How Phishers Exploit the Coronavirus Pandemic: A Content Analysis of COVID-19 Themed Phishing Emails

Naci Akdemir1 and Serkan Yenal2

Abstract
This empirical study is an exploration of the influence methods, fear appeals, and urgency cues applied by phishers to trick or coerce users to follow instructions presented in coronavirus-themed phishing emails. To that end, a content analysis of 208 coronavirus-themed phishing emails has been conducted. We identified nine types of phishing messages crafted by phishers. Phishing emails purporting to provide information about the spread of the disease were the most common type of unsolicited emails. Authority, liking and commitment emerged as the most common influence methods. Fear appeals and urgency cues were present in almost all of the sampled phishing messages. Finally, the analysis of coronavirus-themed phishing emails revealed a shift in the modus operandi of phishers. The implications of these results are discussed in this paper.

Keywords
social sciences, criminology, crime, criminology and criminal justice, sociology, law, & deviance, sociology of law, cybercrime, cybersecurity, phishing, victimization

Introduction
The recent outbreak of coronavirus, which was later declared a pandemic, offered online perpetrators new opportunities to defraud users. Covid-19-related domains experienced a dramatic increase due to people’s interest in understanding the extent of the threat and searching for protection methods (Check Point, 2020a; World Health Organization [WHO], 2020). The Check Point Threat Intelligence report reveals that 3% of these domains were malicious, and 5% of them were suspicious (Check Point, 2020b). Cybersecurity reports indicate a substantial surge in malicious email activity. Google announced that its artificial intelligence-powered protection filter detected more than 18 million Covid-19 themed phishing and malware attacks in one single week in April 2020 (Cybersecurity and Infrastructure Security Agency, 2020; Lyons, 2020). These figures suggest that coronavirus has provided fraudsters with a targeted exploitation topic, which has rendered coronavirus-themed phishing a persistent threat.

As the number of Covid-19-related cyber incidents has increased, so has the amount of research examining the ways and opportunities leveraged by online perpetrators. Kashif et al. (2020) conducted an online survey to understand the extent of the cybercrime threats in Indonesia. Though the research results were descriptive, their analysis suggested a surge in cybercrime incidence. Similarly, Akdemir and Tuncer (2020) examined the Covid-19-related cybercrime risks in Turkey during the lockdown period. Their analysis suggested that the lockdown period significantly altered the frequency of online presence, which increased users’ exposure to motivated offenders. Their results illustrated how users’ changing online habits, such as accessing pirated media to watch movies for free, enhanced the risk of malware infection. However, the results of Hawdon et al. (2020), who also identified a surge in online presence in the U.S. population, contradict this finding. Their findings suggest that the stay-at-home orders did not change users’ cyber-routines; hence, the risk of cybercrime victimization was not heightened. The discrepancies between the results of these studies may be accounted for by the types of online activities in which people engaged during the lockdown period. While the former study indicated a rise in risky online activities, the latter revealed a lack of change in online behavioral patterns.

Put together, the results of these two studies seem to underscore the influence of engaging in risky online activities on the likelihood of experiencing cyber victimization (Akdemir & Yenal, 2020; Holt & Bossler, 2013; Leukfeldt, 2014).

1Gendarmerie and Coast Guard Academy, Ankara, Turkey
2National Defence University TMA, Ankara, Turkey

Corresponding Author:
Naci Akdemir, Department of Security Sciences, Gendarmerie and Coast Guard Academy, İncek Şehit Savcı Mehmet Selim Kiraz Bulvarı, Beytepe, Çankaya, Ankara 06805, Turkey.
Email: naci.akdemir@jsga.edu.tr

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).
The results of research by Naidoo (2020), who suggested a multi-level influence model of Covid-19 themed cybercrime, indicate that online perpetrators utilized situational factors to conduct sophisticated cyber-attacks. Naidoo (2020) has illustrated that online perpetrators also leveraged emotional and psychological factors. Likewise, stress and anxiety caused by lack of socialization during the Covid-19 pandemic were found to increase the likelihood of becoming the victim of a socially engineered online attack (Ventrella, 2020).

The aim of this research is to contribute to users’ protection by exploring online perpetrators’ modus operandi applied to exploit internet users’ coronavirus fears through phishing emails. To that end, the content of 208 coronavirus-themed phishing emails has been examined. To the best of our knowledge, this is the first phishing study in which users’ vulnerability to coronavirus-themed phishing attempts has been examined.

**Literature Review**

Social engineering, which aims to exploit internet users’ weaknesses, plays an essential role in phishing cases (Bullée et al., 2015; Krombholz et al., 2015). Fraudsters target users through emails, including highly sophisticated and challenging social engineering tactics, to solicit financial or personal information (Butavicu et al., 2016; Clark, 2017). Phishing emails are also utilized to lure users into opening attachments or clicking links containing malicious content, thereby facilitating the installation of malware such as ransomware on the target systems or devices (Gomes et al., 2020). Social engineering is initially conceptualized as employing socially tailored tricks to gain sensitive data such as passwords or usernames to access computer systems (Abraham & Chengalur-Smith, 2010). However, the scope of social engineering has been extended to cover the personal and financial information of internet users (Newman & Clarke, 2013). “Alternative routes to persuasion, attitudes and beliefs that affect human interactions and techniques for persuasion and influence” are three socio-psychological components of social engineering while exploiting human vulnerabilities (Peltier, 2006, p. 3).

The aim of social engineering in a phishing context is to manipulate users into divulging personal or financial information (Mishra et al., 2012; Nirmal et al., 2010). To that end, fraudsters exploit internet users’ social, psychological and cognitive vulnerabilities. It is proposed that human reasoning is based on two types of decision-making processes: heuristic and systematic. While the heuristic decision-making process produces quick and spurious decisions, the systematic process yields more carefully evaluated conclusions (Maheswaran & Chaiken, 1991; Schwarz, 2000). Phishing susceptibility research suggests that online perpetrators employ influence methods (Oliveira et al., 2017; Silic & Back, 2016; E. J. Williams et al., 2017; Wright et al., 2014), fear appeals (Jansen, 2015; Jansen & Leukfeldt, 2016; Liang & Xue, 2010; Witte, 1992), time pressure (Kahleman, 2011; Saqib & Chan, 2015; W. Zhang et al., 2012) and urgency cues (Alsharnouby et al., 2015; Ferreira et al., 2015; Harrison et al., 2016; Wang et al., 2012) to coerce users to make spurious decisions based on heuristic reasoning.

Peltier (2006) argued that persuasion and influence techniques are among the three critical social psychological components of social engineering. Phishing studies have applied Cialdini’s (Cialdini, 2009) influence methods to explore the factors that render email users vulnerable to phishing attempts. Cialdini (2009) proposed six influence methods, namely authority, scarcity, liking, social proof, consistency/commitment, and reciprocity. Whereas authority denotes compliance with requests purporting to be from authority figures, scarcity refers to the limited availability of opportunities (Cialdini, 2001). The liking construct assumes that individuals are more likely to obey requests or instructions coming from persons they like. Social proof exploits people’s tendency to make social comparisons with similar others (Cialdini et al., 1999). The consistency/commitment principle suggests that people are inclined to behave in line with their previous actions and obligations (Cialdini & Goldstein, 2004). Finally, reciprocity is the tendency to return a favor. It is based on the assumption that people feel obligated to repay those who have helped them in the past (Cialdini & Goldstein, 2004).

Empirical results yielded inconsistent results with regards to the relative impact of Cialdini’s (2009) influence methods on email users’ decision-making. Wright et al. (2014) found that four influence methods, liking, social proof, reciprocity and scarcity, increased the odds of people responding to phishing emails. Silic and Back (2016), however, suggested that liking is the most potent influence method used to obtain information from employees through social network sites. Research conducted by E. J. Williams et al. (2017) demonstrated that it is the combined effect of different influence techniques and personal or social circumstances that increase the susceptibility of internet users to phishing attacks.

Regarding demographic differences, Oliveira et al. (2017) investigated the effect of influence techniques across the demographic characteristics of email users. They found that different age groups display various vulnerabilities to influence tools. The reciprocation technique was found to be more effective in coercing older internet users into divulging personal information. On the other hand, scarcity, denoting the limited availability of something valuable, emerged as the most effective way to increase the likelihood of young internet users responding to phishing emails. Authority appeared to increase susceptibility to victimization for all age groups.

Fear appeals are considered to be effective deception methods to coerce individuals to comply with given messages (Chen, 2017; Jansen & van Schaik, 2018; Witte 1992, p. 329) defined fear appeals as “persuasive messages.
designed to scare people by describing the terrible things that will happen to them if they do not do what the message recommends.” In other words, fear appeals are persuasive messages prompting both a fear-provoking menace and a suggestion to thwart a depicted threat (K. C. Williams, 2012). Fear appeals have two dimensions: phrases introducing an imminent threat, and expressions suggesting a recommendation to cope with a threat (Vance et al., 2013). The former encompasses fear-arousing statements together with bogus or fabricated scenarios used to increase internet users’ perceived susceptibility to the presented threat. The latter directs email users to bogus websites where personal credentials can be provided.

The results of the empirical studies indicate that account closure, account update, unauthorized access to an account, and unusual account activities are the most frequently used fear appeals (Harrison et al., 2016; Moore & Clayton, 2012; Vishwanath et al., 2011). The existing research suggested a correlation between fear appeals and getting phished (Jansen & van Schai, 2018; Sharma, 2010; Workman, 2008). For example, Goel et al. (2017) found that internet users were more likely to respond to emails related to protecting assets. Disproportionate attention to fear appeals was also found to enhance the likelihood of responding to phishing emails. Empirical evidence suggested that internet users who paid too much attention to fear appeals failed to conduct a sound evaluation of the fabricated scenarios (Ferreira et al., 2015; Ferreira & Lenzini, 2015; Vishwanath et al., 2011).

Source credibility appeared to be another factor that enhanced the believability of emails. Bowen et al. (2011) argued that believability is a crucial factor in overcoming users’ defensive reactions. Empirical evidence suggests that the inclusion of reputable or trusted brands’ names into email messages increased email users’ susceptibility to divulging personal information (Schuetz et al., 2016; Silic & Back, 2016). Urgency cues were also found to divert internet users’ attention from phishing detection cues such as security indicators, and force internet users to make hasty decisions (Wang et al., 2012). Urgency cues such as “update, access, protect, cancel and confirm” were found to enhance the likelihood of people responding to phishing emails (Park & Taylor, 2015; Vishwanath et al., 2011).

Time pressure conveyed in unsolicited email messages was another factor found to impair users’ decisions. Time pressure messages such as “immediately, urgent, within one hour” increase the propensity for people to take risks (Hu et al., 2015; Young et al., 2012). Research has indicated that recipients who were exposed to email messages leveraging time pressure were more likely to respond to phishing emails (Luo et al., 2013; W. Zhang et al., 2012). However, Wang et al. (2012) found that computer literate email users were more successful in thwarting phishing attempts. Similarly, D. Kim and Hyun Kim (2013), who studied the impact of persuasive messages in phishing emails, found no significant relationship between time pressure and the likelihood of someone responding to a phishing email.

**Materials and Method**

**Data Collection**

This first stage of data preparation was gathering images of Covid-19 themed phishing emails. We collected the data between April 1, and April 16, to capture the nature of the lockdown period. The lockdown period was characterized by a lack of information and ambiguity about this new contagious disease. Individuals who were ordered to stay at home were curious and eager to learn about the contemporary situation of virus spread. Thus, opportunistic perpetrators seemed to apply social engineering strategies to exploit peoples’ willingness to acquire information. We searched the terms “COVID-19,” “Coronavirus “COVID” and “novel coronavirus” in conjunction with the phrase “phishing email” to access coronavirus-themed phishing email messages. We searched these terms via three popular search engines: Google, Bing, and Yandex. The image search sections of these search engines were used to access the actual images of phishing emails. This informed decision was made to eliminate the researcher bias caused by journal news related to phishing cases. The real pictures of these phishing emails were mostly collected from official websites such as Action Fraud, FBI, or web pages of universities’ or companies’ IT departments, where internet users were warned about phishing messages. During this period, we collected 2,372 images of phishing emails sent during the lockdown period of the Covid-19 pandemic. Figure 1 illustrates two samples of phishing emails collected from the internet. We also enlisted the help of the newsletters of the WHO (WHO) and Action Fraud to receive phishing email samples.

In the second stage, we aimed to eliminate phishing emails with repeated or irrelevant content. This elimination phase lasted about a week, as the two authors separately conducted a careful reading procedure to prevent loss of data. After three rounds of reading, we had obtained 208 phishing emails with unique content. The emails we received from the mailing lists did not yield sufficient information to be analyzed. Since the data were comprised of images of phishing emails, these emails were transcribed verbatim onto a word processor. This process enabled us to immerse ourselves in the data and acquire first impressions of these phishing messages. As will be detailed in the next section, we initially read the whole email and highlighted various relevant content. During this period, we realized that whereas some emails were information-rich, others were not at all. Though all of the emails were included in the analysis, we mostly utilized these 40 information-rich emails to discern social engineering messages. The whole data, comprising 208 phishing emails, were also analyzed to create a taxonomy of phishing emails.
The decrease in sample size suggests that phishers used different emails and IP addresses to evade security walls; hence, duplicated versions of the same material were used to conduct Covid-19 themed phishing emails. This shrinkage also implies that a small number of motivated offenders would account for a significant proportion of phishing
attacks. The Pareto Principle, known as the 80-20 rule, proposes that roughly 80% of wealth is controlled by 20% of the population (Dunford et al., 2014; Grosfeld-Nir et al., 2007). Traditional crime studies have also illustrated that a small number of offenders are responsible for most of the crimes committed in a specific area (Braga, 2008; Brunson, 2015). The policy implications of this issue will be elaborated in the Conclusion section.

Analytic Strategy

In this study, the qualitative content analysis (QCA) method has been applied to explore the social engineering methods utilized to coerce users to click on the links provided in phishing emails. QCA is an analytic process whereby textual or visual data is described and interpreted through the systematic and objective classification of textual information into categories, patterns, and themes (Sandelowski, 1993; Y. Zhang & Wildemuth, 2009). QCA aims to provide a descriptive account of textual data (Vaimoradi et al., 2013). QCA can be either inductive or deductive, or a combination of both. The aim of the study informs the researcher’s choice of study and the availability of a priori knowledge or theory (Graneheim et al., 2017).

QCA is a flexible approach while discerning trends and patterns in textual data, which renders it a popular analysis tool (Stemler, 2000). However, the lack of standard procedures to be applied throughout the analysis process raises concerns over reliability or trustworthiness (Creswell & Miller, 2000). Delineation of the analysis phases is suggested as the most proper solution to any trustworthiness issues (Elo et al., 2014). Several scholars (Assarroudi et al., 2018; Elo & Kyngäs, 2008; Hsieh & Shannon, 2005; Mayring, 2015; Y. Zhang & Wildemuth, 2009) have proposed standard procedures to be applied to enhance the trustworthiness of the analysis process (please see Assarroudi et al. (2018) for a detailed discussion of these procedures). A review of the literature suggested that although different authors divided the content analysis process into varying stages, these stages can be summarized into three concurrent phases: preparation, organization (data reduction), and reporting (Elo & Kyngäs, 2008; Miles & Huberman, 1994). Since the preparation phase of the process was described above in the data collection section, a description of the analysis process will continue with the organization (data reduction) phase of the analysis.

Data reduction is the phase wherein the data is reduced to its basic content to have a condensed material. The data condensation procedure is a continuous and iterative process, including written summaries and coding (Berg et al., 2004; Braun & Clarke, 2006). Regarding the coding process, two approaches, emergent (inductive) and a priori (deductive) coding, are identified in the literature (Graneheim et al., 2017; Stemler, 2000). Whereas a priori coding relies on the categories derived from the theory or previous research, emergent coding is based on the researcher’s interpretations or abstractions of the data (Krippendorff, 2004; Schreier, 2012). Based on the a priori knowledge on Cialdini’s (2009) six influence methods and the results of the previous research (fear appeals, urgency cues, and source credibility), in this study, the deductive approach, also known as directed content analysis, was applied (Hsieh & Shannon, 2005; Moretti et al., 2011). The goal of the directed content analysis was to explore the factors phishers utilize to convince email users to follow the instructions presented in unsolicited emails. An inductive approach was also employed to create a taxonomy of phishing emails. We followed the six stages proposed by Assarroudi et al. (2018) at the organization phase of the analysis.

For the first part of the analysis, the aim was to distinguish the social engineering methods that were adopted to render internet users susceptible to phishing attacks. A theoretically informed structured deductive approach was employed to attain this goal. Elo and Kyngäs (2008) suggested the use of a structured method, based on the categorization matrix, which illustrates the coding rules. This matrix is also called a codebook (I. Kim & Kuljis, 2010), coding scheme (Thayer et al., 2007), or content categories (Harwood & Garry, 2003). This enables researchers to present a conceptually driven understanding of the data (O’Connor & Joffe, 2020). The matrix should also contain categories and subcategories derived from the theory or literature (Stemler, 2000). Based on these considerations, our categorization matrix comprised three components: category name, definition/explanation, and text examples. We also created two main categories (Cialdini’s influence methods and research findings), which are derived from previous phishing studies. The first category contained six sub categories (authority, liking, social proof, consistency/commitment, scarcity, and reciprocity), and the latter was comprised of three sub categories (fear appeals, urgency cues, and source credibility) (Table 1).

Providing definitions of categories/sub categories and textual data examples can contribute to maintaining trustworthiness (Schreier, 2012). To ensure trustworthiness, we clearly stated the definitions/explanations of the main and sub categories and provided textual examples at the second stage. Based on the literature review, we defined or explained each category. For example, authority is defined as “individuals’ inborn inclination to comply with orders or suggestions in the presence of the figures of authority” (Cialdini, 2009, p. 180), while fear appeals are explained as “online communications informing receivers about an imminent threat or a significant problem besides providing a solution to overcome the mentioned problem” (Witte, 1992). Later, we included examples for each sub category. These “anchor samples” (Assarroudi et al., 2018, p. 50), which act as the identifier for the categories, were obtained from previous phishing susceptibility studies. For example, the anchor sample for the urgency cues category was as follows: “you need to update your account before the link expires, after 24 hours” (Park & Taylor, 2015, p. 3) (Table 1).
Table 1. The Categorization Matrix.

| Category name             | Definition                                                                 | Text example/author                      |
|---------------------------|---------------------------------------------------------------------------|------------------------------------------|
| Research findings         |                                                                           |                                          |
| Fear appeals              | Online communications informing receivers about an imminent threat or a significant problem besides providing a solution to overcome the mentioned problem. | “A review of our records shows permanent error with your XX account. To prevent closure of your account please log in here to your account to resolve the problem.”(Harrison et al., 2016). |
| Urgency cues              | Messages indicating scarcity, time limitation or a warning aim to coerce receivers to focus on the urgency conveying messages to elicit their compliance. | “You need to update your account before the link expires, after 24 hours.”(Park & Taylor, 2015) |
| Source credibility        | Names of big brands appeared to be another factor that enhanced the believability of emails. | “Using logos and names of reputable businesses.”(W. Zhang et al., 2012) |
| Cialdini’s influence methods |                                                                           |                                          |
| Authority                 | Individuals’ inborn inclination to comply with orders or suggestions in the presence of the figures of authority are present. | “Click here”; “confirm your account details”(Ferreira & Lenzini, 2015) |
| Liking                    | People prefer to say yes to those they like.                             | “We realize that this precaution may cause you some inconvenience.” (Wright et al., 2014). |
| Social proof              | People tend to behave as their friends and peers have behaved.           | “We’d really like to keep you happy by continuing to help” (Oliveira et al., 2017) |
| Consistency/commitment    | Individuals are driven to be consistent not only with their trait self-attributions, but with their previous behaviors and commitments as well. | “As you have done before, please update your password using the following link.”(Wright et al., 2014) |
| Scarcity                  | People respond to perceived shortages by placing greater psychological value on perceived scarce items. | “You can save 20% on your next electric bill by filling out our online survey within the next three days.” (Oliveira et al., 2017). |
| Reciprocity               | The tendency to return a favor.                                          | “If you respond you will have a chance to upgrade to our new version” (Baryshevtsev & McGlynn, 2020) |

The second part of the analysis was conducted to create a taxonomy of phishing emails. This process required an examination of textual data and deriving categories from the codes. This part of the analysis, based on the conventional content analysis approach, was more flexible than the first phase. Conventional content analysis (Hsieh & Shannon, 2005), or inductive content analysis (Elo & Kyngäs, 2008), is mostly applied when there are no pre-defined categories (Krippendorff, 2004). The analysis starts with discerning lower-level units, namely codes, and goes on to the creation of categories/sub categories and themes (Patton, 2002). Conventional content analysis may examine latent (having implied meaning) or manifest (available on the textual or visual data) content (Berg et al., 2004; Kondracki et al., 2002). Since the aim of the analysis was to create a taxonomy of phishing attacks, keywords such as “refund,” “information” or “guideline” were used as reference terms to develop codes.

We created two projects using NVivo QSR qualitative analysis software so that each researcher could conduct the analysis independently. Hsieh and Shannon (2005) recommended a two-step coding procedure. At first, the researcher reads the textual data and highlights various parts based on the first impression guided by prior knowledge (theory and/or results of previous research). Later, per the categorization matrix, any highlighted material would be coded. Following this advice, we initially read the textual material via a word processor and highlighted any phrases carrying social engineering and influence messages. We uploaded the files to the NVivo project after highlighting all of the relevant materials.

We individually conducted two rounds of coding at a 1-week interval, since Elo et al. (2014) recommended two rounds of independent coding as an efficient method to enhance trustworthiness, and thereby maintain intra-coder reliability. Promoting coder reflexivity is another benefit of this iterative process.

Following the initial coding process, we worked together to review the codes, discuss the rationale for assigning each text to specific categories/sub categories, and settle fundamental coding disagreements as advised by Thomas and Harden (2008), to ensure intercoder agreement. O’Connor and Joffe (2020) provided a distinction between intercoder reliability and intercoder consistency. Whereas the former relies on a numerical assessment of consensus on the coding of the textual data, the latter involves discussion of discrepancies and accordance. We preferred discussion of the inconsistencies to understand any differences in individual interpretations (DeCuir-Gunby et al., 2011). Due to the Covid-19 pandemic restrictions, these meetings were held online via a video communication platform. In-depth discussion over the coding discrepancies allowed us to reach a consensus about the textual data assigned to sub categories. The
categorization matrix and visual representation of the categories/sub categories were utilized during this discussion.

After agreeing on the assignment of textual context to the sub categories, we utilized tables to display the research findings. Huberman et al. (2014, p. 7) defined display as “an organized, compressed assembly of information that allows conclusion drawing and action.” Since reading and evaluating extended texts can be a cumbersome process due to cognitive overload, extended texts, tables, graphs and diagrams as well as direct quotes can be utilized to present research findings (Owneugbuzie & Dickinson, 2008). To that end, we illustrated the research findings in three tables.

**Results**

**Table 2. Taxonomy of Phishing Attempts.**

| Type                                  | Persuasive message                                                                                                                                                                                                 | No* |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Providing information to prevent the spread of disease | Due to the high volume of information being spread about the Coronavirus disease (COVID-19) pandemic we put together a comprehensive document that contains guidelines WHO recommendations. | 23  |
| Offering financial benefit            | As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund program for dealing with the coronavirus outbreak in its action plan. You are eligible to get a tax refund (rebate) of 128.34 GBP. | 5   |
| Asking for donation                   | Donations support WHO’S work, including with partners, to track and understand the spread of the virus, to ensure patients get the care they need and frontline workers get essential supplies and information, and to accelerate research and development of a vaccine and treatments for all who need them. See below for more ways to give via BTC (Bitcoin). Everyday donations help support life-saving work for the world. | 3   |
| Offering a service                    | We also want you to have confidence that you can bank virtually anywhere anytime with the xxx Mobile® app 1 and xxx.com If you haven’t already Download the xxx Mobile® app> | 2   |
| Offering a cure                       | A group of Corona-Virus Specialist is here in our own direct contract clinical attached for an antiviral called remdesivir. Attached is step one 10 $ to connect with xxxxx on Skype. | 2   |
| Threatening with unauthorized payment or shipment | We are planning to ship the following orders next week but due to the Corona virus we have postponed shipment. Please check details attached new shipping info and the shipping instructions and advice if we should still proceed. If you are no problem with above shipment time, we will proceed the shipment. | 2   |
| Informing account closure             | The pandemic has become a global issue and we’ll be deactivating your email . . . for server propagation on the latest update. Please confirm to avoid affecting your email. Click here to confirm non removal of your email . . . | 1   |
| Asking a favor                        | I will need you to do something for me urgently. About 3 people has been tested positive of Corona down my area so i cant go out for now. Kindly reply back to me via email as my phone is faulty at the moment. | 1   |
| Offering an education program         | In view of these directives, the institution is currently organizing a seminar for all staff to talk about this deadly virus. All employee/staff are hereby ask to quickly participate in the quick survey to show your awareness about the coronavirus and also register for the seminar. | 1   |

*Note. WHO = World Health Organization.*

*aDenotes the number of different message contents related to the same theme.

The results section is comprised of email messages impersonating health organizations and governmental agencies. We identified 23 different email messages crafted to coerce users to download the attachments provided in emails. These emails ask users to view or download attached documents to review safety measures in place to prevent the spread of the disease (Table 2). Offering financial benefits is the second most common theme which emerged (n = 5). Phishing emails that fall into this category are designed to trick users into disclosing their personal identifying information. As in the case of the Her Majesty’s Revenue & Customs (HMRC) tax refund scheme, targets are lured to click on the link and provide their credentials. This attack is an example of a conventional phishing technique, which requires the target to type in their details. Asking for a donation is another theme designed to exploit individuals’ desire to help organizations which are combating coronavirus (n = 3). The threat of unauthorized payment (n = 2), offering a cure (n = 2), offering a service such as a banking application (n = 2), mandatory education programs (n = 1), the threat of account closure (n = 1), and asking for a favor are among the other themes that have fewer variants.
The second part of the analysis dealt with discerning the frequency of social engineering methods applied to leverage individuals’ curiosity, fear and concerns. Since some emails contained more than one social engineering technique, the number of influence methods exceeds the total number of emails examined. Table 3 illustrates the samples of influence methods identified.

Cialdini proposed six influence methods, namely authority, liking, social proof, consistency/commitment, scarcity, and reciprocity. Content analysis of the phishing emails revealed that authority was the most used influence method \((n = 23)\). While commitment appeared 13 times in phishing emails, liking was present in seven email messages. We did not identify scarcity, reciprocity or social proof influence methods in any of the email messages.

Previous phishing susceptibility research identified fear appeals, urgency cues, and credibility cues as factors that perpetrators used to manipulate the decision-making systems of users (Vishwanath et al., 2011; Wang et al., 2012; Wright et al., 2014). Informed by these studies, we included these cues in our analysis. Content analysis suggested that fear appeals were extensively utilized to coerce users to follow the instructions presented in phishing emails \((n = 16)\). Urgency cues were used in twelve phishing emails. Finally, the logos of health organizations, government agencies and companies were present in almost every phishing email, used as a credibility cue.

### The Relationship Between the Type of Attack and Social Engineering Methods

We cross-tabulated social engineering methods and the types of phishing emails identified to examine the distribution of 72 codes across the email messages. As Table 4 illustrates, the authority influence method was mostly used in email messages asking users to download attached documents purporting to provide information about coronavirus \((79.94\%, n = 19)\). However, authority cues were only employed in four types of messages. The commitment and liking influence methods were mostly applied to emails providing information and asking for a donation. Fear appeal messages were...
primarily included in emails containing information (52.37%, \(n = 10\)). Fear appeals were included in six out of nine types of phishing messages. Urgency cues were mostly present in phishing messages offering financial benefits (30.4%, \(n = 3\)). Urgency cues were present almost all of the sampled phishing messages (77.7%, \(n = 7\)).

Frequently Used Words

Finally, we explored the most frequently used words in the coronavirus-themed phishing emails. We excluded certain words, such as “coronavirus” or “click,” to obtain a refined result. Health \((n = 60)\), disease \((n = 20)\), control \((n = 19)\), attached \((n = 15)\), and prevention \((n = 15)\) emerged as the five most commonly used words in these messages. The implications of this result will be evaluated in the Discussion section.

Discussion

Phishers always take advantage of events that have attracted public attention, and the coronavirus pandemic has provided online perpetrators with an opportunity to defraud internet users (Dewan, 2020). Cybersecurity firms (i.e., Norton and Symantec) have highlighted a significant surge in coronavirus-themed phishing attempts. The news media and the reports of security companies have suggested that coronavirus related cyberattacks have become a persistent threat. The aim of this study is to contribute to crime prevention efforts by exploring the social engineering methods employed in coronavirus-themed phishing emails. To that end, we conducted a content analysis of 40 phishing emails with different contents. We identified nine types of coronavirus-themed phishing emails.

The analysis revealed that phishers have designed 23 different email contents purporting to provide information about the recent situation of the spread of coronavirus or ways to evade coronavirus infection. Variants of the email messages asked users to download attached documents. This technique suggests a shift in the modus operandi of phishers, since conventional phishing emails ask users to click on links to provide personal or financial information. This change in phishing attempts may be attributed to several social and technological factors. Cyber security studies suggest that cyber security awareness, which can be promoted by training and educational programs, is the key initiative for reducing user susceptibility to socially engineered attacks (Aldawood & Skinner, 2018; Korpela, 2015). Given that schools, governments, private sector and non-governmental organizations are increasingly launching new initiatives to raise cyber awareness, it seems reasonable to believe that individuals are now more cyber-aware when compared to the past. Hence, it is hard to convince individuals to type in their credentials using conventional phishing methods. In addition, the proliferation of digitalized technology, which has increased the dependency on digital systems, has rendered them as valuable assets, and the retrieval of data or systems is something for which users have to pay. This issue seems to motivate offenders to devise more sophisticated attacks (i.e., promising ransomware attacks) to achieve their goals.

Agent Tesla Keylogger is the most recent example of these kinds of sophisticated cyber-attacks (Baker, 2020; Riley, 2019). This malware is capable of harvesting user information from different platforms such as emails or social media (e.g., Twitter, Facebook, Instagram) (Ruiz, 2020). A phishing email that says, “You can now download and Access the attached My Health Zip file from a Windows Computer only,” supports our proposition, since Agent Tesla Keylogger operates only on Windows-based operating systems (“Review—Navigating Cybersecurity During a Pandemic,” 2020). It is evident that phishers are now conducting joint attacks designed to compromise individuals’ and businesses’ online accounts rather than coercing users to provide their credentials. Hence, users should be informed about this new threat that preys on the inadvertent downloading of coronavirus-related documents.

Content analysis of the coronavirus-themed phishing emails suggested that authority, commitment, liking, fear appeals, and urgency cues were the most frequently employed influence methods. This result is in line with previous research indicating that Cialdini’s influence methods, (Silic & Back, 2016; E. J. Williams et al., 2017; Wright et al., 2014), fear appeals (Jansen, 2015; Jansen & Leukfeldt, 2016; Liang & Xue, 2010; Witte, 1992) and urgency cues (Alsharnouby et al., 2015; Ferreira et al., 2015; Harrison et al., 2016; Wang et al., 2012) were used to trick users into yielding their personal identifying information. Fear appeals and urgency cues were present in almost all of the coronavirus-themed phishing emails. In addition, authority was mostly employed in emails pretending to offer information about the disease. These results suggest that authority, fear and urgency are the three essential constructs that phishers utilize to coerce the user to make hasty decisions based on their heuristic decision-making processes.

Regarding the composition of messages, phishing emails designed to provide information about the coronavirus allegedly included all of the influence methods that are mostly used in phishing messages. While emails pretending to offer a service used commitment and liking to influence users, those which aimed to present a threat of unauthorized payment or shipment included only fear appeals and urgency cues. It appears that phishers craft their messages very carefully and employ the most appropriate influence methods in their phishing messages.

We analyzed the most frequently used words in the coronavirus-themed phishing emails. “Health,” “disease “control,” “attached” and “prevention” appeared to be the most commonly used words. This result indicates that the phishers designed the structure of these messages to illicit the users’ concerns related to preventing disease or curiosity about the latest information. Social engineering methods such as influence techniques or fear appeals are disguised in these
messages which seemingly provide background information about the attached files.

**Conclusion**

The lockdown period, characterized by the mass quarantine of individuals, unprecedentedly changed the way we socialize and work. People were ordered to remain at home and work remotely. This new normal way of living, socializing and working had some unavoidable adverse consequences. The social, economic and psychological repercussions of the lockdown period on individuals and organizations are well-documented (Rahman et al., 2020; Sumner et al., 2020; Vahia et al., 2020; Xiong et al., 2020). An increased cybersecurity victimization risk emerged as another ramification of the lockdown era which followed the declaration of the Covid-19 pandemic. A massive surge in Covid-19 related domain names suggested that online perpetrators were quick to impersonate health institutions, governments, and organizations to exploit health-related vulnerabilities. The aim of this study has been to discern the social engineering methods employed in Covid-19 themed phishing emails during the lockdown period. Creating a taxonomy of Covid-19 themed phishing emails was another goal of this research. To these ends, content analysis of 208 phishing emails collected between 1st April and 16th April 2020 was conducted.

**Key Findings**

Content analysis of the Covid-19 themed emails yielded significant results. Distinguishing the shift in the modus operandi of phishers is one of the novel contributions of this study. Phishers have mostly employed social engineering methods to coerce individuals to provide their financial details via links presented in email messages. However, as individuals are more computer savvy nowadays, this technique has become less effective. Although phishing emails are also used to infect target computers via website links, our analysis results illustrated that a majority of the Covid-19 themed emails analyzed were asking users to download attached documents which included malicious content. Attached documents that allegedly contained information related to the Covid-19 pandemic were used to conduct more sophisticated attacks such as ransomware. This result suggests that socially engineered phishing attacks coupled with code-based threats (i.e., ransomware) will become more common.

Presenting a taxonomy of the Covid-19 themed emails was another contribution of this study. We identified nine variations of phishing emails targeting individuals, businesses and organizations. The most frequently employed type of phishing emails were those allegedly offering solutions to prevent the spread of the coronavirus outbreak. This finding illustrates that phishers who were rational actors were quick to take advantage of the fear and anxiety of individuals in the wake of the spread of the virus.

Regarding the influence methods applied in the Covid-19 themed phishing emails, of the six influence methods proposed by Cialdini, authority emerged as the most frequently used. It is argued that people learn to obey authority at an early age, which promotes the pre-disposition to trust or obey authority figures (Bouchard, 2009). Authority’s perceived expertise, individuals’ felt obligation to obey, and authority’s presumed coercive power, were suggested as factors promoting obedience to authority (Lutsky, 1995). It seems that phishers exploit users’ inclination to obey figures of expertise through emails pretending to provide information about the Covid-19 pandemic to gain compliance.

**Policy Implications**

The data collection phase of the study suggested that although there were 2,372 emails sent from different accounts, 208 emails remained after removing the duplicated content. This shrinkage implies that a small proportion of online offenders account for the majority of the phishing attempts. Focused deterrence policing strategies are designed to decrease the offending behavior for a particular crime type through targeting specific offenders (Tillyer et al., 2012). Focused deterrence policing strategies applied to dealing with core criminals have yielded successful results in terms of preventing traditional crimes such as homicide or gang violence (Braga et al., 2019; Braga & Weisburd, 2012). This strategy requires the co-operation of several actors, such as law enforcement or social services, to deter offending behavior (Tillyer & Kennedy, 2008). Most cybercriminals think that their actions are undetected; hence they continue engaging with illegal and illicit online activities. We believe that focused deterrence strategies entailing direct communications with potential offenders to inform them that their actions have received legal attention (Brunson, 2015) will have some success in reducing phishing intention. Phishers who are aware that increased law enforcement attention has been placed on them may choose to receive guidance to find a legal means of earning a living, or may decide to stop offending behavior.

Content analysis of the Covid-19 themed phishing emails suggested that emails purporting to provide coronavirus information were the most common type of phishing attempt. This result illustrates the desire to acquire information, as social engineers exploit vulnerabilities in the targeted population. Human error is generally conceived as the weakest link in cybersecurity (Akdemir & Lawless, 2020; Clark, 2017; Heartfield et al., 2016). Training and education programs related to cyber threats have been found to be effective in decreasing user susceptibility and increase cyber awareness (McCrohan et al., 2010; Zwilling et al., 2020). In this regard, providing timely and accurate information about the
threat could soothe the public desire to acquire knowledge. In addition, publicly available programs via social media or TV could also help to promote cybersecurity awareness.

Limitation and Research Implications

Though this research has yielded some impressive results, still it has some limitations that need to be addressed. The focus of this research has been on the content of the phishing emails; hence, the success rates of these phishing emails remained unexplored. Future research may involve applying experimental designs to understand the relative significance of Cialdini’s influence techniques and fear appeals on individuals’ decisions to reply or follow the instructions presented in Covid-19 themed emails. Future researchers may also examine whether individual differences, such as personality traits, affected users’ susceptibility to Covid-19 related emails. The small sample size was another limitation of this study. The central aim of this study was to understand the social engineering methods applied in phishing emails during the lockdown period. Since the website search captured phishing emails sent before April 1, it reflected the characteristics of a particular era, namely the lockdown period. Future researchers may obtain more samples of Covid-19 themed phishing emails; thus, new insights may be gained.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. Technology in Society, 32(3), 183–196.

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. Internet Research, 30(6), 1665–1687. https://doi.org/10.1108/INTR-10-2019-0400

Akdemir, N., & Tuncer, C. O. (2020). Covid-19 salgını sonrasında siber suç mağduriyeti riskleri üzerine bir değerlendirmeye. In İ. H. Demircioğlu, Z. Aysar, & C. O. Tuncer (Eds.), Salgınla Yaşamak: Güvenli Gelecek (pp. 111–133). Pegem Akademi.

Akdemir, N., & Yenal, S. (2020). Card-not-present fraud victimization: A routine activities approach to understand the risk factors. Security Sciences, 9(1), 243–268. https://doi.org/10.28956/gbd.736179

Aldawood, H., & Skinner, G. (2018, December 4–7). Educating and raising awareness on cyber security social engineering: A literature review [Conference session]. 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE). https://ieeexplore.ieee.org/document/8615162

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies, 82, 69–82.

Assaroudi, A., Heshmati Nabavi, F., Armat, M. R., Ebadi, A., & Vaismoradi, M. (2018). Directed qualitative content analysis: The description and elaboration of its underpinning methods and data analysis process. Journal of Research in Nursing, 23(1), 42–55.

Baker, P. (2020, April 22). Oil & gas spearphishing campaigns carry Agent Tesla Spyware. Channel Futures. https://www.channelfutures.com/mssp-insider/oil-gas-spearphishing-campaigns-carry-agent-tesla-spyware

Baryshevtsev, M., & McGlynn, J. (2020). Persuasive appeals predict credibility judgments of phising messages. Cyberpsychology, Behavior, and Social Networking, 23(5), 297–302.

Berg, B. L., Lune, H., & Lune, H. (2004). Qualitative research methods for the social sciences (Vol. 5). Pearson.

Bouchard, T. J. (2009). Authoritarianism, religiousness, and conservatism: Is “obedience to authority” the explanation for their clustering, universality and evolution? In E. Voland & W. Schiehenhövel (Eds.), The biological evolution of religious mind and behavior (pp. 165–180). Springer.

Bowen, B. M., Devarajan, R., & Stolfo, S. (2011, November 15–17). Measuring the human factor of cyber security [Conference session]. 2011 IEEE International Conference on Technologies for Homeland Security (HST). https://ieeexplore.ieee.org/document/6107876

Braga, A. A. (2008). Pulling levers focused deterrence strategies and the prevention of gun homicide. Journal of Criminal Justice, 36(4), 332–343.

Braga, A. A., & Weisburd, D. L. (2012). The effects of “pulling levers” focused deterrence strategies on crime. Campbell Systematic Reviews, 8(1), 1–90.

Braga, A. A., Weisburd, D. L., & Turchan, B. (2019). Focused deterrence strategies effects on crime: A systematic review. Campbell Systematic Reviews, 15(3), Article e1051.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101.

Brunson, R. K. (2015). Focused deterrence and improved police-community relations: Unpacking the proverbial black box. Criminology & Public Policy, 14, 507–514.

Bullée, J.-W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. Journal of Experimental Criminology, 11(1), 97–115.

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. arXiv preprint arXiv:1606.00887. https://arxiv.org/abs/1606.00887

Check Point. (2020a, January 2). January 2020’s most wanted malware: Coronavirus-themed spam spreads malicious Emotet malware. https://blog.checkpoint.com/2020/02/13/january-2020s-most-wanted-malware-coronavirus-themed-spam-spreads-malicious-emotet-malware/

Check Point. (2020b, March 5). Update: Coronavirus-themed domains 50% more likely to be malicious than other domains. https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/
Chen, Y. (2017, October). Examining internet users' adaptive and maladaptive security behaviors using the extended parallel process model [Conference session]. ICIS 2017. https://www.semanticscholar.org/paper/Examining-Internet-Users%27-Adaptive-and-Maladaptive-Chen/abf11fed80ffa76012e-0f018efe94eff48e19a53

Cialdini, R. B. (2001). Harnessing the science of persuasion. Harvard Business Review, 79(9), 72–81.

Cialdini, R. B. (2009). Influence: Science and practice (Vol. 4). Pearson Education.

Cialdini, R. B., & Goldstein, N. (2004). Social influence: Compliance and conformity. Annual Review of Psychology, 55, 591–621.

Cialdini, R. B., Wosinska, W., Barrett, D. W., Butner, J., & Gornik-Durose, M. (1999). Compliance with a request in two cultures: The differential influence of social proof and commitment/consistency on collectivists and individualists. Personality Social Psychology Bulletin, 25(10), 1242–1253.

Clark, J. W. (2017). Trends in social engineering: Securing the weakest link. NSI. http://docplayer.net/78444755-Trends-in-social-engineering-securing-the-weakest-link.html

Creswell, J. W., & Miller, D. L. (2000). Determining validity in qualitative inquiry. Theory Into Practice, 39(3), 124–130.

Cybersecurity and Infrastructure Security Agency. (2020). COVID-19 exploited by malicious cyber actors. https://www.us-cert.gov/ncas/alerts/aa20-099a

DeCuir-Gunby, J. T., Marshall, P. L., & McCulloch, A. W. (2011). Developing and using a codebook for the analysis of interview data: An example from a professional development research project. Field Methods, 23(2), 136–155.

Dewan, A. (2020, February 25). Warning: Email scam uses list of “corona-virus affected company staff” to deliver malicious payload. Mail Guard. https://www.mailguard.com.au/blog/warning-email-scam-uses-list-of-corona-virus-affected-company-staff-to-deliver-malicious-payload

Dunford, R., Su, Q., & Tamang, E. (2014). The Pareto principle. The Plymouth Student Scientist, 7(1), 140–148.

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative content analysis: A focus on trustworthiness. SAGE Open, 4(1). https://doi.org/10.1177/2158244014522633

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. Journal of Advanced Nursing, 62(1), 107–115.

Ferreira, A., Coventry, L., & Lenzini, G. (2015, July 13). Principles of persuasion in social engineering and their use in phishing [Conference Session]. The International Conference on Human Aspects of Information Security, Privacy, and Trust. https://link.springer.com/chapter/10.1007%2F978-3-319-20376-8_4

Ferreira, A., & Lenzini, G. (2015, July 13). An analysis of social engineering principles in effective phishing [Conference Session]. 2015 Workshop on Socio-Technical Aspects in Security and Trust. https://ieeexplore.ieee.org/document/7351971

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. Journal of the Association for Information Systems, 18(1), Article 2.

Gomes, V., Reis, J., & Alturas, B. (2020, June 24–27). Social engineering and the dangers of phishing [Conference Session]. 2020 15th Iberian Conference on Information Systems and Technologies (CISTI). https://ieeexplore.ieee.org/document/9140445.

Graneheim, U. H., Lindgren, B.-M., & Lundman, B. (2017). Methodological challenges in qualitative content analysis: A discussion paper. Nurse Education Today, 56, 29–34.

Grosfeld-Nir, A., Ronen, B., & Kozlovsky, N. (2007). The Pareto managerial principle: When does it apply? International Journal of Production Research, 45(10), 2317–2325.

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails: How attention and elaboration protect against phishing. Online Information Review, 40(2), 265–281.

Harwood, T. G., & Garry, T. (2003). An overview of content analysis. The Marketing Review, 3(4), 479–498.

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: The initial results from a natural experiment. American Journal of Criminal Justice, 45, 546–562.

Heartfield, R., Loukas, G., & Gan, D. (2016). You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks. IEEE Access, 4, 6910–6928.

Holt, T. J., & Bossler, A. M. (2013). Examining the relationship between routine activities and malware infection indicators. Journal of Contemporary Criminal Justice, 29, 420–436. https://doi.org/10.1177/1043986213507401

Hsieh, H.-F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. Qualitative Health Research, 15(9), 1277–1288.

Hu, Y., Wang, D., Pang, K., Xu, G., & Guo, J. (2015). The effect of emotion and time pressure on risk decision-making. Journal of Risk Research, 18(5), 637–650.

Huberman, A. M., Miles, M., & Saldana, J. (2014). Qualitative data analysis: A methods sourcebook. SAGE.

Jansen, J. (2015, June 3). Studying safe online banking behaviour: A protection motivation theory approach [Conference Session]. The Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015, June 3). https://www.semanticscholar.org/paper/Studying-Safe-Online-Banking-Behaviour%3A-A-Theory-Jansen/1cdf4ac6f68d69e2690e4bf44d7c641f5c6f16

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. International Journal of Cyber Criminology, 10(1), 79–91.

Jansen, J., & van Schaik, P. (2018). Persuading end users to act cautiously online: A fear appeals study on phishing. Information & Computer Security, 26(3), 264–276.

Kahneman, D. (2011). Thinking, fast and slow. Macmillan.

Kashif, M., Javed, M. K., & Pandey, D. (2020). A surge in cybercrime during COVID-19. Indonesian Journal of Social and Environmental Issues, 1(2), 48–52.

Kim, D., & Hyun Kim, J. (2013). Understanding persuasive elements in phishing e-mails: A categorical content and semantic network analysis. Online Information Review, 37(6), 835–850.

Kim, I., & Kuljis, J. (2010). Applying content analysis to web-based data: An example from a professional development research project. The Plymouth Student Scientist, 7(1), 140–148.

Kondracki, N. L., Wellman, N. S., & Amundson, D. R. (2002). Methodological challenges in qualitative content analysis: A discussion paper. Nurse Education Today, 56, 29–34.
Korpela, K. (2015). Improving cyber security awareness and training programs with data analytics. Information Security Journal: A Global Perspective, 24(1–3), 72–77.

Krippendorff, K. (2004). Content analysis: An introduction to its methodology. SAGE.

Krombholz, K., Hobel, H., Huber, M., & Weiplt, E. (2015). Advanced social engineering attacks. Journal of Information Security and Applications, 22, 113–122.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. Cyberpsychology, Behavior, and Social Networking, 17(8), 551–555.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems, 11(7), 394–413.

Luo, X. R., Zhang, W., Burd, S., & Sezzau, A. (2013). Investigating phishing victimization with the heuristic–systematic model: A theoretical framework and an exploration. Computers & Security, 38, 28–38.

Lutsky, N. (1995). When is “obedience” obedience? Conceptual and historical commentary. Journal of Social Issues, 51(3), 55–65.

Lyons, K. (2020, April 16). Google saw more than 18 million daily malware and phishing emails related to COVID-19 last week. The Verge. https://www.theverge.com/2020/4/16/21223800/google-malware-phishing-covid-19-coronavirus-scams

Maheswaran, D., & Chaiken, S. (1991). Promoting systematic processing in low-motivation settings: Effect of incongruent information on processing and judgment. Journal of Personality and Social Psychology, 61(1), 13–25.

Mayring, P. (2015). Qualitative content analysis: Theoretical background and procedures. In A. Bikner-Ahsbahs, C. Knipping, & N. Presmeg (Eds.), Approaches to qualitative research in mathematics education (pp. 365–380). Springer.

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. Journal of Internet Commerce, 9(1), 23–41.

Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook. SAGE.

Mishra, M., Gaurav, A. J., & Jain, A. (2012). A preventive anti-phishing technique using code word. International Journal of Computer Science and Information Technologies, 3(3), 4248–4250.

Moore, T., & Clayton, R. (2012, October). Discovering phishing dropboxes using email metadata [Conference Session]. eCrime Researchers Summit (eCrime). 2012. https://www.researchgate.net/publication/261038322_Discovering_phishing_dropboxes_using_email_metadata

Moretti, F., van Vliet, L., Bensing, J., Deledda, G., Mazzi, M., Rimondini, M., Zimmermann, C., & Fletcher, I. (2011). A standardized approach to qualitative content analysis of focus group discussions from different countries. Patient Education and Counseling, 82(3), 420–428.

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. European Journal of Information Systems, 29(3), 306–321.

Newman, G. R., & Clarke, R. V. (2013). Superhighway robbery. Routledge.

Nirmal, K., Ewards, S. V., & Geetha, K. (2010, December 3–50). Maximizing online security by providing a 3 factor authentication system to counter-attack “phishing” [Conference Session]. Emerging Trends in Robotics and Communication Technologies (INTERACT), 2010 International Conference. https://ieeexplore.ieee.org/document/5706185

O’Connor, C., & Joffe, H. (2020). Intercoder reliability in qualitative research: debates and practical guidelines. International Journal of Qualitative Methods, 19. https://doi.org/10.1177/1609406919899220

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., Lin, T., & Ebner, N. (2017, May 2). Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing [Conference Session]. 2017 CHI Conference on Human Factors in Computing Systems. https://dl.acm.org/doi/10.1145/3025453.3025831

Onwuegbuzie, A. J., & Dickinson, W. B. (2008). Mixed methods analysis and information visualization: Graphical display for effective communication of research results. Qualitative Report, 13(2), 204–225.

Park, G., & Taylor, J. M. (2015). Using syntactic features for phishing detection. arXiv preprint arXiv:1506.00037. https://arxiv.org/abs/1506.00037

Patton, M. Q. (2002). Qualitative research & evaluation methods (3rd ed.). SAGE.

Peltiler, T. R. (2006). Social engineering: Concepts and solutions. Information Security Journal, 15(5), 13–21.

Rahman, M. A., Zaman, N., Asyhari, A. T., Al-Turjman, F., Bhuiyan, M. Z. A., & Zolkpili, M. (2020). Data-driven dynamic clustering framework for mitigating the adverse economic impact of Covid-19 lockdown practices. Sustainable Cities and Society, 62. https://doi.org/10.1016/j.scs.2020.102372

Review—Navigating cybersecurity during a pandemic: Latest malware and threat actors. (2020, April 22). News Lagoon. https://newsLagoon.com/en/review-navigating-cybersecurity-during-a-pandemic-latest-malware-and-threat-actors/16206

Riley, A. (2019). Agent Tesla Keylogger is now a top phishing threat. Cofense. https://cofense.com/agent-tesla-keylogger-now-top-phishing-threat/

Ruiz, D. (2020, April 2). Cybercriminals exploit coronavirus with wave of new scams. Isbuzz. https://www.informationsecuritybuzz.com/articles/cybercriminals-exploit-coronavirus-with-wave-of-new-scams/

Sandelowski, M. (1993). Theory unmasked: The uses and guises of qualitative research: debates and practical guidelines. Research in Nursing & Health, 16(3), 213–218.

Saqib, N. U., & Chan, E. Y. (2015). Time pressure reverses risk awareness and training on cyber security. Patient Education and Counseling, 98, 362–372.

Schreier, M. (2012). Qualitative content analysis in practice. SAGE.

Schuetz, S., Lowry, P. B., & Thatcher, J. (2016, August 24). Defending against spear-phishing: Motivating users through fear appeal manipulations [Conference Session]. PACIS 2016. https://aisel.aisnet.org/pacis2016/74/

Schwarz, N. (2000). Emotion, cognition, and decision making. Cognition & Emotion, 14(4), 433–440.
Sharma, K. (2010). An anatomy of phishing messages as deceiving persuasion: a categorical content and semantic network study. *EDPACS, 42*(6), 1–19.

Silic, M., & Back, A. (2016). The dark side of social networking sites: Understanding phishing risks. *Computers in Human Behavior, 60*, 35–43.

Stemler, S. (2000). An overview of content analysis. *Practical Assessment, Research, and Evaluation, 7*(1), Article 17.

Sumner, A., Hoy, C., & Ortiz-Juarez, E. (2020). *Estimates of the impact of COVID-19 on global poverty* (WIDER Working Paper Series, Working Paper No. 2020-43). World Institute for Development Economic Research (UNU-WIDER).

Thayer, A., Evans, M., McBride, A., Queen, M., & Spyridakis, J. (2007). Content analysis as a best practice in technical communication research. *Journal of Technical Writing & Communication, 37*(3), 267–279.

Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research Methodology, 8*(1), Article 45.

Tillyer, M. S., Engel, R. S., & Lovins, B. (2012). Beyond Boston: Applying theory to understand and address sustainability issues in focused deterrence initiatives for violence reduction. *Crime & Delinquency, 58*(6), 973–997.

Tillyer, M. S., & Kennedy, D. M. (2008). Locating focused deterrence approaches within a situational crime prevention framework. *Crime Prevention and Community Safety, 10*(2), 75–84.

Vahia, I. V., Blazer, D. G., Smith, G. S., Karp, J. F., Steffens, D. C., Forester, B. P., Tampi, R., Agronin, M., Jeste, D. V., & Reynolds, C. F. (2020). COVID-19, mental health and aging: A need for new knowledge to bridge science and service. *The American Journal of Geriatric Psychiatry: Official Journal of the American Association for Geriatric Psychiatry, 28*(7), 695–697. https://doi.org/10.1016/j.jagp.2020.03.007

Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences, 13*(3), 398–405.

Vance, A., Eargle, D., Ouimet, K., & Straub, D. (2013, January 7–10). Enhancing password security through interactive fear appeals: A web-based field experiment [Conference Session]. 2013 46th Hawaii International Conference on System Sciences. https://ieeexplore.ieee.org/document/6480204

Ventrella, E. (2020). Privacy in emergency circumstances: data protection and the COVID-19 pandemic. *ERA Forum, 21*, 379–393. https://doi.org/10.1007/s12027-020-00629-3

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phishing? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576–586.

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication, 55*(4), 345–362.

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior, 72*, 412–421.

Williams, K. C. (2012). Fear appeal theory. *Research in Business and Economics Journal, 3*, 63–82.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs, 59*(4), 329–349.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 662–674.

World Health Organization. (2020). *Beware of criminals pretending to be WHO*. https://www.dakotaprairiebank.com/beware-of-criminals-pretending-to-be-who/

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research Note—Influence techniques in phishing attacks: An examination of vulnerability and resistance. *Information Systems Research, 25*(2), 385–400.

Xiong, J., Lipsitz, O., Nasri, F., Lui, L. M. W., Gill, H., Phan, L., Chen-Li, D., Iacobucci, M., Ho, R., Majeed, A., & McIntyre, R. S. (2020). Impact of COVID-19 pandemic on mental health in the general population: A systematic review. *Journal of Affective Disorders, 277*, 55–64. https://doi.org/10.1016/j.jad.2020.08.001

Young, D. L., Goodie, A. S., Hall, D. B., & Wu, E. (2012). Decision making under time pressure, modeled in a prospect theory framework. *Organizational Behavior and Human Decision Processes, 118*(2), 179–188.

Zhang, W., Luo, X., Burd, S. D., & Seazzu, A. F. (2012, January 4–7). How could I fall for that? Exploring phishing victimization with the heuristic-systematic model [Conference Session]. 2012 45th Hawaii International Conference on System Sciences. https://ieeexplore.ieee.org/document/6149302

Zhang, Y., & Wildemuth, B. (2009). Qualitative analysis of content. In B. Wildemuth (Ed.), *Applications of social research methods to questions in information and library science* (pp. 308–319). Libraries Unlimited.

Zwilling, M., Klien, G., Lesjak, D., Wiechtek, L., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 1–16*. https://doi.org/10.1080/08874417.2020.1712269