[77] H. Preis, B. Mahaffey, C. Heiselman, and M. Lobel, "Vulnerability and resilience to pandemic-related stress among U.S. women pregnant at the start of the COVID-19 pandemic," *Soc. Sci. Med.*, vol. 266, p. 113348, Dec. 2020, doi: 10.1016/J.SOCSCIMED.2020.113348.

[78] M. Mosheva *et al.*, "Anxiety, pandemic-related stress and resilience among physicians during the COVID-19 pandemic," *Depress. Anxiety*, vol. 37, no. 10, pp. 965–971, 2020, doi: 10.1002/da.23085.

[79] C. Hadnagy, "Unmasking the Social Engineer: The Human Element of Security," in *Journal of Chemical Information and Modeling*, vol. 53, 2014, pp. 1689–1699.

[80] S. Mittal, "Understanding the Human Dimension of Cyber Security," *Indian J. Criminol. Crim.*, 2015, Accessed: Nov. 21, 2021. [Online]. Available: https://www.researchgate.net/publication/349466767.

[81] J. Denno, "Attacking the human - the weakest link in cybersecurity," *ProQuest Diss. Theses*, no. December, p. 64, 2016, Accessed: Nov. 21, 2021. [Online]. Available: http://library.capella.edu/login?url=https://search-proquest-com.library.capella.edu/docview/1861984809?accountid=27965.

[82] M. L. Jensen, M. Dinger, R. T. Wright, and J. B. Thatcher, "Training to Mitigate Phishing Attacks Using Mindfulness Techniques," *J. Manag. Inf. Syst.*, vol. 34, no. 2, pp. 597–626, Apr. 2017, doi: 10.1080/07421222.2017.1334499.

[83] R. Khweiled, M. Jazzar, and D. Eleyan, "Cybercrimes during COVID -19 Pandemic," *Int. J. Inf. Eng. Electron. Bus.*, vol. 13, no. 2, pp. 1–10, 2021, doi: 10.5815/ijieeb.2021.02.01.

[84] R. A. Ramadan, B. W. Aboshosha, J. S. Alshudukhi, A. J. Alzahrani, A. El-Sayed, and M. M. Dessouky, "Cybersecurity and Countermeasures at the Time of Pandemic," *J. Adv. Transp.*, vol. 2021, 2021, doi: 10.1155/2021/6627264.

[85] C. M. Coelho, P. Suttiwan, N. Arato, and A. N. Zsido, "On the Nature of Fear and Anxiety Triggered by COVID-19," *Front. Psychol.*, vol. 11, p. 3109, Nov. 2020, doi: 10.3389/FPSYG.2020.581314/BIBTEX.

[86] J. Beard, "Scammers now 'psychological experts' as fraud rises by a fifth," 2022. Accessed: Feb. 16, 2022. [Online]. Available: https://www.telegraph.co.uk/money/consumer-affairs/scammers-now-psychological-experts-fraud-rises-fifth/.

[87] K. Lewin, "Principles of Topological Psychology," 1936.

[88] A. Ertan, D. Rikke, and B. Jensen, "Everyday Cyber Security in Organisations Researchers and principal authors," 2020.

[89] L. Oliveira J. e Silva, M. V. Vidor, V. Zarpellon de Araújo, and F. Bellolio, "Flexibilization of Science, Cognitive Biases, and the COVID-19 Pandemic," *Mayo Clin. Proc.*, vol. 95, no. 9, pp. 1842–1844, Sep. 2020, doi: 10.1016/J.MAYOCP.2020.06.037/ATTACHMENT/A823FB27-3C3A-4EF2-AD0A-4F35F73B14E0/MMC1.MP4.

[90] G. Crossland, "Biases in Perceptions of Information Security Threats - Infosecurity Magazine." Accessed: Feb. 20, 2022. [Online]. Available: https://www.infosecurity-magazine.com/next-gen-infosec/biases-perceptions-threats/.

[91] C. Cavaglieri, "Omicron variant fake PCR test emails and texts – Which? Conversation," 2022. Accessed: Feb. 05, 2022. [Online]. Available: https://conversation.which.co.uk/scams/omicron-variant-pcr-test-fake-email/.

[92] S. Mishra and D. Soni, "Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis," *Futur. Gener. Comput. Syst.*, vol. 108, pp. 803–815, Jul. 2020, doi: 10.1016/J.FUTURE.2020.03.021.

[93] H. Flett, Amie Ballantyne, "Expert warns how scammers are taking advantage of Covid & storm damage," 2021. Accessed: Dec. 21, 2021. [Online]. Available: https://www.thecourier.co.uk/fp/news/angus-mearns/2793012/covid-expert-scam-omicron-storm-arwen/.

[94] "What is Business Email Compromise?," 2022. Accessed: Feb. 14, 2022. [Online]. Available: https://www.barracuda.com/glossary/business-email-compromise.

[95] B. Bracken, "Omicron Phishing Scam Already Spotted in UK | Threatpost," 2021. Accessed: Dec. 20, 2021. [Online]. Available: https://threatpost.com/omicron-phishing-scam-uk/176771/.

[96] B. Honan, "Ubiquiti Networks victim of $39 million social engineering attack," 2015. Accessed: Mar. 08, 2022. [Online]. Available: https://www.csoonline.com/article/2961066/ubiquiti-networks-victim-of-39-million-social-engineering-attack.html%0Ahttp://www.csoonline.com/article/2961066/supply-chain-security/ubiquiti-networks-victim-of-39-million-social-engineering-attack.html.

[97] "What is Email Spoofing & How Does It Work | Proofpoint UK," 2022. Accessed: Feb. 06, 2022. [Online]. Available: https://www.proofpoint.com/uk/corporate-blog/post/how-does-email-spoofing-work-and-why-it-so-easy.

[98] GOV.UK, "Prime Minister's Statement on Coronavirus (COVID-19): 23 March 2020," 2020. Accessed: Feb. 12, 2022. [Online]. Available: https://www.gov.uk/government/speeches/pm-address-to-the-nation-on-coronavirus-23-march-2020.

[99] "Kr3pto Puppeteer Kits: Dynamic Phishing Kit Targeting UK Banking Customers." Accessed: Oct. 19, 2021.

[Online]. Available: https://www.wmcglobal.com/blog/kr3pto-puppeteer-kits-dynamic-phishing-kit-targeting-uk-banking-customers.

[100] "NCSC shines light on scams being foiled via pioneering new... - NCSC.GOV.UK," 2020. Accessed: Feb. 13, 2022. [Online]. Available: https://www.ncsc.gov.uk/news/cyber-experts-shine-light-on-online-scams.

[101] Cabinet Office, "Government confirms £500 million hardship fund will provide council tax relief for vulnerable households," 2020. Accessed: Feb. 13, 2022. [Online]. Available: https://www.gov.uk/government/news/government-confirms-500-million-hardship-fund-will-provide-council-tax-relief-for-vulnerable-households.

[102] "How we fought Search spam on Google in 2020 | Google Search Central Blog | Google Developers," 2020. Accessed: Feb. 13, 2022. [Online]. Available: https://developers.google.com/search/blog/2021/04/how-we-fought-search-spam-2020.

[103] "Create a coronavirus NHS QR code for your venue - GOV.UK," 2022. Accessed: Feb. 14, 2022. [Online]. Available: https://www.gov.uk/create-coronavirus-qr-poster.

[104] "Deepfake phishing: Should we be concerned?," 2022. Accessed: Feb. 14, 2022. [Online]. Available: https://www.egress.com/resources/cybersecurity-information/phishing/deepfake-phishing.

[105] H. F. Tipton and H. F. Krause, "Social Engineering: The Forgotten Risk," *Inf. Secur. Manag. Handb.*, pp. 242–252, 2021, doi: 10.1201/noe0849385858-19.

[106] T. R. Peltier, "Social engineering: Concepts and solutions," *Inf. Syst. Secur.*, vol. 15, no. 5, pp. 13–21, 2006, doi: 10.1201/1086.1065898X/46353.15.4.20060901/95427.3.

[107] M. Silic and A. Back, "The dark side of social networking sites:Understanding phishing risks," *Comput. Human Behav.*, vol. 60, pp. 35–43, Jul. 2016, doi: 10.1016/J.CHB.2016.02.050.

[108] B. Fogg, "A behavior model for persuasive design," *ACM Int. Conf. Proceeding Ser.*, vol. 350, 2009, doi: 10.1145/1541948.1541999.

[109] M. Workman, "Gaining access with social engineering: An empirical study of the threat," *Inf. Syst. Secur.*, vol. 16, no. 6, pp. 315–331, 2007, doi: 10.1080/10658980701788165.

[110] R. Cialdini, *Influence: The Psychology of Persuasion*. Harper, 2001.

[111] D. Kelley, "The psychology of social engineering—the 'soft' side of cybercrime," 2020. Accessed: Feb. 12, 2022. [Online]. Available: https://www.microsoft.com/security/blog/2020/06/30/psychology-social-engineering-soft-side-cybercrime/.

[112] D. Todd, "Omicron Variant Phishing Emails in the Wild," 2021. Accessed: Dec. 20, 2021. [Online]. Available: https://www.secureworld.io/industry-news/omicron-covid-phishing-email-examples.

[113] R. E. Guadagno and R. B. Cialdini, "Preference for consistency and social influence: A review of current research findings," 2010. doi: 10.1080/15534510903332378.

[114] BBC News, "Clap for Carers: UK applauds NHS staff and key workers," 2020. Accessed: Feb. 12, 2022. [Online]. Available: https://www.bbc.co.uk/news/av/uk-52143223.

[115] R. B. Cialdini and N. J. Goldstein, "Social influence: compliance and conformity," *Annu. Rev. Psychol.*, vol. 55, pp. 591–622, Jan. 2004, Accessed: Dec. 13, 2021. [Online]. Available: https://go.gale.com/ps/i.do?p=AONE&sw=w&issn=00664308&v=2.1&it=r&id=GALE%7CA114167291&sid=googl

eScholar&linkaccess=fulltext.

[116] M.Race, “The tricks scammers use to steal your money - BBC News,” 2022. Accessed: Feb. 15, 2022. [Online]. Available: https://www.bbc.co.uk/news/business-60380467.

[117] J. S. Lerner, Y. Li, P. Valdesolo, and K. S. Kassam, “Emotion and Decision Making,” *http://dx.doi.org/10.1146/annurev-psych-010213-115043*, vol. 66, pp. 799–823, Jan. 2015, doi: 10.1146/ANNUREV-PSYCH-010213-115043.

[118] S. Côté, *Incidental vs. Integral: Understanding Your Emotions*. 2014.

[119] D. of H. and S. C. Cabinet Office, “Emergency bill to strengthen coronavirus ({COVID}-19) response plans,” 2020. Accessed: Feb. 13, 2022. [Online]. Available: https://www.gov.uk/government/news/emergency-bill-to-strengthen-coronavirus-covid-19-response-plans.

[120] W. Janes, “‘Inconsistent and unclear’ UK Covid alert system ‘costing lives’, report says,” 2022. Accessed: Jan. 11, 2022. [Online]. Available: https://uk.news.yahoo.com/inconsistent-unclear-uk-covid-alert-000100478.html.

[121] Cabinet Office, M. & S. Department of Digital, Culture, O. Dowden, and P. Mordaunt, “Government cracks down on spread of false coronavirus information online,” 2020. Accessed: Feb. 13, 2022. [Online]. Available: https://www.gov.uk/government/news/government-cracks-down-on-spread-of-false-coronavirus-information-online.

[122] G. Bondanini, G. Giorgi, A. Ariza-Montes, A. Vega-Muñoz, and P. Andreucci-Annunziata, “Technostress Dark Side of Technology in the Workplace: A Scientometric Analysis,” *Int. J. Environ. Res. Public Health*, vol. 17, no. 21, pp. 1–25, Nov. 2020, doi: 10.3390/IJERPH17218013.

[123] P. Ekman, “What is Fear? | What Causes Fear? | Paul Ekman Group,” 2020. Accessed: Feb. 13, 2022. [Online]. Available: https://www.paulekman.com/universal-emotions/what-is-fear/.

[124] DHSC and PHE, “New guidance for households with possible COVID-19 infection,” 2020. Accessed: Feb. 12, 2022. [Online]. Available: https://www.gov.uk/government/news/new-guidance-for-households-with-possible-covid-19-infection.

[125] Gov.uk, “Prime Minister announces national lockdown,” 2021. Accessed: Feb. 13, 2022. [Online]. Available: https://www.gov.uk/government/news/prime-minister-announces-national-lockdown.

[126] H. Treasury, “Coronavirus Job Retention Scheme - GOV.UK,” 2020. Accessed: Feb. 13, 2022. [Online]. Available: https://www.gov.uk/government/collections/coronavirus-job-retention-scheme.

[127] Department for Education and G. Williamson, “Schools, colleges and early years settings to close,” 2020. Accessed: Feb. 12, 2022. [Online]. Available: https://www.gov.uk/government/news/schools-colleges-and-early-years-settings-to-close.

[128] A. Doucet, D. D. Netolicky, K. Timmers, and F. J. Tuscano, “Thinking about Pedagogy in an Unfolding Pandemic by Education International - issuu,” *Educ. Int.*, p. 58, 2020, Accessed: Jan. 27, 2022. [Online]. Available: https://issuu.com/educationinternational/docs/2020_research_covid-19_eng.

[129] National Cyber Security Centre (NCSC), “More ransomware attacks on UK education - NCSC.GOV.UK,” 2021. Accessed: Feb. 13, 2022. [Online]. Available: https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector.

[130] R. Wearn, “Parcel delivery scam texts to spike this Christmas - BBC News,” 2021. Accessed: Jan. 06, 2022. [Online].

Available: https://www.bbc.co.uk/news/business-59760326.

[131] Cabinet Office, “Home Secretary announces new public health measures for all UK arrivals - GOV.UK,” 2020. Accessed: Feb. 13, 2022. [Online]. Available: https://www.gov.uk/government/news/home-secretary-announces-new-public-health-measures-for-all-uk-arrivals.

[132] T. Allas, M. Canal, and V. Hunt, “COVID-19 in the UK: The impact on people and jobs at risk | McKinsey,” 2020. Accessed: Feb. 13, 2022. [Online]. Available: https://www.mckinsey.com/industries/public-and-social-sector/our-insights/covid-19-in-the-united-kingdom-assessing-jobs-at-risk-and-the-impact-on-people-and-places.

[133] Office for National Statistics, “Early insights of how the coronavirus (COVID-19) pandemic impacted the labour market - Office for National Statistics,” 2021. Accessed: Feb. 13, 2022. [Online]. Available: https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/earlyinsightsofhowthecoronaviruscovid19pandemicimpactedthelabourmarket/july2020#vacancies-and-unemployment-overview.

[134] World Health Organization, “Classification of Omicron (B.1.1.529): SARS-CoV-2 Variant of Concern,” 2021. Accessed: Jan. 06, 2022. [Online]. Available: https://www.who.int/news/item/26-11-2021-classification-of-omicron-(b.1.1.529)-sars-cov-2-variant-of-concern.

[135] I. S. and L. B. Nicola Davis, “When did Omicron Covid variant arrive in UK and is it spreading?,” 2021. Accessed: Feb. 20, 2022. [Online]. Available: https://www.theguardian.com/world/2021/dec/01/when-did-omicron-variant-arrive-in-uk-and-is-it-spreading.

[136] F. Hassan, L. London, and G. Gonsalves, “Unequal global vaccine coverage is at the heart of the current covid-19 crisis,” *BMJ*, 2021, doi: 10.1136/bmj.n3074.

[137] R. H. Mathieu Edouard, “Coronavirus (COVID-19) Vaccinations - Statistics and Research - Our World in Data,” 2021. Accessed: Jan. 14, 2022. [Online]. Available: https://ourworldindata.org/covid-vaccinations.

[138] “COVID-19 Vaccination – Africa CDC,” 2022. Accessed: Jan. 14, 2022. [Online]. Available: https://africacdc.org/covid-19-vaccination/.

[139] W. Health and O. Headquarters, “Enhancing response to Omicron SARS-CoV-2 variant : Technical brief and priority actions for Member States,” *World Heal. Organ.*, no. January, pp. 1–28, 2022.

[140] H. Brennan, “Elderly waiting for booster jabs a target for criminal gangs,” 2021. Accessed: Dec. 21, 2021. [Online]. Available: https://www.telegraph.co.uk/money/consumer-affairs/elderly-waiting-booster-jabs-target-criminal-gangs/.

[141] H. Brennan, “Fraudsters ‘prey on omicron fears’ with new NHS Covid test scam,” 2021. Accessed: Feb. 03, 2022. [Online]. Available: https://www.telegraph.co.uk/money/consumer-affairs/fraudsters-prey-omicron-fears-new-nhs-covid-test-scam/.

[142] G. Tsakalidis and K. Vergidis, “A Systematic Approach Toward Description and Classification of Cybercrime Incidents,” *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 49, no. 4, pp. 710–729, Apr. 2019, doi: 10.1109/TSMC.2017.2700495.

[143] “All adults to be offered COVID-19 boosters by end of January - GOV.UK,” 2021. Accessed: Jan. 16, 2022. [Online]. Available: https://www.gov.uk/government/news/all-adults-to-be-offered-covid-19-boosters-by-end-of-

january.

[144] UK Government, “Prime Minister confirms move to Plan B in England,” 2021. Accessed: Jan. 16, 2022. [Online]. Available: https://www.gov.uk/government/news/prime-minister-confirms-move-to-plan-b-in-england.

[145] “UK COVID Alert Level increased from Level 3 to Level 4,” 2021. Accessed: Jan. 16, 2022. [Online]. Available: https://gov.wales/uk-covid-alert-level-increased-level-3-level-4.

[146] J. Grierson, “Lateral flow test kits unavailable on official website in England | Coronavirus | The Guardian,” 2021. Accessed: Jan. 16, 2022. [Online]. Available: https://www.theguardian.com/world/2021/dec/13/no-more-home-covid-tests-available-says-nhs-england.

[147] “Covid: London ‘major incident’ declared due to Omicron rise - BBC News,” 2021. Accessed: Jan. 30, 2022. [Online]. Available: https://www.bbc.co.uk/news/uk-england-london-59710649.

[148] C. Cavaglieri, “Scam alert: Omicron variant PCR test phishing emails – Which? Conversation,” 2021. Accessed: Dec. 20, 2021. [Online]. Available: https://conversation.which.co.uk/scams/omicron-variant-pcr-test-fake-email/.

[149] “Watch out: Omicron variant scams being used to steal your identity | Tom’s Guide,” 2021. Accessed: Dec. 20, 2021. [Online]. Available: https://www.tomsguide.com/news/omicron-variant-phishing-scams.

[150] C. Stringer, “EXPOSED: Fraudsters offering FAKE fit to fly certificates to dodge Omicron rules | The Argus,” 2021. Accessed: Jan. 16, 2022. [Online]. Available: https://www.theargus.co.uk/news/19778502.exposed-fraudsters-offering-fake-fit-fly-certificates-dodge-omicron-rules/.

[151] K. Doody, “NHS Covid pass scam warning amid Boris Johnson’s booster jab expansion | News and Star,” 2021. Accessed: Dec. 21, 2021. [Online]. Available: https://www.newsandstar.co.uk/news/19780426.nhs-covid-pass-scam-warning-amid-boris-johnsons-booster-jab-expansion/.

[152] O. Jenkinson, “Surrey warning over booster vaccine scam | Surrey Comet,” 2021. Accessed: Dec. 21, 2021. [Online]. Available: https://www.surreycomet.co.uk/news/19796397.surrey-warning-booster-vaccine-scam/.

[153] C. Harrison, “Omicron PCR test phishing email scams and all of the other warnings you need to beware of - CoventryLive,” 2021. Accessed: Dec. 20, 2021. [Online]. Available: https://www.coventrytelegraph.net/in-your-area/omicron-pcr-test-phishing-email-22458509.

[154] B. Young, “Omicron PCR test scam in Berkshire at Christmas - police warning | Reading Chronicle,” 2022. Accessed: Jan. 06, 2022. [Online]. Available: https://www.readingchronicle.co.uk/news/19805051.omicron-pcr-test-scam-berkshire-christmas---police-warning/.

[155] S. W. Kleinknecht, “Hacking Hackers,” 2003, Accessed: Mar. 06, 2022. [Online]. Available: https://macsphere.mcmaster.ca/handle/11375/10956.

[156] T. M. Ajayi, “Anti-language, Slang and Cyber Scam Subculture among Urban Youth in Southwestern Nigeria,” *Int. J. Cyber Criminol.*, vol. 13, no. 2, pp. 511–533, 2019, doi: 10.5281/zenodo.3709011.

[157] “Online fraud & Cybercrime | Metropolitan Police,” 2022. Accessed: Mar. 03, 2022. [Online]. Available: https://www.met.police.uk/advice/advice-and-information/fa/fraud/online-fraud/.

[158] P. Nilsson, “Online fraud up by a third in the UK during the pandemic,” 2021. Accessed: Mar. 03, 2022. [Online]. Available: https://www.ft.com/content/e820cc8a-090c-4632-95f3-cb295d3d31ad.

[159] R. Jones, “More than £2.3bn lost in a year as scams surge during pandemic | Scams | The Guardian,” 2021.

Accessed: Feb. 26, 2022. [Online]. Available: https://www.theguardian.com/money/2021/jul/15/more-than-23bn-lost-in-a-year-as-scams-surge-during-pandemic.

[160] D. Sheridan, "Social media giants like Facebook accused of failure to act against 'horrific' online abuse," 2021. Accessed: Feb. 26, 2022. [Online]. Available: https://www.telegraph.co.uk/news/2021/10/24/social-media-giants-like-facebook-accused-failure-act-against/.

[161] B. Woods, "Online safety law sets Ofcom on collision course with tech giants," 2021. Accessed: Feb. 26, 2022. [Online]. Available: https://www.telegraph.co.uk/business/2021/11/21/online-safety-law-sets-ofcom-collision-course-tech-giants/.

[162] T. G, "10 Most Secure Messaging Apps - Best Encrypted Chat App Solutions," 2020. Accessed: Feb. 26, 2022. [Online]. Available: https://getstream.io/blog/most-secure-messaging-apps/.

[163] N. Mott, "FBI Document Shows How Popular Secure Messaging Apps Stack Up," 2021. Accessed: Feb. 26, 2022. [Online]. Available: https://uk.pcmag.com/security/137344/fbi-document-shows-how-popular-secure-messaging-apps-stack-up.

[164] S. Bosman, "How criminals are tracked down on Telegram," 2021. Accessed: Feb. 25, 2022. [Online]. Available: https://www.cybersprint.com/news/how-criminals-are-tracked-down-on-telegram.

[165] Hannah Murphy, "Telegram emerges as new dark web for cyber criminals | Financial Times," 2021. Accessed: Feb. 25, 2022. [Online]. Available: https://www.ft.com/content/cc3e3854-5f76-4422-a970-9010c3bc732b.

[166] K. Worobec, "UK Finance 2 2021 Half year fraud update," 2021.

[167] "iSpoof - The Leading OTP and Spoof Calling Bot. Spoof SMS + Calls | RaidForums," 2021. Accessed: Jan. 13, 2022. [Online]. Available: https://raidforums.com/Thread-iSpoof-The-Leading-OTP-and-Spoof-Calling-Bot-Spoof-SMS-Calls.

[168] "MORTY OTP | $200/M | SPOOF CALLER! (VENMO/CHASE/COINBASE/ROBINHOOD) 75%+ HITRATE | RaidForums," 2021. Accessed: Jan. 13, 2022. [Online]. Available: https://raidforums.com/Thread-SELLING-MORTY-OTP-200-M-SPOOF-CALLER-VENMO-CHASE-COINBASE-ROBINHOOD-75-HITRATE.

[169] "Fraud Definitions Archive - Fraud.net," 2021. Accessed: Jan. 14, 2022. [Online]. Available: https://fraud.net/d/.

[170] J. E. Côté, "The Enduring Usefulness of Erikson's Concept of the Identity Crisis in the 21st Century: An Analysis of Student Mental Health Concerns," 2018. doi: 10.1080/15283488.2018.1524328.

[171] "Tornado.cash," 2022. Accessed: Feb. 22, 2022. [Online]. Available: https://tornado.cash/.

[172] S. Hamilton, "'My son had £6,000 stolen in NHS Covid pass scam,'" 2022. Accessed: Mar. 03, 2022. [Online]. Available: https://www.telegraph.co.uk/money/katie-investigates/son-had-6000-stolen-nhs-covid-pass-scam/.

[173] T. Havard, "Serious youth violence: County lines drug dealing and the Government response Summary 1 Background 2 County lines drug dealing 3 Government response 4 Police response," *House of Commons*, 2022.

[174] M. Evans, "'Betamax' police forces failing to recognise the digital 'crime challenges of today,'" 2022. Accessed: Mar. 01, 2022. [Online]. Available: https://www.telegraph.co.uk/news/2022/02/21/betamax-police-forces-failing-recognise-digital-crime-challenges/.

[175] National Crime Agency, "Cyber choices: Helping you choose the right and legal path," 2020. Accessed: Mar. 30, 2022. [Online]. Available: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyberchoices.

[176] Facebook, “Community Standards Enforcement | Transparency Center,” 2021. Accessed: Jan. 30, 2022. [Online]. Available: https://transparency.fb.com/data/community-standards-enforcement/.

[177] DCMS Committee, “Digital, Culture, Media and Sport Sub-committee on Online Harms and Disinformation,” 2022. Accessed: Jan. 23, 2022. [Online]. Available: https://committees.parliament.uk/committee/438/digital-culture-media-and-sport-subcommittee-on-online-harms-and-disinformation/.

[178] Z. Muhammad, “The EU Fined Tech Companies Over 1 Billion Euros in 2021 / Digital Information World,” 2021. Accessed: Mar. 02, 2022. [Online]. Available: https://www.digitalinformationworld.com/2022/01/the-eu-fined-tech-companies-over-1.html.

[179] C. Cavaglieri, “Bank transfer fraud victims lose £28,000 an hour – Which? News,” 2022. Accessed: Mar. 09, 2022. [Online]. Available: https://www.which.co.uk/news/2022/03/bank-transfer-fraud-victims-lose-28000-an-hour/.

[180] “TSB Fraud Refund Guarantee,” 2020. Accessed: Jan. 29, 2022. [Online]. Available: https://www.tsb.co.uk/Fraud-Prevention-Centre/Fraud-Refund-Guarantee/.

[181] H. Brennan, “£100,000 lost to scammers – yet TSB refuses to pay out,” 2022. Accessed: Feb. 03, 2022. [Online]. Available: https://www.telegraph.co.uk/money/consumer-affairs/100000-lost-scammers-yet-tsb-refuses-pay/.

[182] M. Elkin, “Crime in England and Wales: year ending September 2021,” 2022. Accessed: Mar. 05, 2022. [Online]. Available: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2021.

[183] “Scam - Which? Consumer Rights - Which?,” 2022. Accessed: Mar. 09, 2022. [Online]. Available: https://www.which.co.uk/consumer-rights/scams#latest-news.

[184] P. Walker, “Johnson and Patel’s claims about falling crime ‘misleading’, says UK watchdog | Crime | The Guardian,” 2022. Accessed: Mar. 02, 2022. [Online]. Available: https://www.theguardian.com/uk-news/2022/feb/03/johnson-and-patels-claims-about-falling-crime-misleading-says-uk-watchdog.

[185] C. Cavaglieri, “Banks denying refunds to scam victims who ignore new warnings – Which? News,” 2020. Accessed: Mar. 09, 2022. [Online]. Available: https://www.which.co.uk/news/2020/01/banks-denying-refunds-to-scam-victims-who-ignore-new-warnings/.

[186] M. Russon, “Ofcom asks phone networks to block foreign scam calls - BBC News,” 2021. Accessed: Mar. 05, 2022. [Online]. Available: https://www.bbc.co.uk/news/business-59032795.

[187] M. La Morgia, A. Mei, A. M. Mongardini, and J. Wu, “Uncovering the Dark Side of Telegram: Fakes, Clones, Scams, and Conspiracy Movements,” Nov. 2021, Accessed: Feb. 27, 2022. [Online]. Available: http://arxiv.org/abs/2111.13530.

[188] B. Gao *et al.*, “50 Tracking Counterfeit Cryptocurrency End-to-end,” 2020, doi: 10.1145/3428335.

[189] P. Xia *et al.*, “Don’t Fish in Troubled Waters! Characterizing Coronavirus-themed Cryptocurrency Scams,” 2020.

[190] “CryptoRefills » Buy Gift Cards and Mobile Top Ups with Bitcoin and Crypto,” 2021. Accessed: Feb. 27, 2022. [Online]. Available: https://www.cryptorefills.com/.

[191] “How KYC Helps Keep Users Safe in the EEA & UK | Binance Blog,” 2021. Accessed: Feb. 27, 2022. [Online]. Available: https://www.binance.com/en/blog/markets/how-kyc-helps-keep-users-safe-in-the-eea--uk-421499824684903175.

[192] “Government censorship of Telegram Messenger - Wikipedia,” 2022. Accessed: Mar. 05, 2022. [Online]. Available: https://en.wikipedia.org/wiki/Government_censorship_of_Telegram_Messenger.

[193] Action Fraud, “Money muling | Action Fraud,” 2021. Accessed: Mar. 20, 2022. [Online]. Available: https://www.actionfraud.police.uk/a-z-of-fraud/money-muling.

[194] “Scam Alerts | Which?,” 2022. Accessed: Jan. 30, 2022. [Online]. Available: https://campaigns.which.co.uk/scam-alert-service/.

[195] “Take Five - To Stop Fraud | To Stop Fraud,” 2022. Accessed: Jan. 30, 2022. [Online]. Available: https://www.takefive-stopfraud.org.uk/.

[196] “Authy Two-factor Authentication (2FA) App & Guides,” 2022. Accessed: Mar. 20, 2022. [Online]. Available: https://authy.com/.

[197] “Authentication – Google Safety Centre,” 2022. Accessed: Mar. 20, 2022. [Online]. Available: https://safety.google/authentication/.