Journal of Cyber Forensics and Advanced Threat Investigations

CFATI

Volume 2(1), 50-62. https://doi.org/10.46386/ijcfati.v2i1.29

Exploring the Shift from Physical to Cybercrime at the Onset of the COVID-19 Pandemic

Miloslava Plachkinova[1]

Abstract

The novel coronavirus has made an impact on virtually every aspect of our lives. The current study utilizes secondary data to identify patterns and trends related to shifting crime from the physical to the cyber domain. With millions, if not billions, people staying at home, attackers now look for new ways to commit crimes. Our findings indicate that while a lot of crimes such as robbery, assault, rape, and murder have declined at the beginning of the pandemic, we are also witnessing a rise in cybercrime, vehicle theft, and domestic violence. The current study looks specifically at phishing and what new trends are observed due to COVID-19. The current work is grounded in routine activity theory and demonstrates its relevance to both the physical and cyberspace. The implications of our work can be used by scholars who want to continue researching this new phenomenon. Practitioners can utilize our findings to look for ways to improve the corporate security posture by protecting the employees and customers working from home. Developing new phishing training and awareness programs should be focused around possible scenarios involving COVID-19. Our study suggests victims are more likely to fall prey to those during times of fear and uncertainty like the current pandemic.

Notes for Practice

- We utilize Routine Activity Theory to explain a current phenomenon.
- We provide practitioners with examples of the growing threat of cybercrime as a result of the COVID-19 global pandemic.
- We offer recommendations for practitioners on how to redesign current security education, training, and awareness programs to reflect the new threats corporations and individuals are facing because of the pandemic.

Keywords

Cybercrime, Phishing, COVID-19, Pandemic, Coronavirus, Routine Activity Theory.

Submitted: 09/04/2021 — **Accepted: 19**/05/2021 — **Published: 23**/05/2021

[1]Email: mplachki@kennesaw.edu, Address: Coles College of Business, Kennesaw State University. 560 Parliament Garden Way NW, Room 492, MD 0405, Kennesaw, GA 30144, USA, ORCID ID 0000-0003-0338-7813

1. Introduction

Cybercrime has been on the rise in the last decade. According to a recent report by Accenture[1], the average number of security breaches in 2018 grew by 11 percent from 130 to 145 and the average cost of cybercrime for an organization increased US$1.4 million to US$13.0 million. The authors estimate that the global costs of cybercrime will reach $US5.2 trillion over the next five years. This is a significant increase compared to 2013 when Konradt et al. (2016) estimated that the global cost of cybercrime was $445 billion. Most of the financial damages are a result of hijacked accounts and stolen credit card numbers, which is often achieved by phishing attacks.

Phishing is a type of cybercrime where the attackers make malicious emails look legitimate. The goal is to steal user credentials, credit card, and other sensitive personal information, which can lead to identity theft, fraud, and device compromise (Kirda & Kruegel, 2006). Phishing emails combine social engineering and spoofing techniques to convince individuals to

[1] https://www.accenture.com/us-en/insights/security/cost-cybercrime-study, accessed on April 9, 2021

provide their information. Online activity such as banking or shopping can increase the likelihood of phishing victimization (Reyns, 2015).

Due to the recent COVID-19 outbreak, millions, if not billions of people all over the world were ordered to stay at home and observe quarantine. This new reality made a significant impact on virtually every aspect of our everyday lives – working from home, online education, shopping, banking, telemedicine, etc. became the new normal. Such a major shift is unprecedented in the world's history and presented us with a number of challenges. One of them is the shift from physical to cybercrime that was observed in the initial stages of the pandemic.

According to routine activity theory (Cohen & Felson, 1979), in order for a crime to occur there should be a motivated offender, a suitable target, and a lack of capable guardianship. However, since significantly fewer people are out on the streets – going to work, to school, to bars, and restaurants, the potential for offenders to attack victims has significantly decreased. In Chicago, one of America's most violent cities, drug arrests dropped 42% in the weeks when the city shut down in March 2020, compared with the same period last year[2]. Miami was without a homicide for seven weeks, which is the first time since 1957[3]. While some may consider this a victory and a positive outcome of the pandemic, a deeper analysis of the current trends in cybercrime points out that offenders are shifting from the physical to the cyber domain. On March 24, 2020 the president of the European Commission, Ursula von der Leyen, warned that cybercrime in the EU has increased due to the coronavirus outbreak. She emphasizes that attackers are now following their victims online and even using the pandemic to their advantage by devising phishing campaigns based on COVID-19 concerns.[4] These examples point out how at the onset of the pandemic, criminals immediately began exploring alternative opportunities to offend.

Adding the steady growth of cybercrime in the last decade to the fear and anxiety of the novel coronavirus creates a unique situation that offenders can exploit. Furthermore, the commoditization of cybercrime (Van Wegberg et al., 2018) makes it very easy for someone with minimal skills and experience to outsource cybercrime activities, thus lowering the barriers to entering the field. According to them, at least $15 to 17 million have been spent on cyber-crime commodities in the US between 2011 and 2017. The authors mention how phishing emails are one of the most common channels for distributing malicious software. Furthermore, phishing scams are easy to accomplish because they require very limited resources and technical skills. The combination of these factors makes phishing very attractive and lucrative for motivated offenders. Their current inability to commit physical crimes is a major driver for a shift from physical to cybercrimes. Thus, there is a pressing need to further study this phenomenon and develop a better targeted and comprehensive strategy to prevent phishing victimization.

The goal of the current study is to examine the shift from physical to cybercrime at the onset of the COVID-19 pandemic. This is an unprecedented global historic event and we are still gathering data to better understand the coronavirus itself and its broader impact on society. The dynamic nature of the pandemic presents some unique challenges. Thus, our work aims to shed more light on how crime initially moved to cyberspace and what are the implications for organizations and individuals. The research question guiding the study is: "What are the implications of COVID-19 on crime in the onset of the pandemic?" and our hypothesis is that there was a shift from physical to cybercrime as a result of the mass quarantine around the world at the beginning of the pandemic.

H1: There is a shift from physical to cybercrime due to COVID-19 lockdowns at the onset of the pandemic.

To answer the research question and test the hypothesis, the author uses secondary data. One of the challenges of this study is the novelty of the topic and the lack of available scholarly resources on the impact of COVID-19 on crime. Thus, the author is exploring a variety of news articles, government reports, and private sector publications to identify current trends in crime and examine whether there are any possible shifts in how it occurs during a pandemic. Our work is grounded in routine activity theory as it has been widely used in the context of both physical (Groff, 2007; Robinson, 1999; Tewksbury & Mustaine, 2003) and cybercrime victimization (Holt & Bossler, 2008; Leukfeldt & Yar, 2016; Yar, 2005).

2. Literature Review

2.1. Cybercrime

Cybersecurity concerns have been growing as we become more and more reliant on technology in our everyday lives. The

[2] https://www.nbcchicago.com/news/local/chicago-drug-arrests-down-42-since-start-of-coronavirus-pandemic/2254436/, accessed on May 12, 2021

[3] https://www.cbsnews.com/news/miami-no-homicide-seven-weeks/, accessed on April 9, 2021

[4] https://euobserver.com/coronavirus/147869, accessed on April 9, 2021

targets vary greatly – large corporations with millions of customers/employees affected (Target, Marriott Hotels, Facebook, Equifax), local and federal governments (IRS, the Clinton campaign, US Office of Personnel and Management), and single individuals whose identities have been stolen. According to Sarno et al. (2019), oftentimes such attacks are a result of phishing scams in which individuals are tricked into clicking on malicious links in emails that are spoofed to look legitimate. According to one study exploring 2019 data[5], phishing accounts for 90% of data breaches; 76% of businesses reported being a victim of a phishing attack in the last year; and 30% of phishing messages get opened by targeted users. Business email compromise scams accounted for over $12 billion in losses.

These numbers are in the context of business organizations that have dedicated IT and security functions. Furthermore, most organizations provide some kind of phishing training and awareness for employees and use sophisticated filtering systems to block suspicious emails. Since so many employees are now working from home, that creates a lot more challenges for IT professionals to secure their networks and devices. Furnell et al. (2007) conducted a study and found that there is an increased danger for home users. For instance, when organizations tighten their defenses, home user systems suddenly become more attractive targets for compromise due to their generally lower protection mechanisms. As a result, they can be exploited in botnets and distributed denial of service (DDoS) attacks. The study found that even though users had a high degree of confidence in their ability to protect their systems and devices, there were several areas in which desirable knowledge and understanding were lacking. These issues are now transferred from personal to enterprise networks and devices essential for home offices during the pandemic. Thus, the attack surface of any organization is increased and can be a potential target for criminals.

When it comes to cybercrime, there is a lot of organized activity. The cybercrime umbrella encompasses a wide range of skillsets – from script kiddies who have little knowledge and rely on existing exploits, to nation-states who use advanced persistent threats (APT). However, those with more access to resources are the biggest threat and they are typically crime syndicates and organizations. Organized cybercrime has been linked to phishing attacks (Birk et al., 2007), national security threats (Grabosky, 2015), cyber racketeering (Jian et al., 2020), terrorism (Shelley, 2003), and the underground economy (Yip et al., 2012). Cybercrime was already the modern-day mafia even before the pandemic[6]. Thus, it is reasonable to assume that criminal organizations will focus their efforts on cybercrime, especially in the initial stages of the pandemic when targets were spending most of their time in front of their screens and not on the street.

2.2. Phishing

When it comes to phishing, while there is not a universal definition that all scholars agree on, many of the existing definitions cover the same basic concepts. Kirda and Kruegel (2006) focus on the financial aspect of phishing and their main concern is how identity theft can be used to gain access to bank accounts and credit cards of the victims. Sarno et al. (2019) use a definition that is more concerned with the defrauding of individuals with the purpose of stealing their personal information. This is also consistent with how Dhamija et al. (2006) describe the phenomenon. They also emphasize the fraudulent practices applied by phishers to bait users into clicking on links in emails.

The lack of a consensual definition of phishing was addressed by Lastdrager (2014) who conducted a systematic literature review of peer-reviewed publications. The proposed consensus definition incorporates several important aspects such as scalability, deception, impersonation, and target. The study incorporated many criminology theories such as routine activity theory (Cohen & Felson, 1979), rational choice theory (Cornish & Clarke, 1985), and crime pattern theory (Brantingham & Brantingham, 2013). The novelty in this study is related to viewing phishing as a scalable crime. This is due to the idea that the same phishing email can be sent to one or thousands of different individuals with very little effort. Such an approach is very different from physical crime and can lead to much bigger benefits while at the same time reducing the risk for the attackers.

Due to the overall increase in phishing scams, it is important to better understand the victim profile, so we can provide more awareness and training to prevent future attacks. Technology plays an important role as a mechanism to block suspicious emails, but studies have shown that humans are the weak link (Laszka et al., 2013) and any prevention programs have to be targeted at them rather than at the automated tools.

[5] https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html, accessed on April 9, 2021
[6] https://www.forbes.com/sites/tonybradley/2015/10/16/cybercrime-is-the-modern-day-mafia/, accessed on May 12, 2021

2.3. Cybercrime vs Physical Crime

Cybercrime and physical crime have some characteristics in common. For example, Lusthaus (2013) argues that cybercrime can be organized in the same way as a traditional crime. More specifically, the author explores the rise in professional cybercriminals and the development of numerous online groupings, where these cybercriminals join together in plots. Social platforms and places like the Darknet have further facilitated their communication and have contributed to establishing cybercrime syndicates (Wehinger, 2011).

In another study, Yar (2005) provides a comparison between 'virtual' and 'terrestrial' crimes based on routine activity theory. The study explores the extent to which the theory's concepts can be transposed to crimes committed in a 'virtual' environment and concludes that although some of the theory's core concepts can be applied to cybercrime, there remain important differences between 'virtual' and 'terrestrial' worlds. Thus, Yar (2005) argues that 'cybercrime' does indeed represent the emergence of a new and distinctive form of crime.

The notion of cyberspace as an extension of physical space has been supported by a number of more recent studies as well. Weulen Kranenbarg et al. (2019) demonstrate that there is considerable victim-offender overlap and correlates like low self-control. They demonstrate how routine activities partly explain differences in victimization, offending, and victimization-offending when it comes to cybercrimes. Furthermore, the authors found some cybercrime correlates that are related to both digital and traditional crime. The victim-offender overlap suggests that many victims are observed to be offenders and many offenders turned out to have experienced victimization (Jennings et al., 2010). While this was originally explored in the context of physical offenses, the trend remains even when it comes to cybercrime (Marcum et al., 2014).

One of the main issues with cybercrime is establishing jurisdiction. According to Brenner (2006), physical crime is almost always a local phenomenon because the perpetrator and the victim are both at the same place and time when the crime occurs. Thus, crime is considered territorial and its location determines the jurisdiction. This becomes a problem when we look at cybercrimes, because they are not physically bound to a single location. The victim and the offender can even physically be in different countries. In those cases, different sovereigns can claim various pieces of the crime. A further complication of cybercrimes is that some countries may not have extradition treaties. Thus, even if law enforcement can prove who committed the crime, they may not be able to prosecute the perpetrator. And finally, legislation on cybercrime is still developing, so often times it may be challenging to bring to justice those who commit cybercrimes.

The commoditization of cybercrimes (Sood & Enbody, 2013; Van Wegberg et al., 2018) combined with the inability to investigate and prosecute them, make cybercrimes a lucrative business for offenders. The initial stages of the COVID-19 reality, when most of the population was ordered to stay at home, presents attackers with a unique opportunity to easily switch from the physical to the cyber domain. Multiple sources have already reported an increase in cybercrime since the pandemic started. For example, the US Department of Homeland Security issued an alert on April 8, 2020[7] reporting that there was a 127% increase in attacks against remote desktop protocol (RDP) endpoints, which are typically devices employees would use to remotely access enterprise resources. The alert also warns about COVID-19 themed phishing attacks, malware distribution, registration of new domains related to COVID-19, and attacks against remote access and teleworking infrastructure.

At the same time, we witness an interesting change in physical crime at the beginning of the pandemic. Chicago, known for its violent crimes, has seen a 42% decrease in drug arrests since the pandemic. There has been a 10% decline in all crimes in Chicago after the COVID-19 lockdown and this trend has been observed globally. Furthermore, even regions that have the highest levels of violence outside of war zones, were reporting fewer murders and robberies[8]. However, law enforcement warned about an increase in domestic violence and child abuse. In fact, even the United Nations Secretary-General António Guterres expressed concerns about the sharp increase in those incidents and called on governments to provide more support and resources for the victims[9]. These various examples indicate that many criminals and crime syndicates looked for alternative means to offend when their normal routines were disrupted at the onset of the pandemic. It is worthwhile exploring these patterns further from an academic perspective, because it can shed more light on how organizations and individuals can better protect themselves from the ever-increasing cybersecurity threats.

3. Theoretical Foundation

[7] https://www.us-cert.gov/ncas/alerts/aa20-099a, accessed on April 24, 2020
[8] https://dayton247now.com/news/coronavirus/crime-drops-around-the-world-as-covid-19-keeps-people-inside, accessed on April 24, 2020
[9] https://www.npr.org/sections/coronavirus-live-updates/2020/04/06/827908402/global-lockdowns-resulting-in-horrifying-surge-in-domestic-violence-u-n-warns, accessed on April 24, 2020

Routine activity theory is prevalent when it comes to describing and defining cybercrime and phishing victimization in particular. The theory was originally proposed by Cohen and Felson (1979) and its main tenet is the physical intersection between a motivated offender, a suitable target, and the lack of capable guardianship. The theory is among the most popular ones in the field of criminology, because it considers the victim as an active participant in the crime and their actions (or lack thereof) can have an impact on whether or not a crime occurs. It also argues that the probability of a crime occurring is influenced by our "routine activities" – including work, family, leisure, and consumption activities. The main proposition of the theory is that the rate of criminal victimization is increased when there is a "convergence in space and time of the three minimal elements of direct-contact predatory violations" (Cohen and Felson, 1979: 589). Furthermore, routine activities are defined by Cohen and Felson (1979) as "recurrent and prevalent activities that provide for basic population and individual needs… formalized work, as well as the provision of standard food, shelter, sexual outlet, leisure, social interaction, learning, and childbearing" (p. 593).

Routine Activity is widely used in the context of cybercrime. For instance, Leukfeldt and Yar (2016) conducted a theoretical and empirical analysis on an individual level and found out that certain elements, such as visibility on social media, are more applicable than others. Similar results were also found on a national level as well where wealthier countries are more common targets of phishing attacks (Kigerl, 2012). Furthermore, Reyns (2013) provides evidence that individuals who use the Internet for banking and/or e-mailing/instant messaging are about 50 percent more likely to be victims of identity theft than others. Similarly, online shopping and downloading behaviors increased victimization risk by about 30 percent. These studies demonstrate that routine activity theory can successfully explain both physical and cybercrimes. While other criminological theories, such as deterrence, rational choice, social learning, exist, routine activity has been the most commonly used in the context of cybercrime. The hypothesis of the current study is that those who have already been committing a crime before the pandemic started did not stop, but rather changed their methods to adjust to the new normal and shifted from physical to street crime.

Due to the initial global COVID-19 lockdown, the majority of individuals were unable to go out and meet their needs in person – either because stores were closed or because it was not safe to be in public. Thus, most people changed their habits and shifted from in person, to online routine activities. Many now still work, study, exercise, and consume products in the safety of their own homes. According to routine activity theory, this shift in habits and lifestyles would also cause a shift in the environment where the crime occurs. Since the majority of people have been staying at home, there has been a decrease in robbery, murder, assault, and rape. However, other types of crimes such as vehicle theft, domestic and family abuse, burglary of commercial business left vacant, hate crimes, and financial scams have increased[10]. There is already evidence of the effect of COVID-19 on crime and we are definitely seeing a shift in criminals' practices as they also adjust to the new reality of social distancing.

4. Methodology

Due to the unique nature of the COVID-19 situation, we are still in the process of gathering data and understanding the full implications of the pandemic. It has impacted virtually any aspect of our lives, including how crime is committed. For the purposes of the current study, the author examines a number of publicly available resources such as news articles, government reports, and private sector publications.

To demonstrate how COVID-19 has affected crime, our study is referring to the US Secret Service (USSS) Cyber Fraud Task Force Bulletin issued in April, 2020. The goal of the publication is to identify current trends and resources and to provide guidance for individuals and organizations to avoid being victimized. This is an official communication from the US government and is based on reliable and comprehensive data that the agency has access to. Another source for this study is the Federal Bureau of Investigation (FBI) data and press releases. These sources are used for analyzing trends and patterns in criminal behavior during the onset of the pandemic.

5. Results

5.1. Stimulus Scams

In 2020, the US Congress recently passed a large COVID-19 relief and stimulus package. The USSS Cyber Fraud Task Force

[10] https://www.safewise.com/blog/covid-19-crimes/, accessed on April 24, 2020

Bulletin (2020) indicated that the agency is seeing an increase in stimulus relief fraud and expect the trend to continue throughout the pandemic. Some of the techniques fraudsters use are spoofing US Treasury officials and requesting individuals to provide their personally identifiable information (PII) in order to receive their share of the stimulus (Appendix A).

In addition to email, offenders are also using SMS/text, robocalls, and other messaging platforms to contact potential victims. Criminal actors are using hyperlinks in texts to direct recipients to websites where they can enter their personal and financial information, as well as emails and passwords. Appendix B provides an example of such messages using the COVID-19 stimulus relief to lure users into providing their sensitive information to fraudulent websites. Something interesting that the USSS points out in their report is that their foreign partners are also starting to observe similar messages. Thus, while the crime itself may not be novel, the context and timeliness of the phishing scams make them relevant and increase the likelihood that someone will click on the links.

5.2. COVID-19 Emails with Malicious Attachments

Another phishing scenario used in the context of the pandemic is leveraging legitimate emails from various organizations regarding COVID-19 updates. As this communication becomes more frequent, attackers are starting to take advantage of this familiarity. For example, criminals embed malicious attachments targeting both individuals and corporations. Their goal is to remotely install malware to harvest credentials, install keyloggers, or lockdown systems for ransomware. The USSS is emphasizing that the impact of these attacks may not be immediate, but it may result in business email compromise or other fraud in the future. An implication of this finding for corporations is that they should be more cautious as attackers can potentially pose as vendors, members of the supply chain, or other familiar entities that may not raise awareness if spoofed.

Another scenario for phishing emails during the pandemic is related to individuals receiving emails disguised as coming from a hospital informing them that they may have been in contact with someone who tested positive for COVID-19. The email instructs the recipient to download a file, fill it out, and bring it to the nearest hospital for further testing. As in the previous example, here the attackers have embedded malicious code in the file and their goal is to steal login credentials, lookup cryptocurrency wallets, discover open shares on the network, and obtain the IP address. Another variation of this scam is disguising as the US Department of Health and Human Services. The emails target potential suppliers of medical equipment and requesting them to provide any medical equipment included in the attached file (Appendix C).

5.3. COVID-19 Research

According to the FBI, instances of cybercrime have increased by 300% since the pandemic. The Bureau's Internet Crime Complain Center (IC3) said that it is now receiving between 3,000 and 4,000 cybersecurity complaints every day, up from the average 1,000 complaints per day the center had before the COVID-19 outbreak. Furthermore, the FBI claims that this is due to the fact that most of our daily activities are now taking place online and newly remote workers have limited knowledge on even basic security measures. In addition, the agency is attributing a lot of the attacks to nation-states who are after the latest COVID-19 research findings. The deputy assistant director of the FBI's Cyber Division, Tonya Ugoretz, said that "Countries have a very high interest in information on the virus … such as information on a vaccine. We have certainly seen reconnaissance activity and some intrusions into some of those institutions, especially those who have identified themselves as working on COVID research."[11] These findings showcase the diversity of offender motivation out there – from PII, to financial gain, and the latest COVID-19 vaccine developments.

6. Discussion

COVID-19 is still a developing situation with many unknowns. As we tirelessly conduct medical research on the novel coronavirus and focus on recovering the global economy, we should also pay attention to the shifts in society. No one has ever experienced anything like this before and while we are still in the process of collecting data, it is important to be able to draw some conclusions and identify patterns that can help our society move forward. Our work aimed to answer the question *"What are the implications of COVID-19 on crime in the onset of the pandemic?"* Based on the secondary data that the author examined, the study identified shifts in criminal behavior and how offenders were approaching crime in the early stages of the global epidemic.

Our findings indicate that initially there was a decline in certain types of physical crimes such as robbery, assault, rape, and murder, but others such as domestic violence, vehicle theft, and online scams were on the rise. Through secondary data,

[11] https://www.engadget.com/fbi-cybercrime-complaints-increase-fourfold-covid-19-091946793.html, accessed on April 24, 2020

the author was able to find support for the hypothesis that we observed a shift in crime in the initial stages of the pandemic. Many researchers agree that criminals are opportunists and they see major events as opportunities (Okoye & Gbegi, 2013; Watson, 2005). The COVID-19 situation is no different. In fact, it presents a prime opportunity for enterprising criminals because they take advantage of one of the most basic human conditions – fear (McManus, 2011; Smith, 2009). Fear has been proven to bias perceptions and impact the decision-making (Petty & Briñol, 2015). Thus, in a pandemic where people are worried about the lives of their family and loved ones, they become more vulnerable and, consequently, more susceptible to phishing and other forms of social engineering.

COVID-19 has significant implications on society. When it comes to crime, we see a growing number of scams and many of them are carefully crafted to reflect the current situation. As most individuals work from home, they likely use unprotected home networks with limited security features. Zoom, the most popular platform for videoconferencing at the moment, has had multiple security and privacy issues[12]. This lack of capable guardianship and the vulnerability of victims make them suitable targets for motivated offenders who are now moving from the physical to the cyber domain. As the events are still unfolding, we expect to see even more cybercrimes happening in the near future while the stay at home orders are in place.

7. Limitations and Future Work

COVID-19 presents some unique challenges to all aspects of our lives. This situation is still ongoing, and more data needs to be collected to have a better understanding of the full impact of the pandemic on society. This is an exploratory study on a very broad topic that we still know very little about. Thus, our colleagues are encouraged to continue researching the implications of COVID-19 on cybercrime. The more information we gather on this complex topic, the easier it will be to protect individuals and corporations and educate them on the measures they can take to avoid becoming victims of phishing attacks.

The current study utilizes secondary data sources such as news articles, government reports, and private sector publications. The author acknowledges the challenge of collecting primary data during these uncertain times. Hopefully, in the future, our colleagues can build upon our study and utilize additional data sources. Using triangulation is a valuable technique to improve our understanding of this complex problem and add more rigor to future studies (Jones & Bugge, 2006).

8. Implications for Theory and Practice

The current study contributes to building a body of knowledge of scholarly work on the novel coronavirus. In these unprecedented times, it is important for researchers to address various aspects of how COVID-19 has been impacting society. The author specifically examines crime and how it has shifted from physical to cyberspace due to the new environment and circumstances. Criminals are smart and opportunistic, so they will always look for new ways to exploit human weaknesses. The pandemic is no different and through the current work, the author aims to point out patterns and trends that scholars and practitioners can leverage in the future.

Our study can aid scholars as they build upon the idea of routine activity theory in the context of shifting crime patterns. Our findings are consistent with prior work on extending the theory to explain cybercrime (Holt & Bossler, 2008; Jansen & Leukfeldt, 2016; Yar, 2005). In fact, the author touches upon all three aspects of it – the suitable targets who are now quarantined at home, the lack of capable guardianship as organizational IT and security functions have very little control over the employees' home environment and systems, and the motivated offenders who are now exploiting the COVID-19 situation to create more relevant and credible phishing scams and to attack facilities doing research and development on new vaccines.

In terms of practical implications, the study recommends organizations to use this time to educate their clients and employees on the best practices of working from home. From simple tips such as how to secure your Zoom meeting, to phishing campaigns aimed at increasing awareness about the potential scams out there. Even though the current situation is unprecedented, and millions of individuals had to quickly find ways to work from home, now that things are settling down, and we need to shift our focus to providing capable guardianship and securing our assets. For example, we can provide additional resources such as virtual private networks (VPNs) so that clients can have an encrypted channel of communicating with the servers, and multifactor authentication (MFA) to improve access controls. Furthermore, this is a great time to conduct maintenance and upgrades to corporate networks, as it will cause minimal interruptions to users.

[12] https://www.fastcompany.com/90487814/the-zoom-privacy-and-security-issues-you-still-have-to-worry-about, accessed on April 24, 2020

9. Conclusion

COVID-19 has affected virtually every aspect of our lives and while we are still adjusting to doing a variety of activities online, we need to recognize that we can be victimized even in the comfort of our own homes. We should not be letting our guard down and allowing fear to take over. On the contrary, we need to be even more vigilant than ever because criminals are always looking for new ways to attack us. Our findings show that while some crimes have decreased in the beginning of the pandemic, cybercrime is on the rise, as it does not require physical contact between the victim and the offender. Organizations and individuals should be carefully evaluating any communication they receive and always verify the source. We can leverage routine activity theory to look for innovative ways to protect ourselves and our assets. Just like criminals, we should shift our focus and explore how we can stay safer at home – both physically and virtually.

Declaration of Conflicting Interest

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

References

Birk, D., Gajek, S., Grobert, F., & Sadeghi, A.-R. (2007). Phishing phishers-observing and tracing organized cybercrime. Second International Conference on Internet Monitoring and Protection (ICIMP 2007), 1-5 July 2007, San Jose, CA, USA. doi: 10.1109/ICIMP.2007.33

Brantingham, P., & Brantingham, P. (2013). Crime pattern theory. In *Environmental criminology and crime analysis* (pp. 100-116). Willan. doi: 10.4324/9780203118214-13

Brenner, S. W. (2006). Cybercrime jurisdiction. *Crime, law and social change*, *46*(4-5), 189-206. doi: 10.1007/s10611-007-9063-7

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588-608. doi: 10.2307/2094589

Cornish, D., & Clarke, R. (1985). Rational choice theory: Chapter.

Cyber Fraud Task Force Bulletin: Sharing News Among Our Law Enforcement and Industry Partners. (2020).

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. Proceedings of the SIGCHI conference on Human Factors in Computing Systems, April 22-27, 2006, Montréal, Canada. doi: 10.1145/1124772.1124861

Furnell, S., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security*, *26*(5), 410-417. doi: 10.1016/j.cose.2007.03.001

Grabosky, P. (2015). Organized cybercrime and national security. In *Cybercrime Risks and Responses* (pp. 67-80). Springer. doi: 10.1057/9781137474162_5

Groff, E. R. (2007). Simulation for theory testing and experimentation: An example using routine activity theory and street robbery. *Journal of Quantitative Criminology*, *23*(2), 75-103. doi: 10.1007/s10940-006-9021-z

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*(1), 1-25. doi: 10.1080/01639620701876577

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.

Jennings, W. G., Higgins, G. E., Tewksbury, R., Gover, A. R., & Piquero, A. R. (2010). A longitudinal assessment of the victim-offender overlap. *Journal of Interpersonal Violence*, *25*(12), 2147-2174. doi: 10.1177/0886260509354888

Jian, J., Chen, S., Luo, X., Lee, T., & Yu, X. (2020). Organized Cyber-Racketeering: Exploring the Role of Internet Technology in Organized Cybercrime Syndicates Using a Grounded Theory Approach. *IEEE Transactions on Engineering Management*. doi: 10.1109/TEM.2020.3002784

Jones, A., & Bugge, C. (2006). Improving understanding and rigour through triangulation: an exemplar based on patient participation in interaction. *Journal of advanced nursing*, *55*(5), 612-621. doi: 10.1111/j.1365-2648.2006.03953.x

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social science computer review*, *30*(4), 470-486. doi: 10.1177/0894439311422689

Kirda, E., & Kruegel, C. (2006). Protecting users against phishing attacks. *The Computer Journal*, *49*(5), 554-561. doi: 10.1093/comjnl/bxh169

Konradt, C., Schilling, A., & Werners, B. (2016). Phishing: An economic analysis of cybercrime perpetrators. *Computers &*

Security, *58*, 39-46. doi: 10.1016/j.cose.2015.12.001

Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, *3*(1), 9. doi: 10.1186/s40163-014-0009-y

Laszka, A., Johnson, B., Schöttle, P., Grossklags, J., & Böhme, R. (2013). Managing the Weakest Link. In *Computer Security–ESORICS 2013* (pp. 273-290). Springer. doi: 10.1007/978-3-642-40203-6_16

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263-280. doi: 10.1080/01639625.2015.1012409

Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime*, *14*(1), 52-60. doi: 10.1080/17440572.2012.759508

Marcum, C. D., Higgins, G. E., Freiburger, T. L., & Ricketts, M. L. (2014). Exploration of the cyberbullying victim/offender overlap by sex. *American Journal of Criminal Justice*, *39*(3), 538-548. doi: 10.1007/s12103-013-9217-3

McManus, S. (2011). Hope, fear, and the politics of affective agency. *Theory & Event*, *14*(4). doi: 10.1353/tae.2011.0060

Okoye, E. I., & Gbegi, D. (2013). Forensic accounting: A tool for fraud detection and prevention in the public sector.(A study of selected ministries in Kogi state). *Okoye, EI & Gbegi, DO (2013). Forensic Accounting: A Tool for Fraud Detection and Prevention in the Public Sector.(A Study of Selected Ministries in Kogi State). International Journal of Academic Research in Business and Social Sciences*, *3*(3), 1-19.

Petty, R. E., & Briñol, P. (2015). Emotion and persuasion: Cognitive and meta-cognitive processes impact attitudes. *Cognition and Emotion*, *29*(1), 1-26. doi: 10.1080/02699931.2014.967183

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216-238. doi: 10.1177/0022427811425539

Reyns, B. W. (2015). A routine activity perspective on online victimisation. *Journal of Financial Crime*, *22*(4), 396-411. doi: 10.1108/JFC-06-2014-0030

Robinson, M. B. (1999). Lifestyles, routine activities, and residential burglary victimization. *Journal of Crime and Justice*, *22*(1), 27-56. doi: 10.1080/0735648X.1999.9721081

Sarno, D. M., Lewis, J. E., Bohil, C. J., & Neider, M. B. (2019). Which Phish Is on the Hook? Phishing Vulnerability for Older Versus Younger Adults. *Human factors*. doi: 10.1177/0018720819855570

Shelley, L. I. (2003). Organized crime, terrorism and cybercrime. *Security sector reform: Institutions, society and good governance*, 303-312.

Smith, R. (2009). Understanding entrepreneurial behaviour in organized criminals. *Journal of Enterprising Communities: People and Places in the Global Economy*. doi: 10.1108/17506200910982019

Sood, A. K., & Enbody, R. J. (2013). Crimeware-as-a-service—a survey of commoditized crimeware in the underground market. *International journal of critical infrastructure protection*, *6*(1), 28-38. doi: 10.1016/j.ijcip.2013.01.002

Tewksbury, R., & Mustaine, E. E. (2003). College students' lifestyles and self-protective behaviors: Further considerations of the guardianship concept in routine activity theory. *Criminal Justice and Behavior*, *30*(3), 302-327. doi: 10.1177/0093854803030003003

Van Wegberg, R., Tajalizadehkhoob, S., Soska, K., Akyazi, U., Ganan, C. H., Klievink, B., Christin, N., & Van Eeten, M. (2018). Plug and prey? Measuring the commoditization of cybercrime via online anonymous markets. 27th USENIX Security Symposium, 15-17 August, 2018, Baltimore, MD, USA.

Watson, M. (2005). Environmental crime in the United Kingdom. *Eur. Envtl. L. Rev.*, *14*, 186.

Wehinger, F. (2011). The Dark Net: Self-regulation dynamics of illegal online markets for identities and related services. 2011 European Intelligence and Security Informatics Conference, September 12-14, 2011, Athens, Greece. doi: 10.1109/EISIC.2011.54

Weulen Kranenbarg, M., Holt, T. J., & van Gelder, J.-L. (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior*, *40*(1), 40-55. doi: 10.1080/01639625.2017.1411030

Yar, M. (2005). The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407-427. doi: 10.1177/147737080556056

Yip, M., Shadbolt, N., Tiropanis, T., & Webber, C. (2012). The digital underground economy: A social network approach to understanding cybercrime.

Appendix A:

From: U.S Treasury [redacted]
Sent: [redacted] March [redacted], 2020 [redacted]
To: Recipients [redacted]
Subject: COVID-19 Funds Release Update.

New information is being released by The U.S. Treasury About The global funds release Programe, initiated by the world health organization (W.H.O) and empowered by The World bank Organisation.

Your are among the First Email ID batch list to receive payment $450.000.00 on this exercise,the purpose for these funds is to give relief to the global citizens of the world, due to corona virus pandemic which is the reason the world bank decided to carry out this exercise of empowerment to humanity globally.

You are Assigned to a Senior supervisor Agent who will handle your filing and also monitor the processing of your funds release.He also will be responsible to give our office report about your empowerment funds usage.

We plan to create a world where every one becomes financially independent,stable and individual accountability. You are to reconfirm your details below for immediate payment filing.

Full Name :
Address:
City / Country:
Profession:
Phone Number:
Gender:
Birth Date:
Identification

Sincerely
U.S Treasury Headquarters.
Treasury Building 1500 Pennsylvania Avenue,
NW Washington, D.C.,
United States Of America.

Figure 1. Phishing Email Example

Appendix B:

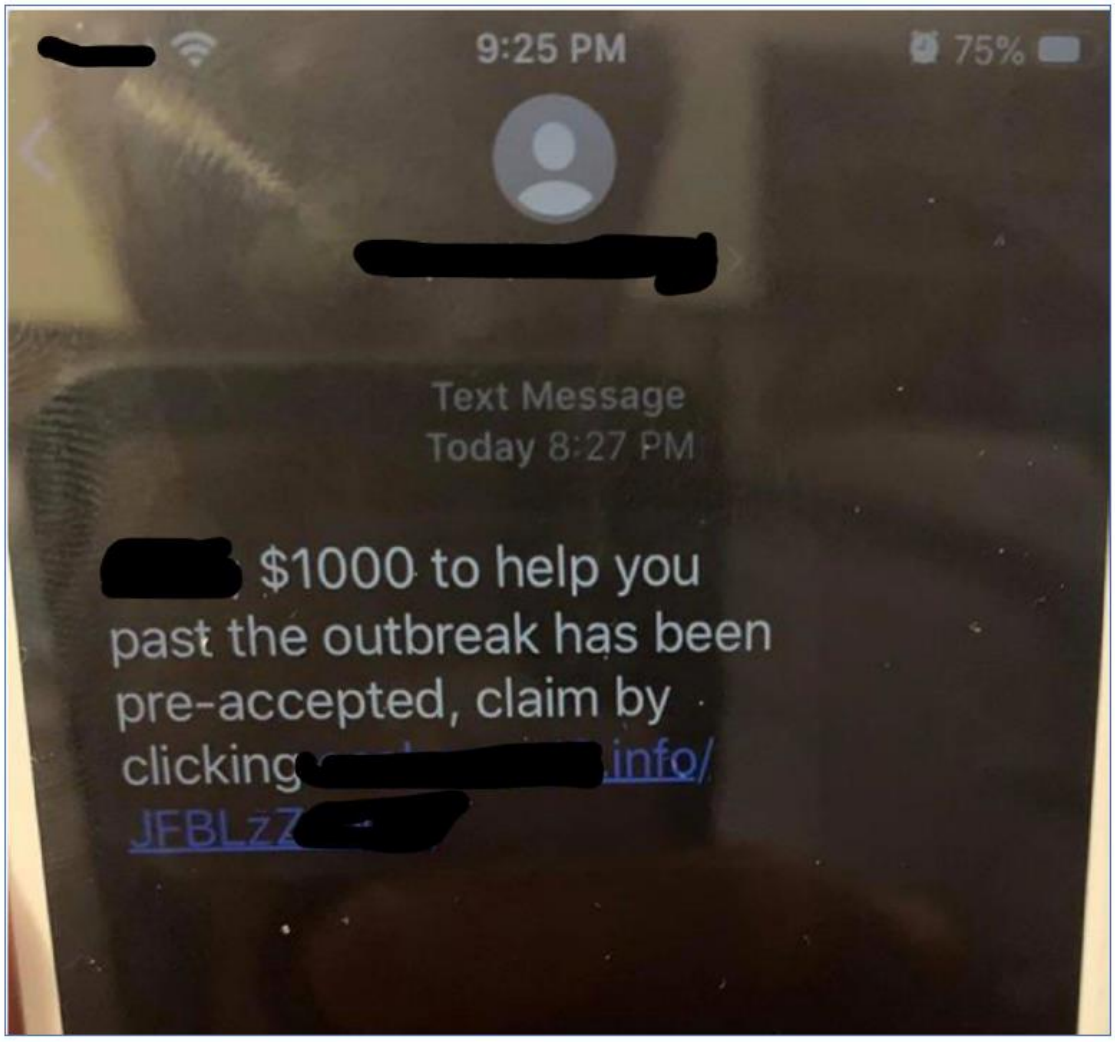

Figure 2. Text Message Example 1

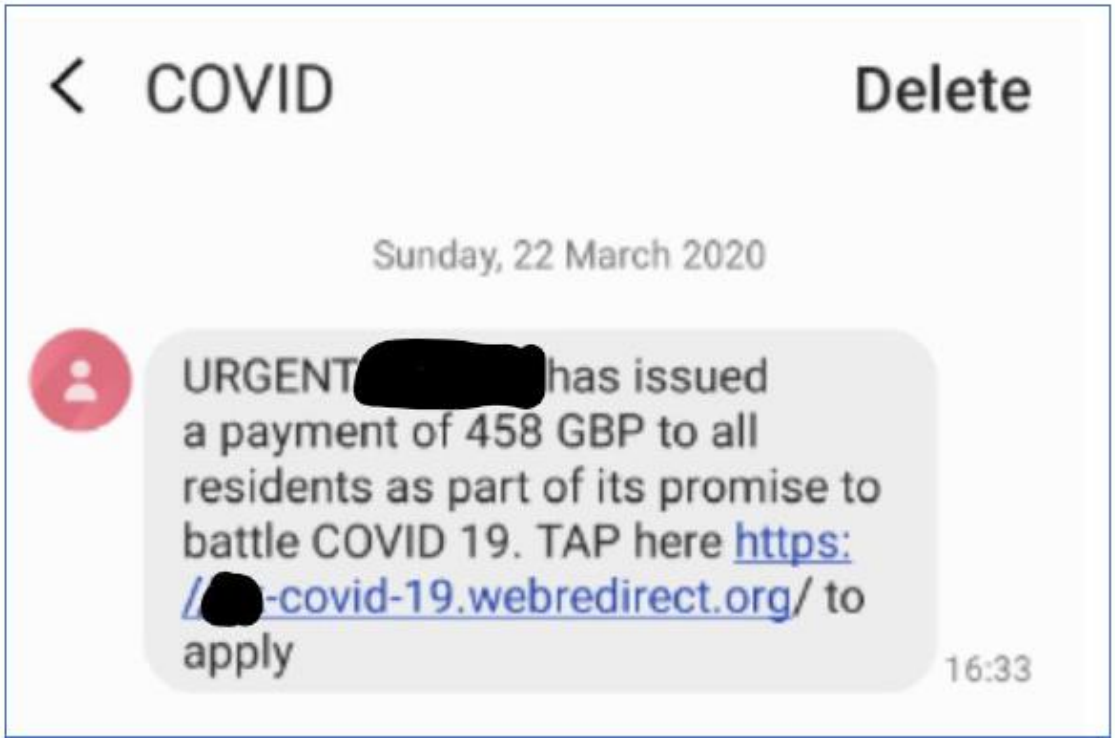

Figure 3. Text Message Example 2

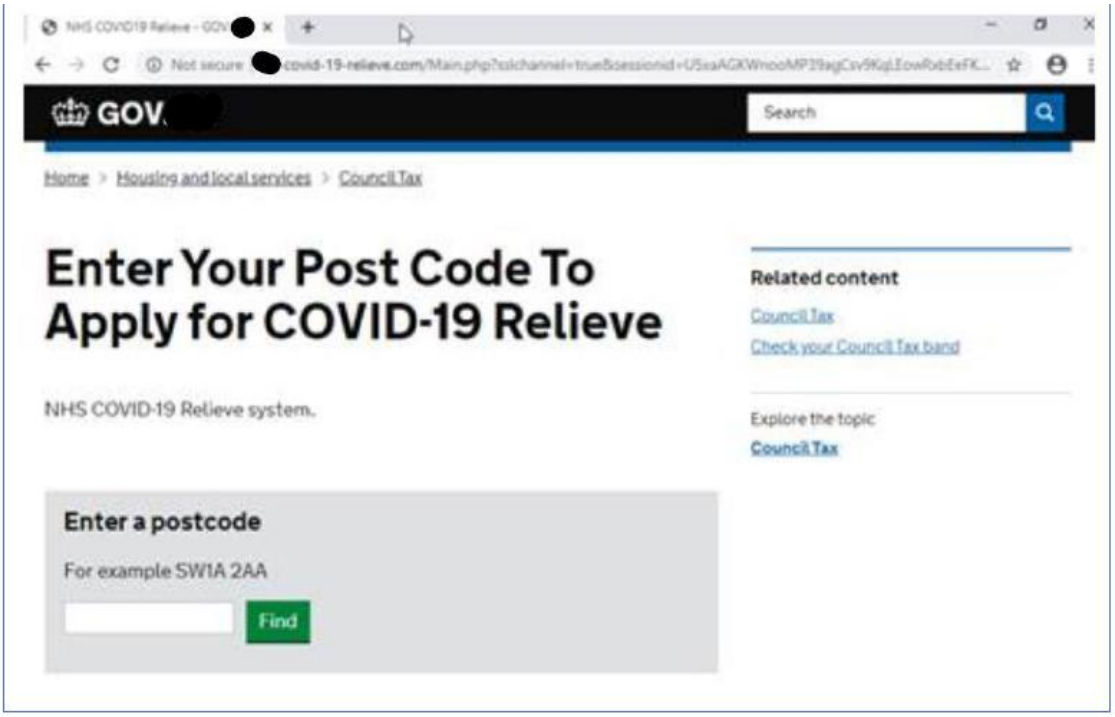

Figure 4. Spoofed Website Example

Appendix C:

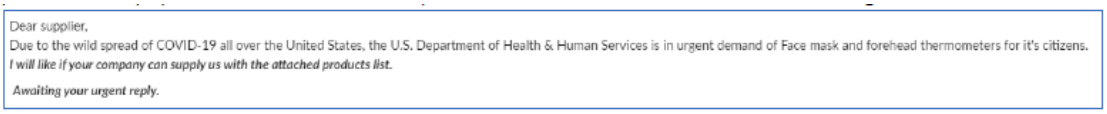
Dear supplier,
Due to the wild spread of COVID-19 all over the United States, the U.S. Department of Health & Human Services is in urgent demand of Face mask and forehead thermometers for it's citizens.
I will like if your company can supply us with the attached products list.
Awaiting your urgent reply.

Figure 5. Supply Chain Phising Email Example