COVID-19 PANDEMIC AND CYBERCRIME: INSIGHTS FROM PRACTITIONERS

Emmanuel Owusu-Oware; E-mail: emmanuel.owusu-oware@upsamail.edu.gh, Godfred Koi-Akrofi, Chris Quist & Selasi Ocansey, University of Professional Studies, Accra

ABSTRACT

The scare of the COVID-19 pandemic in the early stages and subsequent lockdowns by countries worldwide caused many business organisations to shut down their operations. To mitigate the effects of the ensuing socioeconomic hardships, businesses resorted to work-from-home and online digital interactions. However, as economic activities migrated online, criminals followed suit. This study employs qualitative research methodology and the combined theories of rational choice and general deterrence to explore the relationship between online activities during COVID-19 and cybercrime. The findings from this study show that COVID-19 norms increased and deepened the social circumstances that cybercriminals exploit to engage in their nefarious acts. These circumstances include stay-at-home, charity, global attention, known authorities, urgency, system vulnerabilities, lack of cybersecurity awareness training, and lack of qualified cybersecurity professionals. The study has implications for cybersecurity practices for business organisations and research.

KEY WORDS: COVID-19, cybercrime, cybersecurity, qualitative study

1. INTRODUCTION

The onset of the COVID-19 pandemic and the subsequent lockdowns by many countries to curb the spread of the virus forced businesses to work from home, aided by digital technologies. However, as business activities migrated online, criminals joined, creating a surge in cybercrime (Savić, 2020). Cybercrime refers to illegal computer-mediated activities that often occur through a network of computers (Srivastava et al., 2020), typically the internet. Recent reports in cybercrime indicate growth in severity, with the prediction of loss of $6 trillion by end of 2021, an increase of $3 trillion from 2015 (Herjavic Group, 2020). Yet a recent survey revealed that only 30% of business organisations surveyed have clearly defined cybersecurity policies (Srivastava et al., 2020). There is, therefore, the need for researchers and businesses to give more attention to cybercrime, especially under COVID-19 conditions, with evidence showing that cybercrime threats have increased five-folds (Williams et al., 2020).

This study, therefore, seeks to explore the relationship between online activities during COVID-19 and cybercrime from practitioner perspectives to inform cybersecurity policies and practices. The study is motivated by the objective of raising awareness about cybercrime to help reduce its adverse impact on businesses and society in general. Accordingly, this research engaged three experts in the fields of cybercrime and cybersecurity through a webinar to gain insights into the phenomenon. Insights gained from the experts were then analysed using theories in criminology.

The research questions guiding this study are:

- How have online activities during COVID-19 pandemic shaped cybercrime within the business environment?
- What cybersecurity measures are being employed to curb the challenges of cyber threats and attacks?

To answer these research questions, the study employed qualitative research methodology (Myers, 2013) and the combined theories of rational choice (Cornish & Clarke, 1987) and general deterrence (Silberman, 1976).

The remaining part of this paper is organised as follows. Section 2 reviews the literature on cybercrime, its relation to COVID-19 as well as theories on cybercrime. Section 3 presents the qualitative research methodology for this study. Section 4 presents the study's findings. Section 5 analyses and discusses the findings, while Section 6 concludes the study with recommendations on cybersecurity at the individual, organisational and government levels. Future research areas and the study's limitations are also presented in the concluding section.

2. LITERATURE REVIEW

2.1 Cybercrime

Cybercrime refers to criminal offences committed on the Internet, such as slander, threat of violence, identity theft, fraud, or sexual harassment (Mikkola et al., 2020). The upsurge in cybercrime in recent times, and the loss of many businesses and investments, can be attributed to increase in internet traffic (Wiggen, 2020). With the increasing use of digital technologies, many socio-economic activities and, inappropriately, crime have shifted online (Hiscox, 2021; Srivastava et al., 2020). Analysis and research show that cybercrime is here to stay due to its lucrative and low-risk level (McGuire, 2018). Research indicates that cybercrime causes financial losses in the billions of dollars annually on a global scale, affecting millions of individuals as victims (Mikkola et al., 2020). Factors that create opportunities for cybercriminals include panic, distraction, time constraints, work pressure, situational changes, medical and home-based e-work (Kshetri, 2019; Nurse, 2018). These factors cause people to be susceptible to deception because of uncertainties, anxieties, and pressure, which lead to mistakes.

Cybersecurity is defined as "technologies and processes used to protect computers, hardware, technology devices, software, networks, and data from unauthorised access and vulnerabilities" (Neo et al., 2021, p. 55). Information system resources include data, networks, servers, and end-user computer systems. Cybersecurity policies include raising user awareness of scams (Naidoo, 2020), updating passwords and security software, using firewalls, backing up systems and data, and using surge protectors. Other policy measures include maintaining access controls, implementing redundant systems, and using system activity and intrusion detection monitors (Workman et al., 2009). Cybersecurity technologies include firewalls, intrusion detection systems, anti-viruses, anti-spam, and anti-spyware malware (Naidoo, 2020; Srivastava et al., 2020). The changing nature of cybercrimes poses challenges to cybersecurity (Srivastava et al., 2020; Workman et al., 2009). Therefore, cybersecurity policies and technologies require regular updates in step with changing trends.

2.2. COVID-19 and Cybercrime

The COVID-19 pandemic brought about enormous disruptions around the world, with new realities ("new normal") such as working from home and a reduction in social interactions and physical activities (NHS UK, 2020). The increase in digital interactions over the internet due to COVID-19 norms has resulted in significant increase in scams and malware attacks (Gallagher & Brandt, 2020), with phishing claimed to have surged by 600% in March 2020 (Shi, 2020). To boost their chances of succeeding, cybercriminals target high-demand commodities, such as personal protective equipment (PPE), coronavirus testing kits and medications, potentially lucrative investments in COVID-19 related stocks, and impersonations of companies' representatives. Brute force attacks on Microsoft Remote Desktop Protocol (RDP) systems have also increased (Galov, 2020), indicating that attacks are also on technology. It is evident that cybercriminals are taking advantage of the pandemic's disruption within the business environment.

3. 3 Cybercrime Theories

Various theories have been advanced to understand general crime in the social context. Since the motives behind cybercrime are similar to general crime, these theories can be applied to cybercrime, though its context is unique (Srivastava et al., 2020). The frequently used theories of general crime are rational choice theory (RCT) and general deterrence theory (GDT).

RCT posits that an individual will act based on the associated opportunities, costs, and benefits (Cornish & Clarke, 1987). If the benefits are seen to be more than the cost, then the individual will act. Applying rational choice theory to cybercrime suggests that cybercriminals are likely to exploit a surge in online activity because they perceive it as a convenient and low-cost opportunity for defrauding their targets. GDT, on the other hand, considers deterrence as the discouragement of criminal activity by the threat of punishment, whether implicit or explicit (Silberman, 1976). When applying GDT to cybercrime, the underlying idea is that cybercriminals attack their targets because they believe that the chances of being apprehended and facing consequences are extremely slim. Srivastava (2020) applied RCT and GDT to explain factors that affect cybercrime by testing the influence of three broad category factors, namely economic capital, technological capital, and cybersecurity preparedness. In this study, we use the two theories as sensitising devices (Klein & Myers, 1999), that is, not to test but to understand the relationship between online activities during COVID-19 and cybercrime. In the case of GDT, the assumption is that cybercriminals will attack their targets, knowing that the possibility of being caught and punished is negligible.

3. METHODOLOGY

This study draws on qualitative research approach (Myers, 2013) to gain in-depth understanding of the phenomenon from the perspectives of experts in the field. Following purposive sampling (Patton, 2005) and focus group data collection method (Eigner et al., 2017) three cybersecurity and cyberforensic experts were invited as the panellists on a webinar organised by the authors' university on 17th March 2021. The purpose of the webinar was to raise awareness on the relationship between COVID-19 pandemic and cybercrime and how governments, business organisations and the industry are responding to the increased cybercrime threats as a result of COVID-19 norms.

The three panellists were purposively selected to represent three perspectives on the subject, namely, industry, government, and corporate organisation. The profile of each panellist is shown in Table 1.

Table 1 – Brief Profile of Panellists

Panellists	Brief Profile
Panellist 1	• A PhD holder and 20+ years of professional experience • chief operating officer of an international cybersecurity company and founder of a training academy in cybersecurity in the United States of America (USA). • Cybersecurity professional qualifications include CISSP, Security+, Cybersecurity Analyst (CySA+), Pentest+, AWS Cloud Practitioner, Security Analytics Professional (CSAP), Security Network Professional (CNSP), Network Vulnerability Assessment (NVA). • Cybersecurity consultant • A skilled ethical hacker
Panellist 2	• A PhD holder and 20+ years of professional experience • A cybersecurity advisor at the national level and playing a key role at the national cyber security centre in Ghana • Founder of a digital forensics company that operates in West Africa • Cybersecurity consultant who has consulted with international and local organisations, including Interpol, UN, European Commission, and Commonwealth
Panellist 3	• 20+ years of professional experience and a MSc holder • A chief technology security officer at a multinational telecommunications company in Ghana • Consultant in information systems security audits and assurance, and digital forensic investigation

The panellists responded to questions on the subject asked by the webinar's moderator, who was one of the authors of this study. The following questions were posed to the panellists:

1. Can you share your perspectives on cybercrime concerning the methods, technologies that these criminals employ, what they do, and the effects?
2. Would you say there has been an increase in cybercrime across the world as a result of an increase in online transactions due to the social distance requirement of COVID-19? Please share any evidence you have concerning the surge in cybercrime
3. What policies, strategies, and technologies are available to combat the threat of cybercrime at the individual, organisation, and country levels?

Further questions were also asked of the panellists by the webinar participants. The responses by the panellists were recorded as part of the webinar's proceedings. The recordings were then transcribed.

Data analysis was data- and theory-driven. The data-driven analysis involved reading transcribed material several times to identify themes (Braun & Clarke, 2006). The theory-driven analysis involved using the principles and concepts of RCT and GDT theories (see Section 3.3) to analyse the relationship between online activitites (induced by COVID-19) and cybercrime. With RCT, it is anticipated that cybercriminals will find it easy and less costly to take advantage of the increase in online activity to defraud their victims. In the case of GDT, the assumption is that cybercriminals will attack their targets, knowing that the possibility of being caught and punished is negligible.

4. FINDINGS

In this section, we present the panellists' insights on the phenomena of cybercrime and cybersecurity, arising from COVID-19 pandemic. The panellists' responses have been organised into three sections: 1) cybercrime, methods, and technologies; 2) COVID-19 induced cybercrime and effects; 3) cybersecurity under COVID-19.

4.1 Cybercrime, Methods, and Technologies

The panellists were asked to share their perspectives on what constitutes cybercrime, the methods and technologies used by criminals to attack their victims. In their responses, the panellists explained the key concepts, namely ***cybercrime, social engineering,*** and ***phishing***.

Cybercrime is crime that involves use of computers, phones, and electronic devices. Cybercriminals employ *social engineering,* which is the exploitation of social circumstances to psychologically manipulate people into performing actions or disclosing confidential information. Social engineering is the most used method of cybercrime.

> Social engineering is a very popular, common, and effective cybercrime method used by cybercriminals. Phishing is a common form of social engineering. (panellist 1)

Phishing is the practice of using unsolicited communications such as email, short message service (SMS) or phone to scam a person into doing something he or she will not do. A cybercriminal scams people by using "fake identities based on email addresses, domain and websites that mirror recognised entities such as governments, international bodies and organisations" (panellist 1). Typically, the target is enticed to click on links or download attachments sent through email.

The panellists described phishing types, indicating that they predate Covid-19.).
The phishing types reflect the different channels cybercriminals use to send unsolicited content and the target groups. The phishing types are

- email phishing (use of electronic mail),
- smishing (use of short message service),
- vishing (use of voice/phone),

- spear-phishing (targeting a specific group), and
- whaling (targeting CEOs /top management).

For instance, smishing is sending unsolicited SMS messages. Vishing is by voice, currently used by most mobile money scammers. The phishing types indicate that a cyber target can be an individual, organisation and even a country. In emphasising that no one is immune to phishing attacks, one panellist cited a recent attack on the United States government.

> …the United States government was hacked almost about 2 months ago. And these attackers were in their systems almost 6 months before they were detected.

4.2 COVID-19 and cybercrime

Panellists were asked to speak on the effect of COVID-19 norms on cybercrime and provide evidence of any increase in cybercrime. Panellists noted that COVID-19 is unique because many countries were under lockdown and social distancing rules required many to stay home.

> During the early stages of COVID-19, there was confusion and fear due to lack of information about the virus. The lockdown, social distancing, and ban on social gatherings created a lot of idle time for everyone. So, governments, businesses, churches, and schools moved their activities online. Guess who also moved online? Criminals! The more virtual you go, the more cyber risks there are (panellist 1).

Thus, the COVID-19 norms of social and physical distancing provided many social circumstances that cybercriminals exploited. The panellists enumerated some of the social circumstances that COVID-19 created for scammers. These circumstances are interrelated and include stay-at-home, personal gain, charity, global attention, known authorities, urgency, system vulnerabilities, lack of cybersecurity awareness training, and lack of qualified cybersecurity professionals.

The COVID-19 *stay-at-home* directive by governments created more cyber targets as many individuals and organisations moved online for social and economic reasons. *Personal gain* is when a victim is enticed with a financial reward. *Charity* is where the scammer appeals to the target's generosity in combating disasters. COVID-19 provided many such opportunities because of the global attention in fighting the virus. As a result, cybercriminals impersonate *known authorities* (or organisations) such as the UN and WHO to scam their victims. They leverage on *urgency*, that is, fear of a situation, to demand urgency from their targets. They also identify vulnerable targets; these include unsecured organisational networks (e.g., those without robust firewalls and authentication systems) and persons who lack cybersecurity awareness training. Also, the general lack of qualified cybersecurity professionals throughout the world is an indication of an exposed world to cyber-attacks. According to panellist 1, there were about 3.1 million unfilled cybersecurity jobs around the world, projected to reach 3.5 million by the end of 2021.

All panellists noted that COVID-19 has provided much space for cybercriminals to operate. With COVID-19, many of the phishing types (i.e., channels) were being exploited – that is, email, phone, SMS and social media. According to panellist 1, the latest threats that came with COVID-19 were: malicious domains, i.e., registered domains on the internet that contain the terms "coronavirus", "corona-virus", "covid19" and "covid-19"; online scams and phishing, data-harvesting malware, disruptive malware (ransomware and DDoS) and vulnerability of working from home.

Concerning the impact of cybercrime during COVID-19, panellists shared their experiences. According to panellist 2, reports received at the national cybersecurity centre revealed all kinds of crime including identity fraud, recruitment fraud, blackmail, and sexual offence:

> There has been increase in use of social media in view of COVID-19, we have a lot of fraudsters engaging on that platform. A lot of people have been scammed. Recruitment fraud is one of the major reported cases of COVID-19 related phishing attacks. There have also been incidence reports of sexual offences in terms of nude pictures being taken and posted on social media and other platforms, people making contacts on WhatsApp they don't know. Sexual offences are the second most reported cases in the centre.

At the organisational level, panellist 3 shared his experience in the corporate world:

> Within the first two months when everybody had to work from home we saw 100%-fold increase in phishing attacks, scamming alerts on the network …… so a lot of people used covid as the agenda to get into people's network, and their personal lives.". That's why we saw a lot of phishing attacks related to covid.

Citing some online reports, panellist 1 gave a global view of the impact of COVID-19 on cybercrime which showed an upsurge in cybercrime:

1. Interpol (2020) January to April, 2020: some 907,000 spam messages, 737 incidents related to malware and 48,000 malicious URLs all related to COVID-19 were detected.
2. FBI (2021): Internet Crime Complaint Centre (IC3) of the FBI recorded a 300% increase in the daily reported cases of cybercrime since the onset of the COVID-19 pandemic, surging from the pre-COVID-19 daily reports of about 1000 to between 3000 and 4000 during the pandemic (Federal Bureau of Investigation (FBI), 2020)
3. Tidy (2020): A BBC online news report that according to Google scammers are sending 18 million hoax emails about COVID-19 to Gmail users every day. In addition, Google was blocking 100 million phishing emails daily.
4. KPMG Ghana (2021): Organised crime mounted large scale campaigns to defraud banking customers, preying on fear and anxiety related to Covid-19.

Panellists concluded that cybercrime would continue to evolve to take advantage of online and social behaviour and trends.

4. 3 Cybersecurity under COVID-19

The panellists were asked to discuss policies, strategies, and technologies used to combat the threat of cybercrime at the individual, organisation, and country levels. One panellist defined cybersecurity as the practice of protecting digital assets from criminals or unauthorised use.

Panellists agreed that cybersecurity, whether at the organisational or national level, starts with the individual. "If individuals can avoid being scammed, then cybercrime could be stopped" (panellist 3)". Cybersecurity measures were identified as largely behavioural. At the individual level, panellists stressed vigilance as the key to stopping cybercrime. Vigilance implies the state of being suspicious of electronic communications. A vigilant person will not:

1) click links of unknown source;
2) entertain unsolicited email, phone call, SMS and social media post;
3) call the official source or known person to verify a communication;
4) keep his or her personal data safe by not sharing password and backing up important files;
5) perform software updates to keep his or her device with the latest version of software.

Panellist 1 stated that individuals and organisations can avoid being scammed by systematically addressing the social circumstances mentioned above that criminals exploit as opportunities under COVID-19. For instance, to deal with lack of cybersecurity awareness training, panellist 1 advised that organisations should organise periodic cybersecurity awareness training for employees. Panellist 3 emphasised cybersecurity awareness programme and equipping employees with secured mobile computing systems at the organisational level.

> A robust security awareness programme can stop a lot of phishing attacks. Because the more people are aware, the more they stop clicking on these things... So awareness reduce your threat levels.
>
> … equipping staff with a corporate laptop that is well secured using VPN connectivity. With that there is no way you can get into our environment…also blocking all the ports on the laptop so you cannot use a flash drive…. You get to use a specially encrypted flash drives which we whitelist for you if you need to use it.

Panellist 2 stressed that cybersecurity should be seen as an ecosystem where intra- and inter-cooperation is needed. “A chain is as strong as its weakest link”, panellist 2 remarked. Accordingly, panellist 2 described happenings at the national level in Ghana. He explained that cybersecurity at the national level is essentially about enabling interventions at all levels of society. He described the national cybersecurity interventions in five thematic areas: 1) legal and policy, 2) technical, 3) organisational, 4) capacity building and 5) international cooperation.

At the legal and policy level, Ghana enacted a cybersecurity ACT in December, 2020 (Cybersecurity Act 2020 (Act 1038)). The national cybersecurity policy and strategy have also been revised. The ACT establishes the Cyber Security Authority, protects the critical information infrastructure of the country, regulates cybersecurity activities, provides for the protection of children on the internet and develops Ghana’s cybersecurity ecosystem. The technical component of the ACT involves protection of critical national information infrastructure, establishing national cybersecurity centre and incident reporting points of contact across the country. The organisational aspect involves bringing together players within the cybersecurity ecosystem of the country to identify and implement cybersecurity initiatives. Capacity building concerns training programs for public sector workers. Finally, international cooperation affords cooperation through conventions such as the African Union Convention on Cyber Security, Personal Data Protection (Malabo Convention), Convention on Cybercrime (Budapest Convention) and countries’ judicial authorities.

5. Analysis and Discussion

This section uses the theories of RCT and GDT to analyse the practitioners’ perspectives on the relationship between COVID-19 pandemic, cybercrime, and cybersecurity presented in Section 4. Following the analysis, we discuss the findings in relation to the research questions.

RCT suggests that people commit crime when there are opportunities to do so, and the benefits can be gained with little effort or least cost. From the panellists’ submissions and literature, during the COVID-19 era, cybercrime shot up. By RCT logic, COVID-19 norms presented many opportunities which were easy to exploit by cybercriminals. The RCT logic is supported by the study’s findings, which show that the COVID-19 era offered several social circumstances as opportunities for cybercriminals. For instance, the stay-at-home directive by governments and the new normal of digital interactions (as opposed to physical interactions) increased internet traffic (Gallagher & Brandt, 2020). Thus, COVID-19 was a catalyst for internet traffic growth, creating more cybercrime opportunities (Williams et al., 2020).

GDT posits that threat of punishment, directly or indirectly, is a disincentive to committing crime. The study’s findings show that in the COVID-19 era, the threat of punishment or the possibility of being caught is minimal or nonexistent. The possibility of being caught is low because scammers use fake identities or impersonation, as the study’s findings show. The use of fake identities and impersonation is not exclusive to the COVID-19 era. However, the many phishing channels and increase in traffic during the pandemic are factors that the criminal mind will consider worthwhile. Moreover, punishment of cybercriminals is uncommon. The low-risk level and lucrative nature of cybercrime (McGuire, 2018) should therefore be of great concern to business organisations.

From the foregoing, it is evident that COVID-19 pandemic restrictions presented cybercrime opportunities as many businesses and individuals were forced to engage in online activities. While working from home is not unique to the COVID-19 era, online activities shot up significantly under the pandemic. Some estimates on internet service usage indicate increase from 40 to 100% (De' et al., 2020). It is said that criminals go where people are congregated. Again, with lack of cybersecurity awareness training, COVID-19 increased the population of people who lacked awareness of cybercrime, as evidenced by the study's findings.

With respect to cybersecurity, the study's findings show that the measures are mainly policy, strategy, and behavioural-based at the individual, organisational and national levels. Vigilance at the individual level has been stressed, while at the organisational level, awareness training programmes. At the national level, enabling policy interventions at all levels have been advocated. From the RCT perspective, cybersecurity measures decrease vulnerabilities technically and socially and therefore make the channels of cyber-attacks less effective. As one of the panellists stressed, individual vigilance, such as not clicking links from unknown sources, can stop criminals. From the GDT perspective, cybersecurity measures can be used to increase the possibility of catching criminals as pertains to cyber forensics and biometric systems – these are areas worth exploring within the context of COVID-19.

6. Conclusion.

This study explored the relationship between online activities during COVID-19 and cybercrime from practitioner perspective. The key finding of the study is that the significant increase in cybercrimes under COVID-19 era is the result of the substantial increase in digital interactions, leading to increase in crime opportunities at the individual and organisation levels. Under COVID-19 era, the cybercrime opportunities identified in the study as social circumstances that cybercriminals exploit, include stay-at-home, charity, global attention, known authorities, urgency, network vulnerabilities, lack of cybersecurity awareness training, and lack of qualified cybersecurity professionals. These opportunities are themselves the basis for strengthening cybersecurity policies and systems.

This study's practitioner's perspective has also emphasised the interrelatedness of cybercrime and cybersecurity at the individual, organisation, and national levels. With increase in internet traffic under COVID-19 norms, vigilance, awareness and enabling interventions at the individual, organisation, and national levels, respectively, have been emphasised by the practitioners. For business organisations, the implication is that cybersecurity policies should be exhaustive in covering these levels.

6. 1 Summary of Recommendations:

From the analysis of the findings, the paper makes the following recommendations:

Individuals: Should exercise vigilance in all forms of electronic communications. Individuals are admonished to be careful of personal information put out on social media, as attackers can use such information to impersonate and profile them for future cyber-attacks
Businesses/ Organisations: Establish a programme of awareness and sensitisation on cybercrime and cybersecurity periodically throughout the year; continually monitor and review system security. Organisations should invest heavily in cybersecurity training of employees and upgrade their infrastructure to prevent security breaches onsite and from remote connections.

Government: Should sustain the enabling interventions and work with the private sector to establish a robust cybersecurity ecosystem. Governments should enact/review laws on cybercrime and cybersecurity, promote public awareness and education, and, together with private entities institutionalise comprehensive cybersecurity training and education to produce qualified cybersecurity professionals as well as maintain a well-resourced National Cybersecurity Centre.

6. 2 Implications for Research

For research, this study serves as one response to the call to information systems scholars to bridge the gap between practice and research (Taylor et al., 2012). This study provides insights into cybercrime and cybersecurity under COVID-19 norms from practitioner perspective and a theoretical basis using RCT and GDT to understand the phenomenon. For subsequent studies, researchers can consider building on the combined theories of RCT and GDT to develop a framework for understanding disasters, cybercrime, and cybersecurity. Another area worth exploring is the use of cyber forensics and biometric systems to combat cybercrime within the context of COVID-19.

6.3 Limitation of study

The study findings are limited by the three panellists' perspectives on the relationship between COVID-19 pandemic, cybercrime, and cybersecurity. However, the theoretical understanding of the relationship can be generalised.

REFERENCES

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Psychiatric Quarterly*, *3*(2), 77–101.

Cornish, D. B., & Clarke, R. V. (1987). Understanding Crime Displacement: An Application of Rational Choice Theory. *Criminology*, *25*(4), 933. https://doi.org/doi:10.1111/j.1745-9125.1987.tb00826.x

De', R., Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International Journal of Information Management*, *55*(June), 102171.

Eigner, I., Hamper, A., Wickramasinghe, N., & Bodendorf, F. (2017). Decision Makers and Criteria for Patient Discharge - A Qualitative Study. *BLED 2017 Proceedings*, 41.

FBI. (2021). *Internet Crime Complaint Center 2020 Internet Crime Report*. https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics

Gallagher, S., & Brandt, A. (2020). *Facing down the myriad threats tied to COVID-19*. https://news.sophos.com/en-us/2020/04/14/covidmalware/

Galov, D. (2020). *Remote spring: the rise of RDP bruteforce attacks*. https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/

Herjavic Group. (2020). *The 2020 Official Annual Cybercrime Report*. https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/#:~:text=According to the 2020 Official,the biggest problems with mankind

Hiscox. (2021). *Hiscox Cyber Readiness report*. https://www.hiscox.co.uk/cyberreadiness

Interpol. (2020). *COVID-19 Cybercrime Analysis Report*.

Klein, H. K., & Myers, M. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*, *23*(1), 67–94.

KPMG Ghana. (2021). *COVID-19 frauds and scams*. https://home.kpmg/gh/en/home/insights/2020/04/covid-19-frauds-and-scams.html

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77–81.

McGuire, M. (2018). Understanding the growth of the cybercrime economy. *RSA Conference, USA, 2018*.

Mikkola, M., Oksanen, A., Kaakinen, M., Miller, B. L., Savolainen, I., Sirola, A., & Paek, H. J. (2020). Situational and individual risk factors for cybercrime victimization in a cross-national context. *International Journal of Offender Therapy and Comparative Criminology*, *0306624X20*.

Myers, M. (2013). *Qualitative research in business & management* (N. S. Kirsty Smy (ed.); 2nd ed.). Sage Publications.

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

Neo, H. F., Teo, C. C., & Peng, C. L. (2021). Safe Internet: An Edutainment Tool for Teenagers. In *Information Science and Applications: Proceedings of ICISA 2020* (pp. 53–70). Springer.

NHS UK. (2020). *10 tips to help if you are worried about COVID-19*. https://www.nhs.uk/every-mind-matters/coronavirus/10-tips-covid-19-anxiety/

Nurse, J. R. C. (2018). Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit. In *The Oxford Handbook of Cyberpsychology* (pp. 662–690). Oxford Library of Psychology.

Patton, M. (2005). Qualitative research. In *Encyclopedia of statistics in behavioral science*. John Wiley & Sons, Ltd.

Savić, D. (2020). COVID-19 and work from home: Digital transformation of the workforce. *Grey Journal*, *16*(2), 101–104.

Shi, F. (2020). *Threat Spotlight: Coronavirus-related phishing*. https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/

Silberman, M. (1976). Toward a theory of criminal deterrence. *American Sociological Review*, *41*(3), 442–461.

Srivastava, S. K., Das, S., Udo, G. J., & Bagchi, K. (2020). Determinants of Cybercrime Originating within a Nation: A Cross-country Study. *Journal of Global Information Technology Management*, *23*(2), 112–137.

Taylor, H., Artman, E., & Woelfer, J. P. (2012). Information technology project risk management: Bridging the gap between research and practice. *Journal of Information Technology*, *27*(1), 17–34.

Tidy, J. (2020). *Google blocking 18m coronavirus scam emails every day*. Bbc.Com. https://www.bbc.com/news/technology-52319093

Wiggen, J. (2020). Impact of COVID-19 on cyber crime and state-sponsored cyber activities. In *Facts and Findings*. Konrad-Adenauer-Stiftung e. V.

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. *Journal of Medical Internet Research*, *22*(9), 7–10.

Workman, M., Bommer, W. H., & Straub, D. (2009). The amplification effects of procedural justice on a threat control model of information systems security behaviours. *Behaviour and Information Technology*, *28*(6), 563–575.