TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Markus Joonas Palu 242729IVCM

MAPPING PANDEMIC EVENTS, ATTACKER ADAPTATION, AND PSYCHOLOGICAL MANIPULATION IN COVID-19 PHISHING

Master's Thesis

Supervisor: Kaido Kikkas
PhD,
Associate professor

Tallinn 2026

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Markus Joonas Palu 242729IVCM

PANDEEMIAGA SEOTUD SÜNDMUSTE, RÜNDAJATE KOHANEMISE JA PSÜHHOLOOGILISE MANIPULEERIMISE KAARDISTAMINE COVID-19 ANDMEPÜÜGIS

Magistritöö

Juhendaja: Kaido Kikkas

PhD,

Associate professor

Tallinn 2026

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis and that this thesis has not been presented for examination or submitted for defense anywhere else. All used materials, references to the literature, and work of others have been cited.

Author: Markus Joonas Palu

19.05.2026

Abstract

This thesis analyses the evolution of phishing and social engineering attacks throughout the COVID-19 pandemic from the perspectives of crisis context, attacker adaptation, persuasion, and human vulnerability. These components are examined together because they collectively contribute to phishing susceptibility. The current literature does not fully examine the interconnections between these elements and overly emphasises the technical approaches to defending against phishing attacks. This research addresses that limitation through a qualitative review and synthesis of academic literature, reports, institutional publications, and selected real-world examples on topics such as social engineering, psychology, and crisis-related susceptibility.

To examine this evolution, the analysis was organised into early, mid, and later pandemic stages to compare changes in context, narratives, and persuasive elements. The findings show a shift from early outbreak-related lures involving authority impersonation, uncertainty, scarcity, and urgent information needs, towards mid-pandemic remote-work, authentication, and e-commerce themes. The later-stage phishing themes mainly involved vaccine, travel, refund, and hybrid-work narratives. Across these stages, authority, urgency, scarcity, and routine legitimacy were the most prominent persuasive elements, which increased the perceived credibility, importance, and familiarity of the messages.

The findings led to the development of a conceptual framework linking crisis context, attacker adaptation, persuasive elements, target vulnerability, message plausibility, and compliance. The constructed framework helps understand crisis-related phishing as an interaction between these factors, while also explaining why certain messages become believable and persuasive under crisis conditions. The findings could help develop crisis-oriented cybersecurity awareness training in addition to defensive planning and preparations against phishing attacks during future crises.

The thesis is in English and contains 62 pages of text, 8 chapters, 1 figure.

Annotatsioon

PANDEEMIAGA SEOTUD SÜNDMUSTE, RÜNDAJATE KOHANEMISE JA PSÜHHOLOOGILISE MANIPULEERIMISE KAARDISTAMINE COVID-19 ANDMEPÜÜGIS

Käesolev lõputöö analüüsib õngitsus- ja manipuleerimisrünnakute arengut koroonapandeemia jooksul kriisikonteksti, ründajate taktikalise kohanemise, mõjutamise ja inimliku haavatavuse vaatenurgast. Kõiki nimetatud komponente analüüsitakse ühtse tervikuna, sest need kõik mõjutavad koos andmepüügi õnnestumist. Olemasolev kirjandus ei käsitle piisavalt nende faktorite omavahelisi seoseid ja keskendub liigselt tehnilistele kaitsemeetoditele. Selleks et siduda senises kirjanduses eraldi käsitletud vaatenurki, tugineb lõputöö kvalitatiivsele kirjanduse ülevaatele ja baseerub ka akadeemilisele kirjandusele, raportitele ja asutuste väljaannetele. Lisaks on valitud päriselulisi näiteid sotsiaalse manipuleerimise, psühholoogia ja kriisist tingitud haavatavuste kohta.

Et paremini mõista andmepüügi arengut, jaotati analüüs varaseks, keskmiseks ja hilisemaks etapiks, et võrrelda muutusi kontekstis, narratiivides ja mõjutamisvõtetes. Tulemused näitavad, et varajases etapis hõlmasid ründed autoriteedi imiteerimist, ebakindlust, piiratud kättesaadavust ja kiiret teabevajadust. Keskmises pandeemiaetapis keskendusid rünnakud rohkem kaugtöö, autentimise ja e-kaubandusega seotud teemadele. Peamised hilisema etapi andmepüügiteemad olid seotud vaktsiinide, reisimise, tagasimaksete ja hübriidtöötamisega. Psühholoogilisest ja mõjutamise perspektiivist esinesid kõigis etappides kõige sagedamini autoriteet, kiireloomulisus, piiratud kättesaadavus ja ootuspärasusest tulenev usutavus. Need aspektid aitasid muuta sõnumid usutavaks, oluliseks, ootuspäraseks või jätta mulje kui tavapärasest suhtlusest.

Tulemuste põhjal töötati välja kontseptuaalne raamistik, mis seob kriisikonteksti, ründajate taktikalise kohanemise, mõjutamise elemendid, inimeste haavatavuse, sõnumite usutavuse

ja soovitud tegevuse sooritamise. Loodud raamistik aitab kriisidega seotud andmepüüki paremini mõista nende tegurite koosmõjuna. Lisaks, see loob arusaama, miks teatud sõnumid muutuvad kriisiolukorras usutavaks ja veenvaks. Tulemused võivad aidata kujundada kriisipõhiseid küberturvalisuse teadlikkuse koolitusi ning toetada paremat ettevalmistust tulevaste kriisiolukorras esinevate andmepüügirünnakute vastu.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 62 leheküljel, 8 peatükki, 1 joonis.

List of abbreviations and terms

APWG	Anti-Phishing Working Group
BEC	Business Email Compromise
CDC	Centers for Disease Control and Prevention
ENISA	European Union Agency for Cybersecurity
FDA	Food and Drug Administration
IRS	Internal Revenue Service
NHS	National Health Service
PPE	Personal Protective Equipment
TTP	Tactics, Techniques, and Procedures
VPN	Virtual Private Network
WHO	World Health Organization

Table of contents

1 Introduction 11

1.1 Motivation 11

1.2 Research Problem 12

1.3 Research Goal 13

1.4 Research Scope 14

1.5 Research Questions 14

1.6 Novelty 15

2 Literature Review 16

2.1 Phishing and Social Engineering 16

2.2 Psychological Foundations of Phishing 17

2.2.1 Persuasion and Influence in Phishing 18

2.2.2 Crisis-related Susceptibility 19

2.3 Crisis Events and Cybercriminal Adaptation 20

2.4 Research Gaps 21

2.5 Conceptual Basis for the Framework 23

3 Methodology 25

3.1 Research Design 25

3.2 Data Collection 26

3.3 Source Selection Criteria 27

3.4 Analytical Approach 27

3.5 Framework Development Approach 29

3.6 Reliability, Limitations, and Ethical Considerations 30

4 Analysis of COVID-19-themed Phishing Evolution 32

4.1 Pandemic Stages and Phishing Context 32

4.2 Early Pandemic Phishing Narratives 34

4.3 Mid-pandemic Phishing Narratives 37

4.4 Later-stage Phishing Narratives 39

5 Psychological Analysis of Phishing during COVID-19 43
5.1 Authority and Institutional Legitimacy 43
5.2 Scarcity and Urgency 46
5.3 Routine Legitimacy 48
5.4 Integrated Analysis 50
6 Framework for Crisis-related Phishing Situations 52
6.1 Purpose and Rationale for the Framework 52
6.2 Structure and Core Elements of the Framework 53
6.3 Visual Representation of the Framework 56
6.4 Application of the Framework to the COVID-19 Case 57
6.5 Broader Applicability of the Framework 57
6.6 Limitations of the Framework 58
7 Discussion 60
7.1 Answers to the Research Questions 60
7.1.1 RQ1: Evolution of Pandemic-themed Phishing 60
7.1.2 RQ2: Influence of Pandemic-related Developments 61
7.1.3 RQ3: Psychological Vulnerabilities and Social Influence Factors 64
7.1.4 RQ4: Implications for Crisis-specific Awareness and Defence 65
7.2 Theoretical Implications 66
7.3 Practical Implications 67
7.4 Limitations 68
7.5 Future Research 70
8 Conclusion 71
References 73
Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis 79

List of figures

Figure 1. Conceptual framework of COVID-19-themed phishing effectiveness. 56

1 Introduction

COVID-19 could be seen as a disruptive event that emerged unexpectedly and affected the way people conducted their lives. As a result, it created ideal circumstances for the cybercriminals to exploit the situation due to the disruption in people's lives. The pandemic was a large-scale disruption in which there was a constant change in situational context, psychological vulnerabilities, and even the attack narratives throughout the pandemic. The attackers also exploited these emerging conditions by adjusting their strategies accordingly. Hence, this thesis analysed how social engineering and phishing have evolved during the pandemic.

1.1 Motivation

As the coronavirus pandemic progressed, so did the tactics used during phishing and social engineering attacks. The attacks increasingly became related to the current crisis situation and the current concerns people were facing. In order to continue routine interactions uninterrupted in such conditions, work, education, travelling or health-related interactions shifted online. This created new societal needs for digital communication. In such an uncertain situation, cybercriminals would constantly change their techniques that would take advantage of the rapid social and digital change [1] [2]. Their attacks evolved based on the psychological vulnerability of people and their digital dependence [3]. At the same time, attacks reflected the current events, which were highly related to the surrounding situation [1].

Humans remain the weakest link in cybersecurity, and became even weaker during the pandemic. This meant that pandemic-themed phishing and social engineering attacks became even more prominent. This is reflected in the report by Anti-Phishing Working Group (APWG), a major international organisation focused on phishing monitoring. Their report highlighted a significant rise during 2020 [4]. Additionally, the beginning of 2022 is described as the worst quarter the organisation had ever seen [5]. The

success can be explained by the situational message design. Particularly, the type of message that the attackers used varied depending on the context in which the attack took place. Cybercriminals leveraged themes such as health warnings, government messages, financial aid, and work-from-home communications [1] [6]. In each case, the attack was contextualised depending on the ongoing situation and expectations.

The pandemic led to a rapid adoption of technology in the workplace and daily routines. As people had to suddenly get adjusted to the new conditions, it highlighted human weaknesses that cannot be protected by any technological measures. Due to these new circumstances, people found themselves suffering from stress, isolation, and information overload [7]. Therefore, under the psychological pressure, people became more prone to manipulation. Cybercriminals used psychological and contextual phishing scams to take advantage of this [3]. Not only were these messages manipulative, but also persuasive. Attackers would rely on elements of influence such as authority, urgency, scarcity, helpfulness that made the messages convincing [8] [9]. Analysing the evolution of such tactics throughout the pandemic will help better understand the reason behind their efficiency.

This problem is significant as it raises questions about society's preparedness for the sudden transition to virtual environments [10]. During that time, there was an urgent need for social distancing, but this proved to be a challenge. This became difficult because some activities necessary in daily life were reliant on social interactions. In this case, it became necessary for people to start performing their tasks using digital platforms. Cybercriminals realised this vulnerability and successfully capitalised on this opportunity. This creates a demand for research that analyses the connection between crisis context, attacker adaptation, and psychological vulnerability. It is important to note that the proposed approach could provide a basis for future research and development during crises.

1.2 Research Problem

A considerable amount of research has been developed on detecting and mitigating phishing attacks using technical measures, including machine learning classification, domain analysis, and automated content filtering [1]. While these technical countermeasures play an essential role in identifying phishing patterns, they do not provide a complete understanding of why phishing attacks succeed [11]. The reasons behind people's vulnerability to phishing

attacks are not exclusively technical, but also involve psychological, behavioural, contextual, and situational factors [12] [13].

Furthermore, COVID-19 phishing is often examined either as a static phenomenon or through limited parts of the pandemic. This makes it difficult to analyse how attacks, persuasion strategies, and psychological triggers evolved over time. Although such studies provide valuable insights, individual analyses do not fully explain the broader development of coronavirus-related phishing attacks. Constructing a more integrated analysis is therefore necessary because phishing attacks changed depending on the developments and crisis conditions of the pandemic. Without this knowledge, it remains unclear how pandemic evolution affected attacker strategy and victim vulnerability. To address this gap, the pandemic stages should be analysed in relation to the psychological vulnerabilities exploited and the ways in which attackers adapted their techniques.

Similarly, phishing research does not always integrate psychological and behavioural factors in enough depth. This makes it difficult to explain how persuasive mechanisms, social influence, and situational pressure affect vulnerability to phishing. Consequently, a thorough study of COVID-19-themed phishing requires stronger attention to these aspects.

Lastly, if phishing strategies are not connected to pandemic-related developments, it remains difficult to explain how attackers adjusted their methods to exploit changing crisis conditions and psychological vulnerabilities. Such understanding can support the development of more context-specific awareness programmes and defensive strategies.

1.3 Research Goal

The objective of this thesis is to analyse how COVID-19-themed phishing and social engineering attacks evolved across different stages of the pandemic. Moreover, the goal is to investigate the changes in attackers' narratives, techniques, and persuasion under the shifting circumstances of the COVID-19-related developments. The study then aims to examine the psychological and behavioural vulnerabilities exploited in these attacks. Then, it seeks to interpret them through a systematic understanding of the psychological and persuasive factors. Based on this analysis, the thesis seeks to develop a conceptual framework that explains the relationship between crisis context, attacker adaptation,

persuasive mechanisms, and human susceptibility to phishing. Eventually, the study aims to produce insights that can support the development of more crisis-specific cybersecurity awareness, defensive strategies, and response measures.

1.4 Research Scope

The thesis concentrates mainly on the period of the COVID-19 pandemic and studies the instances of phishing and social engineering attacks between 2020 and 2023 that explicitly leveraged pandemic-related themes. The study analyses how these attacks progressed in response to changing pandemic conditions, with particular attention to attacker adaptation, psychological vulnerabilities, and persuasive strategies. The research is conducted through a structured review and qualitative synthesis of existing sources, including academic publications, cybersecurity reports, and publicly available datasets. The study does not involve primary data collection or experimental work. Instead, it synthesises and connects existing findings from multiple sources.

Furthermore, to gain a more thorough understanding of human behaviour and psychological manipulation, the study also considers pre-pandemic and post-pandemic research in psychology, behavioural science, persuasion, and cybersecurity. The use of these additional sources helps contextualise the findings and strengthen the analysis of crisis-themed phishing and social engineering, particularly in relation to influence mechanisms and user susceptibility. Even though the primary emphasis of the study is the pandemic era, these secondary sources contribute to a comprehensive understanding of how crisis conditions influenced phishing strategies and user susceptibility.

1.5 Research Questions

RQ1: How did pandemic-themed phishing and social engineering attacks evolve across different stages of the COVID-19 pandemic?

RQ2: How did major pandemic-related developments influence phishing narratives, delivery methods, and persuasive techniques?

RQ3: Which psychological vulnerabilities and social influence factors were exploited in relation to different pandemic stages and phishing techniques?

RQ4: How can understanding crisis-driven phishing adaptation and psychological manipulation support the development of crisis-specific cybersecurity awareness and defensive strategies?

1.6 Novelty

The novelty of this thesis comes from its event-oriented analysis of COVID-19-themed phishing and social engineering attacks. Existing literature often examines pandemic-related cyberattacks, psychological vulnerabilities, and persuasive strategies as separate topics. In contrast, this study brings these elements together by analysing how pandemic-related developments, attacker adaptation, persuasive strategies, and human susceptibility interacted throughout different stages of the crisis.

The thesis provides a structured analysis between pandemic-developments, phishing narratives, attack techniques, and the psychological vulnerabilities. Rather than treating pandemic-themed phishing as a static phenomenon, the study examines how attacker strategies evolved in response to changing crisis conditions. Particularly, how these changes were reflected in the persuasive and psychological dimensions of phishing campaigns. In this way, the thesis provides a contextual understanding of why phishing attacks changed during the pandemic and why they were effective under different crisis conditions.

In addition, the thesis contributes by developing a conceptual framework that links crisis developments, attacker behaviour, persuasive mechanisms, and human susceptibility. This contribution goes beyond descriptive analysis by offering a structured way to understand how phishing and social engineering adapt in crisis contexts. Although the framework is developed through the COVID-19 case, it may also support future research and the design of crisis-specific awareness measures, defensive strategies, and cybersecurity responses in other large-scale disruptions.

2 Literature Review

Phishing is a major and persistent cybersecurity threat because it exploits not only technical conditions but also human behaviour and decision-making. Research shows that phishing remains effective by taking advantage of user vulnerabilities, trust in digital communication, and social or contextual information that can make deceptive messages more convincing [14] [15].

2.1 Phishing and Social Engineering

Even though there are slight differences in how phishing is defined, the existing literature offers a consistent understanding of phishing. To be exact, phishing can be viewed as a deceptive practice in which an attacker impersonates a trusted entity in order to obtain valuable information from a target [14] [16]. Based on the existing literature, deception, impersonation, and the acquisition of information, are emphasised as the main elements of phishing [15] [16].

Social engineering is a broader concept than phishing. It refers to the manipulation of individuals through psychological persuasion in order to gain access to information, systems, or other assets that the attacker should not be able to obtain [17]. Instead of attacking technical systems directly, social engineering focuses on individuals by exploiting cognitive, behavioural, and social vulnerabilities [17] [18]. The literature therefore describes social engineering as a psychological form of attack that seeks to persuade victims to act as intended by the attacker [18]. This persuasion often relies on trust, authority, urgency, fear, and other human tendencies [17].

Phishing can be understood as a specific form of social engineering because it applies this broader logic of psychological manipulation through deceptive digital communication [18]. While social engineering refers more broadly to influencing people's behaviour in order to gain access to information, systems, or other assets, phishing does so through deceptive messages [17] [18]. These messages rely on impersonation and persuasion to

prompt the target to act in the attacker's interest [17] [18]. The Anti-Phishing Working Group (APWG), a major international organisation focused on phishing monitoring defines phishing similarly to the previous authors [19]. Precisely, APWG defines it as a criminal mechanism that employs both social engineering and technical subterfuge to steal personal and financial information [19]. This definition further supports the view that phishing should be understood not only as a technical threat, but also as a form of social engineering. Features commonly observed in phishing messages, such as authority, urgency, scarcity, and social proof, therefore function as persuasive mechanisms. They are used to influence the target's behaviour and increase the likelihood that the target will comply with the attacker's request [17] [18]. In conclusion, this thesis understands phishing as a deceptive form of social engineering in which an attacker impersonates a trusted source to obtain information or prompt action from the target.

2.2 Psychological Foundations of Phishing

Phishing is both a technical and a psychological threat because its effectiveness relies on manipulating people into performing actions that benefit the attacker [20]. Rather than only relying on technical compromise, phishing also exploits human judgement, attention, and behaviour, especially in situations where security is not their main priority [20] [21]. Existing literature also suggests that phishing is more likely to succeed when people rely on intuitive thinking rather than more careful analytical thinking [20]. Moreover, phishing often works when individuals lack the knowledge needed to detect warning signs [20] [21]. It is important to note that in spite of existing technical measures being present, the user often becomes the last line of defence once a phishing message reaches its target [20]. All in all, a clear understanding of phishing requires attention to both its technical mechanisms and the cognitive and behavioural vulnerabilities that attackers exploit [20] [21].

The reason behind the success of phishing is often due to the deceptive message design as well as the vulnerabilities and situational conditions of the target. Wang et al. state that attacks operate through the interaction between attack methods, exploited psychological vulnerabilities, and what triggers those vulnerabilities [13]. In this sense, phishing does not succeed simply because of a deceptive message. It is designed to persuade, manipulate, or influence the target [13]. The effectiveness comes from the judgement affected by

distraction, lack of security awareness, habitual behaviour, emotional arousal, or mental shortcuts [13]. Also, an attack may appear more credible when it is framed within a socially relevant or current context which makes the message appear more expected, meaningful, or urgent [22]. In conclusion, phishing should be viewed as a form of social engineering in which compliance depends on both the persuasive attack design and psychological and situational susceptibility of the target [13] [22].

2.2.1 Persuasion and Influence in Phishing

Persuasion is a key element of phishing effectiveness because in addition to involving technical deception, target's behaviour is influenced in a way that benefits the attacker. The literature describes social engineering as persuasive by nature with a goal of influencing people to act in the attacker's interest [17] [18]. From this perspective, phishing is not only meant to deceive, but also to encourage compliance through messages that appear legitimate, credible and relevant to the recipient [18] [19]. Research also suggests that these attacks are often designed to trigger quick or automatic responses, and make closer inspection less likely [18] [20]. Persuasion is therefore important for understanding phishing because it helps explain how exactly attackers influence decision-making and achieve compliance even with technical protections in place [17] [18].

A useful supporting framework for analysing persuasion in phishing is Robert Cialdini's theory of influence, which identifies six principles that shape human compliance: authority, scarcity, social proof, liking, reciprocity, and commitment/consistency [9]. This framework was not developed specifically for cybersecurity but is still highly useful in analysing persuasive mechanisms in phishing. It helps explain how deceptive messages lead to immediate responses without careful examination [23]. In the contexts of social engineering and phishing, these principles help explain how attackers influence behaviour by making the messages more credible and by making intuitive responses more likely [2]. This is especially visible in phishing messages that focus on authority, scarcity, or social proof. This may involve impersonating trusted institutions, presenting limited-time opportunities, or making it appear that others are already acting in the same way [2] [23].

In practice, phishing messages often rely on a smaller set of persuasive principles that make requests appear more credible and urgent. The literature shows that phishing frequently

relies on authority, urgency or scarcity, and social proof to make deceptive messages appear legitimate and to encourage quick responses [2] [23]. Attackers usually create authority by impersonating trusted institutions such as health agencies or government bodies [2] [9]. In addition, scarcity and urgency are introduced through limited-time offers, deadlines, or warnings requiring immediate action [2] [9]. Social proof is present when messages indicate that others have already responded or participated, which strengthens the legitimacy of the request [23].

Additional principles are also present in phishing, where they support the same persuasive goal. Reciprocity can be created through offers of assistance, rewards, or free services that create a sense of obligation [2] [23]. Liking and familiarity are supported by the imitation of trusted brands, warm language, and familiar visual or social cues [2] [23]. Attackers may exploit commitment and consistency by first making a small request and then encouraging further action once the target has already responded [9] [23]. Overall, these patterns show that phishing messages do not only depend on deception, but also on identifiable persuasive mechanisms to turn attention into trust and trust into action.

2.2.2 Crisis-related Susceptibility

Crises can create conditions where careful evaluation becomes more difficult, increasing susceptibility to phishing. Research shows that crisis situations create instability and stress, which can affect mental well-being and make people more vulnerable to social engineering [8]. In such situations, people may be less likely to detect phishing because their cognitive attention is focused more on the emergency itself than on identifying deceptive messages [24]. Feelings of uncertainty, fear, and stress can further worsen this vulnerability, which can reduce mental focus, impair judgement, and make it harder to evaluate deceptive messages critically [8] [24]. As a result, crisis-related panic and distraction can reduce careful assessment and increase the credibility of urgent messages [24] [25].

The literature also indicates that phishers exploit crises in an opportunistic way [8] [25]. This is done by linking messages with current events, public announcements, and urgent information needs, making those messages appear more meaningful and relevant to the target [8] [25]. Findings from the COVID-19 period suggest that higher levels of fear, anxiety, and stress were connected to increased vulnerability to both pandemic-themed

and common phishing scams [24]. In crisis situations, messages offering immediate relief, safety, or guidance are more likely to gain trust and compliance, especially if the messages are associated with authoritative institutions [8] [24]. Heightened emotions and reduced attention during a crisis affect overall vulnerability and also the way how phishing messages are perceived and responded to [24] [25].

Disruption during a crisis can create opportunities for attackers because it increases dependence on timely information, guidance, and assistance [8] [25]. The sudden shift to remote work and growing dependence on digital platforms, messaging platforms, and online communication changed everyday routines and also increased vulnerability to phishing opportunities [26]. Under these circumstances, digital security may receive less attention [8]. This is because people give greater priority to immediate problems and short-term needs, especially when health, safety, or financial stability are affected [8]. As a result, attackers can more easily match phishing lures to the concerns, needs, and priorities that arise during a crisis [8]. In conclusion, these conditions help explain why certain phishing themes became especially convincing at different stages of the pandemic.

2.3 Crisis Events and Cybercriminal Adaptation

Cybercriminals quickly adapt to various crisis events by treating them as evolving opportunities for phishing campaigns that match the ongoing context and current developments. According to the literature, crises can make conditions more favourable for attacks by disrupting normal routines, increasing uncertainty, and increasing public demand for information, guidance, or financial aid [25]. Instead of developing completely new attack methods, cybercriminals usually transform familiar phishing patterns to fit recent developments, public announcements, and media attention [1] [25]. This means that attacker adaptation follows the evolving public and institutional context of the crisis [8] [25]. Phishing lures are then shaped around the events and responses that are the most relevant at that time [8] [25].

In practice, this adaptation can be seen in the changing phishing narratives [25], impersonation strategies [8], and delivery methods [1]. Literature also shows that attackers repeatedly changed these elements to match the main concerns present at different moments of the crisis [8] [25]. Cybercriminals also impersonated various authoritative institutions

that were the most relevant to the current stage of the crisis. Various such examples include health authorities, government agencies, trusted companies, and essential service providers [1] [25]. Moreover, delivery methods and technical execution also changed, as phishing campaigns used channels such as email, SMS, and messaging platforms [1] [25]. Techniques such as obfuscation, malware delivery, or ransomware payloads were used to make attacks more effective and stay undetected [1] [25]. These types of patterns indicate that adaptation to crisis conditions involves more than just message content, but also sender impersonation and delivery strategy [1] [8].

Over the course of the crisis, phishing narratives also changed so that they reflected public concerns, routine activities, and psychological needs. The existing literature shows that early phishing campaigns mainly focused on health, safety, and outbreak-related themes, including protective equipment, medical guidance, and information about the spread of the virus [1] [25]. These themes were effective because they matched the public's need for fast and reliable information during the chaotic early stage of the crisis [8].

Early phishing campaigns mainly focused on health, safety, and outbreak-related themes. These included medical goods such as face masks [1], protective equipment fraud and fake protection guidance impersonating the WHO or NHS [25], and messages impersonating government authorities about high-risk locations or new COVID-19 cases [8]. As lockdowns continued and the economic impact worsened, phishing themes increasingly became related to financial relief, refunds, emergency financial support, and other money-related narratives linked to immediate basic needs [8] [25]. In the later stages, phishing narratives became broader and started to include product offers, testing, and screening-related messages [25]. Other sources also identify related phishing themes involving advertisements, business information, reopening, and regulations [1] [8]. This type of stage-based evolution suggests that cybercriminal adaptation was closely connected to changing needs and expectations throughout the pandemic [1] [8]. This adaptive pattern helps construct the analysis of how COVID-19-themed phishing narratives evolved over the course of the pandemic.

2.4 Research Gaps

While existing literature offers important knowledge about phishing, cybercrime, and social engineering, it does not bring these elements together as an integrated framework.

Nowakowski also mentions a similar gap that social engineering TTPs are well-researched but the main gap is a comprehensive and holistic framework that would put all of those granular elements together [27]. Specifically, there is a lack of a conceptual framework for explaining how exactly crisis context, attacker adaptation, persuasion, and human susceptibility interact. Research has often treated these elements separately, for example by focusing on victim characteristics, message features, or technical attack processes, instead of understanding how they relate to each other [23] [28]. Studies on social engineering also suggest that existing frameworks are often too focused on technical aspects or too fixed in structure to explain changing attacker behaviour [27]. The problem is that the existing literature does not provide an integrated analytical framework that shows how crisis conditions change attacker behaviour, persuasive strategies, and target vulnerability together [23] [27].

A related gap in the literature is the limited attention given to how COVID-19 phishing developed over time. Specifically, there has been a lack of stage-based analysis of COVID-19 phishing over the course of the pandemic. Much of the existing research focuses on short time periods, early-pandemic observations, individual cases, or specific themes, with findings often confined to certain aspects of the pandemic [10] [29]. This makes it difficult to understand exactly how phishing narratives changed over time as the crisis was evolving. J. Laan et al. have also pointed out that the longer-term development of phishing is underexplored [29]. There is a need for more complete datasets to examine if specific themes increased, decreased, or even changed across different stages of the pandemic [29]. Related work also indicates that cybercrime should be understood as an evolving process rather than a set of isolated events [23] [27]. Yet, this way of understanding cybercrime is still not consistently used in COVID-19 phishing studies [23] [27]. As a result, the existing literature still lacks a clear analytical explanation of how phishing developed throughout the pandemic and how narratives were influenced by various stages of COVID-19 [1] [29].

A further gap in the literature is about the limited integration of psychological and behavioural theory into the analysis of phishing and social engineering. Human factors are often mentioned in the literature and analytical frameworks, but there still exists a heavy focus on technical aspects [23] [27]. As a result, the psychological mechanisms that make these attacks effective are not fully explained or understood [23] [27]. An earlier study

on scams also describes the literature as lacking more comprehensive analysis [28]. This study points out that it is weak in explaining the cognitive and motivational processes that are shaping victim responses [28]. There exist studies that apply broader psychological theories of fraud for interpreting phishing or scam contexts without providing new empirical evidence for supporting that [28]. Thus, phishing analysis still does not consistently explain how persuasive cues, cognitive processes, and situational pressures work together to shape compliance during crises [23] [27].

A final gap in the literature is that there is a priority placed on technical detection and mitigation, while less attention is given to explaining why phishing is successful, specifically under crisis-related conditions. According to research around surveys, phishing studies often place an importance on anti-phishing techniques, filtering, detection, and prevention [30] [31]. Other authors have similarly described that the emphasis is often on technical aspects while human factors are overlooked [12] [32]. Less attention is given to the human and psychological factors that help explain the reason why attacks succeed [30] [31]. The social engineering literature further suggests that major analytical frameworks still place too much emphasis on technical aspects. As Nowakowski [27] points out, only 6 of the 200 MITRE ATT&CK techniques directly refer to social engineering, which leaves the important human, cognitive, and situational factors in the background. Research on scams has similarly suggested that the literature pays too much attention to technical issues and solutions rather than on the processes that explain victim response [28]. Detection and mitigation are still important parts of phishing research. However, the existing literature does not explain clearly the reason behind the success of phishing under the conditions of uncertainty, stress, and disruption. Under these conditions, psychological and behavioural vulnerability becomes more important [27] [30].

2.5 Conceptual Basis for the Framework

According to the reviewed literature in this chapter, COVID-19-themed phishing should not be understood through isolated factors alone. Instead, the existing literature suggests that it is important to examine the relationship between factors such as crisis context, attacker adaptation, persuasive mechanisms, and human susceptibility. Existing research has often treated these elements separately, which makes it difficult to develop a clear

understanding of why phishing succeeds in crisis conditions [8] [23]. This gap is also reflected in Nowakowski's research, who highlights the lack of comprehensive frameworks for understanding social engineering tactics [27]. Also, according to Kaliňák, research on phishing psychology has mainly focused either on persuasive techniques or on human susceptibility, rather than bringing these together [8]. Lastly, another study describes the need for a more holistic and process-oriented understanding of cybercrime [23].

Based on the observations made in the existing literature, the conceptual framework of this thesis links crisis-related developments to the previously discussed interconnected factors. Crisis conditions shape both the opportunities for cybercriminals and the conditions that affect potential targets. The effectiveness of phishing emerges through the way the interaction of these elements. This thesis brings together the identified elements in the literature review that have been treated separately. Together, these elements provide the foundation for the framework developed later in the thesis.

3 Methodology

This chapter explains the methodological approach used to analyse COVID-19-themed phishing and social engineering during the pandemic. The study is based on a qualitative review and synthesis of existing academic literature, cybersecurity reports, institutional publications, and selected real-world examples. The chapter describes how the source material was collected and selected, how the analysis was organised across pandemic stages, and how the findings were used to develop the conceptual framework. It also discusses the reliability, limitations, and ethical considerations of the research approach.

3.1 Research Design

This thesis uses a qualitative literature review to explore how COVID-19-themed phishing and social engineering attacks changed across different stages of the pandemic. The study analyses the connections between pandemic-related developments, attacker adaptation, persuasive strategies, and the psychological vulnerabilities exploited in phishing campaigns. Primary data collection is not included in this study. Instead, the study is based on existing academic literature, cybersecurity reports, and other relevant secondary sources. The secondary sources are reviewed to identify and interpret patterns throughout the pandemic.

A qualitative and literature-based approach is suitable because the research questions examine change over time, changing pandemic conditions, persuasion, and human susceptibility. These questions are better explored through interpretations instead of statistical results from one dataset. Investigating this topic requires multiple types of sources to identify recurring patterns in phishing narratives, delivery patterns, influence mechanisms, and crisis-specific behavioural vulnerabilities. This approach also makes it possible to compare how phishing campaigns changed over the course of the pandemic and how these changes were influenced by broader social and crisis-related factors.

The goal of this research design is to move beyond describing the material, but to also provide

interpretation and analysis of the material. In addition to reviewing existing literature, the study aims to organise and synthesise the literature into a stage-based understanding of COVID-19-themed phishing. The study also examines phishing techniques from a psychological and persuasion-based perspective. Based on this synthesis, the thesis develops a conceptual framework that brings these findings together into one explanatory model.

3.2 Data Collection

The source material for this thesis was collected from various academic and professional sources. Academic publications were found through Google Scholar, IEEE Xplore, ScienceDirect, SpringerLink, and ResearchGate. In addition, a few sources were also found through targeted web searches to find relevant institutional and professional sources from reputable organisations such as the Anti-Phishing Working Group (APWG), the World Health Organization (WHO), Europol, and similar organisations. Combining these source types helped provide both academic and practical context for analysing COVID-19-themed phishing and social engineering.

Source collection was iterative and developed alongside the research process. Initial searches focused on broad literature related to COVID-19 phishing, pandemic-related social engineering, phishing psychology, and persuasion. As the study became more focused, additional searches were conducted on phishing across early, middle, and later stages of the pandemic, as well as on themes linked to specific pandemic-related developments and contextual changes. Further material on phishing psychology, social engineering, and broader psychological vulnerability was also collected in order to support the theoretical and analytical parts of the thesis. Searches also included terms related to specific psychological vulnerabilities and crisis-related emotional states, such as anxiety, uncertainty, and information fatigue to better explain phishing susceptibility under pandemic conditions. In addition to direct searching, backward snowballing was used throughout the process by examining the reference lists of relevant papers to identify further suitable sources.

3.3 Source Selection Criteria

Sources were selected based on their relevance to the research questions and the main focus areas of the thesis. The selection process included both academic and professional sources. Academic publications were prioritised where they offered theoretical, empirical, or analytical value for the study. Professional reports and institutional publications were included when they provided relevant evidence on COVID-19-themed phishing, attacker adaptation, impersonation patterns, delivery methods, or crisis-related cybercrime activity. Sources including unclear relevance or insufficient credibility were not used for writing this thesis.

Regarding the selected coronavirus-themed phishing and social engineering material, the publication year boundary was 2020-2026. This period was selected to gather relevant information created during the time of the pandemic. However, there were no such boundaries for the materials regarding the broader literature on phishing, social engineering, persuasion, or psychology. Earlier literature was used where it contributed to the theoretical and conceptual background of the thesis. Blog posts and news reports were considered only when they offered practical examples of phishing activities and narratives. They were only used as supporting contextual material or for illustrating specific phishing examples.

3.4 Analytical Approach

The analysis of this thesis was based on a qualitative synthesis and comparative interpretation of the selected literature. The sources were carefully selected, after which the material was examined in order to identify repeating patterns related to coronavirus themed phishing and social engineering. Particular attention was given to patterns such as phishing narratives, persuasive techniques, and human vulnerabilities. These key elements were analysed in relation to how the pandemic developed over time. This approach was suitable because the aim of the study was precisely to compare and interpret changes throughout different stages of the pandemic. The analytical approach was intended to move beyond just describing existing literature. Rather, the analysis focused on interpreting how phishing evolved during the pandemic and how this evolution was shaped by the surrounding crisis context.

The selected material was then organised into early, mid, and later stage stages of the

pandemic. However, it should be emphasised that these stages were used as analytical categories rather than as strict chronological periods. The early stage is connected to the initial outbreak where uncertainty, urgent need for health information, and official announcements were the central topics. The mid-stage refers to the normalisation of pandemic-related routines as restrictions continued. Remote work, online communication, authentication practices, and delivery-related routines became the main themes. The later stage mainly revolves around the gradual reopening of society in which vaccination, certificates, travel, and hybrid work became more relevant. This was necessary because pandemic developments did not occur at the same time or in the same way across all countries, sectors, and organisations. The purpose of dividing the pandemic into stages allowed for a more accurate analysis of how phishing changed. Particularly, the analysis focused on changes in pandemic developments, digital dependence, everyday routines, and the concerns and expectations of recipients.

Within each of the pandemic stage, the analysis focused on four connected elements. First, the main pandemic developments were identified to clarify the conditions that shaped phishing activity during that stage. Secondly, the changes in behaviour and use of digital dependence were examined, such as changes in work practices, and reliance on digital services. Third, the most prominent phishing narratives, impersonation themes, and lures reported in the literature were analysed. Lastly, these phishing themes were explained in relation to the surrounding context. The final step was necessary for understanding why particular messages were believable or persuasive at that specific stage of the pandemic.

The stage-based analysis of phishing identified how phishing attacks and adaptation patterns changed across the pandemic. These findings were then interpreted using the psychological and persuasion-related concepts discussed in the literature review. This interpretation was important because it helped explain how phishing campaigns exploited changing crisis conditions, digital routines, institutional trust, and psychological vulnerability. Overall, this analytical approach supported the main aim of the thesis by providing a structured way to compare phishing evolution across the pandemic, interpret the relationship between crisis developments and attacker adaptation, and prepare the basis for the conceptual framework developed later in the study.

3.5 Framework Development Approach

Overall, the framework was developed by analysing the existing literature and based on the findings, bringing together the main patterns and identified relationships. Rather than beginning with a fixed model for the framework, it was gradually formed from the relationships that became visible during the research process. These relationships linked crisis context, attacker adaptation, persuasive elements, target vulnerability, and message plausibility. As the connections became clearer, they were applied into a structured analytical model. The purpose of this approach was to explain how crisis-related phishing becomes believable and persuasive under changing crisis conditions.

The initial step for constructing this framework was to examine the researched material for recurring connections between pandemic developments and phishing activity. The sources were not only analysed for the certain phishing examples they described, but also for the reason why these attacks made sense in that particular pandemic situation. This involved paying careful attention to the type of ongoing pandemic event involved as well as the institutions or services being imitated and the communication channels used. Moreover, it also involved considering the social or psychological conditions that made these messages appear relevant to the target.

As a second step, these relationships were examined across the early, mid-, and later stages of the pandemic. This comparison helped identify which aspects changed over time and which remained consistent. For example, specific phishing themes shifted from outbreak alerts and health guidance to remote-work communication, vaccine registration, certificates, and travel-related procedures. However, the same broad pattern remained consistent: attackers adapted their messages to the surrounding crisis context. These messages became more convincing when they matched the needs, expectations, fears, or routines of victims.

The third step was to connect these observed patterns with the psychological and persuasion-related concepts discussed in the literature review. This was a necessary step because the idea of the framework is to describe why the phishing messages could become persuasive and not only how they changed. Examples include authority, urgency, scarcity, routine legitimacy, trust, and uncertainty that were used to show how phishing messages gained credibility and contributed to compliance. These concepts not only help explain the role

of the attacker, but also explain the recipient's perspective in how these messages are perceived in a certain context.

The final step was to organise these identified relationships into a clear conceptual structure. This structure was constructed based on the identified relationships during the analysis. It was used to organise the findings into a coherent explanation of how crisis-related phishing became believable and persuasive under changing conditions. Using this approach made it clear that the framework remained grounded in the thesis analysis rather than being a separate or abstract model.

The framework is based on the outcome of the thesis analysis. It is not intended to measure phishing effectiveness statistically or to predict individual behaviour. Instead, its purpose is to provide a clear analytical structure about the phishing effectiveness that can emerge from the interaction between various crisis conditions. Particularly, the attacker adaptation, persuasive communication, and target susceptibility. Chapter 6 goes into more detail about the details of the framework and applies it to the COVID-19 phishing case.

3.6 Reliability, Limitations, and Ethical Considerations

The reliability of this study was supported by applying a consistent method for collecting, selecting, and analysing sources. The thesis relied on various kinds of literature including academic literature, cybersecurity reports, institutional publications, and selected real-world examples. The varied selection of sources was necessary to view coronavirus themed phishing from more than one angle to construct a comprehensive analysis. Sources were only included when they were directly relevant to the research questions and scope of the study. The research was done through the lens of phishing evolution, attacker adaptation, persuasive strategies and crisis-related susceptibility. The research was done in a way to avoid reliance on isolated examples and to focus on recurring patterns to be identified across different types of material.

Reliability was also supported by the structured organisation of the analysis. The sources that were selected were examined through the same main aspects of pandemic context, changes in digital behaviour, phishing narratives, and the psychological or persuasive factors that made the narratives effective. The use of early, mid-, and later pandemic

stages provided a consistent way to compare material across the pandemic period. Because the study is qualitative and interpretive rather than based on statistical testing, reliability depends on source selection, organisation of the material, and how the analysis was linked to the research questions.

The main methodological limitation is that the thesis is based on secondary sources. It also does not include interviews, surveys, experiments, or the collection of an original phishing dataset. Because of that, the analysis highly depends on the availability and quality of existing academic sources. Some campaigns may be better documented than others, especially if they were widely reported or detected by major cybersecurity organisations. In this way, less visible phishing activity may be underrepresented. This means that the thesis can identify and interpret the most important patterns in COVID-19-themed phishing. It does not claim to provide a complete record of all phishing activity during the pandemic.

Another limitation is that the pandemic stages are used as analytical categories. The early, mid-, and later stages were used to organise the analysis and helped to compare contextual patterns. However, these stages are not to be understood as exact chronological boundaries. This is because pandemic developments were different across countries, sectors, and organisations. Moreover, some phishing themes overlapped between stages. For this reason, the stage-based structure is used as an interpretive tool rather than as a fixed timeline. This limitation is crucial because the study focuses on explaining relationships between crisis context and phishing adaptation. The thesis does not produce a precise chronological analysis.

This thesis is constructed in a way to avoid ethical risks as much as possible as it does not involve human participants, interviews, surveys, or personal data collection. The focus of the thesis is on publicly available and previously published material. Phishing examples are discussed only for analytical purposes to better understand attacker adaptation, persuasive mechanisms, and crisis-related vulnerability. This study does not provide instructions for creating phishing campaigns, bypassing security controls, or conducting social engineering attacks. Studies were selected and examples were presented in a way to support defensive understanding rather than misuse.

4 Analysis of COVID-19-themed Phishing Evolution

The following analysis examines how COVID-19-themed phishing evolved across the early, mid-, and later stages of the pandemic. In each stage, the analysis considers four connected elements: major pandemic developments, changes in social behaviour and digital dependence, the main phishing narratives and lures observed in that period. It then interprets why those narratives became plausible in that specific context.

4.1 Pandemic Stages and Phishing Context

This thesis analyses COVID-19-themed phishing through a stage-based approach. Rather than treating the pandemic as one uniform period, it is divided into early, mid, and later stages. Organising the pandemic periods into stages helps examine how changing social conditions, institutional responses, and patterns of digital dependence shaped phishing narratives over time. This division is important because phishing during COVID-19 did not remain static. Attackers adapted their themes, impersonation strategies, and persuasive framing in response to major pandemic developments and to the changing routines of potential targets.

The stages used in this thesis should be understood as analytical rather than strictly fixed chronological categories. Pandemic developments did not begin and end at the same moment in every country or sector, and some themes overlapped across periods. Nevertheless, a stage-based structure is useful because it captures broader shifts in the pandemic context. The early stage was marked by outbreak shock, emergency declarations, lockdowns, abrupt disruption, and urgent demand for health-related information. The mid-pandemic stage reflected longer-term adaptation, in which remote work, online study, platform-based communication, e-commerce, and other digital routines became more normalised. The later stage was shaped by vaccination rollout, vaccine certificates, travel reopening, and transitions towards hybrid or return-to-office working arrangements. These developments created different conditions of plausibility for phishing at different points in

the pandemic.

Using stages also helps connect phishing content to the social environment in which it appeared. In the early stage, fear, uncertainty, and information scarcity made health authority impersonation, outbreak alerts, tracking dashboards, and scarcity-related scams particularly persuasive. In the mid-stage, phishing became more closely embedded in ordinary digital routines, including remote logins, cloud services, collaboration platforms, delivery notifications, and routine account messages. In the later stage, phishing narratives increasingly aligned with administrative and recovery-oriented processes such as vaccine eligibility, registration, certificates, travel documentation, and workplace transition. Viewing these narratives through stages therefore makes it easier to explain not only what kinds of phishing themes appeared, but also why they appeared when they did.

This stage-based approach supports the central argument of the thesis that phishing during COVID-19 was shaped by the interaction between pandemic-related developments, attacker adaptation, and psychological manipulation. The pandemic altered everyday behaviour, increased dependence on digital communication, and created new forms of uncertainty, urgency, and institutional reliance. These changing conditions affected what kinds of messages users were likely to expect, trust, or respond to. As a result, the success and plausibility of phishing narratives depended not only on general social engineering principles, but also on whether the message matched the specific pandemic context of the time.

The purpose of dividing the pandemic into stages is therefore analytical clarity. It allows the thesis to compare how phishing narratives evolved from crisis-shock messaging to routine-looking digital lures and later to recovery- and verification-related deception. It also helps avoid presenting COVID-19-themed phishing as one consistent pattern. Instead, phishing is examined as adapting to changes in the pandemic context. This provides a clearer basis for the later analysis of early-, mid-, and later-stage phishing narratives and for understanding how broader crisis developments influenced attacker behaviour throughout the pandemic.

4.2 Early Pandemic Phishing Narratives

The early pandemic stage refers to the initial phase of COVID-19 marked by the outbreak, the rapid international spread of the virus, emergency declarations, lockdowns, and abrupt disruption of normal social and organisational routines. This stage was characterised by high uncertainty, strong need for information, and a sudden increase in digital dependence, creating conditions that attackers quickly exploited through health authority impersonation, outbreak-related alerts, tracking-map lures, and scarcity- or relief-themed phishing messages.

This phase was shaped by the rapid escalation of the public health crisis and by the speed with which cybercriminals adapted their activity to it. According to one source, the first reported coronavirus inspired cyber-attack followed only 30 days after the first case was announced in China, and subsequent attacks appeared at increasingly shorter intervals [25]. Another example involved a METALJACK phishing campaign launched against Wuhan district offices on 6 January 2020, showing that threat actors moved quickly to exploit situational urgency, topical relevance, and the credibility of official communication [33]. The WHO declaration of COVID-19 as a pandemic on 11 March 2020 appears to have been a particularly important turning point, with one source noting an initial surge in attacks on that date and highlighting that COVID-19-based attacks were more successful than typical phishing attacks [34]. More broadly, the literature indicates that the early stage of the pandemic showed a close relationship between major pandemic developments and rapid attacker response [1] [25].

At the same time, the early pandemic period brought major changes in social behaviour and digital dependence. COVID-19 was described as an unprecedented event that altered the lives of billions and contributed to a "new normal" in how people lived and worked [25]. As daily activities moved online, people increasingly depended on digital communication for work, education, leisure, shopping, and access to information [29]. This dependence was intensified by lockdowns, border closures, social distancing measures, and the abrupt transition to remote work and studying [26]. In many cases, this shift occurred with little preparation, limited training, and reduced opportunity for routine verification, which increased exposure to phishing attempts [26] [35]. The sudden growth in the use of digital platforms also created new opportunities for attackers. For example, Zoom usage increased

sharply as organisations and schools moved to remote communication, making digital platforms more attractive and credible targets for phishing and related scams [36].

The early stage was also characterised by strong public demand for information. Several sources describe the lockdown period as a period of ambiguity, information scarcity, and confusion about the new disease, with individuals actively seeking updates about virus spread, restrictions, and protective measures [2]. This need for information was also driven by uncertainty. It was further intensified by the broader COVID-19 "infodemic", in which an overwhelming amount of information and conflicting claims made it difficult to determine which sources were trustworthy [23] [37]. As one study notes, the co-existence of pandemic and infodemic conditions created an environment that was highly favourable to cybercriminal exploitation [23]. Increased internet use, uncertainty, and worsened mental well-being during the pandemic further heightened phishing risk [8].

Against this background, several dominant phishing narrative types can be identified in the early stage. One of the clearest patterns was the use of health authority impersonation. Multiple sources note that early phishing messages frequently impersonated the WHO, the CDC, the NHS, and other government or public health bodies [8] [26]. These messages often appeared as official health guidance, infection-prevention advice, or urgent outbreak-related notices. Early phishing therefore relied heavily on impersonating trusted authorities and presenting messages as official guidance. This matched the public's urgent search for trustworthy information and made such messages appear particularly believable in the first phase of the crisis.

A second prominent narrative involved infection maps, tracking dashboards, and outbreak-monitoring tools. As the spread of the virus became a matter of global concern, attackers exploited public interest in monitoring infections and deaths. One example involved malicious use of the Johns Hopkins COVID-19 dashboard theme [38], while another involved COVIDLock [39], an Android application disguised as a coronavirus heat map that functioned as ransomware. These lures were effective because they aligned with a strong desire for real-time information and situational awareness during a rapidly developing crisis.

A third early-stage pattern involved personal protective equipment and scarcity-related scams.

Sources indicate that phishing emails increasingly used terms related to masks, ventilators, chloroquine, vaccines, and other medical or protective equipment, with especially large increases in mask-related lures [29]. In some cases, email subject lines were disguised using real news headlines in order to attract attention and direct victims to fake online stores [1]. Fake PPE offers and mask promotions reflected the commercialisation of pandemic anxiety [25]. Moreover, these scams were plausible because many people were urgently looking for protective supplies that seemed limited or difficult to obtain during the early months of the crisis [25].

A fourth early narrative category consisted of relief, donation, and financial support scams. One study identifies financial benefits as one of the most common themes used to trick users into disclosing personal information, while donation-based messages exploited people's willingness to help during the crisis [2]. Additional examples included scams related to school-support scams [40]. Financial-support phishing also emerged around government stimulus payments. One source explains that phishers impersonated the IRS in order to exploit uncertainty over when stimulus funds would arrive [11]. This was done using phishing websites to steal credentials or social security numbers from users seeking payment-related information [11]. Some of these scams also used urgency cues, such as warnings that a claim would expire within a short period, in order to encourage immediate action [11]. These scams reflected the financial uncertainty of the early pandemic period and show that attackers adapted not only to health fears, but also to the economic and social consequences of the crisis.

These early phishing narratives fit the stage particularly well because they were closely aligned with the immediate conditions of the outbreak. Attackers took advantage of a context characterised by uncertainty, urgent information-seeking, disrupted routines, and rapid migration to digital environments. Official-sounding messages were more persuasive because people were looking for guidance from authorities, while outbreak trackers, health alerts, and PPE offers matched highly visible public concerns. At the same time, remote work and increased online communication made phishing attempts more plausible by moving employees into less familiar and less controlled digital environments [26]. Reduced informal verification between colleagues further weakened ordinary checking practices [35], while broader scam psychology suggests that social isolation can reduce the social

validation needed to evaluate deceptive messages critically [28]. Taken together, the literature suggests that early COVID-19-themed phishing was defined by rapid attacker adaptation to crisis shock, high informational demand, and the sudden restructuring of everyday digital behaviour.

4.3 Mid-pandemic Phishing Narratives

The mid-pandemic stage was marked by continued adaptation to pandemic conditions. Remote work and online study became routine, while digital platforms, cloud services, and remote access tools played a larger role in everyday operations [41] [42]. This shift was visible not only in workplaces but also in areas such as education and healthcare, where services increasingly depended on digital systems and remote interaction [43]. Overall, these changes made digital activities a more regular part of everyday life.

An important development was the growing normalisation of e-commerce, delivery services, and other online transactions. High levels of online shopping and internet-based service use continued after the initial emergency phase, suggesting that pandemic-related digital dependence was no longer limited to work alone [29] [44]. This is important for the phishing analysis because the mid-stage took place in a more stable online environment in which everyday tasks, communication, shopping, and service use were regularly carried out through digital platforms.

The mid-pandemic stage also involved changes in social behaviour and digital dependence. Remote work and online communication became more embedded in everyday life through increased reliance on digital tools such as videoconferencing, cloud services, and VPNs [45]. Moreover, online shopping and internet-based services became more common as routine activities shifted into digital environments [44]. This indicates that the mid-pandemic stage was marked not only by institutional adaptation, but also by the normalisation of online routines in work, study, and daily life.

Several developments shaped this stage. Remote settings reduced day-to-day interaction between co-workers, making it less likely that employees would ask questions or verify concerns, while unfamiliar technologies sometimes further disrupted the flow of information within organisations [35]. The boundary between personal and professional life also became

more blurred, with employees using work devices for personal activities and personal devices for work tasks, creating additional security risks [7] [35]. Research further suggests that home working could encourage more relaxed security behaviour, including shortcut-taking and less attention to standard security precautions [41] [46].

Three phishing categories stand out most clearly in the mid-pandemic stage. The first was remote work and account and login impersonation, including Office 365, login pages, credential prompts, VPN access, and expected or familiar security requests [46] [47]. The second was collaboration platform and work-related communication [25], including messages related to Teams, Zoom, Slack [35], internal coordination, and ordinary work-related email [7]. The third was e-commerce, delivery, and payment-related lures, such as fake orders, shipment notices, account messages, billing checks, and delivery payment scams [29] [48].

These themes were closely tied to established digital routines. Attackers increasingly exploited activities that had become normal parts of everyday life. Examples of such activities include logging in remotely, using communication platforms, checking work email, tracking deliveries, or responding to account-related notifications. Some additional examples, such as COVID-19 reward messages or vaccine-related lures, are relevant supporting cases, but the three categories above best represent the mid-stage patterns. A relevant supporting example was vaccine-related credential phishing during the vaccine rollout. One observed case involved a fake Pfizer-BioNTech website that asked users to log in with Office 365 credentials to sign up for vaccination. This illustrates how mid-stage phishing combined a current pandemic development with a familiar login-based lure [48].

These themes fit the mid-pandemic stage because they matched the digital routines that had become normal by this point. Users had become accustomed to remote logins, additional credential checks, platform-based communication, and frequent online transactions, making phishing lures become more plausible [46]. Attackers could therefore rely on familiarity and routine expectation rather than the unfamiliarity.

Remote work also reduced opportunities for quick in-person checking and made ordinary office practices harder to maintain in work-from-home environments, increasing reliance on just digital communication [41] [46]. This made work-related emails, platform messages,

and credential requests easier to accept as legitimate, especially when they aligned with employees' responsibilities or ongoing routines. In this sense, mid-stage phishing was effective because it blended into an environment already shaped by remote work, platform dependence, and normalised online activity.

4.4 Later-stage Phishing Narratives

During the later stage of the pandemic, the focus moved from initial emergency shock to more specific administrative and recovery-oriented developments. By this stage, phishing narratives were less centred on the first outbreak and more closely tied to vaccination, vaccine certificates, travel reopening, and changing workplace arrangements.

A major later-stage development was the approval and rollout of COVID-19 vaccines. From November 2020 to February 2021, public attention increasingly focused on vaccine effectiveness, government approvals, and deployment [49]. This shift became more particularly visible after Pfizer and BioNTech announced promising results and the FDA granted emergency use authorisation for the Pfizer vaccine in December 2020 [49]. Proofpoint likewise observed that attackers quickly adapted their lures to vaccine-related developments such as government approvals, vaccine logistics, and distribution to frontline groups [50].

These developments took place in a context shaped by pandemic fatigue. Pandemic fatigue has been shown to result in a decreased effort by the public to stay informed, which reduced the overall effectiveness of health messaging [51]. Simultaneously, the growing dependence on digital services meant that vaccination processes became primarily dependent on online registration systems [52] and digital communication became important for accessing health-related information and services [3]. Some users also shared sensitive vaccination-related information online, while cybercriminals created spoofed registration portals to collect personal and identification data [10] [52].

Several phishing narratives stood out in relation to vaccine rollout. One major pattern involved fake vaccine registration, eligibility, and appointment messages, including credential phishing campaigns linked to vaccine sign-up [49] [50]. A second pattern involved vaccine-related delivery and follow-up communication, including shipment-update phishing

and messages asking recipients to reconfirm delivery information [8] [50]. A third pattern involved impersonation and malware delivery using trusted brands such as the WHO and vaccine manufacturers, including targeted phishing aimed at organisations involved in vaccine logistics [50] [53]. The effectiveness of these lures relied on their alignment with official vaccine registration processes, including the use of sign-up forms [49], as well as distribution logistics and delivery notifications [50], which matched the public's expectations of the rollout process [8].

A second major later-stage development was the introduction of vaccine certificates, health passes, and other proof-of-vaccination systems. These were tied to reopening, mobility, public health control, and access to services. ENISA notes that when governments introduced COVID-19 vaccine travel certificates, cybercriminals were observed selling fake versions on the dark web [54]. Furthermore, the same source reports disinformation campaigns being focused on green passes, mandatory vaccination, health passports, mass immunity testing, and lockdowns [54].

These developments were accompanied by conditions that made certificate-related lures effective. By the later stage, digital tools had become deeply embedded in everyday life, while public debate intensified around vaccination mandates, access restrictions, individual rights, and mobility [10] [51]. In this context, proof-of-vaccination requirements became important points of access linked to travel, employment, and participation in daily life. Observed phishing and fraud narratives in this area centred on impersonation, credential harvesting, and document-related deception. In one example, the key issue was no longer obtaining vaccination, but proving vaccination status in order to move, enter, or participate, making certificate-related deception especially believable [10].

A third major later-stage development was the reopening of travel and the gradual restoration of mobility. The pandemic had a dramatic impact on travel behaviour worldwide, while international restrictions kept many aircraft out of service and created uncertainty around cross-border movement [55]. As borders reopened and vaccines slowed the spread of the virus, travel demand began to recover, and threat actors adapted by using travel as a phishing theme [56].

The reopening phase was accompanied by changes in social behaviour and digital de-

pendence. As restrictions eased during 2021 and 2022, many travellers reported feeling more in control of travel again, while uncertainty remained and many adapted by checking cancellation policies, purchasing insurance, buying flexible tickets, and planning more carefully in advance [57]. Travel decisions also depended heavily on digital systems [58], including booking systems and online information about entry requirements, testing rules, passenger locator forms, and COVID-19 certification systems [59].

Several phishing and fraud narratives stood out in relation to travel reopening. One major pattern involved airline, booking, and reservation scams, including travel-related phishing URLs and malicious domains using travel-related keywords [56]. A second pattern involved refund and cancellation scams, with attackers impersonating airlines, travel agents, and banks to obtain bank details and personal information under the pretext of processing refunds [60]. A third pattern involved travel documentation and entry-related scams, including fake vaccine passport messages and attacks involving passenger locator forms and other travel paperwork [60].

A further major later-stage development was the transition from emergency remote work towards return-to-office policies and hybrid working arrangements. Work patterns did not simply return to those that had existed before the pandemic. Instead they had developed into a mixed model in which some employees returned to offices, others continued to work from home, and many operated in hybrid arrangements [61]. In the United States, telework remained a significant part of working life in early 2022 and hybrid commuting models became more common, while in Europe telework declined as restrictions eased but hybrid work gained traction [62] [63].

These developments were accompanied by changes in social behaviour and digital dependence that made phishing related to hybrid-work plausible. Hybrid and telework models became more firmly established, while internet access, digital collaboration tools, and remote connectivity remained essential to everyday work performance [61] [63]. At the same time, the increasing number of applications, devices, authentication requirements, and digital processes contributed to increased digital fatigue [64] [65], while remote work increased exposure through personal devices, home networks, and bring-your-own-device practices [65] [66].

Several phishing and related attack patterns appear particularly relevant in this setting. Sanders has stated that phishing remained one of the most prominent forms of cyberattack in remote or hybrid work environments [62]. The author additionally noted that credential-stuffing attacks grew sharply in the post-COVID period, as the need for remote access increased the availability of exposed login information [62]. Related work also identifies email-based phishing as a leading cause of data breaches during work-from-home conditions. Attackers were exploiting trust in apparently legitimate senders [35], while access-related threats remained relevant [62] because authentication requests, logins, remote-access workflows, and account-related communications had become routine [35] [64]. A key point from the existing literature is that cybersecurity problems are not only caused by working from home, but also because of making changes in workplace arrangements. Authors of a study stated that individuals who shifted between workplaces experienced a wider range of cybersecurity issues than those who remained consistently office-based or consistently remote [61]. In the later stage, workplace transition itself created conditions in which phishing could be disguised more easily as ordinary organisational communication.

5 Psychological Analysis of Phishing during COVID-19

This chapter examines the psychological side of COVID-19-themed phishing by focusing on the persuasive elements that made deceptive messages appear credible, important, or routine. It analyses how these elements changed across the pandemic and how they made recipients more likely to trust and act on deceptive messages under different crisis conditions.

5.1 Authority and Institutional Legitimacy

Authority remained a central persuasive mechanism throughout the pandemic, but the form it took changed over time. In the early stage, phishing relied most heavily on public-health and government authority. As the pandemic progressed, however, attackers increasingly exploited workplace systems, vaccine administration, and service or gatekeeping institutions.

During the early stage of the COVID-19 pandemic, health and government authorities became especially effective phishing identities because they were widely perceived as legitimate and necessary sources of guidance. In the context of uncertainty, changing restrictions, and strong demand for reliable information, institutions such as the WHO, CDC, NHS, and other government bodies played a central role in how people understood the crisis. Attackers exploited this dependence by crafting messages that closely resembled official communication, thereby increasing credibility and reducing suspicion [25] [26].

This pattern appeared in repeated impersonation of the WHO, CDC, and NHS through emails and websites that copied official branding, language, and health-related guidance. One notable case involved a WHO-branded email that appeared to provide legitimate COVID-19 protection advice but actually delivered a data-stealing trojan [26], while similar scams echoed state agency announcements [8] or directed victims to fake gov.uk-style websites linked to relief schemes and support measures [25]. These attacks were persuasive because recognisable authority can function as a shortcut for judgement, especially under uncertainty, and because public-health and government institutions were socially understood

as having the right to prescribe behaviour [9] [28]. In this early phase, phishing succeeded by exploiting the expectation that official institutions should provide trustworthy guidance in a crisis [67].

As the pandemic moved beyond the initial shock phase, phishing authority shifted from public crisis institutions towards organisational systems, workplace platforms, and digital access tools. Remote work and online communication became central to everyday operations, and platforms such as Office 365, Microsoft Teams, Zoom, Slack, and VPN services [35] quickly became embedded in routine work practices. Because these technologies were essential for communication, collaboration, and access to organisational networks [54], messages appearing to come from them gained a strong appearance of legitimacy [26].

A clear example of this shift were attacks using fake meeting invitations [35], deceptive platform messages [35] [54], phishing pages styled as Office 365 logins [50] [54], and lures targeting VPN and other remote-access services [54]. Such messages became especially plausible because the shift to remote work was abrupt and many users were still unfamiliar with the tools they were expected to use [26] [35]. Their effectiveness can be explained by the authority of formal organisational structures [9] [28], the normalisation of communication platforms [28], and the expectation that employees should comply with work-related requests in order to remain functional within the organisation [67]. Here, phishing adapted by exploiting workplace obligation and the routine legitimacy of digital work systems rather than broader public guidance.

In the later stage of the pandemic, phishing increasingly relied on medical-administrative authority through vaccine registration systems, appointment processes, manufacturer branding, logistics communication, and certificate-related procedures. As vaccination became central to public attention, institutions and processes connected to vaccine approval, distribution, and verification became highly visible and widely trusted. Attackers exploited this by imitating the systems through which people expected to receive vaccine information, confirm eligibility, arrange appointments, and later demonstrate vaccination status [50] [54].

This later-stage authority was reflected in fake manufacturer websites [49] [50], vaccine

registration scams [50] [54], logistics-themed phishing such as DHL vaccine-delivery lures [50], and certificate-related fraud involving travel certificates [54]. These attacks were persuasive because they combined expert authority with scarcity: vaccine-related messages seemed credible when linked to trusted medical actors, and they also appeared urgent because access, appointments, and supply were limited [9] [28]. French and Raven define expert power as influence based on the perception that the source possesses special knowledge, which helps explain why messages linked to medical agencies, manufacturers, and vaccine systems appeared especially trustworthy [28]. According to Kelman, internalization occurs when influence is accepted because the message appears to fit one's values and to offer a useful solution to a problem [67]. This helps explain why vaccine-related phishing could seem persuasive during the pandemic, since registration and certification messages could be understood as necessary steps towards protection and recovery [67]. In this way, phishing moved beyond broad health impersonation and became embedded in the medical-administrative systems that organised vaccination and certification.

A further form of authority exploited in COVID-19 phishing involved service and gate-keeping institutions such as banks, airlines, travel agents, documentation systems, and organisations controlling access to payments, travel, or administrative services. During the pandemic, these actors became especially important because individuals depended on them for financial relief, banking services, bookings, refunds, and travel documentation. This made their names and communication styles particularly useful to attackers [25] [26], who could frame phishing messages as routine but important service interactions requiring action [60].

This was visible in bank-themed phishing, fake bank infrastructure [54], bogus travel companies, refund scams, and fraud involving passenger locator forms, insurance cards, and digital vaccine passports [60] through interfaces resembling official platforms [25]. These messages were persuasive because they appeared to come from institutions that controlled access to money, movement, or required documents. Their effectiveness can be explained through reciprocation [9], legitimacy [28], and compliance for gain [67]. Specifically, the recipients could feel helped by relief-oriented messages, accept the authority of institutional roles [8], and respond because they expected access to refunds, documentation, or financial support [8] [28]. In this case, phishing authority no longer relied primarily on guidance or

expertise, but on institutional control over access to essential resources. This demonstrated how attackers adapted to the changing sources of legitimacy that defined everyday life during the pandemic.

5.2 Scarcity and Urgency

During the COVID-19 pandemic, scarcity and urgency became very effective persuasive mechanisms. This is because the crisis made people more likely to make fast and pressured decisions while experiencing uncertainty, anxiety, and changes in everyday routines. Crises such as COVID-19, tend to create an environment that is chaotic and unpredictable which makes essential goods, financial support, and similar forms of access appear limited or difficult to obtain [6] [8]. In these circumstances, phishing messages could appear more convincing by creating the impression that information, products, or opportunities were urgent, limited, or difficult to access. This was effective because time pressure and indicators of scarcity made careful evaluation less likely. Therefore, people were more likely to rely on heuristic judgement [2] [68] instead of more careful analysis of messages [24] [68]. Scarcity made the value of targeted resources appear more limited, while urgency created pressure to take action before an opportunity, resource or means of access was lost [9] [23]. In this sense, scarcity and urgency were not simply features of messages. They functioned as effective psychological pressure mechanisms in a pandemic setting, where people were already prepared to look for guidance, obtain limited resources, and respond quickly to perceived threats or opportunities.

Across different stages of the pandemic, these mechanisms in particular appeared in various phishing lures. Early in the pandemic, cybercriminals took advantage of people's need for information and protective goods [8] [25]. These attacks appeared as outbreak warnings, high-risk zone notices, and scams related to limited medical supplies [8] [25]. There is an example that used the subject line "2019-nCov: Coronavirus outbreak in your city (Emergency)," creating a feeling of immediate personal danger and pressuring recipients to respond quickly [6]. Financial and relief-themed phishing messages also used scarcity [8] and urgency [2] for persuasion. In such cases, messages promoted food vouchers, urgent aid [23], or "timely limited" relief funds [8]. One example of a deadline cue is the phrase "Expires in 2 days," or similar messages suggesting that a benefit would be soon

lost [11]. As the pandemic progressed further, the mechanisms of scarcity and urgency became increasingly visible in administrative and access-related narratives. For example, vaccine-themed phishing exploited the need to receive limited doses by urging users to "confirm your email to be enlisted to receive vaccine," making access seem both scarce and urgent [50]. A very similar logic was seen in logistic-themed messages, such as a DHL-themed "COVID-19 vaccine distribution- Re-confirm your delivery address" scam, which made access seem to depend on responding immediately [50]. The same pattern later appeared in travel and certification scams, where fake digital vaccine passports, passenger locator forms, and other travel documents were made to look like time-sensitive requirements for travel [60]. Across these mentioned examples, attackers adapted the scarcity and urgency themes to match the main concerns of each stage. Over time, the focus shifted from emergency health concerns to financial insecurity, vaccine access, and later administrative requirements for travel and participation.

Psychologically, scarcity and urgency were effective because they changed the way recipients evaluated phishing messages. First, scarcity increased the perceived value of information, goods, relief, or access by making them appear limited, difficult to obtain, or at risk of being lost [9] [23]. Second, urgency created pressure to act before an opportunity expired or a negative consequence occurred [9] [23]. Together, these cues made recipients less likely to examine the message carefully and more likely to rely on quick, heuristic judgements [2] instead of more systematic and careful reasoning [2] [68]. Consequently, phishing messages could more easily shift attention away from warning signs such as suspicious links, unusual wording, or inconsistencies in the sender's identity, especially under urgent situations [2] [69]. In the pandemic context, this effect became even stronger. Uncertainty, anxiety, and urgent need had already reduced people's abilities for careful evaluation and increased their sensitivity to messages promising protection, relief, or access [8] [25]. Therefore, scarcity and urgency worked by making phishing lures seem more important and by pushing targets into a certain way of decision-making where a quick response could feel more reasonable than closer verification.

Overall, scarcity and urgency remained important persuasive mechanisms throughout the pandemic, although the way they appeared changed with the evolving crisis context. Early in the pandemic, they were most closely connected to outbreak shock, urgent health

information, protective goods shortages, and immediate financial uncertainty [8] [25]. Over time, these same mechanisms became part of relief scams [8], vaccine registration, appointment processes [50], and later travel, certification, and similar access-related requirements [60]. This also clearly shows that scarcity and urgency were not fixed or isolated tactics. They were continuously adapted to what people most needed, feared losing, or felt pressured to obtain at certain stages of the pandemic.

5.3 Routine Legitimacy

Routine legitimacy became an important persuasive elements during the pandemic because phishing messages often succeeded when they resembled ordinary, expected, and familiar digital procedures rather than obvious threats. Online environments became more integrated with work, communication, and administrative tasks. Therefore, credential prompts and confirmations, platform messages, and other routine digital interactions became more familiar parts of everyday life [35] [41]. Research further suggests that response behaviour is influenced by work-based norms, habits, and expectations [7] [70]. This means that communications which appear expected or procedurally normal are less likely to trigger suspicion and more likely to be accepted without careful assessment [7] [70]. In this sense, it is not only that phishing became persuasive when it included authoritative or urgent elements. Instead, phishing attacks became highly effective when these elements were blended into familiar workflows and linked to routine digital activity that was unlikely to raise suspicion [23] [54].

Throughout the COVID-19 pandemic, cybercriminals used routine legitimacy in different ways by adapting phishing narratives to the procedures, workflows, and digital habits that had become normal at each stage. Firstly, in the early stage, phishing often mimicked routine health updates, notifications about confirmed cases, and similar outbreak-related communications [6]. These types of communications matched people's daily search for information and were made to appear as expected follow-up notices to the crisis [6]. As remote work and online administration became more common, routine legitimacy became visible in mid-pandemic phishing. This is seen in attacks that imitated familiar workplace and service interactions, including internal communication, credential prompts, invoices, and platform-related requests that blended into ordinary job routines [7] [41]. A clear

example is the PharmCo case, in which attackers modified the bank details on an invoice and sent it to a customer for payment [41]. Under conventional office conditions, this type of discrepancy might have been verified between colleagues [41]. However, under remote-work conditions, employees relied more heavily on the digital workflow and viewed the invoice as a normal part of a routine process [41]. This made it possible for attackers to influence recipients to act through digital procedures. Lastly, in the later stages, attackers extended the same logic to vaccine logistics, QR-code use, and delivery or verification procedures [50] [54]. As a result, phishing messages often resembled routine shipment notifications, address-confirmation steps, and administrative actions linked to vaccination [50] [54]. This pattern appeared in cases where cybercriminals used only a passing mention of COVID-19 within content that employees were already accustomed to processing, such as invoices, deliveries, and purchase orders [54]. Rather than changing the format, they inserted the pandemic reference into a structure already familiar to the recipient [54]. Routine legitimacy did not stay the same throughout the pandemic, but developed alongside the "new normal" [23] [35]. This made it possible for attackers to exploit digital procedures that had become familiar, expected, and unlikely to trigger suspicion [23] [35].

Routine legitimacy made compliance more likely because familiar digital procedures were usually processed through habit. Existing literature describes that repeated digital behaviours, such as checking email or responding to routine work communication, could function like mental scripts with the intent to operate more efficiently [71]. At the same time, familiar-looking messages could be processed faster and more automatically [71]. Cognitive processing theory suggests that such responses are more likely when judgement is based on heuristic cues than on more systematic processing [72]. Cialdini has stated that compliance could sometimes be triggered by a single well-chosen cue that activates an automatic behavioural response [9]. This helps explain why familiar-looking phishing messages succeed so well without being carefully examined. When there is a message that matches established work norms or expectations, it is less likely to be viewed as suspicious, and more likely to receive shallow examination [7]. This means that recipients felt like they were responding within ordinary job routines and did not even suspect the message to potentially be a threat [7]. That influence pattern was strengthened as people would rather depend on automatic mental shortcuts in information-heavy environments, where familiar cues can trigger efficient but more automatic responses [9]. All in all, phishing

did not always need to rely on urgency and authority principles to be effective. Instead, it could also succeed by activating habitual, low-suspicion responses to digital activity that appeared normal and expected [23] [70] .

Overall, routine legitimacy remained an important persuasive element throughout the pandemic, but the way it encouraged recipient action changed together with the normalisation of digital life during the pandemic. As everyday activities moved from crisis-related information-seeking [54] to remote work, online administration [41], and later to vaccine, delivery, and verification procedures [50] [54], different digital actions became routine at different stages of the pandemic. Phishing messages remained believable by aligning with the digital actions that appeared most familiar and least suspicious at that point [7] [41]. This shows that routine legitimacy was not a tactic used at a certain period, but an always-changing influence pattern that evolved with the pandemic, allowing phishing to remain credible by being related to the ordinary digital habits and expectations [23] [35].

5.4 Integrated Analysis

It was not the case that COVID-19-themed phishing was persuasive because of one influence principle in isolation. Instead, the patterns examined in this chapter suggest that phishing messages rather combined multiple persuasive elements in a way that matched the context of the crisis at a certain stage. The persuasive elements that stood out the most were authority, scarcity, urgency, and routine legitimacy. These persuasive mechanisms worked together in a way that made messages appear credible, important, and expected at the same time. This combination increased the likelihood that recipients would trust the message, take immediate action, and comply without careful examination.

The interaction between these persuasive elements changed across the pandemic. In the early stage, authority and urgency often appeared together, for example by impersonating trusted health or government institutions. Such authoritative institutions often presented outbreak information, protective advice, or offers related to relief as time-sensitive or difficult to obtain. In the middle of the pandemic, phishing relied more on routine legitimacy. Various examples showed that phishing exploited workplace systems, communication platforms, invoices, and credential prompts that were made to appear to be part of ordinary routine digital workflows. In the later stage of the pandemic, phishing increasingly combined

routine legitimacy with urgency and institutional authority. These late-stage phishing narratives were linked to vaccine registration, logistics, delivery, and verification-related procedures, where the deceptive requests appeared both necessary and procedurally normal.

In conclusion, these patterns show that the effectiveness of COVID-19-themed phishing is best understood as the interaction between the pandemic conditions, attacker adaptation, persuasive message design, and human susceptibility. Deceptive messages were successful when they aligned with what the recipients were already inclined to trust, what they felt pressured to obtain or avoid losing. Their effectiveness also increased when they fit the digital routines that people had already developed in everyday life. This integrated perspective helps explain how and why phishing narratives changed across the pandemic. In addition, it helps to understand why different forms of deception or social engineering became persuasive at different phases of the pandemic.

6 Framework for Crisis-related Phishing Situations

This chapter introduces the conceptual framework developed in this thesis for understanding crisis-related phishing cases. The idea behind this framework is to integrate all of the major findings obtained in the course of this research and present them in an analytical model. This is achieved by connecting together crisis context, attacker adaptation, persuasive elements, target vulnerability, and message plausibility. The framework is based on the preceding analysis of the evolution of COVID-19 phishing and the role played by persuasive mechanisms. Altogether, this would help provide a clearer understanding of the evolution of phishing success due to changing crisis circumstances. The chapter describes the purpose and core elements of the framework, presents the visual form, applies it to the COVID-19 case, and concludes with a discussion about outside applicability and limitations.

6.1 Purpose and Rationale for the Framework

The goal of this proposed framework is to address the central gap identified in the literature and to support the main aim of the thesis. The available studies provide important insight into various issues such as phishing, cybercrime, persuasion, and psychological vulnerability. The problem is that these elements are studied independently from each other and not as part of one integrated explanation. Moreover, the existing literature does not provide a clear analytical framework for analysing how crisis context, attacker adaptation, persuasive strategies, and human susceptibility interact in crisis-related phishing. As a result, it becomes difficult to explain how phishing changed during the pandemic, particularly why certain phishing narratives became believable and effective under different crisis conditions.

Such a framework is essential because of the objectives and methodology used in the current study. To begin with, one of the goals of the thesis is to analyse how exactly pandemic-themed phishing evolved across different phases of the pandemic. As a second goal, the thesis seeks to analyse how attackers adapted their narratives and techniques to

changing developments. Lastly, the final aim is to understand how cybercriminals exploited persuasive and psychological vulnerabilities. Based on this analysis, the study seeks to develop a conceptual framework that explains the relationship between crisis context, attacker adaptation, persuasive mechanisms, and human susceptibility to phishing. The methodology of the thesis similarly shows that the analysis is intended to do more than to describe phishing trends. It also examines how pandemic conditions, attacker behaviour, and psychological factors were connected across the stages of the crisis. In this context, the framework will be used to structure the findings rather than to add anything new to them.

The purpose of the framework is to explain crisis-related phishing as the result of interacting factors rather than isolated ones. The framework is built on the idea that pandemic-related developments shaped both the opportunities available to attackers and also the conditions affecting potential targets. This framework is based on the understanding that crisis conditions affected both attacker behaviour and the vulnerability of the recipients. This explains phishing effectiveness as something that emerged through the interaction of these factors alongside with persuasive message design. Phishing took place in an environment where people were more dependent on digital systems, normal routines were disrupted, and heuristic decision-making became more likely. The intention behind this framework is to bring these elements together in one analytical structure. In doing so, it explains why exactly different forms of phishing became persuasive at different phases of the pandemic and how similar interactions may also be relevant in other crisis-related phishing contexts.

6.2 Structure and Core Elements of the Framework

The framework developed in this thesis is designed to explain how coronavirus themed phishing became persuasive and effective under the conditions of the pandemic. The structure of the framework consists of five interconnected elements: crisis context, attacker adaptation, persuasive elements, target vulnerability, and message plausibility. The intention is not to treat these elements as isolated variables, but as connected parts of an analytical process that shows which phishing messages become believable and more likely to lead to compliance.

The first element crucial for the framework is the crisis context. In this study, crisis context refers to the social, institutional, and behavioural conditions created by the COVID-19

pandemic. More specifically, these conditions included uncertainty, health fears, social disruption, remote work, increased digital dependence, and institutional responses. Another example would be major pandemic-related developments such as vaccine rollouts and financial support measures. This particular element is important because the pandemic did not just provide new themes to be included in phishing narratives. It also changed the conditions under which people worked, communicated, searched for information, and interacted with institutions through digital means. Crisis context functions as the first step of the framework because it shaped both the strategies used by cybercriminals and the conditions affecting potential targets.

Attacker adaptation is the second element of the framework. This means that attackers adjusted phishing narratives in response to changing pandemic conditions. That adjustment refers to cybercriminals changing phishing narratives, impersonation strategies, timing, and delivery methods. It was done in a way to fit current events, public concerns, and emerging digital routines. Attackers also modified their campaigns alongside developments such as public health messaging, workplace changes, financial disruption, and vaccination-related communication. Thus, attacker adaption explains how the crisis context was translated into concrete phishing strategies.

Thirdly, the framework includes persuasive elements. These refer to the features through which attacks became persuasive to recipients, such as authority, urgency, scarcity, and routine legitimacy. These elements help attackers make phishing messages appear more convincing. For example, impersonation of health authorities, employers, delivery services, or government institutions could be used. As a result, this helped make the message more authoritative and legitimate. On the other hand, time-sensitive requests, limited access, or urgent updates could increase urgency and scarcity. Furthermore, routine legitimacy refers to phishing messages appearing believable because they imitate normal procedures that recipients already expect to complete. Examples of routine legitimacy include logging into a remote system, confirming a delivery, verifying an account, or submitting vaccination-related documentation. In the framework, persuasive elements therefore explain how phishing messages gained credibility and encouraged recipient action.

Target vulnerability is the fourth element that originates from the recipient's perspective rather than the attacker's. Target vulnerability refers to the psychological and behavioural

conditions that shaped how phishing messages were interpreted during the pandemic. It includes factors such as uncertainty, stress, fear, increased digital dependence, institutional reliance, and normal routine disruptions. During the pandemic, new digital habits were formed that are associated with remote work, online communication, and interaction through platforms. It is important to include this element because phishing is not effective solely based on the cybercriminals' operations. It must rather be understood in relation to the conditions of the recipient. For example, the persuasive message could have a different effect depending on whether there is an on-going crisis or if the recipient is under pressure. Also, the phishing message may be more effective if the target is more dependent on digital systems, especially systems they are not fully familiar with, because certain requests may then appear expected or necessary.

The fifth and final element crucial for the framework is message plausibility. This captures how believable, relevant, legitimate, or contextually fitting a phishing message appeared to the recipient. The described element explains how phishing messages transition from being encountered to being acted upon. More specifically, the phishing message did not become effective simply because it contained persuasive cues or the fact that the target was vulnerable. Instead, it became effective when persuasive elements and target vulnerability interacted together in a way that made the message look believable in the pandemic context. In this way, a message was constructed that appears convincing enough to act upon.

The fundamental logic of the framework revolves around the interaction of the above-discussed five elements. The interaction of these elements increases the plausibility and, in turn, the likelihood of compliance. Specifically, the crisis context influences attacker adaptation by influencing which phishing narratives, impersonation strategies, and delivery methods become the most successful under changing pandemic conditions. On the other hand, crisis context is also important in shaping target vulnerability by affecting the emotional, behavioural, and situational conditions under which recipients encounter phishing messages. Persuasive elements used in the attacker adaptation include authority, urgency, scarcity, and routine legitimacy. They increase message plausibility by making phishing messages appear believable, important, and legitimate. Target vulnerability also contributes to message plausibility by influencing how recipients understand and evaluate the message within a specific crisis context. In other words, when the message appears

plausible enough, the likelihood of compliance increases. Therefore, the framework explains phishing effectiveness as a process in which the pandemic conditions influenced both the construction of phishing messages and the way recipients interpreted them.

The key takeaway of this framework is that COVID-19-related phishing was effective because there are multiple interconnected variables that were operating simultaneously. Firstly, the pandemic created a crisis environment that impacted the behaviour of both the attackers and the recipients. This created an ideal situation for cybercriminals, where phishing campaigns were tailored to that environment. Secondly, persuasive elements of such attacks made them highly convincing at the message level, while the vulnerability of the recipients affected how those messages were interpreted. Once all these factors aligned to make the messages more plausible, compliance by recipients became almost inevitable. In summary, the framework therefore supports the thesis argument that COVID-19 phishing is best understood as the result of interacting crisis context, attacker adaptation, persuasive elements, target vulnerability, and message plausibility.

6.3 Visual Representation of the Framework

Figure 1 presents the structure of the proposed framework and illustrates how the main elements are connected.

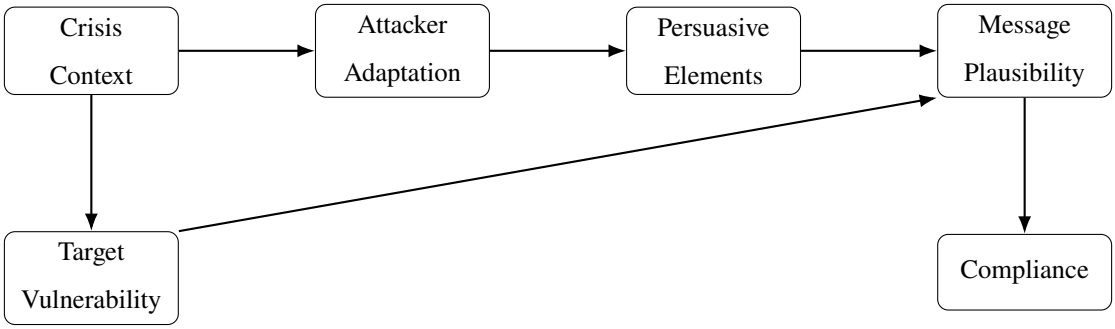

Figure 1. Conceptual framework of COVID-19-themed phishing effectiveness.

Figure 1 illustrates how crisis context shaped both attacker adaptation and target vulnerability during the COVID-19 pandemic. Attacker adaptation is expressed through persuasive elements embedded in phishing messages. Target vulnerability influences how such messages are interpreted by recipients. These two pathways converge in message plausibility, which functions as one of the intermediate steps between exposure to a phishing message and the likelihood of compliance.

6.4 Application of the Framework to the COVID-19 Case

This framework developed in this thesis is applied to the COVID-19 case to provide a structured explanation of how phishing became effective under changing pandemic conditions. Its main value is that it connects separate findings into an analytical explanation of how phishing messages became believable and persuasive during the crisis. Instead of treating these elements as isolated factors, the framework emphasises the effectiveness of phishing when they are interconnected. The COVID-19 case supports the framework by demonstrating that the high success of phishing was not the result of a single factor. Instead, it developed through a broader process where crisis conditions shaped how phishing messages were constructed and also the conditions affecting their reception and interpretation. More specifically, the framework connects the stage-based analysis of phishing evolution with the psychological analysis of persuasive elements and target vulnerabilities.

Applying the framework to the coronavirus case shows that phishing narratives and persuasive forms changed throughout the pandemic. However, the overall structure of the framework remained the same across these changes because phishing effectiveness continued to depend on the interaction of the same elements, namely crisis context, attacker adaptation, persuasive elements, target vulnerability, and message plausibility. What changed was the specific way these elements appeared under different pandemic conditions. Different crisis conditions made certain messages seem plausible and encouraged different forms of recipient action. The COVID-19 case therefore demonstrates the value of the framework as a way of bringing the thesis findings together into a structured explanation of how phishing effectiveness developed under changing crisis conditions.

6.5 Broader Applicability of the Framework

Although this framework was developed through the COVID-19 case, its broader value comes from showing how crisis conditions can influence the way phishing messages are constructed, interpreted, and made plausible. More specifically, the framework may be relevant to other crisis-related phishing situations in which disruptive conditions alter public behaviour. Moreover, the framework becomes relevant in situations where people become increasingly dependent on digital communication. Further examples of usefulness

are cases where people have urgent information needs or doubts about who or what they see as trustworthy or legitimate. In such contexts, cybercriminals may similarly adapt their narratives and techniques to the surrounding conditions and take advantage of persuasive elements. Consequently, the attackers exploit target vulnerability with the goal to make certain messages believable. The framework therefore may offer a useful analytical structure for examining phishing and social engineering in other similar large-scale disruptions. It is applicable in other crises despite of the specific events, timelines, and message themes differing from those observed in the COVID-19 case. This is because the applicability lies less in the stage structure used in this thesis. Instead, it is used to explain how crisis context, attacker adaptation, persuasive elements, target vulnerability, and message plausibility can interact under evolving conditions.

In addition, the framework may also have practical value for crisis-specific cybersecurity awareness and defensive planning. Since attackers may change their phishing themes as a crisis develops, the framework can help organisations and cybersecurity practitioners consider which messages are likely to become plausible under changing crisis conditions. This supports the use of the framework as an analytical tool for adaptive awareness and defensive planning. In conclusion, the framework may support future research on crisis-related phishing by providing a structured way to compare different crises without assuming that they unfold in the same way. For this reason, the framework should be understood not as a predictive model, but as an analytical tool for examining how phishing messages may become believable and persuasive during large-scale disruptions.

6.6 Limitations of the Framework

There are various limitations of the framework presented above. First of all, it is developed through the lens of the COVID-19 case and is therefore shaped by the specific social, institutional, and behavioural conditions of that crisis only. The interaction between crisis context, attacker adaptation, persuasive elements, target vulnerability, and message plausibility may also be relevant in other crisis-related phishing situations. Nevertheless, the exact form and development of these elements may be different across crises. Secondly, the framework does not give much attention to technical, organisational, and sector-specific factors that may also influence phishing outcomes. There might be filtering systems,

security training, organisational culture, or differences between work environments having an influence on the effectiveness. Another limitation is that the framework does not capture every factor that may influence phishing effectiveness. Thus, the third limitation comes from its specificity. In other words, since it is meant to analyse the most important factors, it cannot be considered as a full explanation of all phishing in all situations since there may be other factors that affect phishing effectiveness. These limitations do not undermine the value of the framework, but they simply indicate that it should be understood as a focused interpretive model rather than a representation of all phishing dynamics.

7 Discussion

Instead of viewing COVID-19 phishing as a single, static phenomenon, the findings of this thesis suggest that it should be understood as a dynamic process influenced by multiple interconnected factors. This perspective is important because the coronavirus pandemic changed over time. Examining these elements together helps better understand how the phishing susceptibility changed during each stage of the pandemic. The discussion therefore brings together the three major areas of analysis: the stage-based development of phishing narratives, the psychological and persuasive analysis, and the conceptual framework that links the main factors together.

7.1 Answers to the Research Questions

This section synthesises the findings of the thesis by answering each research question in relation to the stage-based analysis, psychological analysis, and conceptual framework.

7.1.1 RQ1: Evolution of Pandemic-themed Phishing

The first question asked how pandemic-themed phishing and social engineering attacks evolved across different stages of the COVID-19 pandemic. From the reviewed literature, it is evident that COVID-19 phishing was not a crisis that remained static or constant. It was a dynamic event that changed according to the developments taking place during the pandemic. It also became clear that phishing narratives followed the changing crisis context.

At each stage, different factors were responsible for making the phishing seem believable. In the early stage, the plausibility was shaped by the anxiety and fear caused by the lack of knowledge about how the virus would affect the society. The lack of knowledge was also related to receiving timely health-related information from spoofed authoritative sources, such as WHO, CDC, and NHS [25] [26]. In the middle stages, plausibility was more associated with changed routines. Many individuals were required to work, study, as well as

spend their free time on online platforms, resulting in sudden changes in their daily routines. These changed routines made phishing examples such as Office 365-style login pages [50], VPN-related access requests [54], and messages involving Microsoft Teams, Zoom, and Slack [35] appear more familiar and plausible. Authentication requests were also related to the increase of online activities as well as deliveries of goods, since people spent more time indoors. In the later stage, plausibility shifted towards access, verification, and recovery processes. People were attempting to gain access to vaccines, while proof of vaccination or related documents became prerequisites for travelling. This created opportunities for phishing examples such as fake Pfizer-BioNTech websites, which imitated vaccine-related registration processes [49].

Furthermore, the normalisation of everyday life led to individuals returning to office work or adopting hybrid environments. The workplace transition itself became a source of uncertainty. As an example of this, employees who shifted between work environments experienced more cybersecurity issues than those who remained consistently office-based or consistently remote [61]. Therefore, authentication requests, remote-access workflows, and account-related messages became easier to present as ordinary organisational communication. The key takeaway connected to this research question is that phishing changed because what people considered normal, urgent, or trustworthy also changed. In other words, during the pandemic, the context was in a constant change, and it was the adaptation to the context that made phishing more convincing.

Also, the pandemic did not necessarily create completely new phishing methods. Instead, attackers used familiar methods, such as impersonation, fake login pages, and fake forms, and incorporated pandemic-related concerns into them. This identified evolution of phishing provides evidence for the main argument made throughout the thesis: phishing effectiveness during COVID-19 depended on the interaction between crisis context, attacker adaptation, message plausibility, and human susceptibility. To conclude, the pandemic should be understood as a dynamic phishing environment rather than a static and unchanging event.

7.1.2 RQ2: Influence of Pandemic-related Developments

The second research question is how major pandemic-related developments influence phishing narratives, delivery methods, and persuasive techniques. The thesis explained

that major pandemic-related developments influenced phishing by changing what people expected to receive, trusted, and felt required to respond to. It is based on the point of view of the recipient, as the crisis created real communication needs that could be mimicked by the cybercriminals. These developments influenced phishing by turning real pandemic-related processes, such as health communication, remote-work access, travel documentation and vaccine administration, into believable phishing narratives. For example, a DHL-themed "COVID-19 vaccine distribution - Re-confirm your delivery address" scam made vaccine logistics appear like a normal delivery-confirmation process [50]. The main argument is that these narratives seemed realistic because they reflected communication that people already expected during the pandemic.

This theme was also examined from the attackers' perspective as the recipients' expectations and vulnerabilities were known to the cybercriminals. As new developments of the pandemic arose, the attackers changed their narratives accordingly. Cybercriminals incorporated persuasive and psychological tactics to make their messages more plausible. The thesis identified various examples of the events and the psychological themes attached to them. The outbreak and lockdowns increased the credibility of health warnings and authority impersonation. One phishing email, for example, used the subject line "2019-nCov: Coronavirus outbreak in your city (Emergency)," making the message appear urgent and personally relevant [6]. The shift to remote work created a context in which login prompts, and communication platforms more plausible. Increased online shopping made delivery and payment messages more believable, while the vaccine rollout made registration, and appointment messages more credible. The main implication is that the attacker adaptation followed the practical needs and concerns created by the pandemic.

The phishing delivery methods were shown to be influenced by the communication habits during the pandemic. The use of email became more important for work and thus it became a common delivery method. This was reflected in phishing emails that imitated normal work messages and used company logos and urgent actionable links to make the request appear legitimate and work-related [7]. Fake login pages became believable as well due to authentication becoming more common in online environments. Because people expected quick updates, service notifications, and SMS became plausible. For example, one SMS-based lure asked recipients to take a mandatory COVID-19 "preparation" test

and directed them to a website that downloaded malware [25]. Moreover, fake websites and forms became convincing because various pandemic processes required online registration, verification, or documentation. The important takeaway is that delivery methods became successful when they matched the digital channels and routines people were already using.

Pandemic developments also strengthened persuasive techniques because authority, urgency, scarcity, and routine legitimacy matched users' crisis-related expectations and pressures. They became useful because of the surrounding crisis conditions. Since people were reliant on health agencies, governments, employers, banks, and service providers, authoritative messages became convincing. Furthermore, urgency was a highly effective persuasion mechanism because restrictions, health advice, and administrative messages changed frequently throughout the pandemic. Scarcity worked well because people feared losing access to financial support, vaccine appointments, travel opportunities, or protective goods. One study identified several fake PPE offers that directed users to malicious websites shortly after reports emerged that hospitals were running out of protective equipment [25]. Lastly, routine legitimacy was effective because login requests, platform communication, delivery notices, and administrative confirmations became ordinary. This can be seen in the PharmCo case, where attackers modified the bank details on an invoice and sent it to a customer for payment, making the request appear like part of a routine business process [41]. These mentioned persuasive techniques were not only effective because of their appearance in the messages. They were rather effective because the pandemic context made them seem reasonable and expected.

The second research question supports the idea that crisis context shaped both attacker behaviour and the plausibility of messages. To answer the question, the thesis shows that the pandemic developments influenced phishing in three connected ways. Firstly, the changing conditions gave attackers relevant narratives to imitate. Then, the attackers would adjust their delivery methods and communication channels that seemed normal to the recipients. Finally, the persuasive elements were incorporated matching the people's experiences during the pandemic.

7.1.3 RQ3: Psychological Vulnerabilities and Social Influence Factors

The third research question refers to the vulnerabilities and social influence factors that were exploited in relation to different pandemic stages and phishing techniques. From the findings obtained in the course of the research, it became evident that psychological vulnerability was not the same throughout the pandemic. Similarly to the overall context of the dynamic nature of the pandemic, the vulnerabilities and social influence factors across the stages and attacker techniques also remained dynamic. The main point revealed in the thesis is that phishing susceptibility was situation-dependent. Individuals did not fall victim merely as a result of their own vulnerabilities, but because of the particular conditions during the pandemic.

The early-stage vulnerabilities were associated mostly with the shock of the outbreak. The pandemic caused fear, uncertainty, and anxiety about the virus due to its unpredictable nature. Reliable information was hard to identify, and hence there was an urgent need for health information. Moreover, there was a heightened trust in public-health and government institutions, as people needed reliable information from authorities. From the above examples, the main social influence factors involve authority, urgency, and scarcity.

The study results indicate that mid-pandemic vulnerability became more associated with altered patterns of behaviour and routines. As work, education, communication, and services became more dependent on digital platforms, phishing messages could more easily imitate ordinary online interactions. For example, one study found that phishing emails appearing to come from a compromised colleague's account were difficult to detect because recipients treated them as normal workplace communication [35]. Authority and urgency would still be apparent, yet routine legitimacy became particularly important because phishing messages looked like normal digital procedures. Phishing in the mid-stage of coronavirus was effective since it blended into everyday online behaviour.

Lastly, towards the later stage of the pandemic, the vulnerability was mainly linked to administrative and recovery-related pressures. People had to complete administrative procedures connected to vaccination, travel, refunds, and changing work arrangements. In this stage, authority was important because phishing messages often appeared to come from institutions or service providers having control over vaccination, travel, refunds, or

workplace procedures. For example, a fake NHS digital vaccine passport email asked recipients to enter personal and credit card details for a small "postage fee" [60]. Routine legitimacy was also relevant since these phishing messages imitated normal administrative processes that people expected to complete, such as registration, verification, confirmation, or documentation.

From the thesis, the way how persuasive techniques and psychological vulnerabilities work together becomes clear. It is important to note that influence factors did not operate in isolation but were interconnected. Authority worked because people needed guidance. Urgency was effective because of the quickly changing conditions. Because access or resources seemed limited during the pandemic, scarcity became effective. Finally, because people were doing their daily activities on digital platforms, messages were made to look like normal digital procedures rather than suspicious requests. Therefore, phishing susceptibility during COVID-19 was shaped by the interaction between emotional pressure, digital dependence, persuasive message design, and the surrounding crisis context.

7.1.4 RQ4: Implications for Crisis-specific Awareness and Defence

The final research question asks if the understanding crisis-driven phishing adaptation and psychological manipulation can support the development of crisis-specific awareness and defensive strategies. The findings suggest that defensive strategies should evolve alongside the crisis. Therefore, organisations should not employ the same countermeasures throughout the whole crisis. As the crisis develops, attackers change their phishing themes, so defenders need to revise their warning messages to users. General phishing awareness is still useful, but it is not enough during crises.

In addition to educating the users on verifying links, sender addresses, or typos, they must learn to identify the factors that contribute to the credibility of phishing emails during a crisis. Training should also therefore cover psychological factors such as authority, urgency, scarcity, and routine legitimacy. The idea identified here is that the users may be better prepared if they understand how attacks exploit emotions, expectations, and crisis-related pressure.

Organisations should monitor crisis developments and predict what attackers may imitate next. For example, when WHO declared COVID-19 as a pandemic, defenders could have

already anticipated early-pandemic phishing themes from that announcement. This thesis and its framework may also support defensive predictions in future crisis events since different crises may share similar patterns. The core idea is that the defenders should not only react to phishing after it appears, but anticipate which messages are likely to become plausible.

This conceptual framework helps answer the question by helping organisations understand the connection between crisis context, attacker adaptation, persuasive elements, target vulnerability, message plausibility, and compliance. Overall, crisis-specific cybersecurity should be adaptive, contextual, and psychologically informed. Technical tools can help detect and block phishing, but crisis-related phishing also requires users and organisations to understand how attackers adapt their messages to changing conditions.

7.2 Theoretical Implications

This thesis contributes theoretically by providing a more integrated understanding of phishing. Existing literature tends to focus on one dimension of phishing, either its technicality, psychology, or communication aspect of the attack. Nevertheless, this fails to demonstrate how these isolated factors interact to make phishing successful within a particular context. The thesis shows that crisis-related phishing is better understood through the interaction between various interconnected factors, as explained in the framework chapter.

This thesis highlights the importance of treating COVID-19 phishing as a dynamic process rather than a static one. It is clear from the analysis that phishing changed alongside the crisis context. This aspect is important because existing literature is mostly limited to short timeframes or early pandemic cases of phishing, making it harder to understand longer-term development. The thesis shows that phishing narratives evolved during the different stages of the pandemic. Specifically, attackers were changing their strategy depending on public concerns and routines. Message plausibility changed because believable messages reflected the needs and concerns of each pandemic stage. Therefore, the thesis supports the idea that phishing should be studied as an evolving process.

The theoretical perspective of phishing is provided by the thesis through linking psycho-

logical vulnerability and social influence factors. As highlighted in the literature review, the psychological mechanisms are hardly fully explained, particularly in terms of phishing success under crisis conditions. This thesis, therefore, reveals that psychological vulnerability is not static, and the susceptibility changes based on the crisis scenario. The primary identified persuasion elements are authority, urgency, scarcity, and routine legitimacy, which appeared differently depending on the crisis situation. Moreover, the persuasive techniques are also more influential when they match the recipient's emotional state, routines, or needs. The theoretical implication here is that different forms of vulnerability become relevant at different moments.

The conceptual framework adds theoretical value by showing how the main findings can be understood through a connected explanatory model. The framework shows how crisis context shapes both attacker adaptation and target vulnerability. Attacker adaptation is then expressed through persuasive elements, while target vulnerability affects how these messages are interpreted. Together, persuasive elements and target vulnerability contribute to message plausibility, which increases the likelihood of compliance. This framework gives future researchers a structured way to analyse crisis-related phishing without treating attacker behaviour, persuasive design, and human vulnerability as separate topics.

7.3 Practical Implications

Organisations should not only rely on generic phishing awareness during crisis. General advice to check links, sender addresses, or spelling mistakes are still useful. However, sophisticated attacks often manage to avoid these obvious indicators and instead rely on more advanced manipulation strategies. Awareness should also not be generic but would benefit from changing according to the crisis developments. More specifically, training should reflect the most likely phishing themes at that moment. The thesis supports this argument by showing that the dynamic nature of crises requires phishing awareness programmes to be updated in response to changing attacker narratives and user vulnerabilities.

Related to the previously mentioned practical implication would be the anticipation of phishing themes. Major crisis developments should be treated as possible indicators of future narratives. This means that defence from the human perspective should not be reactive but anticipatory, focusing on what attackers are likely to imitate next. An

example would be public announcements creating phishing opportunities. Moreover, attackers are likely to exploit the confusion around new rules, digital platforms, deadlines, or official procedures. This means that security teams must follow crisis developments and translate them into timely warnings for users. This thesis contributes to this implication by showing that attacker adaptation during COVID-19 was closely connected to major pandemic developments. Therefore, the findings may help in anticipating potential phishing narratives in similar future crises.

It is not only that security teams must follow crisis developments, but organisations and public institutions could make official communication clear and predictable. As uncertainty and urgency around communication during the coronavirus was a prominent theme, organisations should clearly tell employees or users where official messages will come from. Furthermore, they must use consistent channels for crisis communication and give timely warnings when attackers have been suspected exploiting crisis themes. The contribution of this thesis is that it shows how uncertainty around trusted sources, official procedures, and expected communication increased message plausibility, which supports the need for clearer and more predictable crisis communication.

The identified limitation was reliance on technical indicators and less on psychological manipulation. As this study identified authority, urgency, scarcity, and routine legitimacy as the key persuasive elements, recipients should be knowledgeable why a message feels convincing. Users should learn how authority impersonation creates trust, urgency pressures quick action, and scarcity makes opportunities or resources seem limited. Also, routine legitimacy makes phishing look like ordinary work or administrative processes. Training should reflect that phishing can be convincing precisely because it matches the user's fears, routines, expectations, and needs. The framework developed in this thesis can support adaptive training by helping organisations identify which crisis conditions, attacker narratives, persuasive elements, and user vulnerabilities are most likely to make phishing messages believable.

7.4 Limitations

The thesis uses a qualitative and interpretive approach to identify patterns and relationships between crisis context, attacker adaptation, persuasion, and susceptibility. Because it

identifies patterns rather than measuring effects, it cannot determine how frequent each phishing theme was, which persuasive element was most effective, or how strongly each factor influenced compliance. Therefore, these findings should not be used to make quantitative or statistical comparisons.

The division of the research into the early, mid-, and later stages was useful for structuring the analysis and interpreting the changes across the pandemic. However, these stages are not supposed to be perceived as strict chronological boundaries. The value of the stage-based analysis may be limited when applied to future crises, because every crisis develops differently, although certain patterns or stages may still be comparable. Moreover, the pandemic developments did not happen at the same time everywhere. Rather, different countries, sectors, and organisations experienced the pandemic differently. The study also identified some phishing patterns appearing across more than one stage. The stage-based structure is beneficial for identifying broad developments, but it simplified a more complex and uneven pandemic timeline.

This thesis focuses on broad COVID-19 phishing patterns across the pandemic rather than comparing how phishing developed in specific sectors. A sector-specific analysis would also be important because different sectors have different communication routines, security awareness, or attacker incentives. For example, phishing affecting healthcare organisations may rely more strongly on medical authority and urgent health communication, while phishing in private companies may focus more on remote work, invoices, and authentication. While the thesis can identify broad patterns in crisis-related phishing, it cannot explain in detail how these patterns differed between various sectors.

The thesis discusses susceptibility based on existing literature, reported examples, and the surrounding crisis context. However, it does not observe recipient interactions with phishing messages. Moreover, it does not include interviews, surveys, or experiments. Recipients may differ in how they were psychologically affected by the pandemic, as well as in their level of training and digital literacy. The thesis identifies conditions that may increase phishing susceptibility, but it does not directly measure actual user behaviour or decision-making.

7.5 Future Research

Future research could use primary data collection methods, such as surveys, interviews, controlled experiments, or phishing simulation studies, to examine how users respond to crisis-themed phishing messages. This would be beneficial for measuring how users actually respond to crisis-themed phishing. Moreover, it could be measured which persuasive elements and psychological vulnerabilities have a stronger or weaker influence on user compliance. Future research could build on the interpretive findings of this thesis by testing identified relationships through measurable evidence.

Due to the broad nature of this thesis, future research could examine more specifically how phishing differs across sectors. Relevant sectors identified in this thesis but not analysed in depth would be healthcare, education, government, and private companies. This would show whether certain sectors are more exposed to specific phishing themes. Furthermore, this would explain how sector-specific communication, work routines, and trust in institutions affect message plausibility.

Since the main contribution of this thesis is the framework which was developed through the COVID-19 case, future studies could test or adapt it in other crisis contexts. Possible crises would be natural, economic, political, and geopolitical crises. This would test whether the interaction between the crisis context, attacker adaptation, persuasion, vulnerability, and plausibility also appears in other crises. It would also become apparent if other crises follow similar or different stage divisions. Understanding to what extent the framework applies beyond the COVID-19 pandemic could further refine the framework as well.

The thesis focuses mainly on the human and situational factors. However, since the main identified emphasis in the existing literature is on technical analysis, future studies could examine the technical and human factors together. Phishing messages could also become more plausible because of stronger technical realism that might also incorporate persuasive elements. For example, a realistic fake website or sender domain can make authority impersonation more convincing or a well-timed SMS can make urgency more believable. There is definitely future research that could be done integrating technical phishing analysis with the human analysis to give an even more comprehensive understanding into phishing compliance during crises.

8 Conclusion

This thesis demonstrated that phishing and social engineering attacks related to COVID-19 cannot be treated as static or constant. They evolved according to the changing environment of the pandemic. The outbreak of COVID-19 could be viewed as a disruptive process where changes occurred in the situational, psychological, and attacker narrative contexts. The cybercriminals capitalised on the changing circumstances through adjusting their approaches to the phishing attacks. Consequently, the thesis reveals that the success of phishing and social engineering attacks during the pandemic was influenced by the interaction of the crisis situation, attacker adaptation, and human vulnerability.

This study showed that the evolution of COVID-19-themed phishing can be better understood by examining how attacker narratives changed across early, mid-, and later-stage pandemic conditions. The most common features in the early stage were mainly uncertainty, authority impersonation, urgent information needs, and scarcity. The key themes for mid-pandemic phishing were remote working, authentication, delivery, and e-commerce. The later-stage phishing themes mainly involved vaccines, travel reopening, refunds, and hybrid-work. For the phishing narratives to be successful, attacks capitalised on the human element by taking advantage of the persuasive techniques. The application of authority, urgency, scarcity, and routine legitimacy in conducting the phishing attacks proved successful since they matched the needs, fears, and habits of people during the pandemic.

The thesis developed a conceptual framework which links the main factors associated with phishing susceptibility. These factors involved the crisis context, attacker adaptation, persuasive elements, target vulnerability, message plausibility, and compliance. The value of the framework is that it helps understand crisis-related phishing as an interaction between these elements. Furthermore, this thesis explains how crisis conditions make certain messages believable, persuasive, and likely to be acted upon. The results of this research could contribute to facilitate better crisis-oriented cybersecurity awareness training and defensive planning. Also, it may also help recognise how phishing risks can change as

public concerns, digital routines, and institutional dependencies change during a crisis. The main limitation is that it relies mainly on secondary sources, and it is purely based on qualitative analysis. In addition, it does not provide a statistical measurement of all phishing activities related to COVID-19.

Future research could build on these findings through primary research methods to measure how users respond to crisis-themed phishing messages. Further research could also apply the conceptual framework to other crisis contexts in order to examine whether similar patterns of attacker adaptation, persuasion, vulnerability, and message plausibility emerge. Overall, this thesis shows that understanding how phishing adapts to changing crisis conditions is essential for improving preparedness against social engineering attacks in future disruptions.

References

[1] R. Hoheisel et al. „The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains“. In: *Computers & Security* 128 (2023), p. 103158. DOI: 10.1016/j.cose.2023.103158.

[2] N. Akdemir and S. Yenal. „How phishers exploit the coronavirus pandemic: A content analysis of COVID-19 themed phishing emails“. In: *SAGE Open* 11.3 (2021). DOI: 10.1177/21582440211031879.

[3] F. Carroll, J. Adejobi, and R. Montasari. „How good are we at detecting a phishing attack? Investigating the evolving phishing attack email and why it continues to successfully deceive society“. In: *SN Computer Science* 3 (2022). DOI: 10.1007/s42979-022-01069-1.

[4] Anti-Phishing Working Group. *Phishing Activity Trends Report: 3rd Quarter 2020*. [Online]. Accessed: May 18, 2026. 2020. URL: https://docs.apwg.org/reports/apwg_trends_report_q3_2020.pdf.

[5] Anti-Phishing Working Group. *Phishing Activity Trends Report: 1st Quarter 2022*. [Online]. Accessed: May 18, 2026. 2022. URL: https://docs.apwg.org/reports/apwg_trends_report_q1_2022.pdf.

[6] Cybersecurity and Infrastructure Security Agency. *COVID-19 Exploited by Malicious Cyber Actors*. Alert AA20-099A, Apr. 8, 2020. [Online]. Accessed: May 18, 2026. 2020. URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-099a.

[7] J. Scott. „Phishing Ecosystem: A Qualitative Analysis of Phishing Susceptibility in Employees Who Work from Home“. [Online]. Accessed: May 18, 2026. MA thesis. School of Informatics, University of Skövde, 2022. URL: https://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-22262.

[8] V. Kaliňák. „Psychology of Phishing Attacks during Crises: The Case of COVID-19 Pandemic“. [Online]. Accessed: May 18, 2026. MA thesis. Faculty of Social Sciences, Charles University, 2021. URL: https://dspace.cuni.cz/bitstream/handle/20.500.11956/151604/120398706.pdf?sequence=1&isAllowed=y.

[9] R. B. Cialdini. *Influence: The Psychology of Persuasion*. rev. ed. New York, NY, USA: Harper Business, 2007.

[10] B. Sharma et al. „Don't be a victim during a pandemic! Analysing security and privacy threats in Twitter during COVID-19“. In: *IEEE Access* 11 (2023), pp. 29769–29789. DOI: 10.1109/ACCESS.2023.3260643.

[11] M. Bitaab et al. „Scam pandemic: How attackers exploit public fear through phishing“. In: *2020 APWG Symposium on Electronic Crime Research (eCrime)*. Boston, MA, USA, 2020, pp. 1–10. DOI: 10.1109/eCrime51433.2020.9493260.

[12] H. Abroshan et al. „Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process“. In: *IEEE Access* 9 (2021), pp. 44928–44949. DOI: 10.1109/ACCESS.2021.3066383.

[13] Z. Wang, H. Zhu, and L. Sun. „Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods“. In: *IEEE Access* 9 (2021), pp. 11895–11910. DOI: 10.1109/ACCESS.2021.3051633.

[14] G. Desolda et al. „Human factors in phishing attacks: A systematic literature review“. In: *ACM Computing Surveys* 54 (2022), p. 35. DOI: 10.1145/3469886.

[15] T. N. Jagatic et al. „Social phishing“. In: *Communications of the ACM* 50.10 (2007). Oct. 2007, pp. 94–100.

[16] E. E. Lastdrager. „Achieving a consensual definition of phishing based on a systematic review of the literature“. In: *Crime Science* 3 (2014), p. 9. DOI: 10.1186/s40163-014-0009-y.

[17] A. H. Washo. „An interdisciplinary view of social engineering: A call to action for research“. In: *Computers in Human Behavior Reports* 4 (2021), p. 100126. DOI: 10.1016/j.chbr.2021.100126.

[18] R. Montañez, E. Golob, and S. Xu. „Human cognition through the lens of social engineering cyberattacks“. In: *Frontiers in Psychology* 11 (2020), p. 1755. DOI: 10.3389/fpsyg.2020.01755.

[19] Anti-Phishing Working Group. *Phishing Activity Trends Report: 4th Quarter 2014*. [Online]. Accessed: May 18, 2026. 2014. URL: https://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf.

[20] S. Zhuo et al. *SoK: Human-Centered Phishing Susceptibility*. 2022. DOI: 10.48550/arXiv.2202.07905.

[21] R. Dhamija, J. D. Tygar, and M. Hearst. „Why phishing works“. In: *Conference on Human Factors in Computing Systems - Proceedings*. Vol. 1. 2006, pp. 581–590. DOI: 10.1145/1124772.1124861.

[22] K. Kikerpill and A. Siibak. *Mazephishing: The COVID-19 Pandemic as Credible Social Context for Social Engineering Attacks*. 2021. DOI: 10.31124/advance.14607894.

[23] R. Naidoo. „A multi-level influence model of COVID-19 themed cybercrime“. In: *European Journal of Information Systems* 29.3 (2020), pp. 306–321. DOI: 10.1080/0960085X.2020.1771222.

[24] H. Abroshan et al. „COVID-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic“. In: *IEEE Access* PP (2021), pp. 1–1. DOI: 10.1109/ACCESS.2021.3109091.

[25] 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“. In: *Computers & Security* 105 (2021), p. 102248. DOI: 10.1016/j.cose.2021.102248.

[26] A. F. Al-Qahtani and S. Cresci. „The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19“. In: *IET Information Security* 16.5 (2022), pp. 324–345. DOI: 10.1049/ise2.12073.

[27] W. Nowakowski. „Social engineering analysis framework: A comprehensive playbook for human hacking“. In: *IEEE Access* 13 (2025), pp. 18827–18849. DOI: 10.1109/ACCESS.2025.3532999.

[28] P. Fischer, S. Lea, and K. Evans. *The Psychology of Scams: Provoking and Committing Errors of Judgement*. Tech. rep. Research report, 2009. Office of Fair Trading, 2009.

[29] J. Laan et al. „The impact of the COVID-19 pandemic on phishing frequency and content: The impact of routine activities theory and a rational choice model of crime“. In: *SSRN Electronic Journal* (2023). DOI: 10.2139/ssrn.4322333.

[30] R. Alabdan. „Phishing attacks survey: Types, vectors, and technical approaches“. In: *Future Internet* 12.10 (2020), p. 168. DOI: 10.3390/fi12100168.

[31] P. Wang and P. Lutchkus. „Psychological tactics of phishing emails“. In: *Issues in Information Systems* 24.2 (2023), pp. 71–83. DOI: 10.48009/2_iis_2023_107.

[32] M. Hijji and G. Alam. „A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: Challenges and prospective solutions“. In: *IEEE Access* 9 (2021), pp. 7152–7169. DOI: 10.1109/ACCESS.2020.3048839.

[33] S. Henderson et al. *Vietnamese threat actors APT32 targeting Wuhan government and Chinese Ministry of Emergency Management in latest example of COVID-19 related espionage*. Google Cloud Blog, Apr. 22, 2020. [Online]. Accessed: May 18, 2026. 2020. URL: https://cloud.google.com/blog/topics/threat-intelligence/apt32-targeting-chinese-government-in-covid-19-related-espionage.

[34] Menlo Security. *Sophisticated COVID-19–based phishing attacks leverage PDF attachments and SaaS to bypass defenses*. Apr. 2, 2020. [Online]. Accessed: May 18, 2026. 2020. URL: https://www.menlosecurity.com/blog/sophisticated-covid-19-based-phishing-attacks-leverage-pdf-attachments-and-saas-to-bypass-defenses.

[35] T. Koski. „Increase in Remote Work - Effects on Phishing“. [Online]. Accessed: May 18, 2026. MA thesis. Faculty of Information Technology, University of Jyväskylä, 2021. URL: https://urn.fi/URN:NBN:fi:jyu-202106083555.

[36] Anti-Phishing Working Group. *Phishing Activity Trends Report: 1st Quarter 2020*. [Online]. Accessed: May 18, 2026. 2020. URL: https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf.

[37] J. Zarocostas. „How to fight an infodemic“. In: *The Lancet* 395.10225 (2020), p. 676. DOI: 10.1016/S0140-6736(20)30461-X.

[38] N. A. Khan, S. Brohi, and N. Z. Jhanjhi. „Ten deadly cyber security threats amid COVID-19 pandemic“. In: *TechRxiv* (2020). May 2020. DOI: 10.36227/techrxiv.12278792.v1.

[39] DomainTools. *CovidLock update: Deeper analysis of coronavirus Android ransomware*. Mar. 16, 2020. [Online]. Accessed: May 18, 2026. 2020. URL: https://www.domaintools.com/blog/covidlock-update-coronavirus-ransomware.

[40] J. Rodger. *The school meals coronavirus text scam which could trick parents out of thousands*. BirminghamLive, Mar. 25, 2020. [Online]. Accessed: May 18, 2026. 2020. URL: https://www.birminghammail.co.uk/news/midlands-news/school-meals-coronavirus-text-scam-17975311.

[41] M. Lang and L. Connolly. „Managing the cybersecurity risks of teleworking in the post-pandemic 'new normal'“. In: *SSRN Electronic Journal* (2021). Jun. 30, 2021. DOI: 10.2139/ssrn.4146506.

[42] M. Bispham et al. „Cybersecurity in working from home: An exploratory study“. In: *SSRN Electronic Journal* (2021). DOI: 10.2139/ssrn.3897380.

[43] T. Weil and S. Murugesan. „IT risk and resilience—Cybersecurity response to COVID-19“. In: *IT Professional* 22 (2020), pp. 4–10. DOI: 10.1109/MITP.2020.2988330.

[44] J. C. L. Siu, H. Zhong, and A. Nivette. „Exploring the impact of routine activity and financial strain on fraud victimization during the COVID-19 pandemic in Hong Kong“. In: *Asian Journal of Criminology* 19 (2024), pp. 441–458. DOI: 10.1007/s11417-024-09438-w.

[45] OECD. *Teleworking in the COVID-19 pandemic: Trends and prospects*. Tech. rep. Paris: OECD Publishing, 2021. DOI: 10.1787/72a416b6-en.

[46] M. Lang et al. „The evolving menace of ransomware: A comparative analysis of pre-pandemic and mid-pandemic attacks“. In: *Digital Threats: Research and Practice* 4.4 (2023). Art. no. 52, pp. 1–22. DOI: 10.1145/3558006.

[47] J. Yang and L. Linkeschová. „Remote Working and Cybersecurity in the Pandemic: Research on the Employee Perceptions of Remote Work and Cybersecurity in an International Organisation during COVID-19“. [Online]. Accessed: May 18, 2026. MA thesis. Université de Genève, 2021. URL: https://archive-ouverte.unige.ch/unige:154452.

[48] A. Gryszczyńska. „The impact of the COVID-19 pandemic on cybercrime“. In: *Bulletin of the Polish Academy of Sciences: Technical Sciences* 69.4 (2021), e137933. DOI: 10.24425/bpasts.2021.137933.

[49] L. Hu. *Fake websites used in COVID-19 themed phishing attacks, impersonating brands like Pfizer and BioNTech*. Unit 42 Threat Research, Mar. 24, 2021. [Online]. Accessed: May 18, 2026. 2021. URL: https://unit42.paloaltonetworks.com/covid-19-themed-phishing-attacks/.

[50] Proofpoint. *Attackers use COVID-19 vaccine lures to spread malware, phishing and BEC*. Proofpoint Blog, Jan. 14, 2021. [Online]. Accessed: May 18, 2026. 2021. URL: https://www.proofpoint.com/us/blog/threat-insight/attackers-use-covid-19-vaccine-lures-spread-malware-phishing-and-bec.

[51] World Health Organization. *Pandemic Fatigue: Reinvigorating the Public to Prevent COVID-19*. Revised version, Nov. 2020. [Online]. Accessed: May 18, 2026. 2020. URL: https://iris.who.int/server/api/core/bitstreams/3ed4b3dc-e449-477e-8a0b-3c6fe2902c52/content.

[52] A. Choudhary et al. „Emerging cyber security challenges after COVID pandemic: A survey“. In: *Journal of Internet Services and Information Security* 12 (2022), pp. 21–50. DOI: 10.22667/JISIS.2022.05.31.021.

[53] C. Zaboeva and M. Frydrych-Dean. *IBM uncovers global phishing campaign targeting the COVID-19 vaccine cold chain*. IBM Think X-Force, 2020. [Online]. Accessed: May 18, 2026. 2020. URL: https://www.ibm.com/think/x-force/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain.

[54] European Union Agency for Cybersecurity. *ENISA Threat Landscape 2021*. Tech. rep. Oct. 2021. [Online]. Accessed: May 18, 2026. ENISA, 2021. URL: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202021.pdf.

[55] M. de Haas, R. Faber, and M. Hamersma. „How COVID-19 and the Dutch 'intelligent lockdown' change activities, work and travel behaviour: Evidence from longitudinal data in the Netherlands“. In: *Transportation Research Interdisciplinary Perspectives* 6 (2020), p. 100150. DOI: 10.1016/j.trip.2020.100150.

[56] A. Chung and S. Balla. *Phishing eager travelers*. Unit 42 Threat Research, Sep. 15, 2021. [Online]. Accessed: May 18, 2026. 2021. URL: https://unit42.paloaltonetworks.com/travel-themed-phishing/.

[57] X. Wang and J. F. Petrick. „Understanding traveler behavior before, during, and post COVID-19“. In: *International Journal of Tourism Research* 27.5 (2025), e70137. DOI: 10.1002/jtr.70137.

[58] Z. Wang, W.-J. Huang, and B. Liu-Lastres. „Impact of user-generated travel posts on travel decisions: A comparative study on Weibo and Xiaohongshu“. In: *Annals of Tourism Research Empirical Insights* 3.2 (2022), p. 100064. DOI: 10.1016/j.annale.2022.100064.

[59] J. I. Blanford et al. „Navigating travel in Europe during the pandemic: From mobile apps, certificates and quarantine to traffic-light system“. In: *Journal of Travel Medicine* 29.3 (2022), taac006. DOI: 10.1093/jtm/taac006.

[60] Which? Press Team. *Which? warns of six new holiday scams and rip-offs as travel opens up again*. Feb. 26, 2022. [Online]. Accessed: May 18, 2026. 2022. URL: https://www.which.co.uk/policy-and-insight/article/which-warns-of-six-new-holiday-scams-and-rip-offs-as-travel-opens-up-again-a1hul9e5icuI.

[61] P. Esteve-Gonzalez et al. „Cybersecurity implications of changing patterns of office, home, and hybrid work: An exploratory global survey“. In: *SSRN Electronic Journal* (2023). DOI: 10.2139/ssrn.4322366.

[62] N. Sanders. „The Effects of COVID-19 Lockdowns on Cybersecurity“. [Online]. Accessed: May 18, 2026. MA thesis. Electronic Theses, Projects, and Dissertations, 2024. URL: https://scholarworks.lib.csusb.edu/etd/2069.

[63] Eurofound. *The Future of Telework and Hybrid Work*. Tech. rep. [Online]. Accessed: May 18, 2026. Luxembourg: Publications Office of the European Union, 2023. URL: https://www.eurofound.europa.eu/en/publications/all/future-telework-and-hybrid-work.

[64] R. Todorov. „Compliance with Corporate ICT Security Practices in Work from Home Environment: Attitude Changes in the Move from Office to Home“. [Online]. Accessed: May 18, 2026. MA thesis. Dept. of Informatics, Linnaeus University, 2023. URL: https://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-125458.

[65] R. Hasan and M. Elweskiöld. *Phishing in Remote Work: An Understanding of Factors That Enhance Employee Susceptibility to Phishing Attacks: A Qualitative Study*. [Online]. Accessed: May 18, 2026. 2025. URL: https://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-244871.

[66] S. Jenifer. „Securing the distributed workforce: A framework for enterprise cybersecurity in the post-COVID era“. In: *ICRCEDA2025 Conference Proceeding, International Journal of Emerging Research in Engineering and Technology*. 2025. DOI: 10.63282/3050-922X.ICRCEDA25-127.

[67] H. C. Kelman. „Compliance, identification, and internalization: Three processes of attitude change“. In: *Journal of Conflict Resolution* 2.1 (1958), pp. 51–60.

[68] N. Akbar. „Analysing Persuasion Principles in Phishing Emails“. Oct. 2014. [Online]. Accessed: May 18, 2026. MA thesis. Enschede, The Netherlands: University of Twente, 2014. URL: https://purl.utwente.nl/essays/66177.

[69] J. C. Auton and D. Sturman. „Persuasion under pressure: The influence of persuasion principles and time constraints on phishing email susceptibility“. In: *Information and Computer Security* 33.5 (2025), pp. 845–859. DOI: 10.1108/ICS-07-2024-0163.

[70] E. J. Williams, J. Hinds, and A. N. Joinson. „Exploring susceptibility to phishing in the workplace“. In: *International Journal of Human-Computer Studies* 120 (2018), pp. 1–13. DOI: 10.1016/j.ijhcs.2018.06.004.

[71] A. Vishwanath. „Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack“. In: *Journal of Computer-Mediated Communication* 20.5 (2015), pp. 570–584. DOI: 10.1111/jcc4.12126.

[72] S. Chaiken, A. Liberman, and A. H. Eagly. „Heuristic and systematic information processing within and beyond the persuasion context“. In: *Unintended Thought*. Ed. by J. S. Uleman and J. A. Bargh. New York, NY, USA: Guilford Press, 1989, pp. 212–252.

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Markus Joonas Palu

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "MAPPING PANDEMIC EVENTS, ATTACKER ADAPTATION, AND PSYCHOLOGICAL MANIPULATION IN COVID-19 PHISHING", supervised by Kaido Kikkas
    1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
    1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright
2. I am aware that the author also retains the rights specified in clause 1 of the nonexclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

19.05.2026

[1]The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive licence shall not be valid for the period.