A multi-level influence model of COVID-19 themed cybercrime

Rennie Naidoo

Department of Informatics, University of Pretoria, Pretoria, South Africa
rennie.naidoo@up.ac.za

ABSTRACT

The recent severity and frequency of cybercrime has been dominated by a single theme – the COVID-19 pandemic. This research develops a multi-level influence model to explore how cybercriminals are exploiting the COVID-19 pandemic by assessing situational factors, identifying victims, impersonating trusted sources, selecting attack methods, and employing social engineering techniques. The model extends upon prior work on influence techniques and emotional appeals that cybercriminals employ, by bringing into sharper focus the role of situational factors in COVID-19 related cybercrime attacks. Content and thematic analysis was conducted on 185 distinct COVID-19 cybercrime scam incident documents, including text, images, and photos, provided by a global online fraud and cybersecurity company tracking COVID-19 related cybercrime. The analysis reveals interesting patterns about the sheer breadth and diversity of COVID-19 related cybercrime and how these crimes are continually evolving in response to changing situational factors. It is hoped that these insights and recommendations for end-users and organisations can contribute to a safer digital world as we cope with many other pressing challenges during the COVID-19 pandemic.

KEYWORDS:

COVID-19, cybersecurity, cybercrime, social engineering, infodemic, pandemic

1. Introduction

An 'Unprecedented' Wave Of Coronavirus Scams Is Coming.[1]

FBI sees spike in cyber crime reports during coronavirus pandemic.[2]

COVID-19-related phishing attacks up by 667%.[3]

[Recent headlines from Online Media]

As borne out by the headlines cited above, the COVID-19 pandemic has become the dominant theme in the recent upsurge of cybercrime. The critical dependency on virtual environments by organizations and individuals during the COVID-19 pandemic is being exploited by cybercriminals. During the pandemic, computer systems and virtual environments are providing essential communication services, such as local and international news updates, telework, online education, social connectivity, and entertainment. The convergence of digital technology and computing and communication devices has radically transformed the way in which people are socialising and doing business during the pandemic. For many of those individuals practicing social and physical distancing during the lockdown period, there has been a sharp rise in the use of social technologies to maintain and develop deep emotional and social ties. Many individuals are getting their reassurances and comfort from social media, video communications and email contact. For example, research in the US shows a 17% increase in Internet use (Muncaster, 2020). The same study found that online visits to tutoring sites grew by 400% in just four weeks, while categories such as politics (320%), TV (210%) and gardening (200%) also saw sharp increases.

[1] https://www.forbes.com/sites/thomasbrewster/2020/03/18/how-americas-cyber-defenders-are-preparing-to-save-you-from-an-unprecedented-wave-of-coronavirus-scams

[2] https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic

[3] https://ciso.economictimes.indiatimes.com/news/covid-19-related-phishing-attacks-up-by-667-report/74839322

Telework software has become a vital technology for organizations to enable employees to continue to work remotely. A number of organizations had to suddenly adopt a teleworking model, thus the priority was to get users ready as expediently as possible, consequently delivering inadequate security safeguards for remote employees. Many users are now working outside the normal security protections provided by their employers' internal computer systems. For example, a number of employee home networks may contain insecure IoT devices and outdated PCs, and for many organizations, the crucial issue of educating employees about remote work safety has been lacking.

Notwithstanding the COVID-19 pandemic, cybercrime remains one of the greatest threats facing society. At the 2015 IBM Security Summit, Ginni Rometty, IBM's chairman, president and CEO, stated that cybercrime is "the greatest threat to every profession, every industry, every company in the world" (Morgan, 2017). At an annual shareholders meeting in 2017, legendary businessman Warren Buffet, described cybercrime as "the number one problem with mankind" (Morgan, 2017). While these views may sound like overstatements, it nevertheless conveys a sense of urgency that is required to improve cybersecurity across the globe. As expected, the catastrophic impact of cybercrime on society is also reflected in the hard facts. In 2019, the World Economic Forum (WEF) ranked cybercrime among the top 5 risks facing the globe (World Economic Forum, 2019). Accenture estimates the total value at risk from cybercrime globally to be around US$5.2 trillion over a five year period, from 2019 to 2023 (Accenture, 2019). A more recent study by Cybersecurity Ventures predicts that cybercrime's global cost of damages will reach $6 trillion annually by 2021(Morgan, 2019).

Despite the terrible human suffering caused by the coronavirus, cybercrimes are escalating dramatically. More alarming is the high volumes of COVID-19 themed scams that are exploiting the increasing reliance on electronic communication networks and information systems. In addition to 18 million daily malware and phishing emails related to COVID-19 in just one week in April, Google's blog reported more than 240 million COVID-related spam messages daily. Phishing and hacking attacks and threats have increased by 5 to 6 times their usual numbers in the month of March

(Kumaran & Lugani, 2020). By the end of March, more than 42,000 websites with domains containing "COVID" and "corona" had been registered – the majority of these appear to be suspicious (Kumaran & Lugani, 2020). Researchers also observed a substantial spike of 667% in COVID-19 phishing messages recently (Shi, 2020). Between March 1 and March 23, over 9000 email attacks were related to COVID-19 compared to 1,188 in February, and just 137 in January (Shi, 2020). In April, the FBI's Internet Crime Complain Center (IC3) received between 3,000 and 4,000 cybersecurity complaints daily compared to an average 1,000 daily complaints before COVID-19 (Cimpanu, 2020). Not surprisingly, Web credit card skimming increased by 26 percent in March due to the recent growth in online shopping (Segura, 2020).

The COVID-19 pandemic has exposed technological and end-user vulnerabilities that cybercriminals are seeking to exploit. Cybercriminals are exploiting telework vulnerabilities, as more employees grapple with communicating and sharing information over the Internet. Cybercriminals are also exploiting our substantial reliance on technologies for socially connecting by taking advantage of the widespread discussion of COVID-19 in emails and across the web. Cybercriminals are also preying on the emotional vulnerability of people brought about by the uncertainty and difficulties during this pandemic. It is estimated that more than 80% of exploits are successful because of social engineering techniques employed by cybercriminals (Brumfield, 2020). Experts agree that end-users remain the "weakest link" in cybersecurity. This study focuses on how cybercriminals set about targeting end-users. However, no understanding of cybercrime can be complete without a sense of the context. The pandemic provides an ideal opportunity to get a glimpse into how context can influence cybercrime.

Several IS studies have improved our understanding of cybercrime through investigating the individual characteristics of victims and the characteristics of the cybercrime (Wang *et al.*, 2009; Wright & Marett, 2010; Sheng *et al.*, 2010; Chen *et al.*, 2011; Wright *et al.*, 2014). However, a more holistic and integrated approach to cybercrime research that seeks to understand cybercrime from the cybercriminal's perspective is also required (Yar, 2005; Holt & Bossler, 2008). This study seeks to further develop this body of knowledge by developing a multi-level model of cybercrime that

simultaneously explores key situational factors, targets, attack methods, and social engineering techniques. The model can also be used by cybersecurity experts to assess the key situational factors, vulnerabilities, and attack targets that could emerge. The model also enables cybersecurity experts to identify and mitigate some of the novel cyber risks facing their organizations and pre-empt targeted attacks during COVID-19, and perhaps any other future crisis impacting business continuity.

This research relied on secondary data supplied by a reputable global online fraud and cybersecurity services company that is collecting COVID-19 themed cybercrime data from around the globe. Data was subjected to deductive and inductive coding and theme development. This was supplemented with visual thematic analysis for scam documents that contained photos and images. The results of the study demonstrate that COVID-19 cybercrimes are consistently shifting in breadth, diversity, and method of attack by aligning to situational changes during the COVID-19 pandemic. COVID-19 attacks are seeking to increase the susceptibility of end-user targets to social engineering techniques by selecting COVID-19 relevant impersonation targets and cyber technologies. The study also finds that COVID-19 cybercrimes are flexible and evolving, and tapping into a much broader range of social influence techniques and emotional appeals than those documented in previous cybercrime studies. It offers practical guidelines for improving cybersecurity during the pandemic that is perhaps also applicable in a post-pandemic future.

2. Literature review

Gordon & Ford (2006) define cybercrime as "any crime that is facilitated or committed using a computer, network, or hardware device" (p .14). Like many other definitions of cybercrime, emphasis is placed on any criminal activity targeting organizations or end-users that is conducted through the IT infrastructure via internal or external networks, or the Internet (Ciardhuáin, 2004; Wang, 2019). Cybercrime examples include but are not limited to phishing, spam, data breaches, data/information theft, identity theft, fraud, cyberstalking, cyberbullying and harassment, child predation, extortion, blackmail, stock market manipulation, espionage, attacks on critical infrastructure and information

systems, and cyberterrorism (Maimon & Louderback, 2019). Crimeware refers to software tools that are used to commit cybercrimes. These can include but are not limited trojans, viruses, bots (e.g. FriendBot), keyloggers, backdoors, e-skimming, spyware, ransomware, scareware, adware, worms, malicious code, and denial-of-service (Gordon & Ford, 2006). Crimeware excludes legitimate programs which may also be exploited by a cybercriminal (Gordon & Ford, 2006). For example, although targeted applications, such as email and Web browsers are part of the crime, they are not crimeware. Apart from using crimeware, cybercriminals also exploit news stories, hyperlinks, photos, videos, and applications. Cybercrime targets are both technological and nontechnological – exploiting vulnerabilities in end-users and IT.

While cybercrimes can lead to physical attacks, this study is concerned with cyber attacks. The literature suggests it is easier for cybercriminals to 'crack the human firewall' versus technical vulnerabilities – i.e. it is easier to exploit human vulnerabilities (Mitnick & Simon, 2003; Luo *et al.*, 2011; Pfleeger *et al.*, 2014; Algarni *et al.*, 2014; Jensen *et al.*, 2017). Furthermore, while some cybercrime is mostly technological in nature, our focus here is on cybercrime that also has a large human component (Gordon and Ford, 2006). For example, while phishing relies on e-mail technologies, websites, and crimeware to steal personal, financial or any other sensitive information, it also entails the use of social engineering techniques to trick the recipient into providing information (Mitnick & Simon, 2003; Jagatic *et al.*, 2007; Wright *et al.*, 2010).

Social engineering techniques refer to the deceptive use of social influence techniques and emotional appeals by cybercriminals to manipulate end-users into compliance so that they divulge confidential or personal information that may be used for the commission of cybercrime (Algarni *et al.*, 2014; Krombholz *et al.*, 2015). Social engineering techniques share similarities with "confidence games" (or "cons") run by con operators ("con men") who lure their victims (the "marks") into compliance by gaining their trust and disarming them (Orbach, 2018). According to Petty & Cacioppo (1986), people will either think systematically (elaborate) about an issue or take cognitive shortcuts (heuristics) to make a decision. The goal of social engineering techniques is to alter the cognitive and emotional

conditions of the victim so that instead of operating mindfully victims will tend to rely on heuristics to make a judgment (Cialdini & Goldstein, 2004; Ferreira *et al.*, 2015) . Relying on heuristics is an efficient approach to forming judgements in everyday life (Gigerenzer & Todd, 1999), but is vulnerable to the exploits of cybercriminals (Luo *et al.*, 2013). Social engineering techniques aim to arrest elaborate thought long enough to trick the victim (Mitnick & Simon, 2003; Cialdini & Goldstein, 2004; Jagatic *et al.*, 2007).

Cybercriminals assume a false identity to manipulate end-users into providing sensitive information or performing tasks (Bose & Leung, 2007; Abbasi *et al.*, 2010; Jensen *et al.*, 2017). Cybercriminals often impersonate sources that have expertise, authority, competence, and integrity to gain the trust of their victim and make them feel safe (Algarni *et al.*, 2014; Algarni *et al.*, 2017). Impersonation is a type of identity crime and identity fraud which is facilitated by the use of false identities (Clough, 2010). Since impersonation is not difficult to achieve in cyberspace, many cybercriminals exploit the ease of anonymity by targeting and mimicking credible sources. Cybercriminals can impersonate friends on social media, product brands, and technology brands (Westerman *et al.*, 2014). For example, cybercriminals committing phishing attacks mimic email messages from legitimate sources and create mock-ups of trusted websites (Abbasi *et al.*, 2010). According to source credibility theory, the end-user's perceived credibility or the believability of the person or organization being impersonated is more likely to lead to compliance (Hovland & Weiss, 1951; Bhattacherjee & Sanford, 2006; Boss *et al.*, 2015).

Apart from impersonation, there are various other influence techniques that cybercriminals can exploit to persuade a target into divulging sensitive information (Wright *et al.*, 2010). The cybersecurity literature has relied on Cialdini's six persuasion principles to analyse the techniques that cybercriminals employ in their scams (Ferreira *et al.*, 2015; Krombholz *et al.*, 2015). According to Cialdini's social influence model that is drawn from the psychology of compliance literature, these six principles include: authority, consistency, liking, scarcity, reciprocity, and social proof (Cialdini, 2001). Authority refers to the tendency in people to unthinkingly accept the statements and directions

of individuals and organizations who appear to be authorities on a subject (Milgram, 1974; Zimbardo, 2008). They apply the heuristic rule: "If an expert says so, it must be true" (Cialdini, 2001). Instead of being persuaded by the quality of an expert's arguments (Sussman & Siegal, 2003), people tend to be persuaded solely by the expert's status (Cialdini, 2001). This technique invokes the peripheral (heuristic) and not the central routes (systemic) to persuasion (Petty & Cacioppo, 1986).

Cybercriminals also take advantage of people's tendency to perform automatically in line with their commitments. The victim's strong need to be consistent with their commitment can be exploited for the cybercriminal's benefit (Akbar, 2014; Ferreira *et al.*, 2015). According to the scarcity principle, something can appear more valuable when there is limited availability. Cybercriminals take advantage of this principle by claiming on their website that a fake product is in short supply or is quickly running out. Reciprocation is another technique that cybercriminals employ in their scams for gaining the end-user's compliance (Stajano & Wilson, 2011; Ferreira *et al.*, 2015). For example, cybercriminals take advantage of people's generosity or strong sense of obligation to return a favor in online donation scams. Liking and friendship pressures are also employed by cybercriminals to get their victims to comply (Ferreira *et al.*, 2015). For example, cybercriminals exploit the tendency that people are more willing to perform favors for their friends on social networking sites (SNSs). Social proof refers to people's tendency to view a particular behavior as being correct if people similar to them are performing the same behavior (Stajano & Wilson, 2011). Cybercriminals can induce the similarity principle by providing false evidence of broad support.

The role of emotional factors has been downplayed in understanding cybercrime victimization. Emotions generally play an important role in compliance behavior (Richins, 1997; Boss *et al.*, 2015). Cybercriminals who are able to manipulate the emotional state of their victims have a better chance of manipulating end-users into compliance (Mitnick & Simon, 2003). In invoking the scarcity principle mentioned above, the cybercriminal often resorts to emotional appeals by appearing to reward the end-user for prompt action or penalise them for delayed action. For example, the cybercriminal impersonating a bank may use penalties as a scare tactic. This is likely to lead to an intense feeling

and therefore induce users to react quickly out of fear, to avoid a bad credit record or the inconvenience of having their account placed on hold. Emotional appeals are not limited to negative affective states such as anger, fear or threat (Boss *et al.*, 2015), cybercriminals can also exploit positive affective states, such as pride, relief and enjoyment (Richins, 1997; Agarwal & Karahanna, 2000). The role of emotional appeals is to distract the victim thus preventing them from analyzing the content of the message carefully (Workman, 2008). The Dual-Systems Model of Affect can account for both positive and negative affective states (Dillard & Peck, 2006), while the Extended Parallel Process Model is used in cybercrime research to account for fear/threat appeals (Witte, 1992; Boss *et al.*, 2015).

The role of situational factors has also been downplayed in understanding cybercrime victimization (Cohen & Felson, 1979; Miethe *et al.*, 1990; Yar, 2005; Jagatic *et al.*, 2007). The dominant approach in the literature is to provide individual dispositional explanations of cybercrime victimization (Wright & Marett, 2010; Luo *et al.*, 2011). However, these individualistic explanations of cybercrime fail to account for the role of situational trends and patterns (Ngwenyama & Lee, 1997; Ngo, 2011). Some researchers predict that cybercriminals will incorporate greater elements of context into their scam designs (Jagatic *et al.*, 2007). The Routine Activity Theory (RAT) postulates that high trends in cybercrime rates are related to the changes in the "routine activities" of everyday life (Cohen & Felson, 1979). Three theoretical constructs from routine activities theory include (1) exposure to motivated criminals, (2) target suitability, and (3) capable guardianship (Holt & Bossler, 2008; Moneva *et al.*, 2020) . For example, during COVID-19, the theory predicts that cybercriminals will be motivated by the recent, abrupt changes to remote work and reliance on online tools (exposure) as remote workers (target suitability) are no longer operating under the same strict security provided in the workplace (capable guardianship) (Yar, 2005). Some studies on crime in general show that situational factors lead people to lower their guard and make themselves significantly more vulnerable and suitable targets for victimization (Moneva *et al.*, 2020; Holt *et al.*, 2020). Table 1 summarises the interdisciplinary approach pursued in this study.

Table 1 Theories and key sensitising concepts

Theory	*Area*	*Sensitizing Concepts*
Routine Activity Theory (RAT) (Cohen & Felson, 1979; Holt & Bossler, 2008)	Situational Factors	Online behaviors Suitable targets for impersonation and victimization People and technology vulnerabilities
Source Credibility Theory (Hovland & Weiss, 1951; Sussman & Siegal, 2003)	Source Credibility	Impersonation
Social Influence Model (Cialdini, 2001; Cialdini & Goldstein, 2004)	Social Engineering	Social influence principles
Dual-Systems Model of Affect (Dillard & Peck, 2006)	Social Engineering	Positive and negative emotions

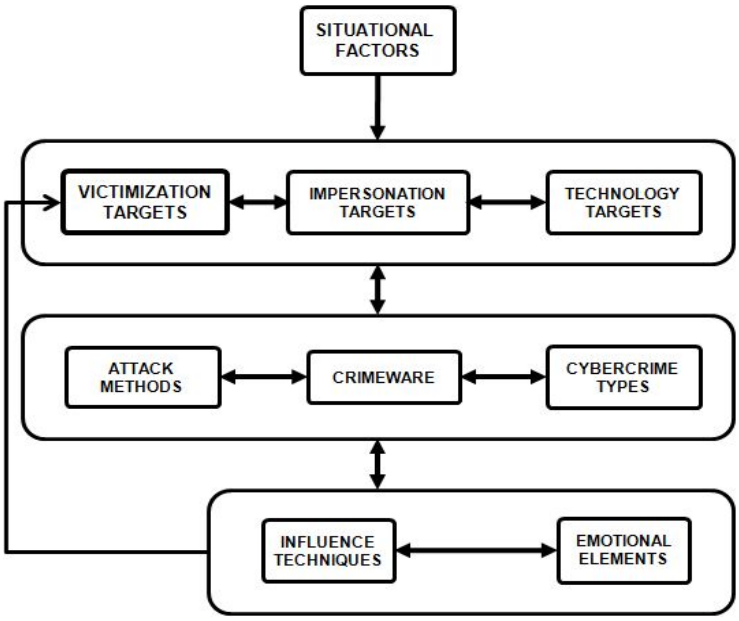


Figure 1. Exploratory sensitising model for cybercrimes

3. Research Methodology

The study of situational factors, targets of cybercrime, attack methods, influence techniques and emotional appeals employed in cybercrime during a pandemic is not easily examinable using

conventional research approaches. Even under normal conditions, researchers have to rely on secondary data to get a momentary peek into the cloaked world of cybercriminals and their criminal activities. Consequently, published secondary sources become a pivotal source of data for the researcher (Sørensen *et al.*, 1996; Myers, 2009). Secondary documents and records specific to COVID-19 related cybercrime were supplied by FraudWatch International. FraudWatch International is a global online fraud and cybersecurity services company that collects cybercrime data from around the globe. The author receives daily updates of FraudWatch International's "COVID-19 Cyber Intelligence Datafeed".

The archived documents and records of COVID-19 related cybercrime between mid-March and mid-April 2020 were coded for situational factors, targets of cybercrime, attack methods, influence techniques and emotional appeals using content and thematic analysis. The use of the multi-level influence framework allowed the researcher to make an informed analysis of the data. The intention here was not to generalise the findings to a wide range of cybercrime scam designs (Lee & Baskerville, 2003; Ruddin, 2006). Instead the goal was to perform an analytical generalisation – that is, to generalise a particular set of results to the study's theoretical propositions about cybercriminals and cybercrime scam designs. The completeness of the dataset is recognized as a limitation of this study. Each record contains the type of scam (phishing or social network sites) and a brief description. In some cases, only phishing website information was provided and not the accompanying phishing email. The phishing email data would have been more explicit about the emotional appeals used. Furthermore, it was difficult to assess to what extent the phishing email and phishing website were using the consistency principle. Moreover, the archive documents were limited to active scams.

Table 2 Summary of secondary sources

No	*Data Source*	*Period*	*Description*
1	COVID-19 Cyber Intelligence Datafeed Reports on the daily number of incidents, open or closed status, and types of open incidents	17/03/2020 - 17/04/2020	Type: Email data feed Format: Text only Total number of incidents: 43131
2	COVID19 Active Scam/Incidents Documents providing details about active incidents	26/03/2020 - 17/04/2020	Type: Online archive Format: Text and Images Total number of distinct archived incidents: 185

Source: FraudWatch International

The data were analysed using Fereday & Muir-Cochrane's (2006) guidelines for conducting a hybrid approach to deductive and inductive coding and theme development. The deductive analysis began with the development of a coding template (Crabtree & Miller, 1992). The coding template contained codes informed by the literature study (See Table 1). Major sensitizing coding categories were identified. For social engineering, these included: influence techniques and emotional appeals. A number of lower-level operational codes were also identified. For example, 'influence techniques' was broken down into six possible categories 'authority', 'consistency', 'liking', 'scarcity', 'reciprocity', and 'social proof'). These tables also provide formal definitions of each of the techniques.

The next step in the analysis involved testing the applicability of these codes. This was done by coding the documents and assigning the predetermined codes from the coding template. As the researcher worked through the scam texts line by line to assign the predetermined codes, inductive codes were assigned to segment data where the units of meaning could not be appropriately captured by the predetermined codes. This allowed for new insights to emerge as these codes either constituted something new, refined or extended the existing codes. Gleeson's (2011) guidelines for visual

thematic analysis were adopted to analyse the scam documents that contained photos (examples: health workers, patients) and images (examples: virus) (See Figure A.2). The researcher analysed the photos and images iteratively. To avoid restricting interpretations in the initial stages, the visual data were analysed independently of the coding template and textual data contained in the scams. Initially, a tentative set of visual themes that seemed to be portrayed by the images was recorded. A short descriptive note was also written for each theme that emerged. Only then were the coding template and textual data revisited to help refine the initial analysis.

185 unique documents were analysed. Examples representing the different ways in which these influence techniques and emotional techniques were employed are also provided. Furthermore, a quantitative content analysis was performed to establish the prevalence and robustness of the study's main themes from these documents (Table 2). Version 6.2 of ATLAS.ti – a qualitative research software tool – was used to store and analyse all the documents. The author independently coded the content and achieved consensus with an assistant researcher in case of any discrepancies. An independent judge, not familiar with project, acted as an auditor and reviewed the key categories and operational definitions, and provided reasonable verification of the accuracy of the coding procedure. The judge was provided with 20 randomly chosen documents, assigning 75 out of 100 of the same categories as the author, yielding a 75% level of agreement. Triangulation was assured by comparing archived documents and records from different sources to provide further confirmation of the themes found, and to throw more light on the contextual detail of the competing discourses (McKenna *et al.*, 2017). The types of cybercrime identified in our FraudWatch International dataset are not unique and the findings are generally applicable to many other monitoring services across the globe. Similar scam incidents can be found in the FBI and Google's datasets.

Several categories were observed in the documents and entered into a database. For example, influence techniques and emotional appeals reported in the tables were selected on the following basis: (1) the example is unambiguous as an indicator of the category; (2) it is representative of a number of statements in the dataset; (3) it reflects important cybercriminal activities related to the

pandemic. The most illustrative of these were included in this article. The documents and records were also categorized by key situational factors (examples: remote work, social connectivity via SNS, unemployment), by key victimisation targets (example: SNS users, remote workers), the type of cybercrimes (examples: phishing, fake products, fake social media profiles), the type of crimeware (examples: FriendBot, keyloggers), the online technologies targeted (examples: email, social media technologies, video telephony and online chat services, cloud file hosting services, and streaming media services) and the types of organizations that were the targets of impersonation (examples: banks, technology brands, product brands, and government agencies). Secondary themes were derived from primary themes. For example, the ` social network site users ' were inferred from the fact that major social media organizations were being targeted. Version 6.2 of ATLAS.ti and Excel was used to code and store the categories and themes. Content analysis was performed using frequency analysis to establish the prevalence and robustness of the study's themes from the records and documents.

4. Analysis and results

Figure 2 shows the number of new domains that are being registered to take advantage of both the online and offline media attention given to COVID-19. Registrations of COVID-19 related sites, from March 28 to April 20, averaged approximately 1900 per day. During this same period, over 43000 new domains were registered. While many of these sites may be legitimate, an equally high number may be fraudulent. Some suspiciously named domains include: *whatkillscovid-19.com; usacaresfundcovid-19.com; windowcleaningcovid19.com; worldaftercovid19.in.*

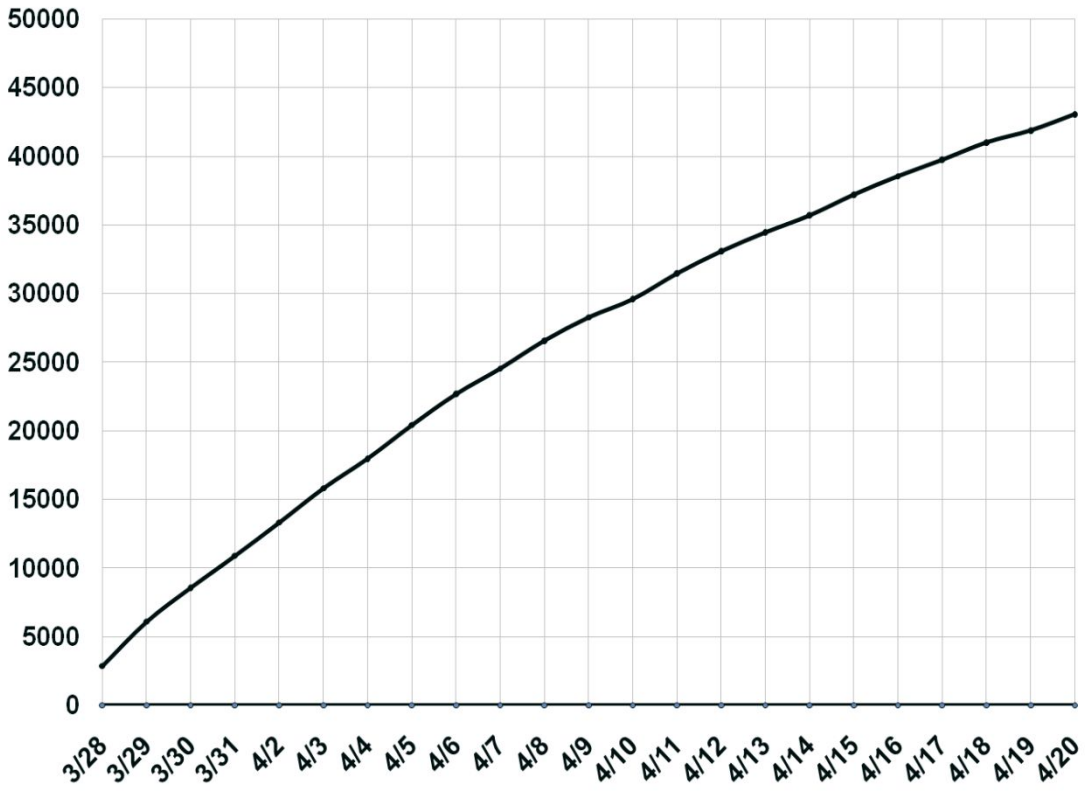


Figure 2 Cumulative number of new COVID-related domains registered

The domain name "*worldaftercovid19.in.*" mentioned above captures the suspected cybercriminal's preparedness for the changing situational context of the COVID-19 pandemic. Overall, cybercriminals are currently exploiting the following key situational factors brought about by the COVID-19 pandemic: the need for social connectivity, the change to remote work, rising unemployment and the availability of relief funds, the need for entertainment/leisure as a result of the lockdown and stay-at-home orders, and the growing support of charities (See Table 4 and Table 5).

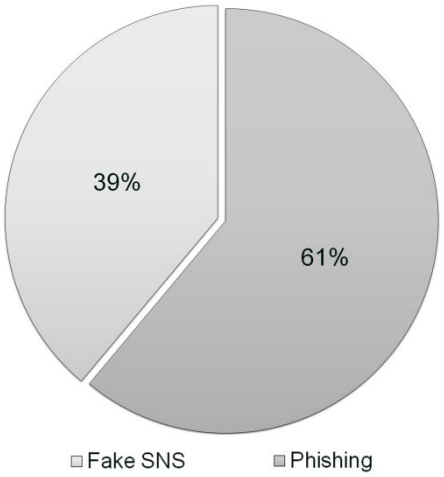


Figure 3 Share of active cybercrime incidents

Figure 3 shows that phishing contributes to more than half (61%) of cybercrime incidents, thus remaining the dominant choice of attack. However COVID-19 cybercriminals have also been targeting the vulnerabilities of people using SNSs (39%) to socially connect. A wide array of COVID-19 linked situational factors are influencing the process of target-selection.

Table 3 Types of organizations targeted for impersonation

Type of Organization	*Freq*	*%*
Social Networking Sites (SNS)	72	39%
Financial Services Organizations	45	24%
Technology Firms	39	21%
Government agencies	16	9%
Intergovernmental Organization	3	2%
Other	10	5%
Grand Total	185	100%

The top types of organizations that are targets for impersonation are, currently, Social Networking Sites (39%), Banks (24%), Technology Firms (21%), Government Agencies (9%), Intergovernmental Agencies (2%) and other (5%) (Table 3). The majority of SNS scams targeted Facebook (82%). The detailed information of technology organizations and other key organizations impersonated is also listed in Table 4 and Table 5. The key user categories being victimised includes: online banking consumers, social network site users, remote workers, online shopping users, unemployed, donors,

and airline customers. Table 4 and Table 5 shows that the following situation factors, such as Stay-at-home orders, Remote work, Rising unemployment, Online shopping, Social connectivity, Entertainment/Leisure, Charities, Donations, Treatments, Infections, Illness, Death, Safety measures, Loans/Financial Relief, and Airline booking refunds, were facilitating the commission of cybercrimes.

Table 4 Technologies and Technology Brands Targeted

Technology Type	*Technology Brands Targeted/Impersonated*	*Situational factors*	*Cybercrime*
Email	Gmail	Donations Charities	Fake emails (Phishing) Malware Malicious Websites
Social Media Technologies	Facebook Instagram	Social distancing Social connectivity Donations Charities	Fake Social Media Profiles Misinformation Fake Charities
Videotelephony and online chat services	Zoom Microsoft Teams Whatsapp Apple	Remote work Virtual Meetings	Fake Products
Cloud File Hosting Services	One Drive DropBox	Remote work Virtual Meetings	Fake Products
Streaming media service of television and movies	Netflix	Entertainment/Leisure	Fake Products
Video sharing website	YouTube	Entertainment/Leisure	Fake Products
Broadband and Telecoms Companies	4G (Fake company)	Free Data/Internet	Fake Products
Online payments system	Paypal	Small business loans	Fake Website domain

Table 5 Impersonations of Organizations

Types of Organizations/Brands Impersonated	*Organizational Brands Targeted/Impersonated*	*Situational factors*	*Cybercrime*
Banks and Investment Companies	Banco do Brasil HSBC RBC Royal Bank Bank Of Montreal ING	Relief Programs Donations Charities High growth stocks for drug treatments and cure	Fake Charities Fake Trading Scam
Government Agencies	Federal government of the United States Canada Revenue Agency Government of Canada Internal Revenue Service (IRS)	Relief Programs	Fake Relief Programs
Intergovernmental Agencies/	World Health Organization	Pandemic Information Safety Measures Relief Programs	Disinformation Fake Relief Programs
Humanitarian Organizations	Red Cross	Charities	Fake Charities
Other Brands	Cathay Pacific Woolworths Nike	Refunds Food Protective Clothing	Fake Refunds Fake Products

Table 6 Social influence principle occurrences

Principle	*Phishing*		*Fake SNS*		*Overall Freq*	
	(Freq)	*%*	*(Freq)*	*%*	*%*	*%*
Liking	102	37%	72	50%	174	42%
Social Proof	3	1%	72	50%	75	18%
Scarcity	73	27%	0	0%	73	17%
Authority	68	25%	0	0%	68	16%
Reciprocity	19	7%	0	0%	19	5%
Consistency	10	4%	0	0%	10	2%
	275	100%	144	100%	317	100%

While the analysis suggests that all 6 influence principles are relevant, the top three influence principles are currently, Liking (42%), Social Proof (18%), and Scarcity (17%). Only Liking (50%)

and Social Proof (50%) were adopted by Fake SNS. Some examples of these influences can be found in Table 8.

Table 7 Emotional appeal occurrences

Emotional Appeal	*Phishing*		*Fake SNS*		*Overall Freq*	
	(Freq)	*%*	*(Freq)*	*%*	*%*	*%*
Relief	30	33%	0	0%	30	30%
Fear	16	18%	6	60%	22	22%
Hope	21	23%	1	10%	22	22%
Enjoyment	15	17%	0	0%	15	15%
Threat	3	3%	3	30%	6	6%
Compassion	5	6%	0	0%	5	5%
	90	100%	10	100%	100	100%

Despite the seriousness of the COVID-19 threat, both positive and negative emotional appeals are being used in scams. The top three emotional principles are currently, Relief (30%), Fear (22%), and Hope (22%). The results suggest that cybercriminals are relying more on positive emotional appeals as opposed to negative emotional appeals to manipulate their targeted victims. Some examples of these emotional influences can be found in Table 9. Ironically, the coronavirus image, which under normal circumstances may be categorized as a threat or disgust, is now being used as a familiarity device by cybercriminals to develop trust. Meanwhile, some of the disinformation crimes were attempting to stir panic among end-users.

Table 8 Evidence of influence techniques applied to COVID-19 crime

Principle	*Propositions*	*Example*	*Theme*	*Sample text*[4]
Authority	People tend to comply with a request that comes from an authority figure.	The WHO serves as a respected authority on the pandemic for society.	Safety measures	"Distributed via the CDC Health Network"
Consistency	People, who make a commitment, tend to feel compelled to perform consistently in line with that commitment.	Completing short and easy survey commits one to disclose personal details.	Free Entertainment	"Answer 3 simple questions"
Liking	People's tendency for liking another person or product affects their tendency to comply with that person's request.	Familiarity of popular banking brands. Front line healthcare worker.	Donation Donation	" Select your Financial Institution" See Figure A.2 Photo: Photograph of a front line healthcare worker feeding an intubated Corona virus patient
Scarcity	People tend to value those opportunities that have limited availability (Cialdini 2009, p. 179).	Free groceries. COVID-19 relief funds by government agency. Credit relief by banks. Impersonating Investment company.	Food vouchers Relief Funds Payment Holiday Overdraft support Interest reduction Invest in 'hot' new stocks related to curing the disease Using AI to maximise returns from stock market Drug scarcity	"Hurry up! Collect your free voucher here" "Opps, You are not qualified" "Find out instantly if you are eligible to obtain urgent aid" "Corona Millionaire" (context) "The drug will be shortages fast"

[4] Text quoted verbatim. Spelling errors are from the source.

Principle	*Propositions*	*Example*	*Theme*	*Sample text*[4]
Reciprocity	People tend to comply to a requester who presents them with an initial favor or initial concession (Cialdini 2009, p. 38).	Fake Technology brand offers reward for completing COVID-19 survey.	Free Internet Access and Data	"500 GB of 4G + Internet for free and for everyone!"
Social Proof	People tend to view a particular behavior as being more correct to the degree with which they see others in a similar situation performing the same behavior (Cialdini 2009, p. 88).	Fake Social Media Profiles.	Make new friends Charity	"Increasing Corona virus fundraising statistics"

Examples drawn from www.fraudwatchinternational.com/phishing/

Table 9 Evidence of emotional elements employed in COVID-19 cybercrime messages

Element	*Propositions*	*Example*	*Theme*	*Sample text*[5]
Fear/ Panic	People will tend to be persuaded by fear appeals when they feel vulnerable to an environmental threat.	Keeping informed about the local spread of the virus.	Pandemic Information	"coronavirus update disease (COVID-19) your neighbours tested positive"
Threat/ Panic	People will tend to be persuaded by threat appeals when they feel vulnerable to an environmental threat.	Corona virus taking over the world.	Pandemic Information	Use of the virus images "Youre next"
Enjoyment	People will tend to be persuaded by positive appeals such as enjoyment.	Coping with lockdown and social distancing.	Entertainment	"Staying safe and enjoying the Internet at home" Images of movie covers
Relief	People will tend to be persuaded by positive appeals such as relief, when they feel they will gain a positive outcome such as gaining control over their lives.	Keeping informed about possible cure/treatment.	Treatment information	"Breaking!!! COVID-19 solution announced by WHO At Last.." See Figure A.1
Hope	People will tend to be persuaded by positive appeals such as hope.	Global relief funds. National Relief Funds.	Relief funds	Photo: Joining hands Image: Flags of nations/individual nation
Compassion	People will tend to show compassion for others similar to them.	Empathic concern for patient.	Widespread suffering Donation	Photo: See A2

Examples drawn from www.fraudwatchinternational.com/phishing/

[5] Text quoted verbatim. Spelling and grammatical errors are from the source.

Table 9 provides more details about the nature of the emotional appeals that are being used in COVID-19 cybercrimes.

5. Discussion

Understanding cybercrime during the same period as a social crisis such as the COVID-19 pandemic is crucial, given the catastrophic consequences of the resulting emotional costs, financial losses, and reputational damage. Analysis of the COVID-19 cybercrime attacks shows that cybercriminals tend to follow a dynamic process that comprises four broad levels: gather information about situational factors; identify targets, select attack methods, and employ social engineering techniques. Based on the analysis, this study develops a multi-level influence model of cybercrime (see Figure 4).

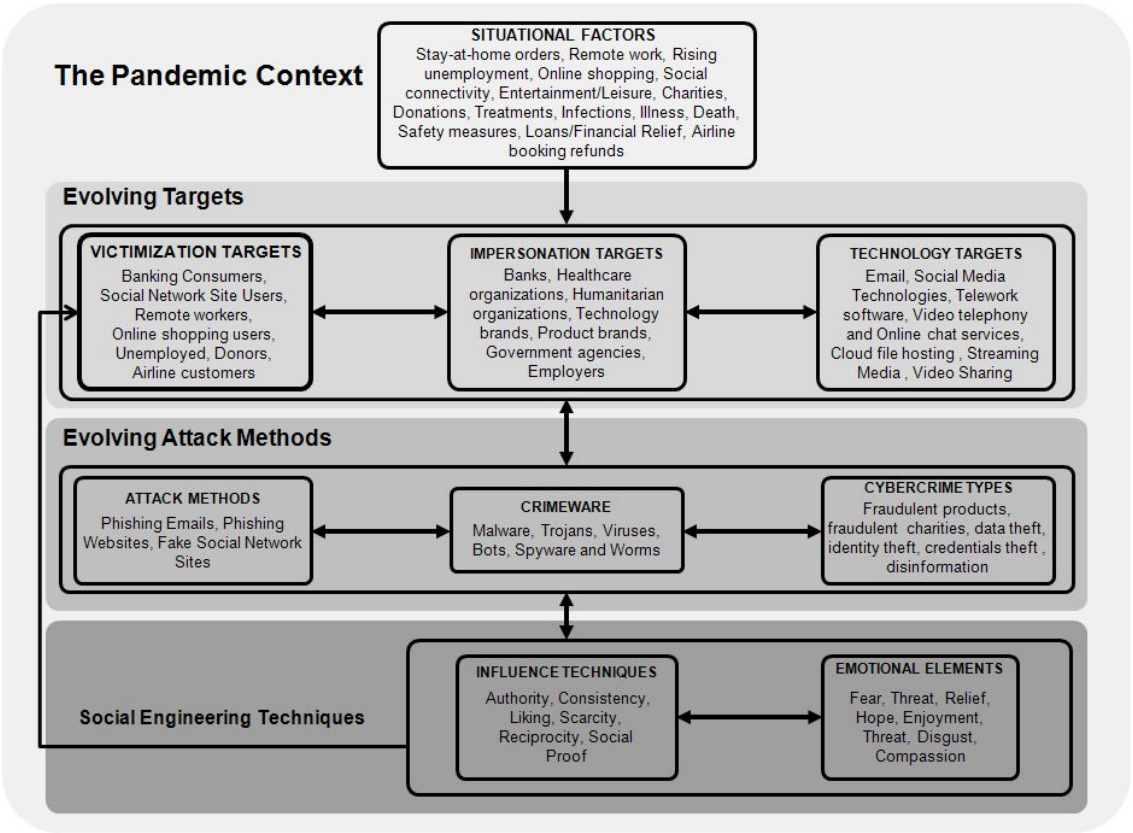


Figure 4. A multi-level influence model of cybercrime

While prior studies on cybercrime in IS have commented on the importance of context (Jagatic *et al.*, 2007; Abbasi *et al.*, 2010), this study is among the first in IS to adopt an approach to cybercrime that recognizes the importance of the facilitating context, such as a global pandemic. This study finds that cybercriminals are resorting to increasingly more devious compliance techniques by integrating greater elements of situational factors into their scam designs. IS scholars seem to have paid little attention to employing criminological theories to account for these situational factors. Routine Activity Theory (RAT) appears to be a promising approach to understand the ecosystem of cyber-crimes (Holt & Bossler, 2008; Holt *et al.*, 2020). The results show how cybercrimes work in concert with publicly available information about COVID-19. For example, the social credibility of the WHO has made them a perfect target for impersonation (Algarni *et al.*, 2017). The study also confirms that cybercriminals are taking advantage of both technical and social vulnerabilities (Mitnick & Simon, 2003). For example, criminals are targeting remote workers by mimicking technology firms that offer videotelephony, online chat services and cloud file hosting services. This study found that a large percentage of cybercrimes targeted SNSs like FaceBook, confirming findings from previous research that SNSs are turning into a major technology target (Algarni *et al.*, 2017). The study also confirms prior findings that influence principles and emotional features are important factors that are exploited by cybercriminals. Furthermore, it also finds that liking, authority and scarcity principles are the most popular principles employed in phishing scams (Wright *et al.*, 2014), while liking and social proof are popular principles employed in SNS scams (Algarni *et al.*, 2017). Cybercriminals are also exploiting multiple social influence principles in a single scam. For example, they often use a combination of liking (I am familiar with the Red Cross and trust this humanitarian organization), and social proof (other people similar to me are donating to this Red Cross COVID-19 charity, therefore I should too). Conventional wisdom suggests that cybercriminals aim to capitalize on the fear and uncertainty of their intended victims (Boss *et al.*, 2015). Despite the seriousness of the COVID-19 threat, both positive and negative emotional appeals are being exploited (Richins, 1997). The pandemic represents both a period of human uncertainty and solidarity so cybercriminals are preying on both the hopes and fears of people (Workman, 2008). Although mainly empirically supporting prior studies mentioned above, by focusing on the pandemic this study's major contribution is in explicating the facilitating

role of the cybercrime context (Yar, 2005; Holt *et al.*, 2020). Furthermore, the results confirm the integrated and process nature of cybercrime that includes gathering information about situational factors; identifying targets, selecting attack methods, and employing social engineering techniques, which represents an important finding.

Implications for theory

Theory building efforts in prior cybercrime studies has generally been framed at a single-level of analysis or on selected aspects, focusing on either the characteristics of victims and the characteristics of the cybercrimes (Wang *et al.*, 2009; Wright & Marett, 2010; Sheng *et al.*, 2010; Chen *et al.*, 2011; Wright *et al.*, 2014). The multi-level influence model of cybercrime offers a way for researchers to move beyond an individual level of analysis to assess cybercrime in a more holistic and integrated way. More importantly, the model underscores the important facilitating role of situational factors in developing a more comprehensive understanding of cybercrime (Cohen & Felson, 1979; Miethe *et al.*, 1990; Yar, 2005; Holt & Bossler, 2008). Furthermore, the model is not only pertinent to the development of a theoretical framework on cybercrime victimization but also has the potential to advance scholarship in areas such as social engineering, fake news, and the dark side of IT (D'Arcy *et al.*, 2014). Moreover, this model expands the concept of social engineering by combining influence principles and emotional appeals that goes beyond the use of fear appeals (Boss *et al.*, 2015). The role of situational factors in influencing perceived source credibility (impersonating someone with credibility) can be valuable in future research on disinformation campaigns and cyberpropaganda (D'Arcy *et al.*, 2014).

This study also makes a theoretical contribution to COVID-19 and pandemic research in general. Apart from the cybersecurity field, the conceptualisation of cybercrime offered in this study has implications for the fields of consumer health informatics and public health informatics (Eysenbach, 2011). These fields have long observed the major information challenge that outbreaks or pandemics present to society (Eysenbach, 2002). In particular, information epidemiology or 'infodemiology'

studies have analysed the spread of health information of varying quality and misinformation during outbreaks and pandemics (Eysenbach, 2011). The term 'infodemic' has been popularised recently to characterise the sheer abundance of COVID-19 misinformation and disinformation (Zarocostas, 2020). Infodemiology researchers tend to attribute the information challenge posed during a pandemic to rumours and questionable information spread by social media users, errors or lack of accuracy in traditional mass media reporting, and health experts or authority figures lacking scientific rigor and evidence-based knowledge (Eysenbach, 2011; Zarocostas, 2020). However, this study has shown that the co-existence of pandemics with infodemics also provides a fertile information ecosystem for cybercriminals to exploit. Therefore, there is an urgent need to broaden the conception of infodemiology, to include the role of cybercriminals and to examine the determinants of cybercrime during outbreaks or pandemics, to better inform public health and public policy. The integrated, multi-level, process approach proposed here could also have greater practical utility compared to cybercrime models that only assess the vulnerabilities of cybercrime victims.

Implications for practice

This multi-level conceptualisation of cybercrime raises a number of practical implications for cybersecurity during times of catastrophic change to society. The proposed model can be used as a systematic framework in threat modelling processes. Many threat response models used by cybersecurity experts rely on techniques such as brainstorming to identify potential cybersecurity threats and vulnerabilities (Myagmar *et al.*, 2005). One of the limitations of brainstorming is that it is likely to omit significant threats and vulnerabilities. By understanding cybercrime from the offender's perspective, security experts can provide a more comprehensive perspective about potential threats and vulnerabilities, thus placing them in a more proactive position to prevent targeted attacks. For example, COVID-19 cybercrimes are taking advantage of the situation that many companies are shifting to remote work during the pandemic as they attempt to keep employees as safe and as productive as possible. The remote work environment is major change for many employees and consequently presents more security vulnerabilities. For a start, cybersecurity or IT departments

should make users aware of the scams targeting remote workers (Hart, 2009; Anderson & Agarwal, 2010). While users working remotely can ensure that their home computer and other devices are protected by installing the latest anti-spam, anti-spyware and anti-virus software and by keeping their operating system up to date, cybersecurity or IT departments can assist by installing anti-malware and anti-phishing solutions to the home devices of remote workers to prevent many of these malicious emails and payloads from reaching them. Furthermore, IT departments should monitor and filter email phishing scams with headers, such as "Coronavirus Sensitive Matter" or "COVID-19 update". Additionally, phishing emails that mimic credible institutions, such as the World Health Organization (WHO) should be filtered. For example, WHO's email address does not end as follows: '@who.com' ,'@who.org' or '@who-safety.org'.

In the past, disaster recovery and business continuity plans focused on natural disasters, however, the current health and cybersecurity crisis suggests that these plans need a major review. These plans need to consider risks, such as future pandemics and even the possibility of a cyberwar. Parts of the multi-level model can be used to re-assess disaster recovery and business continuity plans, especially with regards to technological vulnerabilities that can hamper the organization's response and recovery. The model can also be used to help improve the effectiveness of training by informing simulation exercises during a crisis (Jalali *et al.*, 2019). Situational factors can play an important role in providing information about specific security threats that may arise. As society moves from the lockdown phase of the pandemic to the re-entry phase, the model predicts that cybercrime that will evolve with these trends. For example, employment-related cybercrime scams targeting the unemployed will increase significantly given the burgeoning rate of unemployment expected. Proactive technology-based countermeasures and user education can help to combat the next wave of COVID-19 cybercrime. An increase in collaboration within the broader cybersecurity community will also be required to fight this great threat facing society.

6. Conclusion

This study analysed and interpreted COVID-19 related cybercrime data from across the globe. The sheer scale of COVID-19 cybercrimes observed is alarming. The study finds that these cybercrimes are consistently shifting in breadth, diversity and method of attack by adapting to situational changes during the COVID-19 pandemic. A relatively comprehensive multi-level influence model of cybercrime is proposed that integrates prior IS research with an existing criminological framework – the lifestyle-routine activities theory. Due to methodological limitations, this study could not investigate individual vulnerability differences to cybercrimes. Although key social influence mechanisms and emotional appeals were identified, the extent to which individual differences contribute to cybercrime victimization as opposed to situational factors remains to be seen. For example, it is possible that despite the situational factors, individuals with a high degree of self-control may not fall prey to cybercrime victimization. Despite these limitations, it was important to explore how cybercriminals are attempting to exploit situational factors to deceive end-users in the context of a pandemic. Future studies could use experimental research designs to predict the relative vulnerability of end-users in a simulated social crisis. Hopefully more cybercrime research is done and more effective countermeasures are put in place to ensure a safer digital world while the world continues to be plagued by COVID-19. A safer digital world can help us to cope better with many of the other pressing challenges during the pandemic and new challenges that can be expected in the post-pandemic future.

Appendix

Figure A.1 Phishing Email

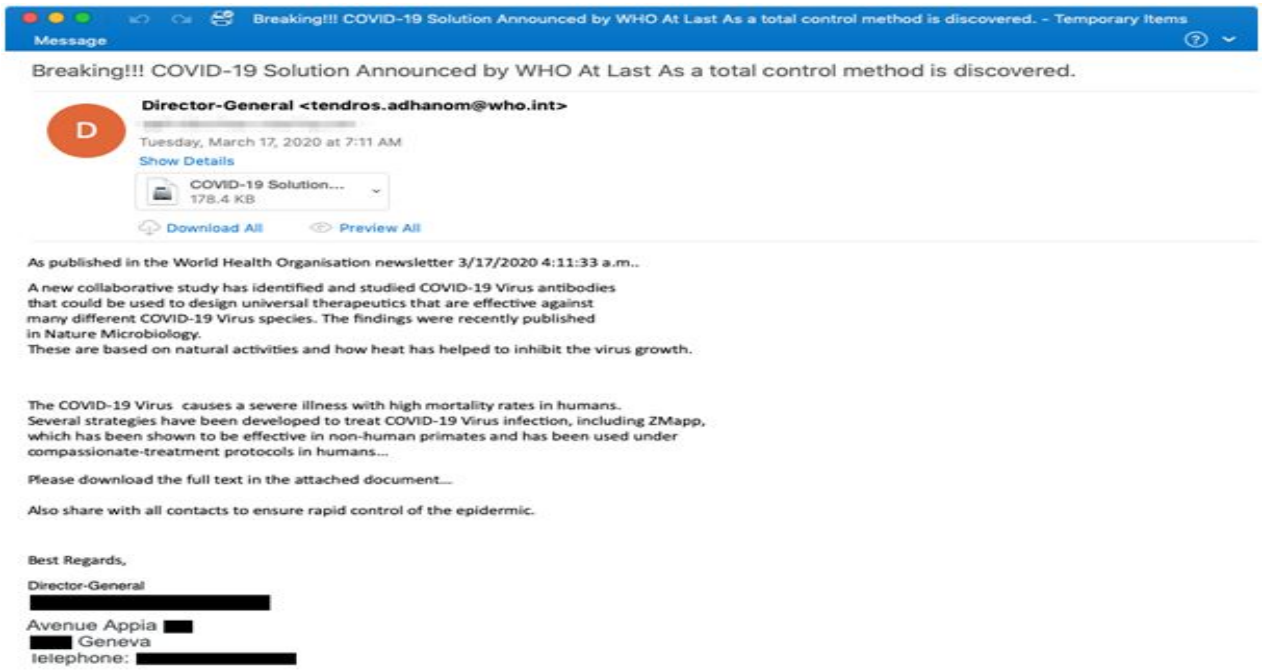
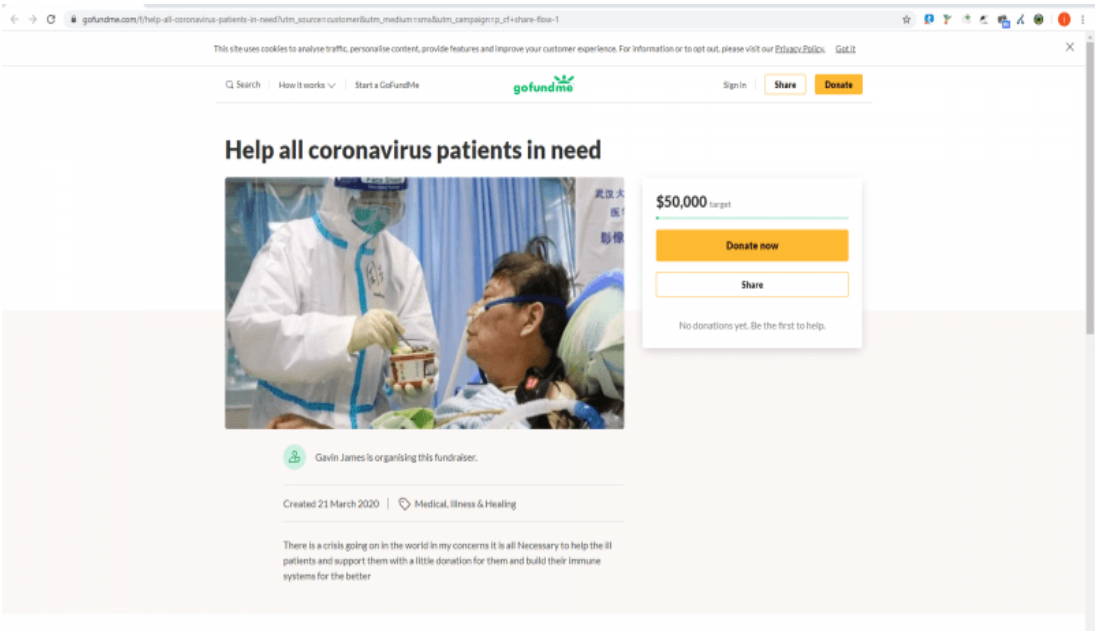


Figure A.2 Fake Web Site



References

ABBASI A, ZHANG Z, ZIMBRA D and CHEN H (2010) Detecting Fake Websites: The Contribution of Statistical Learning Theory. *MIS Quarterly* **34(3)**, 435–461.

ACCENTURE (2019) *The Cost of Cybercrime*. USA. Available at: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study (accessed 25/04/20).

AGARWAL R and KARAHANNA E (2000) Time Flies When You're Having Fun: Cognitive Absorption and Beliefs about Information Technology Usage. *MIS Quarterly* **24(4)**, 665–694.

AKBAR N (2014) *Analysing Persuasion Principles in Phishing Emails*. Masters Thesis. University of Twente.

ALGARNI A, XU Y and CHAN T (2014) Social Engineering in Social Networking Sites: The Art of Impersonation. In *2014 IEEE International Conference on Services Computing* pp 797–804, IEEE, Anchorage, AK, USA.

ALGARNI A, XU Y and CHAN T (2017) An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. *European Journal of Information Systems* **26(6)**, 661–687.

ANDERSON CL and AGARWAL R (2010) Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly* **34(3)**, 613–643.

BHATTACHERJEE A and SANFORD C (2006) Influence Processes for Information Technology Acceptance: An Elaboration Likelihood Model. *MIS Quarterly* **30(4)**, 805–825.

BOSE I and LEUNG ACM (2007) Unveiling the Mask of Phishing: Threats, Preventive Measures, and Responsibilities. *Communications of the Association for Information Systems* **19(24)**. 544-566.

BOSS SR, GALLETTA DF, LOWRY PB, MOODY GD and POLAK P (2015) What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly* **39(4)**, 837–864.

BRUMFIELD C (2020) Beware malware-laden emails offering COVID-19 information, US Secret Service warns. *CSO*. Available at: https://www.csoonline.com/article/3536696/us-secret-service-warns-of-malicious-emails-offering-covid-19-information.html (accessed 24/04/20).

CHEN R, WANG J, HERATH T and RAO HR (2011) An investigation of email processing from a risky decision making perspective. *Decision Support Systems* **52(1)**, 73–81.

CIALDINI RB (2001) *Influence: Science and Practice* Fourth Edition. Allyn and Bacon, Boston.

CIALDINI RB and GOLDSTEIN NJ (2004) Social Influence: Compliance and Conformity. *Annual Review of Psychology* **55(1)**, 591–621.

CIARDHUÁIN SÓ (2004) An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence* **3(1)**, 1–22.

CIMPANU C (2020) FBI says cybercrime reports quadrupled during COVID-19 pandemic. Available at: https://www.zdnet.com/article/fbi-says-cybercrime-reports-quadrupled-during-covid-19-pandemic/ (accessed 20/04/20).

CLOUGH J (2010) *Principles of Cybercrime*. Cambridge University Press, Cambridge.

COHEN LE and FELSON M (1979) Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review* **44(4)**, 588-608.

CRABTREE BF and MILLER WL (1992) A template approach to text analysis: Developing and using codebooks. In *Doing Qualitative Research* pp 93–109, Sage Publications.

D'ARCY J, GUPTA A, TARAFDAR M and TUREL O (2014) Reflecting on the "Dark Side" of Information Technology Use. *Communications of the Association for Information Systems* **35(5)**, 109–118.

DILLARD J and PECK E (2006) Persuasion and the structure of affect: Dual systems and discrete emotions as complementary models. *Human Communication Research* **27(1)**, 38–68.

EYSENBACH G (2002) Infodemiology: the epidemiology of (mis)information. *The American Journal of Medicine* **113(9)**, 763–765.

EYSENBACH G (2011) Infodemiology and Infoveillance. *American Journal of Preventive Medicine* **40(5)**, S154–S158.

FEREDAY J and MUIR-COCHRANE E (2006) Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development. *International Journal of Qualitative Methods* **5(1)**, 80–92.

FERREIRA A, COVENTRY L and LENZINI G (2015) Principles of Persuasion in Social Engineering and Their Use in Phishing. In *Human Aspects of Information Security, Privacy, and Trust* (TRYFONAS T & ASKOXYLAKIS I, Eds), pp 36–47, Springer International Publishing, Cham.

GIGERENZER G and TODD PM (1999) *Simple heuristics that make us smart*. Oxford University Press, US.

GLEESON K (2011) Polytextual thematic analysis for visual data. In *Visual methods in psychology: Using and interpreting images in qualitative research* pp 314–329, Psychology Press, New York.

GORDON S and FORD R (2006) On the definition and classification of cybercrime. *Journal in Computer Virology* **2(1)**, 13–20.
HART J (2009) Remote working: managing the balancing act between network access and data security. *Computer Fraud & Security* **2009(11)**, 14–17.
HOLT TJ and BOSSLER AM (2008) Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior* **30(1)**, 1–25.
HOLT TJ, VAN WILSEM J, VAN DE WEIJER S and LEUKFELDT R (2020) Testing an Integrated Self-Control and Routine Activities Framework to Examine Malware Infection Victimization. *Social Science Computer Review* **38(2)**, 187–206.
HOVLAND CI and WEISS W (1951) The Influence of Source Credibility on Communication Effectiveness. *The Public Opinion Quarterly* **15(4)**, 635–650.
JAGATIC TN, JOHNSON NA, JAKOBSSON M and MENCZER F (2007) Social phishing. *Communications of the ACM* **50(10)**, 94–100.
JALALI MS, SIEGEL M and MADNICK S (2019) Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *The Journal of Strategic Information Systems* **28(1)**, 66–82.
JENSEN ML, DINGER M, WRIGHT RT and THATCHER JB (2017) Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems* **34(2)**, 597–626.
KROMBHOLZ K, HOBEL H, HUBER M and WEIPPL E (2015) Advanced social engineering attacks. *Journal of Information Security and Applications* **22**, 113–122.
KUMARAN N and LUGANI S (2020) Identity and Security. *Protecting businesses against cyber threats during COVID-19 and beyond*. Available at: https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond (accessed 20/04/20).
LEE AS and BASKERVILLE RL (2003) Generalizing Generalizability in Information Systems Research. *Information Systems Research* **14(3)**, 221–243.
LUO X, BRODY R, SEAZZU A and BURD S (2011) Social Engineering: The Neglected Human Factor for Information Security Management. *Information Resources Management Journal* **24(3)**, 1–8.
LUO X, ZHANG W, BURD S and SEAZZU A (2013) Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. *Computers & Security* **38**, 28–38.
MAIMON D and LOUDERBACK ER (2019) Cyber-Dependent Crimes: An Interdisciplinary Review. *Annual Review of Criminology* **2(1)**, 191–216.
MCKENNA B, MYERS MD and NEWMAN M (2017) Social media in qualitative research: Challenges and recommendations. *Information and Organization* **27(2)**, 87–99.
MIETHE TD, STAFFORD MC and SLOANE D (1990) Lifestyle changes and risks of criminal victimization. *Journal of Quantitative Criminology* **6(4)**, 357–376.
MILGRAM S (1974) *Obedience to authority*. Harper, New York.
MITNICK KD and SIMON WL (2003) *The Art of Deception: Controlling the human element of security*. John Wiley & Sons, Inc, New York.
MONEVA A, MIRÓ-LLINARES F and HART TC (2020) Hunter or Prey? Exploring the Situational Profiles that Define Repeated Online Harassment Victims and Offenders. *Deviant Behavior*, 1–16.
MORGAN S (2017) Is cybercrime the greatest threat to every company in the world? *CSO*. Available at: https://www.csoonline.com/article/3210912/is-cybercrime-the-greatest-threat-to-every-company-in-the-world.html (accessed 24/04/20).
MORGAN S (2019) *2019 Official Annual Cybercrime Report*. Cybersecurity Ventures. Available at: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/ (accessed 24/04/20).
MUNCASTER P (2020) Cyber-Attacks Up 37% Over Past Month as #COVID19 Bites. *Infosecurity Magazine*. Available at: https://www.infosecurity-magazine.com/news/cyberattacks-up-37-over-past-month (accessed 25/04/20).
MYAGMAR S, LEE AJ and YURCIK W (2005) Threat Modeling as a Basis for Security Requirements. In *Symposium on requirements engineering for information security (SREIS)* pp 1–8.
MYERS MD (2009) *Qualitative research in business and management* First edition. Sage Publications, London.
NGO FT (2011) Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology* **5(1)**, 773–793.
NGWENYAMA OK and LEE AS (1997) Communication Richness in Electronic Mail: Critical Social Theory and the Contextuality of Meaning. *MIS Quarterly* **21(2)**, 145–167.
ORBACH B (2018) Con Men and Their Enablers: The Anatomy of Confidence Games. *Social Research: An International Quarterly* **85(4)**, 795–822.
PETTY RE and CACIOPPO JT (1986) The elaboration likelihood model of persuasion. In *Advances in Experimental Social Psychology* pp 123–205, Academic Press, New York.

PFLEEGER SL, SASSE MA and FURNHAM A (2014) From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Journal of Homeland Security and Emergency Management* **11(4)**, 489–510.
RICHINS ML (1997) Measuring Emotions in the Consumption Experience. *Journal of Consumer Research* **24(2)**, 127–146.
RUDDIN LP (2006) You Can Generalize Stupid! Social Scientists, Bent Flyvbjerg, and Case Study Methodology. *Qualitative Inquiry* **12(4)**, 797–812.
SEGURA J (2020) Online credit card skimming increased by 26 percent in March. Available at: https://blog.malwarebytes.com/cybercrime/2020/04/online-credit-card-skimming-increases-by-26-in-march/ (accessed 20/04/20).
SHENG S, HOLBROOK M, KUMARAGURU P, CRANOR LF and DOWNS J (2010) Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10* p 373, ACM Press, Atlanta, Georgia, USA.
SHI F (2020) Coronavirus-Related Phishing. Available at: https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/ (accessed 10/04/20).
SØRENSEN HT, SABROE S and OLSEN J (1996) A Framework for Evaluation of Secondary Data Sources for Epidemiological Research. *International Journal of Epidemiology* **25(2)**, 435–442.
STAJANO F and WILSON P (2011) Understanding scam victims: seven principles for systems security. *Communications of the ACM* **54(3)**, 70-75.
SUSSMAN SW and SIEGAL WS (2003) Informational Influence in Organizations: An Integrated Approach to Knowledge Adoption. *Information Systems Research* **14(1)**, 47–65.
WANG J, CHEN R, HERATH T and RAO HR (2009) Visual e-mail authentication and identification services: An investigation of the effects on e-mail use. *Decision Support Systems* **48(1)**, 92–102.
WANG Q-H (2019) See No Evil, Hear No Evil? Dissecting the Impact of Online Hacker Forums. *MIS Quarterly* **43(1)**, 73–95.
WESTERMAN D, SPENCE PR and VAN DER HEIDE B (2014) Social Media as Information Source: Recency of Updates and Credibility of Information. *Journal of Computer-Mediated Communication* **19(2)**, 171–183.
WITTE K (1992) Putting the Fear Back into Fear Appeals: The Extended Parallel Process Mode. *Communication 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 ECONOMIC FORUM (2019) *The Global Risks Report 2019*. World Economic Forum, Geneva. Available at: https://www.weforum.org/reports/the-global-risks-report-2019 (accessed 25/04/20).
WRIGHT R, CHAKRABORTY S, BASOGLU A and MARETT K (2010) Where Did They Go Right? Understanding the Deception in Phishing Communications. *Group Decision and Negotiation* **19(4)**, 391–416.
WRIGHT RT, JENSEN ML, THATCHER JB, DINGER M and MARETT K (2014) Research Note –Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance. *Information Systems Research* **25(2)**, 385–400.
WRIGHT RT and MARETT K (2010) The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems* **27(1)**, 273–303.
YAR M (2005) The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. *European Journal of Criminology* **2(4)**, 407–427.
ZAROCOSTAS J (2020) How to fight an infodemic. *The Lancet* **395(10225)**, 676.
ZIMBARDO P (2008) *The Lucifer Effect: Understanding How Good People Turn Evil*. Random House, New York.

Table 1 Theories and key sensitising concepts

Theory	*Area*	*Sensitizing Concepts*
Routine Activity Theory (RAT) (Cohen & Felson, 1979; Holt & Bossler, 2008)	Situational Factors	Online behaviors Suitable targets for impersonation and victimization People and technology vulnerabilities
Source Credibility Theory (Hovland & Weiss, 1951; Sussman & Siegal, 2003)	Source Credibility	Impersonation
Social Influence Model (Cialdini, 2001; Cialdini & Goldstein, 2004)	Social Engineering	Social influence principles
Dual-Systems Model of Affect (Dillard & Peck, 2006)	Social Engineering	Positive and negative emotions

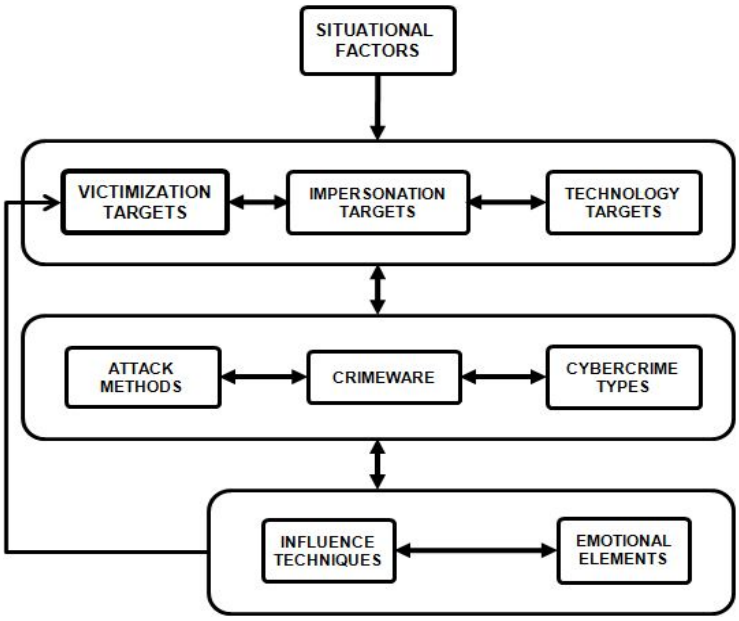


Figure 1. Exploratory sensitising model for cybercrimes

Table 2 Summary of secondary sources

No	*Data Source*	*Period*	*Description*
1	COVID-19 Cyber Intelligence Datafeed Reports on the daily number of incidents, open or closed status, and types of open incidents	17/03/2020 - 17/04/2020	Type: Email data feed Format: Text only Total number of incidents: 43131
2	COVID19 Active Scam/Incidents Documents providing details about active incidents	26/03/2020 - 17/04/2020	Type: Online archive Format: Text and Images Total number of distinct archived incidents: 185

Source: FraudWatch International

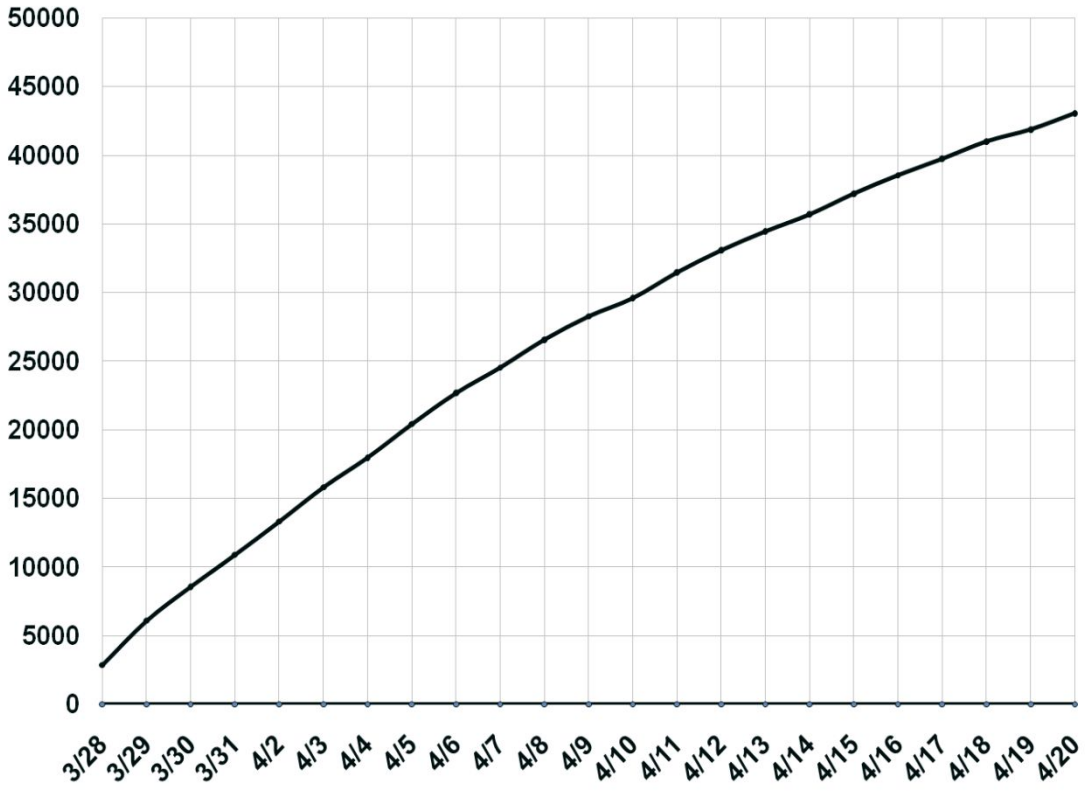


Figure 2 Cumulative number of new COVID-related domains registered

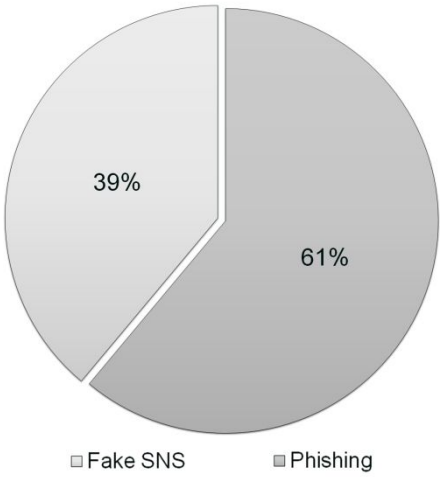


Figure 3 Share of active cybercrime incidents

Table 3 Types of organizations targeted for impersonation

Type of Organization	*Freq*	*%*
Social Networking Sites (SNS)	72	39%
Financial Services Organizations	45	24%
Technology Firms	39	21%
Government agencies	16	9%
Intergovernmental Organization	3	2%
Other	10	5%
Grand Total	185	100%

Table 4 Technologies and Technology Brands Targeted

Technology Type	*Technology Brands Targeted/Impersonated*	*Situational factors*	*Cybercrime*
Email	Gmail	Donations Charities	Fake emails (Phishing) Malware Malicious Websites
Social Media Technologies	Facebook Instagram	Social distancing Social connectivity Donations Charities	Fake Social Media Profiles Misinformation Fake Charities
Videotelephony and online chat services	Zoom Microsoft Teams Whatsapp Apple	Remote work Virtual Meetings	Fake Products

Cloud File Hosting Services	One Drive DropBox	Remote work Virtual Meetings	Fake Products
Streaming media service of television and movies	Netflix	Entertainment/Leisure	Fake Products
Video sharing website	YouTube	Entertainment/Leisure	Fake Products
Broadband and Telecoms Companies	4G (Fake company)	Free Data/Internet	Fake Products
Online payments system	Paypal	Small business loans	Fake Website domain

Table 5 Impersonations of Organizations

Types of Organizations/Brands Impersonated	*Organizational Brands Targeted/Impersonated*	*Situational factors*	*Cybercrime*
Banks and Investment Companies	Banco do Brasil HSBC RBC Royal Bank Bank Of Montreal ING	Relief Programs Donations Charities High growth stocks for drug treatments and cure	Fake Charities Fake Trading Scam
Government Agencies	Federal government of the United States Canada Revenue Agency Government of Canada Internal Revenue Service (IRS)	Relief Programs	Fake Relief Programs
Intergovernmental Agencies/	World Health Organization	Pandemic Information Safety Measures Relief Programs	Disinformation Fake Relief Programs
Humanitarian Organizations	Red Cross	Charities	Fake Charities
Other Brands	Cathay Pacific Woolworths Nike	Refunds Food Protective Clothing	Fake Refunds Fake Products

Table 6 Social influence principle occurrences

Principle	*Phishing*		*Fake SNS*		*Overall Freq*	
	(Freq)	*%*	*(Freq)*	*%*	*%*	*%*
Liking	102	37%	72	50%	174	42%
Social Proof	3	1%	72	50%	75	18%
Scarcity	73	27%	0	0%	73	17%
Authority	68	25%	0	0%	68	16%
Reciprocity	19	7%	0	0%	19	5%
Consistency	10	4%	0	0%	10	2%
	275	100%	144	100%	317	100%

Table 7 Emotional appeal occurrences

Emotional Appeal	*Phishing*		*Fake SNS*		*Overall Freq*	
	(Freq)	*%*	*(Freq)*	*%*	*%*	*%*
Relief	30	33%	0	0%	30	30%
Fear	16	18%	6	60%	22	22%
Hope	21	23%	1	10%	22	22%
Enjoyment	15	17%	0	0%	15	15%
Threat	3	3%	3	30%	6	6%
Compassion	5	6%	0	0%	5	5%
	90	100%	10	100%	100	100%

Table 8 Evidence of influence techniques applied to COVID-19 crime

Principle	*Propositions*	*Example*	*Theme*	*Sample text*[1]
Authority	People tend to comply with a request that comes from an authority figure.	The WHO serves as a respected authority on the pandemic for society.	Safety measures	"Distributed via the CDC Health Network"
Consistency	People, who make a commitment, tend to feel compelled to perform consistently in line with that commitment.	Completing short and easy survey commits one to disclose personal details.	Free Entertainment	"Answer 3 simple questions"
Liking	People's tendency for liking another person or product affects their tendency to comply with that person's request.	Familiarity of popular banking brands. Front line healthcare worker.	Donation Donation	" Select your Financial Institution" See Figure A.2 Photo: Photograph of a front line healthcare worker feeding an intubated Corona virus patient
Scarcity	People tend to value those opportunities that have limited availability (Cialdini 2009, p. 179).	Free groceries. COVID-19 relief funds by government agency. Credit relief by banks. Impersonating Investment company.	Food vouchers Relief Funds Payment Holiday Overdraft support Interest reduction Invest in 'hot' new stocks related to curing the disease Using AI to maximise returns from stock market Drug scarcity	"Hurry up! Collect your free voucher here" "Opps, You are not qualified" "Find out instantly if you are eligible to obtain urgent aid" "Corona Millionaire" (context) "The drug will be shortages fast"

[1] Text quoted verbatim. Spelling errors are from the source.

Principle	*Propositions*	*Example*	*Theme*	*Sample text*[1]
Reciprocity	People tend to comply to a requester who presents them with an initial favor or initial concession (Cialdini 2009, p. 38).	Fake Technology brand offers reward for completing COVID-19 survey.	Free Internet Access and Data	"500 GB of 4G + Internet for free and for everyone!"
Social Proof	People tend to view a particular behavior as being more correct to the degree with which they see others in a similar situation performing the same behavior (Cialdini 2009, p. 88).	Fake Social Media Profiles.	Make new friends Charity	"Increasing Corona virus fundraising statistics"

Examples drawn from www.fraudwatchinternational.com/phishing/

Table 9 Evidence of emotional elements employed in COVID-19 cybercrime messages

Element	*Propositions*	*Example*	*Theme*	*Sample text*[2]
Fear/ Panic	People will tend to be persuaded by fear appeals when they feel vulnerable to an environmental threat.	Keeping informed about the local spread of the virus.	Pandemic Information	"coronavirus update disease (COVID-19) your neighbours tested positive"
Threat/ Panic	People will tend to be persuaded by threat appeals when they feel vulnerable to an environmental threat.	Corona virus taking over the world.	Pandemic Information	Use of the virus images "Youre next"
Enjoyment	People will tend to be persuaded by positive appeals such as enjoyment.	Coping with lockdown and social distancing.	Entertainment	"Staying safe and enjoying the Internet at home" Images of movie covers
Relief	People will tend to be persuaded by positive appeals such as relief, when they feel they will gain a positive outcome such as gaining control over their lives.	Keeping informed about possible cure/treatment.	Treatment information	"Breaking!!! COVID-19 solution announced by WHO At Last.." See Figure A.1
Hope	People will tend to be persuaded by positive appeals such as hope.	Global relief funds. National Relief Funds.	Relief funds	Photo: Joining hands Image: Flags of nations/individual nation
Compassion	People will tend to show compassion for others similar to them.	Empathic concern for patient.	Widespread suffering Donation	Photo: See A2

Examples drawn from www.fraudwatchinternational.com/phishing/

[2] Text quoted verbatim. Spelling and grammatical errors are from the source.

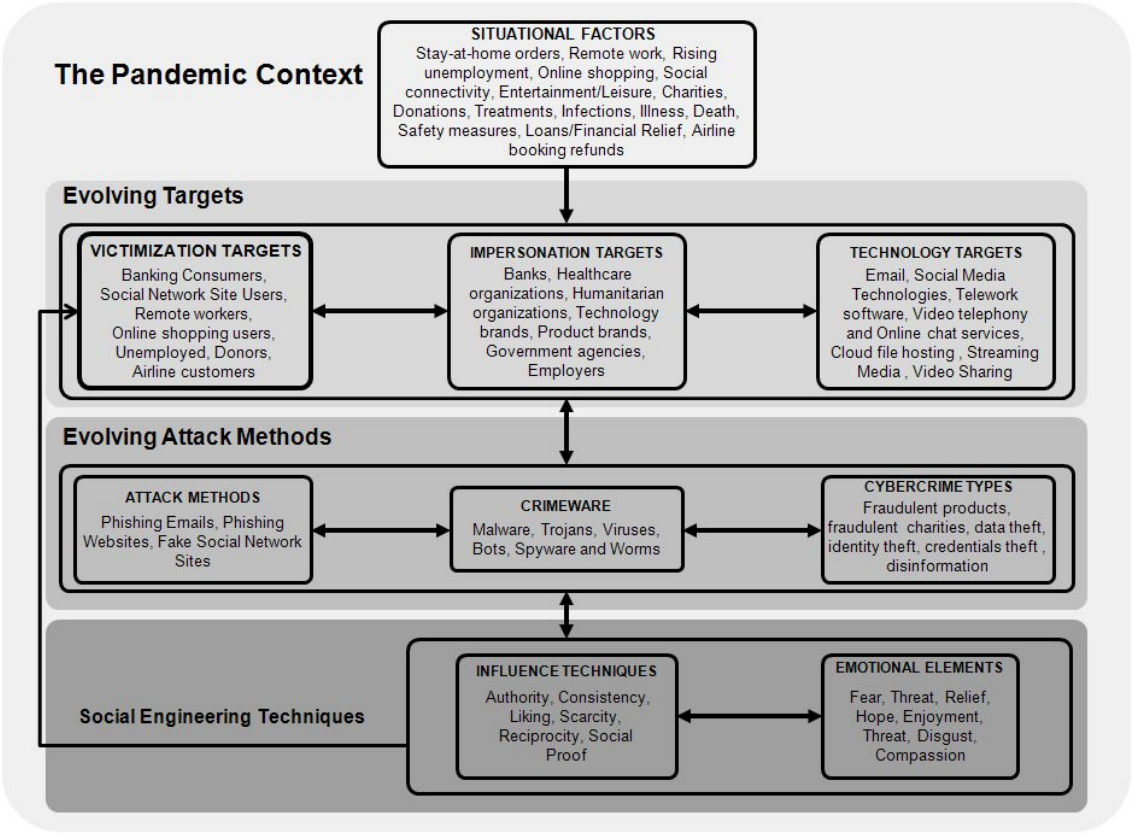


Figure 4. A multi-level influence model of cybercrime

Appendix

Figure A.1 Phishing Email

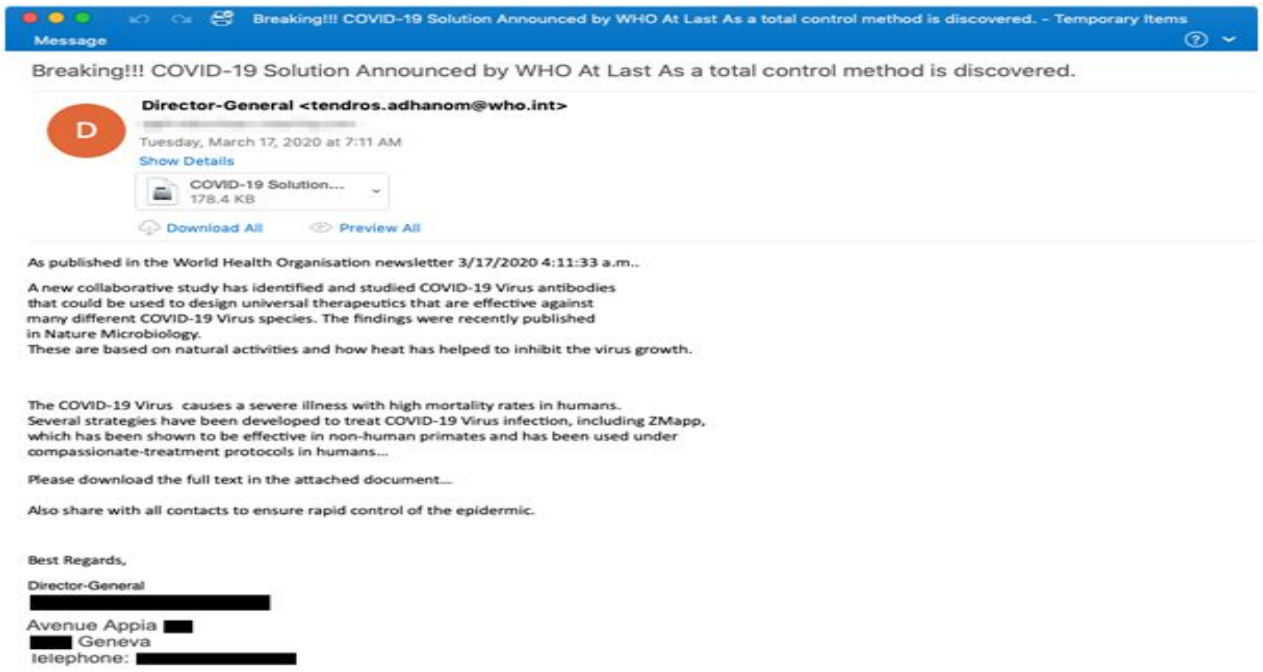


Figure A.2 Fake Web Site