CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Department of Political Science

Master's Thesis

2021 **Viliam Kaliňák**

CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Department of Political Science

Psychology of Phishing Attacks during Crises: The Case of COVID-19 Pandemic

Master's thesis

Author: Viliam Kaliňák

Study program: Political Science (N6701)

Supervisor: Mgr. David Erkomaishvili, Ph.D.

Year of the defense: 2021

Declaration

1. I hereby declare that I have compiled this thesis using the listed literature and resources only.
2. I hereby declare that my thesis has not been used to gain any other academic title.
3. I fully agree to my work being used for study and scientific purposes.

In Prague on July 26, 2021. Viliam Kaliňák

References

KALIŇÁK, Viliam. *Psychology of Phishing Attacks During Crises: The Case of COVID-19 Pandemic*. Praha, 2021. 65 pages. Master's thesis (Mgr.). Charles University, Faculty of Social Sciences, Department of Political Studies. Supervisor Mgr. David Erkomaishvili, Ph.D.

Length of the thesis: 90 029 characters

Abstract

Events and circumstances that accompany crises such as losses of loved ones, losses of material resources, dislocation, or physical harm, have an overall negative impact on people's mental health. It is this impaired state of man which makes him vulnerable to manipulation of social engineers who wants to take advantage of him in order to enrich themselves. This was also the case of the COVID-19 pandemic, the unprecedented crisis in modern history, during which phishing and fraud campaigns rapidly increased as people have been forced to stay safe at home and spent most of a day online. This work analyzes the psychological strategies of cybercriminals on a sample of more than 200 phishing e-mails in order to understand how the situation was abused and what can be learnt to prevent it in the future. It also provides theoretical and research frameworks for researchers who can apply it also on other types of crises. The results contribute to the fields of psychology, cybercrime as well as crisis management.

Abstrakt

Obecně platí, že události a okolnosti, které doprovázejí krize, jako jsou ztráta blízkých, materiální ztráty, dislokace nebo fyzická újma, mají celkově negativní dopad na duševní zdraví lidí. Právě tento narušený stav člověka ho činí zranitelným vůči manipulaci sociálních inženýrů, kteří to chtějí zneužít k svému vlastnímu obohacení. To byl také případ pandemie COVID-19, bezprecedentní krize v moderní historii, během níž rychle rostl počet phishingových a podvodných kampaní, jakmile byli lidé donuceni k tomu, aby zůstali v bezpečí doma a trávili většinu času online. Tato práce proto analyzuje psychologickou hru kyberzločinců na vzorku více než 200 e-mailů, aby zjistila, jak byla tato situace zneužívána a jaké ponaučení z ní plynou, aby se podobným případům do budoucna zabránilo. Její součásti jsou také teoretické a analytické rámce pro výzkumníky, kteří je mohou aplikovat také na jiné typy krizí. Výsledky přispívají do oblasti psychologie, počítačové kriminality i krizového řízení.

Keywords

COVID-19, phishing, social engineering, psychology, persuasion, crises, pandemic, impersonation, pretexting

Klíčová slova

COVID-19, phishing, sociální inženýrství, psychologie, přesvědčování, krize, pandemie, impersonace, pretexting

Title

Psychology of phishing attacks during crises: The case of COVID-19 pandemic

Název práce

Psychologie phishingových útoků během krizí: Případ pandemie COVID-19

Acknowledgement

I would like to express my gratitude to Mr. David Erkomashvili who supervised my thesis and provided me with valuable advice, support, understanding and patience.

Table of Contents

INTRODUCTION **1**

1. THEORETICAL FRAMEWORK **3**

1.1. Theoretical Background 3

1.2. Theoretical Framework 4

1.3. Related Research 6

2. METHODOLOGY **7**

2.1. Hypotheses and Research Questions 8

2.2. Research Framework 9

2.2.1. Principles of Persuasion *11*

2.2.2. Impersonation *13*

2.2.3. Pretexting *13*

2.3. Methods 14

2.3.1. Stages of Crisis *15*

2.3.2. Principles of Persuasion *16*

2.3.3. Impersonation *18*

2.3.4. Pretexting *20*

2.3.5. Explanation *22*

2.4. Coding Example 22

2.5. Transcribed E-mail Example 23

2.6. Data 25

3. STAGE #1: JANUARY TO MID-MARCH 2020 ..... **26**

3.1. Description of the Situation 26

3.2. Explanation of the Situation 27

3.3. Transcribed E-mail Example 28

4. STAGE #2: MID-MARCH TO JULY 2020 30

4.1. Description of the Situation 30

4.2. Explanation of the Situation 31

4.3. Transcribed E-mail Example 33

5. STAGE #3: AUGUST TO DECEMBER 2020 35

5.1. Description and Explanation of the Situation 35

5.2. Transcribed E-mail Example 37

6. DISCUSSION ON PSYCHOLOGY OF PHISHING ATTACKS DURING CRISES 39

7. LIMITATIONS 41

CONCLUSION 42

BIBLIOGRAPHY 45

LIST OF APPENDICES 53

APPENDIX NO. 1: SAMPLE OF PERFECT DATA 54

APPENDIX NO. 2: SAMPLE OF IMPERFECT, BUT STILL USABLE DATA 55

APPENDIX NO. 3: SAMPLE OF UNUSABLE DATA 56

Introduction

The old saying is that on the Internet, nobody knows you are a dog. This was true in the beginnings of this network of networks and is still true today. The problem is that nobody can stop people from making up their own personas or impersonating the real ones. And bad guys are very well aware of these social engineering opportunities. They leverage the imaginary fog of the internet to trick people online into revealing sensitive information about themselves, giving them money or downloading malicious attachments.

Considering how easy is to register an e-mail address and come up with a fake story, no wonder that, according to cybersecurity firms, fraudulent phishing messages are the top initial vector used in approximately a third of all cyberattacks (IBM X-Force 2021, Verizon 2021). However, these are not necessarily as banal as the Nigeria-prince-scam likes. In 2020, even sophisticated cybercriminal threat actors, such as Emotet, or state-sponsored hacking groups from Iran and Russia used them to enrich themselves or steal secret documents (IBM X-Force 2021, p. 14, 24, 25).

National and international security bodies acknowledge this situation by putting phishing among the top threats which they and their citizens face in cyberspace (see ENISA 2020, FBI 2020). The reason is that cyber criminals heavily exploit human weaknesses upon which all security systems are dependent on. Unless users, students and employees are trained to recognize them, they can easily lead to exfiltration of data, disruptions and other damages to critical information systems and computer networks. Therefore, phishing awareness as part of a broader education agenda has been put among the top priorities for cybersecurity of many states (see Ministerstwo Cyfryzacji 2019, NBÚ 2021, NÚKIB 2020).

However, most of these plans and precautions had been launched during peacetime prior to one of the biggest crises in history of humankind – the global COVID-19 pandemic which for more than a year now has been banishing people from work to homes. It was in this unprecedented time when people's lives largely moved to online space. Home-office workers and students who have been spending most of a day online have suddenly had to face a sharply increased phishing and fraud campaigns that leveraged the coronavirus crisis and the lockdown topics (INTERPOL 2020).

In the beginnings of the crisis, it was basically a trial of fire for institutions around the world to ensure that their staff is ready to counter cyber threats over the next few months. People

have been given advice, recommendations, tutorials etc. to learn their cyber hygiene. However, too many factors have impact on success of this training.

When people are locked down at home for several days, weeks or months during a pandemic, or when they lose a job, material resources or even relatives as a consequence of it, their mental health is significantly challenged. And once they identify the environment and atmosphere around them as stressful, the inevitable tendency is to focus attention on the immediate proximal problem, for example to procure the basic needs for food, water, shelter, procreation, and so forth (Hancock and Matthews 2015, pp. 553-554).

It is exactly in times like this when cybercriminals can leverage the situation for their own benefit. If governments order the mandatory wearing of protective face masks but they are sold out in shops, or when a man is short of money and there are no vacancies, criminals can impersonate someone who can allegedly provide him with a solution over the internet.

This work will therefore focus on how cybercriminals abuse the situation and what can be learnt from phishing and fraud campaigns during this pandemic for cybercrime preventive initiatives and future research. Specifically, it will analyze the psychology of fraudulent messages in order to determine what human weaknesses are exploited.

In the first chapter, the work provides a theoretical framework which describes the overall functioning of phishing attacks during crises. Despite that its main focus is on the COVID-19 pandemic, it suggests two approaches for research of phishing which can explain susceptibility of people to such e-mails during any type of crisis as well as how specific circumstances of the crisis are abused.

The second chapter is devoted to methodology and research framework which unifies and builds on previous research. It also includes a clear procedure for how to analyze individual components of messages as well as suggestion on how to proceed and get the most out of the analysis of phishing campaigns that take place over long periods of time.

In chapters three, four and five, the work analyses the development of cybercriminal techniques and the most representative phishing e-mails from individual stages of the crisis, and explains why attackers used certain principle of persuasion, impersonated entity and pretext. Examples of such message are also included.

The last two chapters are dedicated to discussion of results, recommendations for crisis communication and security solutions, suggestion for further research and limitations of the work.

1. Theoretical Framework

This chapter will discuss theoretical framework, its strengths and weaknesses, and contribution to the field of psychology of phishing. Firstly, a background of the work which draws from the fields of crisis management, cybercrime, and psychology will be presented. Then, the chapter will set the theoretical framework into the crisis scene and explain its logic and possible use. It will explain why under such circumstances researchers cannot fully replicate the phishing campaign in an experimental work. Finally, it will discuss differences between and shortcomings of previous works. It finds that only one author has contributed to research of phishing attacks during a crisis so far.

1.1. Theoretical Background

According to Garayev (2013), crises are unexpected negative changes which emerge suddenly and create a chaotic, dangerous, and unstable situation at all the levels of society. They require special crisis management tools, skills, and measures in order to reestablish the previous normality. But whether through significant changes or without them, they consequently test the resiliency of the system and society. In recent years, such were the cases of the global financial crisis in 2008-2009, the Haiti earthquake in 2010, the eastern Ukrainian political crisis since 2014, the Yemen humanitarian crisis since 2015, or the European migrant crisis in 2015-2019.

In general, events and circumstances that accompany crises such as losses of loved ones, losses of material resources, lack of social interaction, dislocation, or physical harm, have an overall negative impact on people and aggravate their existing mental problems or lead to new ones (Jenkins and Meltzer 2012, Ono et al. 2011, Raphael 2000). The same applies to the ongoing COVID-19 pandemic which significantly changed daily lives of people all around the world and set a “new normal”. Mutual trust of states has shaken, economies have fallen into recession, public health institutions have been put under unprecedented pressure, and social life has nearly stopped as people have been forced to stay safe at home. Several studies (see Every-Palmer et al. 2020, Petzold et al. 2020, Talevi et al. 2020) have now

confirmed that these events negatively influenced people's minds especially in terms of stress and anxiety.

Regarding the management of these negative impacts, Zimmerman (2013) argues that a central role plays crisis communication which is to reduce exposure to the risks through timely, accurate, and appropriately disseminated information, to guide people to safe places, to adopt and implement protective action such as vaccines and shelters, or to reduce fear and anxiety. However, both Schwarz (et al. 2016) and Bennett (et al. 2010) agree that for this process to be effective, important factors are trust of the public in institutions and authorities, and diversity of information provided, i.e. targeting people with messages adjusted to their background. Otherwise, they will seek other means to obtain required missing information, e.g. on the internet that has become the main source of information gathering and sharing, and opinion shaping.

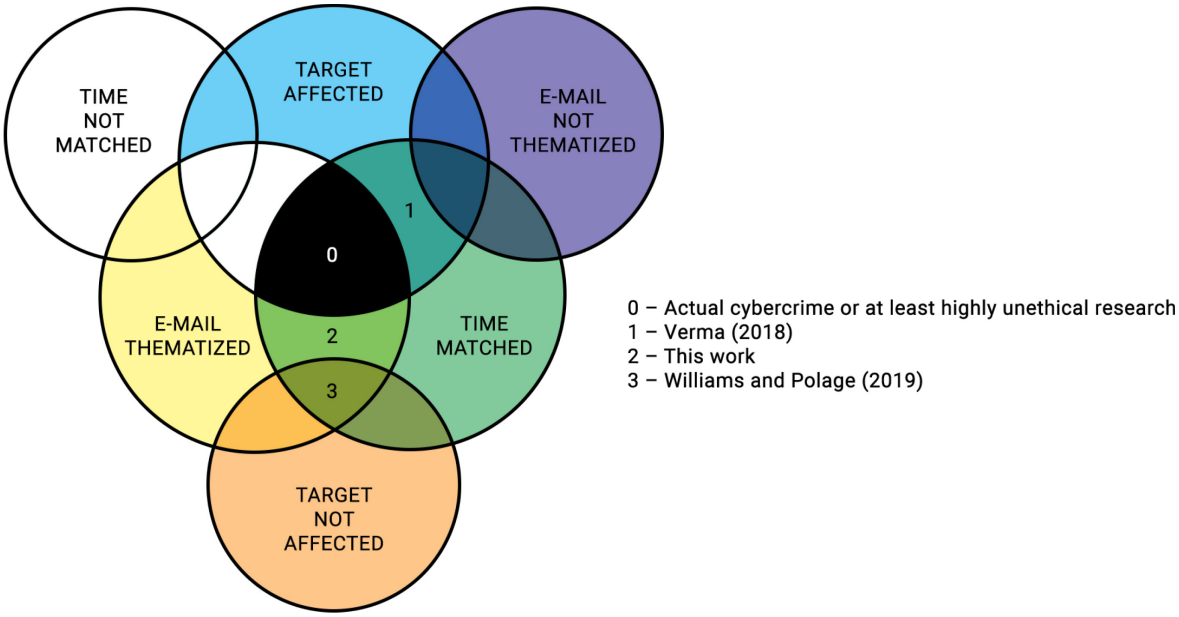
Meanwhile, with more people spending more time on the internet during the COVID-19 pandemic, it is just this impaired mental health with the need for information which rises risks of falling victim to cybercrime through phishing. Jakobsson and Myers (2007) consider phishing attacks as a form of social engineering in which attackers try to persuade their targets into revealing confidential information or installing a malicious software on their computers. For this purpose, Mitnick (2011) and Hadnagy (2010) argue that a bad mental state of the target may be helpful since it can easily distract him and make him more vulnerable to social engineering that stimulates his emotions. According to Hancock and Matthews (2015, p. 554) this may be because under extremes of stress evoked by the chaotic environment, people focus their attention on the immediate proximal problem which is here and now. They do not plan for the distant future nor consider long-term impact since those who do this tend not to exist in that future (Ibid). Therefore, in regard to crisis communication and the information need, social engineers may impersonate authority in charge of the process to create such plausible story which is in accordance with the target's beliefs and expectations, and which could ostensibly solve his problems.

1.2. Theoretical Framework

Theory on psychology of phishing attacks during crises builds on a premise that since crises create a chaotic and unpredictable environment which negatively affects people's mental health, it makes them more vulnerable to manipulation of cybercriminals who will exploit it for their own benefit. Such phishing would be characterized by an e-mail which 1) during or

shortly after a crisis 2) thematizes the message according to the ongoing events in order to benefit 3) on people affected by this situation. The logic of this framework dwells in interconnectedness and dependency between all three factors (see Figure 1).

Figure 1: Theoretical framework for the research on psychology of phishing attacks during crises.



Without a time match, i.e. if a thematized e-mail targeted affected people long after the crisis, targets would not necessarily be as vulnerable and inclined to engage with such an e-mail as during the crisis since their lives and mental health would stabilize and get back to normal by then. Without a thematized e-mail, i.e. if affected people were targeted by e-mails non-related to the ongoing crisis, targets would not necessarily be interested and inclined to engage with such an e-mail since they would not expect that this e-mail would fulfill their need for information related to the ongoing crisis. And without people affected by a crisis as targets. i.e. if thematized e-mails were sent to random people during or shortly after the crisis, targets would not necessarily be interested and inclined to engage with such an e-mail since some of them may had not been affected by these events and thus the situation would not be related to them.

In practice, intersection of these three factors would constitute actual cybercrime or at least highly unethical experiment since the researcher would need to replicate the whole attack on participants disturbed by a crisis. Therefore, in order to avoid these problems, researchers need to work only with two factors, intersection of which would require different methodology. As already examined by Verma (2018), what role do target affected and time matched factors play in phishing attacks was analyzed through survey. Shortly after the

event, participants affected by a crisis were inquired about their experiences with crisis-related e-mails that they had received at that time. On the other hand, the intersection between time matched and e-mail thematized would require content analysis of e-mails sent during a crisis in order to determine how specifically attackers abused the situation. But a problem arises with the third intersection between target affected and e-mail thematized. It is impossible to conduct such a research since it cannot be done in "time vacuum", i.e. it would either fall into the black zone of cybercrime or highly unethical experiment, or would not be reliable due to the above-mentioned hurdles with the time delay. In this regard, the first research would determine whether people are more vulnerable to phishing in such situation, the second one would determine what principles and tools of persuasion were used, but since the third research cannot be conducted, it will not determine to what specific principles and tools of persuasion are people more vulnerable in such situation.

Nevertheless, this framework has three advantages. Firstly, it might help to explain susceptibility of people to phishing in different situations. Secondly, it might help predict "psychological game" of cybercriminals during crises in the future. And thirdly, it might help to mitigate risks of falling victim to cybercrime if potential targets were acquainted with such findings of crisis-related phishing e-mails.

1.3. Related Research

Research on psychology of phishing emails can be divided into two interconnected fields. The first one examines attacker's tools and principles of persuasion deployed in an email. For example, Akbar (2014) analyzed principles of persuasion and pretexting in 207 emails and found out that financial and e-commerce sectors were mostly targeted by account related emails which were associated with *Authority* as the mostly used persuasive principle. Similarly, Atkins and Huang (2013) examined 200 emails and concluded that the principle of *Authority* was used in all of them while the most often pretexting was alert, warning, attention and account verification.

The second field examines people's susceptibility to these techniques and principles. Baryshevtsev and McGlynn (2020) tested susceptibility of students and concluded that participants found principles of *Liking* and *Authority* more credible than *Social proof*. While Wright (et al. 2014) agrees that *Liking* was an influential principle, in his case *Social proof* also increased the likelihood that participating students would respond to phishing email, suggesting that different groups are susceptible to different principles.

However, analyses done so far have been conducted rather on a wide variety of themes from various periods of time and on a variety of groups. Only a small fraction of works from both of these fields actually analyzed phishing emails according to intersection between at least two of three important factors – whether an email is thematized according to current events that directly affect people.

In regard to theme and time match, Williams and Polage (2019) tested phishing emails among participants from Central Washington University. They concluded that references to current events, the Rio Olympics in their case, did not make phishing emails appear any more legitimate than those that did not. On the other hand, in regard to time match and targets affected, Verma (et al. 2018) conducted a survey on experiences with phishing and reaction to it among participants from University of Houston shortly after the hurricane Harvey hit Texas in 2017.

This work showed that participants were more likely to click on a link or download an attachment if they received hurricane-related e-mails during the storm. Verma's research therefore suggests that if a target is being directly confronted with an event that is mentioned in phishing e-mail, it is more likely to be persuaded than in the case of Williams and Polage when the target was not directly affected by the event, i.e. their students did not directly participate in the Olympics. At the same time, in regard to the theory on psychology of phishing attacks during crises, Verma's research also suggests that events related to crises are more sensitive issue than events related to sport, and hence the latter may be a subject of research even during the ongoing event while the former cannot or at least should not be.

2. Methodology

In this chapter, a hypothesis and related research questions will be discussed altogether with an example of perfect scenario that would confirm it if proved to be true. Then, it will describe the proposed research framework based on previous works, and methods used to investigate accuracy of the theory with a clear coding example on a transcribed phishing e-mail. It will also explain why one component was omitted from original framework. Finally, it will describe data collection and filtering process.

2.1. Hypotheses and Research Questions

As already mentioned earlier, the intersection of target affected and time matched had already been analyzed by Verma (et al. 2018). Therefore, this research will focus on the intersection between e-mail thematized and time matched factors. The research will work with one straightforward hypothesis that is inherent to the theoretical framework. Describing from top to bottom, since previous research suggested that one of the mostly used and influential principles of persuasion is *Authority*, it is expected that cybercriminals will deploy e-mail messages in accordance with this principle. For this purpose, the research will examine what different principles do they use to persuade victims into executing a certain action, and what is their frequency.

Secondly, since authorities are in charge of crisis management and communication, it is expected that the mostly impersonated entity associated with the principle of *Authority* will be *State agencies*. In order to investigate this assumption, the research will examine what type of entities can be identified from the information provided in the e-mail message, and what is their frequency with respect to the principles of persuasion.

Finally, it is assumed that when there is an information need during a crisis, phishing e-mails will provide alleged information related to security and safety so as to mimic the crisis communication. It is expected that this type of pretexting will be mostly used by impersonated *State agencies* in combination with the principle of *Authority*. Hence, the research will examine what different types of pretexting can be identified, and what is their frequency with respect to the impersonated entity related to certain principle of persuasion.

If all the three conditional assumptions were proved to be true, the perfect scenario which would confirm the hypothesis would be if crisis-related phishing e-mails were in most of the cases sent, for example, in the name of ministry of health (impersonation of *State agency*) which would order recipients (principle of *Authority*) to download a list of recommended personal protective equipment (*Security guidelines* as the pretext). Hypothesis conditioned in such a way, even if refuted, enables the research to filter out marginal cases and focus only on the most representative ones. Thanks to this approach, the research can better explore psychology of phishing during crises, predict the "psychological game" of attackers in the future, and come up with recommendations on how to mitigate the risk of falling victim to cybercrime.

Table 1: Hypothesis and research questions

Hypothesis	Main research questions	Related research questions
During a crisis, cybercriminals use the principle of authority, the name of state agencies, and alleged security guidelines to persuade their victims.	What is the most frequent principle of persuasion?	What principles of persuasion can be identified?
	What type of impersonated entity is mostly associated with the most frequent principle of persuasion?	What types of entities can be identified?
	What type of pretexting does the mostly impersonated entity associated with the most frequent principle of persuasion use?	What type of pretexting can be identified?

2.2. Research Framework

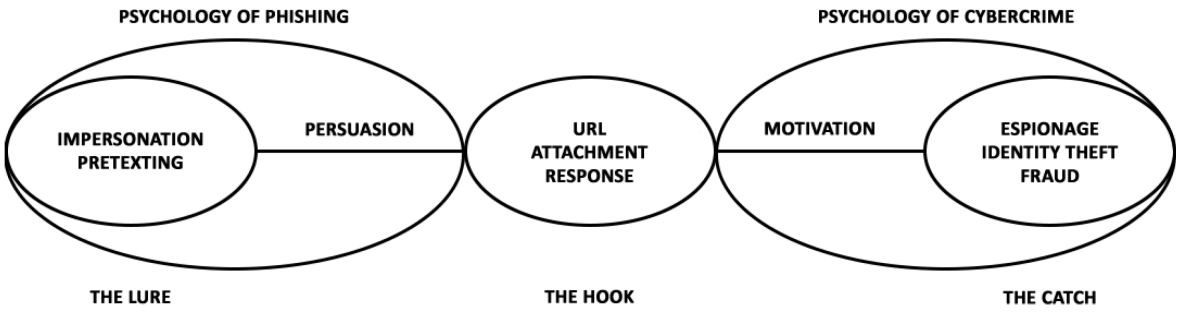
Jakobsson and Myers (2007) described three components of phishing e-mail: the lure, the hook, and the catch. The lure most frequently consists of e-mail messages in which attackers impersonate a legitimate entity and provide a convincing story, the so-called pretext, which encourages the target to engage with the second part, the hook. The hook typically consists of a website that mimics the appearance of that of a legitimate target institution. The last part, the catch, involves the attacker making use of the collected information for some criminal purpose such as fraud, identity theft or espionage.

Based on these three components, a scheme of relations between elements of particular parts can be drawn (see Figure 2). The first relation is persuasion whereby the attacker tries to persuade the victim to "fall into a trap" by impersonation and pretexting. The second is motivation between this trap and the consequent utilization of it. However, the "psychological game" of phishing takes place only in the first relation, i.e. how attackers persuade victims, while the second one is related to more general psychology of cybercrime, i.e. why attackers do what they do.

Nevertheless, the motivation of an attacker is closely interconnected with the persuasion in a way that he firstly needs to create a believable pretext which reflects his motivation, then he needs to create a fake persona in whose name he delivers the pretext, and finally he needs to "sell" the pretext and impersonation in a way which will persuade his victim. For example, if he is motivated by money, his pretext would be a payment request. But this request must

come from a trustworthy entity, not an ordinary man, so he would impersonate for example chief executive officer from victim's company. Finally, he would need to choose the right tactic to deliver this scam – in this case, since it is victim's alleged superior, he would choose principle of *Authority* rather than principle of *Social proof*.

Figure 2: Research framework for analysis of phishing e-mails based on Jakobsson and Myers (2007)



Therefore, impersonation and pretexting may be perceived as tools of persuasion, and the way how social engineers employ them follows, according to Sagarin and Mitnick (2012), Cialdini's six principles of persuasion. These principles may be used either separately, or simultaneously to evoke the impression of time pressure, reciprocal obligations, or small commitments. To better illustrate the difference of individual principles of persuasion, imagine this scenario: Attacker may impersonate victim's colleague from another branch with the pretext being a request for access to certain files. He may utilize these tools either to evoke the impression that this request comes "from above" and is required to be given immediately, or to evoke the impression of compassion that this impersonated colleague had lost the files and now needs a favor so as not to get blamed on for this mistake.

However, it is important to note that according to Ferreira (et al. 2015), besides the work of Cialdini (2007), other authors have also suggested their own principles of persuasion, e.g. Gragg (2003), and Stajano and Wilson (2011), and that their works may serve as a guide in research on social engineering and phishing as well. A comparison of these principles is provided below (see Table 2).

For the purpose of this work, impersonation and pretexting will be regarded as tools of persuasion which are employed by attackers in a way that follows principles of persuasion. Therefore, the research on psychology of phishing is here defined as a study of 1) the employment of tools of persuasion according to principles of persuasion, and 2) susceptibility to these tools and principles of persuasion.

2.2.1. Principles of Persuasion

As Ferreira (2015, 2019) argues, although there are three foundational works on principles of persuasion, it is still unclear what basic principles constitute a clear and complete basis for social engineering and whether what makes social engineering persuasive should be found only among Cialdini's, Gragg's, and Stajano and Wilson's, or somewhere else. Thus, she proposed a reviewed list of principles of persuasion based on comparison and merger of the above-mentioned principles in order to achieve consistency (see Table 3).

Table 2: Comparison of principles of persuasion

Gragg (2003)	Cialdini (2007)	Stajano and Wilson (2011)	Ferreira (2019)
Authority	Authority	Social compliance	Authority
Diffusion responsibility	Social proof	Herd	Social proof
Deceptive relationship	Liking	Deception	Liking, similarity and deception
Integrity and consistency	Commitment and consistency	Dishonesty	Commitment, reciprocation and consistency
Overloading	Scarcity	Time	Distraction
Reciprocation	Reciprocation	Need and greed	
Strong Affect		Distraction	

Table 3: Principles of persuasion according to Ferreira (2019)

Principle	Description	Example
Authority	Society trains people not to challenge authority but to respond without questioning. People usually follow an expert or a figure of authority and will do a great deal for who they think is in charge.	An email purporting to be from the recipient's bank, including the bank name in the subject line.
Social proof	People tend to mimic what the majority of people do or seem to be doing, so let their guard and suspicion down and prefer to share the same responsibilities and risks. In this way, they will not be held solely responsible for their actions if anything goes wrong.	An email from an alleged system administrator with an email address of the company where the recipient works asking him/her to test a link, which is also being tested by his/her colleagues.
Liking, similarity and deception	People prefer to follow or relate to other people whom they know, like, are attracted to, or who seem familiar or similar to themselves. However, people (and things) are not what they seem and are manipulated to believe that they are.	An email from a supposed friend of the recipient asking him/her to visit an interesting website.
Commitment, reciprocation and consistency	Reciprocating a favor or responding to some action can be an automatic response that is linked to a sense of commitment with a previous situation. Also, people will, by default, believe that the person with whom they are talking is telling the truth about what they feel or need.	An email where the sender knows beforehand that the recipient is looking to buy a house, and which promises a very good price for a house with the same characteristics and on the same location the recipient wants. To secure it (commitment), the recipient needs to urgently pay for a deposit (reciprocation).

Distraction	When people focus on what they can gain, lose or need, on strong emotional states or on whether an item will soon be unavailable or is restricted, this can heighten people's emotional state and make them forget other important considerations when making decisions.	An email acknowledging that the recipient has won a substantial lottery prize. The victim focuses mainly on how she/he can have access to the money and attention is diverted from other details such as, for instance, that a lottery ticket has never been bought.

2.2.2. Impersonation

Watson (2014) considers impersonation as acting or playing a role with the impersonated entity being likely to be a fake character specifically designed for the story rather than a real one. The reason is that impersonating a real character involves many challenges of replication such as learning enough information about the impersonated character which if inconsistent, may draw attention and affect the overall act of social engineering. However, he admits that online impersonation via e-mail requires detail for the writing style of impersonated person, and not the specific information about him. Thus, in the latter case, this set of required information does not necessarily need to be broad for successful impersonation. Rather than a list similar to that of Sammons and Cross (2015) which consists of full name, physical address, social security number, passport number, or even a copy of signature, online social engineer only needs a few of them. For example, Mitnick (2011) suggested that sometimes only a name and a phone number may be sufficient to support authenticity and credibility of the character.

2.2.3. Pretexting

Regarding pretexting, authors provide similar definitions. Hadnagy (2010) defines it as a background story which may consist even of lies in order to persuade a targeted victim to release information or perform some action. Watson (2014) regards it as a predesigned sequence of believable events with supportive information to engage the victim. And Andress (2014) as a provision of sufficient reason and cause for the victim to believe that the author of this scenario deserves access to information, or that the asked action needs to be taken. Jakobsson and Myers (2007) typified some of these scenarios into security upgrades, incomplete account information, financial incentive, or false account upgrades,

but they stress that the list of possible types of scenarios is almost limitless as scenarios are getting more sophisticated over time so as to match the context that the victim is expecting. This means that taxonomy of pretexting constantly evolves and depends on attacker's creativity. Therefore it may consist of any story, reason, incentive, and/or event which makes it hard to strictly typify.

2.3. Methods

This research focuses on psychology of phishing "from within" e-mails. It does not analyze tools and principles of persuasion used in the subject lines nor e-mail addresses of senders which are on the "outside" and which purpose is only to persuade the recipient to open such an e-mail. While for this purpose the attacker may not need to make a great effort as any e-mail may be opened out of natural curiosity, he needs more finesse to persuade the recipient to execute the action that is expected from him after reading the e-mail, e.g. a response or a click on the link. Therefore, the research only deals with the content of messages which is visible only after the e-mail was opened. The way the research approaches analysis follows a reversed model described in the research framework part. Unlike the attacker whose process begins with creating a pretext and ends with persuasion, this research starts with analysis of persuasion and ends with the pretext – similar to peeling an onion in layers.

While certain types of crisis may be relatively short in terms of duration, e.g. earthquakes or hurricanes, the duration of COVID-19 pandemic enables the research to better map how persuasion of phishing works thanks to the fact that different stages of it stretch over longer periods of time and are more clearly recognizable. Therefore, the timeline of COVID-19 will be divided into parts that correspond to the stages of crisis as suggested by Antušák and Vilášek (2016). These are the stage of crisis symptoms, the acute stage of the crisis, the chronic stage of the crisis, and the stage of crisis resolution. The research framework will be applied on each of them.

With respect to the theory, this step was not included in the theoretical framework since it is rather optional and recommended only when the nature of the crisis suits it. Therefore, when the duration of crisis is relatively short, e.g. a few days or weeks, it may be analyzed as a whole due to the fact that the findings from different stages might not be of significant informative value.

2.3.1. Stages of Crisis

To describe the evolution of COVID-19 pandemic, this work relied on the timeline provided by World Health Organization (2021). As the pandemic is a global crisis, it is believed that this timeline from international organization responsible for international public health is neutral in respect to geographical regions, and describes the evolution from global perspective. This was important to avoid geographical bias that could distort the course of the pandemic. Delimitation points of particular stages of crisis (see Table 4) were determined by significant key events and dates which "symbolized" transition from one stage to the other. However, since this research was done during the pandemic and therefore covered only those periods already experienced, the timeline obviously omitted the last stage of crisis resolution.

As the delimitating point between the first and the second stage was chosen March 11, 2020, when the situation reached alarming levels of spread and severity and World Health Organization declared COVID-19 as a pandemic. The second delimitating point was chosen July 31, 2020, when World Health Organization on its fourth meeting of the Emergency Committee declared that, despite efforts, it anticipated lengthy duration of the COVID-19 pandemic and therefore declared that this pandemic continued to constitute a public health emergency of international concern.

Table 4: Stages of crisis according to Antušák and Vilášek (2016)

Stages	Description
Stage of crisis symptoms	At this stage, the system is becoming unstable. The crisis manifests itself in slight, negligible symptoms which might be even overlooked and ignored but nevertheless allow one to prepare properly in advance for its further course or even to stop its further course and avert the crisis.
Acute stage of the crisis	The acute stage begins at a time when the discrepancy between the interests of the subject and its external environment deepens to such an extent that it is endangering its interest and existence. Immediate anti-crisis intervention and the deployment of all available means is required to bring the crisis under control.

Chronic stage of the crisis	The chronic stage occurs when the first attempt to overcome the crisis was not effective enough. Although the crisis subsided or tensions were reduced, the cause of the crisis was not sufficiently paralyzed. For this reason, the intensity of the crisis is increasing again after an initial reduction. The course of the crisis can be straightforward, it can take place in waves or even in several directions.
Stage of crisis resolution	If the crisis was managed properly, at this stage, the system is being successfully stabilized and the recovery plan is being implemented.

2.3.2. Principles of Persuasion

To investigate principles of persuasion, the research followed the methodology proposed by Ferreira (2015, 2019) and practically replicated the works. In this regard, content and visual analyses of messages was conducted, and text units were deductively coded into appropriate categories (see Table 5). These units were either excerpts from the text or textual representations of visual components, e.g. logos, images, highlights. Coding of visual components was necessary in order to cover those principles of persuasion which are fully or partially dependent on them, e.g. principle of distraction and highlighted text.

Once coded, the frequency of text units in regard to the principles was counted. Upon this frequency, files in which the mostly used principle appeared were identified for further investigation. The reason why the frequency of text units was chosen over the frequency of number of files where they appeared is that the messages could not be analyzed as a whole but only through particular excerpts. While in the case of impersonation and pretexting the whole e-mail represented the particular category of it since the sender impersonated only one entity with one pretexting in it, in this case he might have used several principles several times in the message. Searching for the mostly used principle throughout the data was important for overall interpretation of attacker's "psychological game", i.e. how ongoing events and fake messages correlated in time.

Table 5: Coding tree for principles of persuasion based on Ferreira (2019)

Parent code	Child code	Description
Authority		Text units based on the premise that people are conditioned to respond to authority figures/authority clues.
Social proof		Text units based on the assumption that people determine the appropriateness of their actions and behaviors by looking to the actions and behaviors of others.
	Herd	Text units based on the assumption that people tend to perform actions, especially risky ones, if people next to them appear to share the same risks.
	Diffusion of responsibility	Text units based on the assumption that people more easily perform an action if the responsibility for his or her actions is perceived as being shared with someone or a group.
	Moral duty	Text units based on the assumption that people more easily perform an action if there is a feeling that she/he is doing something to help someone. The motivation might be truly altruistic or to avoid feeling guilty.
Liking, similarity and deception	Deception	Text units persuade people by manipulation/deceptive scenarios. It excludes deception by establishing relationships.
	Deceptive relationships	Text units suggesting the existence of (false) shared interests, ideals and wants in order to encourage a person to deal with the deceptive character more favorably.
	Liking and similarity	Text units based on the assumption that people are more likely to say 'yes' to the requests of someone they know, like and with whom they share interests, ideals and wants.
Distraction		Text units based on capturing a person attention to a certain information while performing a background action not noticed by the distracted person.
	Scarcity	Text units based on the assumption that people tend to desire more the things they can have less or that are less available.
	Overloading	Text units where people are forced to deal with a lot of information, sometimes within a limited time frame. The sensory overloading tends to affect the person's ability to evaluate the information which is, therefore, passively absorbed.
	Strong affect	Text units that uses a heightened emotional state to distract the person from performing a logical evaluation of the situation. Strong affect includes, but is not limited to fear, excitement or panic.

	Need and greed	Text units based on the assumption that people tend to become more vulnerable when distracted by needs and desires.
Commitment, reciprocation and consistency	Integrity	Text units based on the assumption that people tend to believe that others usually express their true feelings and needs when they make a statement. This assumption is based on their own honesty in expressing feelings.
	Consistency	Text units based on the assumption that people tend to be consistent with the things they have previously said or done, due to personal and interpersonal pressures. Consistency is activated by small initial commitments that can be made.
	Commitment	Text units based on the assumption that people tend to follow through with commitments previously assumed even if those commitments may not have been very wise or receive a lot of thought in the first place.
	Reciprocation	Text units based on the social rule that if someone gives or promise something to another person, the last one tends to feel that she/he must return the favor. This is more evident if the original gift was not requested or even if what is requested in return is far more valuable than what was originally given.

2.3.3. Impersonation

To investigate impersonation, files identified to contain the mostly used principle of persuasion from particular stage were chosen for examination of the supportive information which sender provided about himself so as to compile a list of entities, codes. This list was a sum of the information categories included in the messages themselves, typically in the sender's signature. Namely, they were name, occupation, organization, contact, and logo (see Table 6). However, the preliminary research found two problems.

The first problem was that the data sources had redacted some messages and deprived them of some of this information. Therefore, the subsequent analysis had to be conducted only on those e-mails where such information was clearly observable or could be assumed with certainty (see Data part for clarification).

The second problem was that in some cases senders had provided only a few of the above-mentioned information, or none at all, making identification of the impersonated entity hard to accomplish. Therefore, it was necessary to search for patterns among the supportive information which would enable this process. Consequently, five categories of senders were found – *International organizations*, *State agencies*, *Individuals*, *Anonymous*, and *Other organizations* (see Table 7). The first four were clearly distinguishable from others by

supportive information provided by the sender. But regarding the other organizations, this category subsumed any entity, whether private companies, non-governmental organizations, media or academy, in cases when it was clear that the impersonated entity did not belong to any other category or when the only supportive information provided was for example the occupation. Compared to the first two categories, this information was in their respective cases always accompanied by others making the entity clearly distinguishable.

After obtaining the lists of codes for supportive information and the impersonated entity, the frequency of each element was counted in order to determine which entity was the most impersonated.

Table 6: Coding tree for supportive information

Code	Description
Name	Name of the impersonated person.
Occupation	Job title or affiliated department.
Institution	Name of the affiliated institution.
Contact	Telephone number, office address, etc.
Logo	Logo of the impersonated institution.

Table 7: Coding tree for impersonated entity

Code	Description	Example
International organization	Sender abused name, logo and/or other information related to international organization.	World Health Organization, United Nations
State agency	Sender abused name, logo and/or other information related to state agency.	Ministry of health, Central Bank
Other organization	Sender did not provide sufficient supportive information to determine the type of impersonated entity but indicated he is affiliated with unknown organization and sent the e-mail on its behalf. This category also	CEO, Admin, HR department

	contains entities which clearly did not belong to the others.	
Individual	Sender did not indicate any affiliation with organization, or indicated affiliation with organization but did not send the e-mail on its behalf.	Neighbor, University student
Anonymous	E-mails which did not provide any information about the sender upon which he could be categorized.	

2.3.4. Pretexting

After obtaining the list of files with the most impersonated entity from previous step, pretexting of this entity was examined. However, as stems from the nature of pretexting (see Pretexting in Research framework part), this component is highly variable, and no clear and comprehensive list of categories exists. Thus, the content analysis in this case had to be conducted inductively during the analysis since preliminary inquiry could have omitted some of them. This was done by searching for key words and excerpts in messages which were related to the required action. After coding the key words, they were merged into bigger categories (see Table 8) depending on their nature, e.g. "you are a beneficiary of the fund" and "click here to collect refund" were merged into Money-related category.

Table 8: Coding tree for pretexting

Code	Description	Example
Account-related	Messages prompting recipients to log in to their account, change their passwords, verify information etc.	"For security reasons, We need to verify the sender and receiver of the payment… Log in using your account."
Company communication	Internal communication regarding policies, plans, regulations etc.	"Important company policies regarding the Covid-19 Virus has been uploaded to OneDrive."
Invoice	Invoices for allegedly purchased services.	"Please remember to follow the link below to view invoice."

Job-related	Messages updating the recipient on its employment status, such as promotions, salary reduction or termination. Also job offers.	“Unfortunately, your position… was made redundant… Here is a copy of your report (in PDF) includes your payout…”
Money-related	Any winning of cash prize, financial compensations, cashbacks, investment opportunities as well as financial help and relief from banks, funds and government.	“You have been gifted €1,000,000,00 MILLION EUR, From WHO, courtesy to HSBC Donations on Covid-19”
Newsletter	Alleged news and reports on the COVID-19 pandemic.	“Can people become immune?... If you'd like to unsubscribe and stop receiving these emails click here.“
Security-related	Information on security situation in the recipients surroundings or country, a list of new cases, policies and regulations issued by governmental bodies etc.	“At this time, three new cases have been confirmed around your location today.”
Product offer	Messages offering products such as protective .	“Now we can export disposable mask, civilian KN95 mask, hand sanitiser and wet wipes…”
Service offer	Messages offering IT, news, security etc. services.	“Outlook is focusing its Services and Support operations on helping all active Outlook Users mitigate the impact of this pandemic... “
Screening-related	Messages related to screening forms, test invitation, test results etc.	“Your SARS-CoV-2 Test results ready to be take off.“
Shipment update	Messages pretending to be sent from logistic firms in order to verify personal data such as addresses and telephone numbers of recipients.	“Kindly Re-confirm your delivery address. Failure to verify address might lead to delay in scheduled delivery”

2.3.5. Explanation

Once the whole coding process was done, the final most representative case from particular stage was examined with respect to the WHO timeline and various theories. The answer why attackers used particular principle and tool of persuasion was firstly searched in theories of crisis management, cybercrime, and psychology in order to roughly define the boundaries. Then, this explanation was supported by events, observations, and statements and reports of international organizations which occurred at that time.

2.4. Coding Example

A step-by-step methodology guide is here described in Table 9 on a transcript of an e-mail below. Firstly, individual principles of persuasion had to be identified. For this purpose, individual text units were classified with regard to the codebook. For example, the *[logo]* unit was classified under *Authority* because it depicted an international organization in charge of public health, under *Liking and Similarity* because the recipient was familiar with the logo of the organization and thus the message did not appear anonymous or distinct to him, and *Distraction* because it attracts attention when reading the message. The *UN launches COVID-19 Global Humanitarian Response Plan to help distribute the newly released COVID-19 Vaccine* sentence was a clear *Deception* as at that time no vaccine was available yet. The excerpt *UN launches* was further classified under *Authority* because the sender referred to another organization to support credibility of his message. And *Properly funded, it will provide laboratory materials for testing, supplies to protect health workers and medical equipment to treat the sick* was classified under *Integrity* because the reasoning makes sense and the expressed statement appears to be true.

After coding all the messages and counting all the text units, e-mails in which the most frequent principle of persuasion was used were further investigated for the type of impersonated entity. If this e-mail was among them, it was classified under the International organization category of impersonated entities. The reason is that despite the sender impersonated specific individual, the message was sent on behalf of the organization. This was necessary in order to distinguish it from the category of *Individuals* in which attackers impersonated ordinary people, for example football players or infected people. Consequently, if this e-mail appeared among those with the most impersonated entity being *International organization*, it was investigated one more time for a type of pretexting. In this case, the pretext was *Security-related*.

2.5. Transcribed E-mail Example

[logo of World Health Organization]

TO WHOM IT MAY CONCERN,

UN launches COVID-19 Global Humanitarian Response Plan to help distribute the newly released COVID-19 Vaccine

The UN today issued a $2 billion appeal to fight corona-virus in the most vulnerable countries.

Please find attached Vaccine samples and method of administration.

Properly funded, it will provide laboratory materials for testing, supplies to protect health workers and medical equipment to treat the sick. It will bring water and sanitation to places facing shortages, and will help humanitarian workers and supplies get to where they are needed most to support the COVID-19 response.

ALWAYS WASH YOUR HANDS!

Regards
Dr Luis Jorge Perez, PAHO-PED, World Health Organization Regional Offce for the Americas/Pan American Sanitary Bureau, 525, 23rd Street, N.W, Washington, D.C., USA.

Table 9: Coding example

Text unit	Principle of Persuasion	Impersonated entity	Pretexting
[logo]	Authority, Liking and Similarity, Distraction	International organization	Vaccine information
TO WHOM IT MAY CONCERN	Distraction		
UN launches COVID-19 Global Humanitarian Response Plan to help distribute the newly released COVID-19 Vaccine	Deception		
UN launches	Authority		

The UN today issued a $2 billion appeal to fight corona-virus in the most vulnerable countries.	Deception		
The UN today	Authority		
Please find attached Vaccine samples and method of administration.	Reciprocation		
Properly funded, it will provide laboratory materials for testing, supplies to protect health workers and medical equipment to treat the sick.	Integrity		
It will bring water and sanitation to places facing shortages, and will help humanitarian workers and supplies get to where they are needed most to support the COVID-19 response.	Integrity, Needs and greed		
ALWAYS WASH YOUR HANDS!	Authority, Distraction		
Dr Luis Jorge Perez	Liking and Similarity, Distraction		
World Health Organization Regional Office for the Americas/Pan American Sanitary Bureau	Authority		

2.6. Data

489 e-mails were collected throughout 2020 from various sources. Most of the data came from publicly available databases of private cybersecurity companies Cofense (2020), PhishLabs (2020), and IBM X-force (2020) which published their samples online for free. All these e-mails were labeled as phishing e-mails related to COVID-19 pandemic. The smaller portion was provided by ESET, after an e-mail request, and the researcher from their own private databases. Collection of the data was feasible thanks to the fact that most of it were printscreens in digital image formats JPG, JPEG, and PNG, i.e. images could be widely shared publicly as they only showed the message of the e-mail and not the whole e-mail header with all the technical information about the sender which is considered valuable for security products of these firms.

Since the e-mails came from various sources, they had to be unified and consolidated. Therefore, four rounds of filtering were conducted. The first step was to filter out e-mails which were written in other than English. Secondly, e-mails which did not contain words such as "COVID-19", "coronavirus", "epidemic" and "pandemic" were excluded as they were not valid for the purpose of this research. Thirdly, only those e-mails were admitted in which all the required information could be identified, i.e. they were not redacted, or clearly indicated that the redacted part contained them, e.g. strings such as telephone number: *REDACTED NUMBER* or *Best regards, REDACTED NAME*. Finally, all the valid e-mails were sorted out into particular stages by a date when they were sent and then were again filtered so as to get rid of duplicates. The goal was to have only unique e-mails in each stage. However, if a certain e-mail appeared twice, the first time in the first stage and the second time in the third stage, it was kept in order to better map the distribution of such e-mails over time.

After filtering, all the texts from printscreens of e-mails were extracted by Optical Character Recognition (OCR) software A9T9. This step was important for the coding of words, phrases and excerpts which was done in Taguette software. The extracted texts were then manually checked with respect to the text in images so as to edit incorrectly converted characters and delete parts which were not important for the coding process – for example subject lines, watermarks, source's notes etc. The final number of files available for the research was 213 images and 213 transcripts which covered months from February to November 2020.

3. Stage #1: January to mid-March 2020

3.1. Description of the Situation

The first COVID-19 related phishing e-mails appeared in February 2020 right at the time when World Health Organization (WHO) was searching for information on "unusual pneumonia cases" in China and was repeatedly urging states to take precautions as the coronavirus spread across Asia to Europe and the United States. In this pre-pandemic stage of crisis symptoms the dominant principle of persuasion was *Authority* in combination with *State agency* and *Security-related* as the mostly impersonated entity and pretexting, respectively (see Table 10).

Regarding the pretexting at this time, attackers tried to mimic crisis communication of state agencies by "weaponizing" messages typically with a brief description of the alleged ongoing events and a request to follow the link for additional information about high-risk places and/or new COVID-19 cases. They wanted to evoke an impression of a legitimate message, content of which would help the recipient to avoid potential hazards. They were further accompanied with a bunch of instructions such as "wash hands often", "cover the nose and mouth" or "limit close contact with people who are sick" which were to further support the credibility of e-mails.

These messages were sent in the name of national public health agency responsible for control and prevention of diseases. However, attackers did not include some additional supportive information for this entity such as the name of agency's person responsible for this communication, nor contact in the signature or logo. This fact implies two things. Firstly, despite more or less credible content of messages, attackers failed to completely impersonate a *State agency*. Secondly, in accordance with the principle of authority, by omitting some details about the impersonated entity attackers wanted to avoid further engagement with the recipient and evoke an impression that the provided instructions are sent en masse and are not to be questioned nor negotiated. Therefore, messages also contained direct instructions such as "You are immediately advised to go through the cases" or that the agency "requires you go avoid (HIGH-RISK) zone".

3.2. Explanation of the Situation

The reason why attackers chose such a combination is best explained by two factors which occur during crises – information need and leadership need. According to Giddens (1991: 184-185), crises directly affect people by depriving them of jobs, housing, and other activities and capacities which consequently fuel a general climate of uncertainty, anxiety, and existential questions. It is in times like this when people need fast and accurate information, updates, and instructions how to protect themselves and mitigate the consequences of emergencies (Schwartz 2016: 101). And as the transition to modernity shaped political authorities to the roles of people's protectors and leaders (Zarakol 2017), it was naturally expected that they would seek these information from a state in the first place. However, especially in pre-crisis stage, it is crucial for governmental bodies to build and maintain trusted relationship on time with their citizens because if those felt uncertain about the ability of institutions to control a crisis, they could ignore new instructions and further rely rather on information supplied by family, friends or other sources (Schwartz 2016: 102).

This need for information sharing and leadership of governmental bodies in crisis management was stressed in several statements and guidance documents related to the management of an outbreak which WHO issued to support countries preparedness in January and February. For example, Strategic preparedness and response plan (WHO 2020a) emphasized, among others, that risk communication is a critical part of public health intervention and therefore governments were advised to communicate rapidly, regularly and transparently with the population and public and private organizations. States were urged to sound an appropriate level of alarm and increase a degree of population understanding and acceptance of protective measures to slow transmission and contain COVID-19 (WHO 2020b, 2020c). Those states, and especially their leaders, which responded to and managed the outbreak adequately were praised and thanked by WHO on several occasions while others were indirectly criticized when the number of cases in the world exceeded 100 000 altogether in 114 countries in March (see WHO 2020b, 2020d, 2020e, 2020f).

The use of principle of authority in this case was a natural consequence due to socially obedient environment created by a hierarchical model of our society where individuals are ranked in terms of their power and importance (Wren 1999: 19-20). Whether it is parents, policemen, doctors, supervisors or authoritarian collectives such as hospitals, people are often expected to obey them without questioning (Ibid). Considering this, there was no

reason for attackers to primarily rely on any other principle as the added value of for example *Liking, Similarity and Deception* or *Social proof* would only undermine the authoritarian position of impersonated *State agency*.

3.3. Transcribed E-mail Example

At noon on Tuesday, March 3 the Centers for Disease Control and Prevention (CDC) reported 60 cases of COVID-19 from 12 states. Twenty-two of these cases are travel-related; 11 are believed to be
person-to-person spread; and for the remaining 27 the source of exposure is still under investigation..

Four new cases have been confirmed around your location. The risk to the Public in your city and throughout the World is very HIGH.

* The CDC requires you to avoid (HIGH-RISK) zone around your city to Minimize Chance for Exposures.
* A high-risk person is currently being monitored around your city center.

For additional information about high-risk places around your city, please see below;
[link]

As always, it is recommended to you
* Wash hands often with soap and water for 20 seconds. Use an alcohol-based hand sanitizer if soap and water are not on hand.
* Cover the nose and mouth with sleeve or tissue when coughing or sneezing.
* Avoid (HIGH-RISK) zone, see above for newly updated places to avoid.
* Limit close contact with people who are sick.

National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease Control and Prevention

Table 10: Analysis of phishing e-mails sent during the Stage #1

Principle	Frequency*	Entity	Frequency**	Pretexting	Frequency**
Authority	**50**				
		State agency	**6**		
				Security-related	5
				Money-related	1
		Other organization	2		
		International organization	1		
LSD	**41**				
Liking and similarity	21				
Deception	20				
CRC	**32**				
Commitment	14				
Reciprocation	8				
Integrity	7				
Consistency	3				
Distraction	**30**				
Strong affect	19				
Distraction	4				
Need and greed	4				
Scarcity	3				
Social proof	**12**				
Social proof	8				
Moral duty	4				

* Number of text units.

** Number of files.

4. Stage #2: Mid-March to July 2020

4.1. Description of the Situation

During the second, acute stage, which more or less correlated with the first wave of the pandemic, the crisis quickly accelerated. By early April, the number of cases surpassed 1 million, and the number of deaths was reaching 60 thousands worldwide (WHO 2020g). The situation was badly manifesting itself especially in Europe which became a new epicenter with more reported cases and deaths than the rest of the world combined, apart from China (WHO 2020h). It was at this time when World Health Organization, besides calling for containment measures, launched the COVID-19 Solidarity Response Fund to finance all its activities and activities of its partners which were to jointly address the issues of the pandemic more specifically (Ibid). International organizations and states established various partnerships with private and public sector to spread awareness of the diseases, develop vaccines, produce and distribute medical equipment, fight an infodemic, support endangered communities, and further raise finances for the fund.

Yet, the COVID-19 related phishing e-mails from this period did not abuse any of these crisis management topics. On the contrary, attackers shifted their previous authoritative position of state agencies which wanted to protect people from infection towards a position of Samaritan organizations which wanted to financially help people. In this respect, the e-mails were characterized by a combination of the principle of *Distraction* with *Other organization* and *Money-related* as the mostly impersonated entity and pretexting, respectively (see Table 11).

Regarding the pretext and impersonated entity, attackers sent e-mails on behalf of various organizations, most of which abused the name of legitimate businesses such as Microsoft, Google, Standard Bank, The Asia Foundation, or Oxfam. All of them offered recipients money in one way or another, ranging from hundreds to millions of dollars. These opportunities were mostly presented to be a part of the alleged one's own COVID-19 relief fund, but also as refunds for canceled services, lottery wins, Samaritan giveaways, inheritance after the deceased, or investment opportunities to quickly double the deposit. Messages were primarily addressed to people mostly affected by the crisis who found themselves in financial troubles, e.g. marginalized communities or businessmen. Attackers also supported these pretexts with other distracting means, for example Scarcity whereby the

offers were timely limited or presented as confidential, in order to leverage people's Needs and greed.

However, on the other hand, there was a great variety in terms of supportive information where no specific pattern could be observed. Sometimes attackers included a full name of the alleged sender with his position and associated employer. Sometimes the only information was a name of the department from which the e-mail was sent, e.g. human resources department or management. Further, unlike in the first stage when recipients were ordered to execute certain action without questioning, in several cases from this stage attackers asked recipients to contact them directly on provided e-mail address. This may suggest that attackers differ in terms of their ability to credibly impersonate entities, and/or that decision to include or exclude some supportive information depends on particular pretext since in some of these cases, attackers showed willingness and intention to communicate with their victims.

4.2. Explanation of the Situation

The reason why this combination was chosen is best explained by two factors – impact of containment measures, and anti-phishing awareness campaign. Firstly, since January WHO has been providing governments with guidance and considerations on the use of personal protective equipment, organization of mass gatherings, quarantine, contact tracing, lockdown, or treatment which eventually caused that at the center of attention of all parties involved was predominantly the containment of the diseases. This fact was underlined in WHO Director General's speech in late March at the G20 Extraordinary Leaders' Summit when he acknowledged that many countries had already imposed drastic social and economic restrictions, shut schools and businesses, asked people to stay at home, and yet, he further encouraged them to keep fighting "like hell" because "the best and only way to protect life, livelihoods and economies is to stop the virus" (WHO 2020i). But what he and the international community was missing at that time was full realization of the impact of these measures not only on economy per se, but on people's financial security as well. As Director General pointed out at the summit, only time would tell what the full social, economic and political fallout would be (Ibid).

The problem with this approach dwelled in Maslow's hierarchy of needs. While governments and international organizations were fulfilling the safety and security needs of people, they were unintentionally but gradually disrupting the fulfillment of the most

important human needs which are physiological needs – among them food, warmth, rest. That is, when governments all around the world put restrictions on movement, the migration flow of workforce slowed down, and some businesses were forced to shut down, people consequently lost their income and could not afford to pay for housing, food, water, gas etc.

This aspect was fully acknowledged by international community only in May, when the United Nations (UN) drew attention to "collateral effects on people" in its updated Global Humanitarian Response Plan. Therein, it was noticed that the containment measures and closure of businesses resulted in loss of income for highly vulnerable workers such as workers in mining sector and processing industry, petty traders, migrant workers, or small-scale producers of cash crops (UN 2020a). At that time, it was expected that 200 million jobs would be lost in the second quarter of 2020, most of which in Asia-Pacific (Ibid), while in the update from July it was estimated that by the end of the year 400 million full-time jobs would be lost worldwide in total (UN 2020b). In this regard, as Maslow (1943) pointed out, if physiological needs are not or cannot be well gratified, they motivate and drive people's actions more than others – for the man who is hungry, no other interests exist but food. Therefore, in this stage, attackers proved to be one step ahead of authorities in charge of crisis management when they tried to exploit the Needs and greed of people who were getting short of money and potentially faced existential problems. Any money offer or giveaway could trigger recipient's response so as in an effort to ensure his livelihood.

Secondly, as the first COVID-19 related phishing e-mails were spreading across the internet during the first stage, authorities affected by the impersonation (CDC 2020, WHO 2020j), cybersecurity firms (Ellis 2020), and media (Turton and Sebenius 2020) quickly responded with anti-phishing campaign whereby they warned users against fake e-mails allegedly sent on behalf of *State agencies* or *International organizations*. This campaign which commenced at the turn of March and April explains the relatively low level of impersonation of these entities in the next months as well as rapid increase in impersonation of the others, namely Other organizations and Individuals.

Regarding the organizations, be they private companies or non-governmental organizations (NGOs), they may have been chosen in the first place due to their special role in global health governance even during peacetime. According to Youde (2018), although traditionally the leadership has come from individual states or through their formally established international organizations, in recent years, private and non-state actors have played an increasingly

important role. For example, philanthropic organizations have engaged in global health primarily to distribute funds to other groups, organizations, or entities; and NGOs have acted as direct service providers in the absence of state-run services (Ibid). However, attackers rather leveraged only their good reputation derived from their humanitarian aid as the alleged Microsoft Coronavirus Relief Fund through which attackers promised money to individuals is in contradiction with funding priorities of Microsoft's founder Bill Gates. The Bill and Melinda Gates Foundation focuses its funds on research and development of treatment for infectious diseases rather than on fields which are a primary responsibility of governments (Youde 2013), such as money compensations and subsidies.

4.3. Transcribed E-mail Example

> As the world responds to the outbreak of COVID-19, our thoughts are with the people affected and the medical professionals working around the clock to help those most in need. At Microsoft, we're working to provide technology, tips and resources to our customers to help them do their best work while remote.
>
> In this month of May, Microsoft wishes to commend you for being selected as one of the recipents to receive the Microsoft Coronavirus Relief Fund (MCRF). For more information on how to obtain your relief fund, kindly download and read the PDF attached file very carefully.
>
> NB: This email was sent from a Notification Email address from the sponsors of Microsoft Philanthropies. If this Notification Email Letter hits your Junk/Spam folder, simply move the email from your Junk/Spam folder to your inbox for better viewing and easy accessibility.
>
> Best Regards,
> Jane Meseck
> Sr. Director for Social Impact, Microsoft Philanthropies
> Website: [link]
>
> ©Copyright 2020 Microsoft Corporations

Table 11: Analysis of phishing e-mails sent during the Stage #2

Principle	Frequency*	Entity	Frequency**	Pretexting	Frequency**
Distraction	**470**				
		Other organization	**50**		
				Money-related	**19**
				Company communication	9
				Account-related	7
				Shipment update	6
				Invoice	4
				Job-related	2
				Service offer	2
				Newsletter	1
		Individual	41		
		International organization	17		
		State agency	17		
		Anonymous	15		
Need and greed	152				
Distraction	116				
Strong affect	102				
Scarcity	67				
Overloading	33				
LSD	**410**				
Liking and similarity	247				

Deception	148				
Deceptive relationship	15				
CRC	**398**				
Reciprocation	213				
Integrity	169				
Commitment	13				
Consistency	3				
Authority	**351**				
Social proof	**101**				
Social proof	46				
Moral duty	46				
Diffusion of responsibility	5				
Herd	4				
* Number of text units. ** Number of files.					

5. Stage #3: August to December 2020

5.1. Description and Explanation of the Situation

In the third, chronic stage of the crisis ranging from August to December 2020, which from large part overlapped with the second wave of the pandemic, international community shifted its focus to three main topics – evaluation of the prior response, ensuring fair distribution and access to vaccines, tests and treatments (VTT), and awareness and support campaigns.

According to Preparedness and Response Progress Report, by this time the situation in the former epicenter of the pandemic, Europe, had stabilized but now the region of Latin America raised concerns as it accounted for over half of cases and almost two-thirds of global deaths (WHO 2020k: 5). Eastern Mediterranean, South-East Asian, and African

countries have also reported an increase in the incidence of new cases over the same period (Ibid). Moreover, despite that almost every country in the world (90%) experienced disruptions in health services, they were just these low- and middle-income states that reported the greatest problems (WHO 2020l). Therefore, they became priority countries to receive Global Humanitarian Response Plan's technical and operational support (WHO 2020k: 9-10).

Realizing that in order to beat the pandemic no area must be left behind, leaders across the globe have thus committed themselves on several occasions to support the poorer states and ensure that everyone has early, affordable and equitable access to the new vaccines, therapeutics and diagnostics, especially through programs like the "Access to COVID-19 Tools Accelerator" (WHO 2020m, 2020n, 2020o). So did they recognize the need to protect and help healthcare workers and their families who have become infected with COVID-19, become victims of violence, or even lost their lives in their efforts to combat the disease (WHO 2020p). They emphasized that unlike medicines and equipment, people in the first line cannot be replenished as easily (Ibid: 2), and therefore several media campaigns and calls for action have been launched to pay tribute and show solidarity with them (WHO 2020q), and fight disinformation which has aggravated the public health response (WHO 2020r).

Regarding the phishing during this stage, it seems that attackers did not try to abuse any specific topic like during the other two stages. Although Product offers was the most frequent pretext, the little gap between it and the remaining ones suggests that attackers perhaps tried to pull out all their weapons at the same time after realizing that targeting victims with adjusted seemingly-needed content such as *Security guidelines* and *Money offers* might not have been effective any longer since the international anti-phishing campaign in previous months (see the *Stage #2* chapter). This campaign also explains the sharp decline in the overall number of phishing e-mails since the third quarter of the year (ESET 2020).

As in the second stage, the campaign yet again caused that the most impersonated entity were *Other organizations*. When offering face masks and hand sanitizers, delivering test results or updating on job-related agenda, attackers again used mix of low quality supportive information about the sender on the basis of which the recipient could not tell with a confidence who exactly contacted him. In most of the cases they used only one of the following information – name of the sender, department, name of the organization.

The phishing campaign during this stage seemed to be running from the last breath as attackers relied rather on the pretext than on credible impersonation. Nevertheless, since these messages copied the usual internal and external communication of businesses, attackers tried to exploit their *Integrity* in order to persuade the victims into *Reciprocally* contacting them back. In half of the observed e-mails, attackers specifically used phrases such as "acknowledge you received this information", "feel free to contact me", and "please, email back to us" for this.

5.2. Transcribed E-mail Example

Dear Sir or madam,

Hope you and your family are safe. This is Carmen here.

Let's fight together to get through the COVID-19. We started to produce protective products before the end of 2019, while all products were expropriated by our government before. Now we can export disposable mask, civilian KN95 mask, hand sanitiser and wet wipes, so we would like to do something for you and your country, please tell me what you need and quantity, and then we will offer you the best price. Please feel free to contact me if you have any question. Hope to get your reply soon.

Best regards,
Lina
[e-mail address]

Table 12: Analysis of phishing e-mails sent during the Stage #3

Principle	Frequency*	Entity	Frequency**	Pretexting	Frequency**
CRC	**33**				
		Other organization	**8**		
				Product offer	**3**
				Screening-related	2
				Company communication	1
				Job-related	1

				Shipment update	1
		Anonymous	1		
		Individual	1		
		State agency	1		
Integrity	17				
Reciprocation	13				
Commitment	2				
Consistency	1				
LSD	**25**				
Liking and similarity	14				
Deception	11				
Distraction	**18**				
Strong affect	6				
Distraction	5				
Need and greed	4				
Scarcity	2				
Overloading	1				
Authority	**12**				
Social proof	**3**				
Social proof	2				
Herd	1				
* Number of text units. ** Number of files.					

6. Discussion on Psychology of Phishing Attacks during Crises

The proposed theoretical framework contributes to the theory of psychology of phishing attacks with its ability to identify potential targets and the used principles and tools of persuasion during crises as well as explain how attackers choose them in different situations. On the contrary, the applicability of the proposed research framework is more universal in the field of phishing analysis, especially in mapping and examining the different components of such e-mails. But when both frameworks are combined, they provide results which in the end can help mitigate the risks of falling victim to cybercrime during crises as explained below.

First of all, clear recommendations for crisis communication stem from this work. Keeping in mind that governments and international institutions are the bodies in charge of crisis management, the first stage of COVID-19 pandemic showed that they are also the first ones whose names are abused and whose communication is forged by cybercriminals at the time when a crisis is starting to manifest itself. Therefore, these authorities should timely specify which communication channels will they use to disseminate information needed to protect the public. They should also clarify which information should citizens expect from them, e.g. that the state will not send announcements about adopted regulations or a recommended list of protective equipment in bulk e-mails no matter how credibly they appear.

During the second stage, when the crisis breaks out, authorities should shift the focus of their cybercrime-prevention communication on vulnerable groups which are being affected the most. In the case of COVID-19 pandemic, the aggravation of daily life of people was caused primarily by the adopted safety regulations and measures due to which highly vulnerable labor sectors were closed and the suddenly unemployed were losing their basic needs. However, this can also be caused by natural elements such as tornado or floods which damage housings or otherwise deprive them of material resources or relatives. Therefore, authorities should launch an information campaign targeted for these groups in order to explain them that the financial compensations, giveaways, prizes etc. which they might be offered are most likely nothing but a fraud unless the alleged Samaritan organization has a history of such business and they are aware of it.

The third stage is, however, a tricky one. While names of various organizations are abused similarly as in the previous stage, the phishing campaign is here characterized by variety of

pretexts which seem to be the last effort of attackers how to deceive a victim. The attention is paid to genuineness of messages which aim is to entice the recipient and persuade him into contacting the sender back. Although they decrease in numbers, authorities should not underestimate the situation and warn citizens not to respond to such e-mails.

Secondly, findings of this work may contribute to an improvement of cybersecurity solutions. Further research could analyze what specific key words and phrases the attackers use in crisis-related phishing e-mails in a particular period of time. For example, the first stage of the COVID-19 pandemic was characterized by the use of principle of *Authority*, impersonation of *International organization* and abuse of *Security-related* topic – situation update. These messages usually contained words and phrases such as "you are required", "you are immediately advised", "the risk is very high" or "update on COVID-19" besides the abuse of name of World Health Organization.

On the contrary, the second stage was characterized by the use of principle of *Distraction*, impersonation of *Other organizations* and abuse of *Money-related* content. Attackers in the name of Microsoft, Google, The Asia Foundation or HSBC tried to deceive victims with claims such as "you have been gifted 1 million EUR", "project to help and improve lives of COVID-19 victims", "a second wave of relief to help customers" or "you have been selected as the grand winner in Covid Support Fund".

In the third stage, *Commitment, reciprocation and consistency* (CRC), *Other organizations* and various pretexts, but mostly *Product offers*, were used to engage the recipients in conversation with the sender. Attackers usually used phrases such as "please call at", "feel free to contact me" or "please email back to us". Focusing the cybersecurity and anti-phishing solutions on this content could help with filtering these e-mails out or at least flagging them during the particular period of time when they are expected so that their users are warned of the potential threat.

In regard to psychological aspects, further research could also include an analysis of specific days and time periods of the day to find out when attackers usually send fraudulent messages and when are different groups of people more vulnerable to phishing attacks. This work could not achieve it since the data lacked the needed information.

However, the initial inquiry into this was done by cybersecurity firm Imperva (2016) which noticed that victims responded to phishing e-mails mostly during working hours with more than 35 percent of successful responses occurring between 9:00 a.m. and 12:00 p.m. This is

because morning hours are usually the busiest when people are browsing, replying, and forwarding emails from the past day or weekend (Ibid).

Similarly, another firm eSentire (2019, pp. 6-7), found that most phishing occurred midweek, on Tuesday and Wednesday. Supposedly it is because in these days, employees may be operating in a more automated fashion in contrast to days closer to the weekend when they are in transition and may be less willing to engage in unfamiliar requests (Ibid). Interestingly, fraudulent messages sent on weekends usually targeted people in healthcare who tend to be active at that time due to the nature of their job (Ibid).

Despite that findings of these firms may be biased due to uneven representation of various groups among their customers, they revealed another possible part of cybercriminals' psychological game – not only how to target victims, but also when exactly are they most susceptible.

However, as discussed in the chapter of Limitations, this work had to deal with two big hurdles. Firstly, further work needs to be done on the clarification of coding process. This is because the original author of the coding tree for principles of persuasion did not elaborate on the decision-making process and/or did not provide clear examples. The second problem was availability of data. When collecting them, various sources had to be used and yet they did not provide a suitable set of e-mails which led to their discarding.

7. Limitations

As discussed in the data chapter, the biggest hurdle which the research faced was a lack of suitable data due to censorship. On one hand, not all data might had been published online during the year which could have contributed to the large differences in data distribution throughout the stages. On the other hand, owners decided to redact some information in available data which led to more than a half of them being evaluated as inappropriate for the purpose of the work, and were lost during the filtering process. Thus, the research worked with only 12 and 11 samples in the first and the third stage, respectively, while in the second stage 173 e-mails were analyzed.

However, for evaluation of a research validity, two things need to be stressed about the quantity of e-mails. Firstly, the division of timeline had little impact on distribution of data as both the second and the third stage covered five months each, and the decrease in the latter stage was observed also by private cybersecurity companies since the third quarter of the

year (ESET 2020). Secondly, the research dealt with unique e-mails only in each stage. The overall quantity of e-mails was thus of lesser importance since more e-mails could have led to more duplicates and more data being discarded.

The second hurdle for the research was insufficient information on the methodology provided by Ferreira (2015, 2019) especially in terms of description of particular principles of persuasion. Ambiguity, lack of detailed explanation and/or clear examples led in some cases to doubts about the classification of text units. Therefore, prior to the coding process, the researcher conducted several inquiries into data to get acquainted with the content of e-mails in order to build own approach on how to decide on classification (see Coding example part). Consequently, for future research, this work also provided an improved description of analytical procedure on particular coding example which was based on researcher's experience with decision making.

Thirdly, although the 2020-2021 coronavirus pandemic classifies as crisis, it is unprecedented global situation in modern history of mankind which requires unprecedented protective measures with vast impact. Therefore, although the proposed theoretical and research frameworks might be used on all types of crisis and the findings might be generally valid, one has to have on his mind that this crisis significantly differed from other crises in its range, length, and severity. The unique situation of the "new normal" might have created unique conditions and circumstances which cannot be found during other crises, for example tsunami or war.

Conclusion

This work on psychology of phishing attacks during crises contributes to fields of psychology, cybercrime as well as crisis management by offering theoretical and research frameworks, presenting valuable insight and results of an analysis of cybercriminal operations, and providing recommendations for policy makers, crime prevention initiatives and researchers.

The theory builds on a premise that since crises create a chaotic and unpredictable environment which negatively affects people's mental health, it makes them more vulnerable to manipulation of cybercriminals who will exploit it for their own benefit. Despite its weaknesses, this theory helps to understand how phishing campaigns are carried out by attackers in such difficult situations and how susceptible are people to them.

The research framework provides a clear path for research of such messages, especially in terms on how to filter out marginal cases and focus only on the most representative ones, and how to divide the fraudulent campaign into smaller parts if it stretches over longer periods of time. It also includes transparent and descriptive procedure for replication of this work.

The methodology is based on Ferreira's (2015, 2019) reviewed list of principles of persuasion which combined and merged the principles from three foundational works by Cialdini (2007), Gragg (2003), and Stajano and Wilson (2011) in order to achieve consistency. However, unlike this one, for the second part of methodology dedicated to research of tools of persuasion, i.e. impersonation and pretexting, no uniform or universal coding tree exists and therefore it had to be constructed inductively by inquiring into data.

Application of these frameworks consequently led to valuable insight into cybercrime operations. The goal of the research was to find out which principles and tools of persuasion were used by malicious social engineers during the first year of COVID-19 pandemic by examining more than 200 e-mails which were obtained from various publicly available sources as well as from the private databases of a cybersecurity firm, after a request, and the author of the research. However, it is important to stress that the analyzed data represented less than a half of the original database. The reason were various censorship techniques of the data sources which deprived them of information crucial for this work.

Nevertheless, results specifically showed that in the initial stage of crisis, the stage of symptoms, attackers abused names and communication of state authorities from position of which they ordered recipients to engage with fraudulent e-mails pretending to contain security-related material. The original hypothesis that attackers will use the principle of *Authority* in combination with impersonation of *State agencies* and *Security-related* pretext was thus confirmed. However, only in this stage.

Contrariwise, during the second, acute stage when the crisis prevailed, they switched to impersonation of various organizations such as private companies and non-governmental organizations in whose name they hit on the people's basic needs which they had been deprived of. However, once the anti-phishing campaign was launched, in the third, chronic stage of crisis they pulled out all the weapons and abused any topic in order to persuade the victim to communicate with them.

Learning from these results, it is advised to the managers of crisis that they should prepare their communication in a way that clearly defines what channels and what information will be used and disseminated so that the public is timely aware of potential phishing messages. For example, that they will never use e-mails to inform about recommended protective equipment. A part of this communication should also be an information campaign to warn people of the possible scenarios which could be used by cybercriminals.

On the contrary, for researchers who develop security solutions, it is advised to focus on specific key words and phrases used in individual stages of crisis which can help to flag and/or filter a potential fraud. For example, in the first days, weeks or months of crisis, these solutions should search for phrases such as “you are required” or “you are to immediately check” in contrast to “you have been gifted 1 million EUR” in the second stage and “please, contact me back” in the third. Similarly, further research could also focus on specific days and hours during which attackers usually send messages and during which people are more vulnerable to phishing.

To sum up, the merit of this research stem from the “new reality” established by the COVID-19 pandemic during which people has been spending most of a day online as a result of lockdowns and other restrictions adopted around the world. These conditions made them easy targets for cybercriminals who wanted to benefit on people’s misery and suffering. Therefore, it was important to analyze how exactly phishing and fraud campaigns work in times like this in order to better prepare for similar crisis circumstances in the future.

Bibliography

AKBAR, Nurul, 2014. *Analysing persuasion principles in phishing emails*. Enschede. Master Thesis. University of Twente.

ANDRESS, Jason, 2014. *The Basics of Information Security: Understanding the Fundamentals of Infosec in Theory and Practice*. Oxford: Syngress.

ANTUŠÁK, Emil and Josef VILÁŠEK, 2016. *Základy teorie krizového managementu*. Praha: Karolinum.

BARYSHEVTSEV, Maxim and Joseph MCGLYNN, 2020. Persuasive Appeals Predict Credibility Judgments of Phishing Messages. *Cyberpsychology, Behavior, and Social Networking*. 23(5), 297-302.

BENNETT, Peter, Kenneth CALMAN, Sarah CURTIS and Denis FISCHBACHER-SMITH, 2010. *Risk Communication and Public Health*. Oxford: Oxford University Press.

CENTERS FOR DISEASE CONTROL AND PREVENTION, 2020. COVID-19-Related Phone Scams and Phishing Attacks. *Centers for Disease Control and Prevention* [online]. April 3, 2020 [cit. 2021-4-17]. Available at: https://www.cdc.gov/media/phishing.html

CIALDINI, Robert, 2006. *Influence: The Psychology of Persuasion*. New York: Harper Business.

COFENSE, 2020. Phishing Email Database: Real Phishing Examples & Threats. *Cofense* [online]. [cit. 2021-4-17]. Available at: https://cofense.com/real-phishing-examples-and-threats/

ENISA, 2020. *ENISA Threat Landscape 2020 - List of top 15 threats* [online]. [cit. 2021-7-25]. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-list-of-top-15-threats

ELLIS, Jessica, 2020. COVID-19 Phishing Update: Threat Actors Impersonating CDC, WHO. *PhishLabs* [online]. March 26, 2020 [cit. 2021-4-17]. Available at: https://info.phishlabs.com/blog/covid-19-phishing-update-threat-actors-target-cdc-who

ESENTIRE, 2019. *Q1 2019: Quarterly Threat Report* [online]. [cit. 2021-7-26]. Available at: https://esentire-dot-com-assets.s3.ca-central-1.amazonaws.com/assets/resourcefiles/q1-2019-quarterly-threat-report-esentire.pdf

ESET, 2020. Threat Report: Q3 2020 [online]. [cit. 2021-3-22]. Available at: https://www.eset.com/fileadmin/ESET/CZ/Threat-report/ESET_Threat_Report_Q32020.pdf

EVERY-PALMER, Susanna et al., 2020. Psychological distress, anxiety, family violence, suicidality, and wellbeing in New Zealand during the COVID-19 lockdown: A cross-sectional study. *PLoS ONE* [online]. 15(11) [cit. 2021-1-2]. Available at: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0241658

FBI, 2020. *2020 Internet Crime Report* [online]. [cit. 2021-7-25]. Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

FERREIRA, Ana, Lynne COVENTRY and Gabriele LENZINI, 2015. Principles of Persuasion in Social Engineering and Their Use in Phishing. In: TRYFONAS, Theo and Ioannis ASKOXYLAKIS, ed. *Human Aspects of Information Security, Privacy, and Trust*. Cham: Springer, s. 36-47.

FERREIRA, Ana and Soraia TELES, 2019. Persuasion: How phishing emails can influence users and bypass security measures. *International Journal of Human-Computer Studies*. 125, 19–31.

GARAYEV, Vener, 2013. Crisis, Definition of. In: PENUEL, K. Bradley, Matt STATLER a Ryan HAGEN. *Encyclopedia of Crisis Management*. Los Angeles: SAGE Publications, s. 186-187. ISBN 9781452226125.

GIDDENS, Anthony, 1991. *Modernity and Self-identity: Self and Society in the Late Modern Age*. Stanford: Stanford University Press.

GRAGG, David, 2003. *A Multi-Level Defense Against Social Engineering*. Maryland: SANS Institute.

HADNAGY, Christopher, 2010. *Social Engineering*. Indianapolis: John Wiley & Sons.

HANCOCK, Peter A. and Gerald MATTHEWS, 2015. Stress and Attention. In: FAWCETT, Jonathan, Alan KINGSTONE and Evan RISKO, ed. *The Handbook of Attention*. Cambridge: The MIT Press, s. 547-568.

HOLT, Thomas J. a Danielle C. GRAVES, 2007. A Qualitative Analysis of Advance Fee Fraud E-mail Schemes. *International Journal of Cyber Criminology*. 1(1), 137-154.

IBM X-FORCE, 2020. Covid-19. *IBM X-Force Exchange* [online]. [cit. 2021-4-17]. Available at: https://exchange.xforce.ibmcloud.com/search/covid-19

IBM X-FORCE, 2021. *X-Force Threat Intelligence Index 2021* [online]. [cit. 2021-7-25]. Available at: https://www.ibm.com/downloads/cas/M1X3B7QG

IMPERVA, 2016. *Phishing made easy: Time to rethink your prevention strategy?* [online]. [cit. 2021-7-26]. Available at: https://www.ukngroup.com/hubfs/Imported_Blog_Media/Imperva-HII-phishing-made-easy-1.pdf

INTERPOL, 2020. *COVID-19 Cybercrime Analysis Report - August 2020* [online]. [cit. 2021-7-25]. Available at: https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

JAKOBSSON, Markus and Steven MYERS, 2007. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. New Jersey: John Wiley & Sons.

JENKINS, Rachel and Howard MELTZER, 2012. *The Mental Health Impacts of Disasters* [online]. London: Government Office for Science [cit. 2020-11-29]. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/286994/12-1297-mental-health-impacts-of-disasters.pdf

MASLOW, Abraham Harold, 1943. A Theory of Human Motivation. *Psychological Review*. 50, 370-396.

MINISTERSTWO CYFRYZACJI, 2019. *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024* [online]. [cit. 2021-7-25]. Available at: https://www.dziennikustaw.gov.pl/M2019000103701.pdf

MITNICK, Kevin D. and William L. SIMON, 2011. *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: John Wiley.

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, 2020. *Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025* [online]. [cit. 2021-7-25]. Available at: https://www.nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD, 2021. *Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025* [online]. [cit. 2021-7-25]. Available at: https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Strategia_kybernetickej_bezpecnosti_2021.pdf

ONO, Eisuke et al., 2011. Relationship between Social Interaction and Mental Health. *2011 IEEE/SICE International Symposium on System Integration (SII)* [online]. 246-249 [cit. 2021-1-2]. Available at: https://ieeexplore.ieee.org/document/6147454

PARSONS, Kathryn et al., 2019. Predicting susceptibility to social influence in phishing emails. *International Journal of Human-Computer Studies*. 128, 17-26.

PETZOLD, Moritz Bruno et al., 2020. Risk, resilience, psychological distress, and anxiety at the beginning of the COVID-19 pandemic in Germany. *Brain and Behavior* [online]. 10(9) [cit. 2021-1-2]. Available at: https://onlinelibrary.wiley.com/doi/10.1002/brb3.1745

PHISHLABS, 2020. COVID-19 Threat Intelligence. *PhishLabs* [online]. [cit. 2021-4-17]. Available at: https://www.phishlabs.com/covid-19-threat-intelligence/

RAPHAEL, Beverley, 2000. *Disaster Mental Health Response Handbook.* Sydney: NSW Health.

SAGARIN, Brad and Kevin MITNICK, 2012. The Path of Least Resistance. In: KENRICK, Douglas T., Noah J. GOLDSTEIN and Sanford L. BRAVER, ed. *Six Degrees of Social Influence: Science, Application, and the Psychology of Robert Cialdini*. Oxford: Oxford University Press, pp. 27-38.

SAMMONS, John and Michael CROSS, 2015. *The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy*. Cambridge: Syngress.

SCHWARZ, Andreas, Matthew W. SEEGER and Claudia AUER, 2016. *The Handbook of International Crisis Communication Research*. Chichester: Wiley-Blackwell.

STAJANO, Frank and Paul WILSON, 2011. Understanding Scam Victims: Seven Principles for Systems Security. *Communications of the ACM* [online]. 54(3), 70-75 [cit. 2021-1-6].

TALEVI, Dalila et al., 2020. Mental health outcomes of the CoViD-19 pandemic. *Riv Psichiatr* [online]. 55(3), 137-144 [cit. 2021-1-2]. Available at: https://www.rivistadipsichiatria.it/archivio/3382/articoli/33569/

TURTON, William and Alyza SEBENIUS, 2020. Hackers Posing as CDC, WHO Using Coronavirus in Phishing Attacks. *Bloomberg* [online]. March 12, 2020 [cit. 2021-4-17]. Available at: https://www.bloomberg.com/news/articles/2020-03-12/hackers-posing-as-cdc-who-using-coronavirus-in-phishing-attacks

UNITED NATIONS, 2020. *Global Humanitarian Response Plan: May Update* [online]. Geneva: United Nations [cit. 2021-4-16]. Available at: https://www.unocha.org/sites/unocha/files/GHRP-COVID19_May_Update.pdf

UNITED NATIONS, 2020. *Global Humanitarian Response Plan*: July Update [online]. Geneva: United Nations [cit. 2021-4-16]. Available at: https://www.unocha.org/sites/unocha/files/GHRP-COVID19_July_update.pdf

VERIZON, 2021. *2021 Data Breach Investigations Report* [online]. [cit. 2021-7-25]. Available at: https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf

VERMA, Rakesh et al., 2018. Phishing During and After Disaster: Hurricane Harvey. *2018 Resilience Week (RWS)*. 88-94.

WATSON, Gavin, Andrew MASON and Richard ACKROYD, 2014. *Social Engineering Penetration Testing: Executing Social Engineering Pen Tests, Assessments and Defense*. Oxford: Syngress.

WILLIAMS, Emma J. and Danielle POLAGE, 2019. How persuasive is phishing email? The role of authentic design, influence and current events in email judgements. *Behaviour & Information Technology*. 38(2), 184–197.

WORLD HEALTH ORGANIZATION, 2021. *Timeline: WHO's COVID-19 response* [online]. [cit. 2021-2-25]. Available at: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/interactive-timeline

WORLD HEALTH ORGANIZATION, 2020a. *Strategic preparedness and response plan* [online]. Geneva: World Health Organization [cit. 2021-3-12]. Available at: https://www.who.int/docs/default-source/coronaviruse/jmo-who-ncov-report-4feb-web.pdf

WORLD HEALTH ORGANIZATION, 2020b. Munich Security Conference. *World Health Organization* [online]. February 15, 2020 [cit. 2021-3-12]. Available at: https://www.who.int/director-general/speeches/detail/munich-security-conference

WORLD HEALTH ORGANIZATION, 2020c. *Report of the WHO-China Joint Mission on Coronavirus Disease 2019 (COVID-19)* [online]. [cit. 2021-3-12]. Available at: https://www.who.int/docs/default-source/coronaviruse/who-china-joint-mission-on-covid-19-final-report.pdf

WORLD HEALTH ORGANIZATION, 2020d. WHO Director-General's statement on IHR Emergency Committee on Novel Coronavirus. *World Health Organization* [online]. January 22, 2020 [cit. 2021-3-13]. Available at: https://www.who.int/director-general/speeches/detail/who-director-general-s-statement-on-ihr-emergency-committee-on-novel-coronavirus

WORLD HEALTH ORGANIZATION, 2020e. WHO Director-General's statement on IHR Emergency Committee on Novel Coronavirus (2019-nCoV). *World Health Organization* [online]. January 30, 2020 [cit. 2021-3-13]. Available at: https://www.who.int/director-general/speeches/detail/who-director-general-s-statement-on-ihr-emergency-committee-on-novel-coronavirus-(2019-ncov)

WORLD HEALTH ORGANIZATION, 2020f. WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020. *World Health Organization* [online]. March 11, 2020 [cit. 2021-3-13]. Available at: https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

WORLD HEALTH ORGANIZATION, 2020g. Coronavirus disease 2019 (COVID-19): Situation Report – 75. *World Health Organization* [online]. April 4, 2020 [cit. 2021-4-15]. Available at: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200404-sitrep-75-covid-19.pdf?sfvrsn=99251b2b_4

WORLD HEALTH ORGANIZATION, 2020h. WHO Director-General's opening remarks at the media briefing on COVID-19 - 13 March 2020. *World Health Organization* [online]. March 13, 2020 [cit. 2021-4-15]. Available at: https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-mission-briefing-on-covid-19---13-march-2020

WORLD HEALTH ORGANIZATION, 2020i. WHO Director General's remarks at the G20 Extraordinary Leaders' Summit on COVID-19 - 26 March 2020. *World Health Organization* [online]. March 26, 2020 [cit. 2021-4-16]. Available at:

https://www.who.int/director-general/speeches/detail/who-director-general-s-remarks-at-the-g20-extraordinary-leaders-summit-on-covid-19---26-march-2020

WORLD HEALTH ORGANIZATION, 2020j. WHO reports fivefold increase in cyber attacks, urges vigilance. *World Health Organization* [online]. April 23, 2020 [cit. 2021-4-17]. Available at: https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

WORLD HEALTH ORGANIZATION, 2020k. *Preparedness and Response Progress Report: 1 February to 30 June 2020* [online]. Geneva: WHO [cit. 2021-7-19]. Available at: https://www.who.int/publications/m/item/who-covid-19-preparedness-and-response-progress-report---1-february-to-30-june-2020

WORLD HEALTH ORGANIZATION, 2020l. *Pulse survey on continuity of essential health services during the COVID-19 pandemic* [online]. Geneva: World Health Organization [cit. 2021-7-19]. Available at: https://www.who.int/publications/i/item/WHO-2019-nCoV-EHS_continuity-survey-2020.1

WORLD HEALTH ORGANIZATION, 2020m. Statement from the first ACT-Accelerator Facilitation Council meeting. *World Health Organization* [online]. September 10, 2020 [cit. 2021-7-19]. Available at: https://www.who.int/news/item/10-09-2020-statement-from-the-first-act-accelerator-facilitation-council-meeting

WORLD HEALTH ORGANIZATION, 2020n. Global partnership to make available 120 million affordable, quality COVID-19 rapid tests for low- and middle-income countries. *World Health Organization* [online]. September 28, 2020 [cit. 2021-7-19]. Available at: https://www.who.int/news/item/28-09-2020-global-partnership-to-make-available-120-million-affordable-quality-covid-19-rapid-tests-for-low--and-middle-income-countries

WORLD HEALTH ORGANIZATION, 2020o. WHO Director-General's opening remarks at the G20 Leaders Summit. *World Health Organization* [online]. November 21, 2020 [cit. 2021-7-19]. Available at: https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-g20-leaders-summit

WORLD HEALTH ORGANIZATION, 2020. *Health worker safety: a priority for patient safety* [online]. [cit. 2021-7-19]. Available at: https://www.who.int/docs/default-source/world-patient-safety-day/health-worker-safety-charter-wpsd-17-september-2020-3-1.pdf

WORLD HEALTH ORGANIZATION, 2020q. Kim Sledge and the World We Want partner with WHO Foundation to re-record unity anthem "We Are Family" in response to COVID-19 and to focus on global public health needs. *World Health Organization* [online]. October 19, 2020 [cit. 2021-7-19]. Available at: https://www.who.int/news/item/19-10-2020-kim-sledge-and-the-world-we-want-partner-with-who-foundation-to-re-record-unity-anthem-we-are-family-in-response-to-covid-19-and-to-focus-on-global-public-health-needs

WORLD HEALTH ORGANIZATION, 2020r. Call for Action: Managing the Infodemic. *World Health Organization* [online]. December 11, 2020 [cit. 2021-7-19]. Available at: https://www.who.int/news/item/11-12-2020-call-for-action-managing-the-infodemic

WREN, Kevin, 1999. *Social Influences*. London: Routledge.

WRIGHT, Ryan T. et al., 2014. Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance. *Information Systems Research* [online]. 25(2), 385–400 [cit. 2021-1-6].

YOUDE, Jeremy, 2013. The Rockefeller and Gates Foundations in Global Health Governance. *Global Society*. 27(2), 139-158.

YOUDE, Jeremy, 2018. Contemporary Global Health Governance Actors. *Global Health Governance in International Society*. Oxford: Oxford University Press.

ZARAKOL, Ayşe, 2017. States and ontological security. *Cooperation and Conflict* [online]. 52(1), 48-68 [cit. 2021-3-12]. Available at: https://www.jstor.org/stable/10.2307/48512930

ZIMMERMAN, Rae, 2013. Crisis communication. In: PENUEL, K. Bradley, Matt STATLER and Ryan HAGEN, ed. *Encyclopedia of Crisis Management*. Los Angeles: SAGE Publications, pp. 188-193.

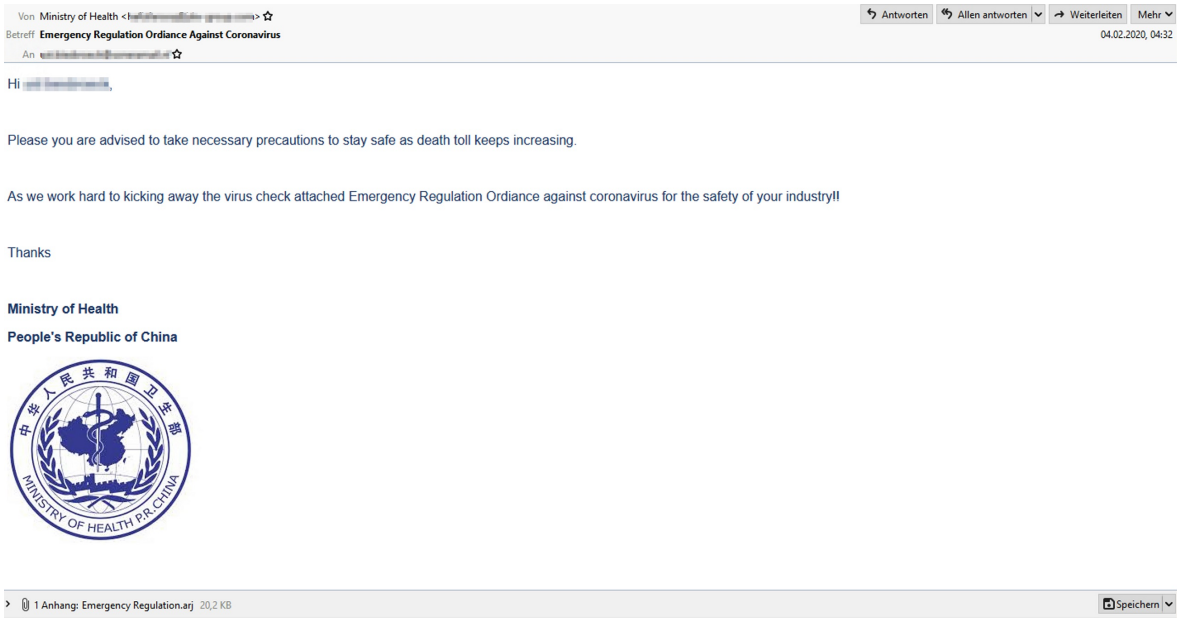
List of Appendices

Appendix no. 1: Sample of perfect data (picture)

Appendix no. 2: Sample of imperfect, but still usable data (picture)

Appendix no. 3: Sample of unusable data (picture)

Appendix No. 1: Sample of perfect data



Von Ministry of Health <[redacted]>

Betreff **Emergency Regulation Ordiance Against Coronavirus**

An [redacted]

Antworten | Allen antworten | Weiterleiten | Mehr

04.02.2020, 04:32

Hi [redacted],

Please you are advised to take necessary precautions to stay safe as death toll keeps increasing.

As we work hard to kicking away the virus check attached Emergency Regulation Ordiance against coronavirus for the safety of your industry!!

Thanks

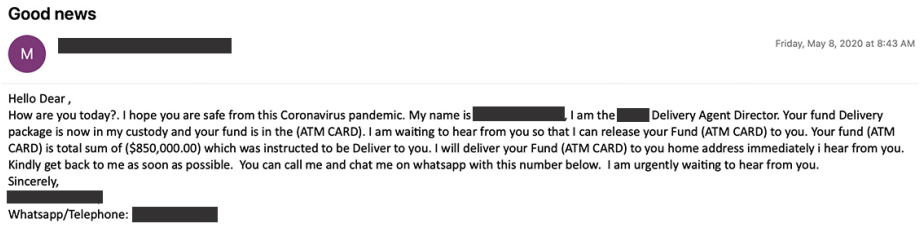
Ministry of Health

People's Republic of China

1 Anhang: Emergency Regulation.arj 20,2 KB

Speichern

Appendix No. 2: Sample of imperfect, but still usable data



Good news

M [redacted] Friday, May 8, 2020 at 8:43 AM

Hello Dear ,
How are you today?. I hope you are safe from this Coronavirus pandemic. My name is [redacted], I am the [redacted] Delivery Agent Director. Your fund Delivery package is now in my custody and your fund is in the (ATM CARD). I am waiting to hear from you so that I can release your Fund (ATM CARD) to you. Your fund (ATM CARD) is total sum of ($850,000.00) which was instructed to be Deliver to you. I will deliver your Fund (ATM CARD) to you home address immediately i hear from you. Kindly get back to me as soon as possible. You can call me and chat me on whatsapp with this number below. I am urgently waiting to hear from you.
Sincerely,
[redacted]
Whatsapp/Telephone: [redacted]

Appendix No. 3: Sample of unusable data