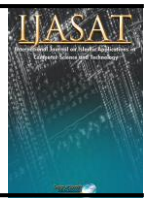


The Impact of COVID-19 Pandemic on the Rise of Cyber Security Risks with An Islamic View

Arwa M. Alromaih [1], Abdulrahman K. Abdulwahab [2], Ahmed M. Zeki [3]

[1,2,3] Department of Information Systems, College of IT, University of Bahrain, Kingdome of Bahrain
[1] 20190266@stu.uob.edu.bh, [2] 202000050@stu.uob.edu.bh, [3] amzeki@uob.edu.bh

Abstract
The COVID-19 pandemic has changed many aspects of people's behaviors, forcing them to adopt a new cautious lifestyle. These impacts include the acceleration of online services, mobile money, reduction of cash transactions, as well as the organizations shift to work from home; consequently, the related cyber-risks have increased. This paper reviews four of the most common cybersecurity risks raised during the pandemic around the world, which are phishing campaigns, financial fraud, social engineering, and the risk of employees' behavior who are working from home. This study also references some examples for some countries comparing their challenges with cybersecurity risks before and after COVID-19 such as Saudi Arabia and the United Kingdom. In addition, this research recommends some of the best practices and the greatest common countermeasures to overcome the mentioned cybersecurity risks. Besides, this paper views those issues and the proposed solutions from an Islamic perspective.

***Keywords*:** COVID-19, Cybersecurity, Phishing, Financial Fraud, Social Engineering security.

1. Introduction
Technology enhances people's lives in many aspects, but it also allows criminals to attack people through the digital world. Thus, some countries developed plans that protect the cyberspace in the country and enable the country to transfer into the digital world. For example, Saudi Arabia has the 2030 vision that involves the digital transformation starting with the critical infrastructure. However, when the COVID-19 pandemic started in 2020, many countries accelerated the digital transformation, which resulted in raising the cybersecurity risks.

The recent COVID-19 pandemic has changed many aspects of people's behaviors and ways of living, forcing them to adapt to a new conservative and cautious lifestyle. One of these impacts was the acceleration of online services in various domains, including e-commerce, online banking, online medical services, social media, news, remote working, and online learning. This paper reviews and evaluates several cybersecurity risks raised during the pandemic, including phishing campaigns, financial fraud, social engineering attacks, and risky employee behaviors. The paper also discusses the basic recommendations that can safeguard users from easy prey for hackers and phishers. Besides, the proposed solutions are aligned with Islam and Sharia value and principles which forbids cybercriminal activities.

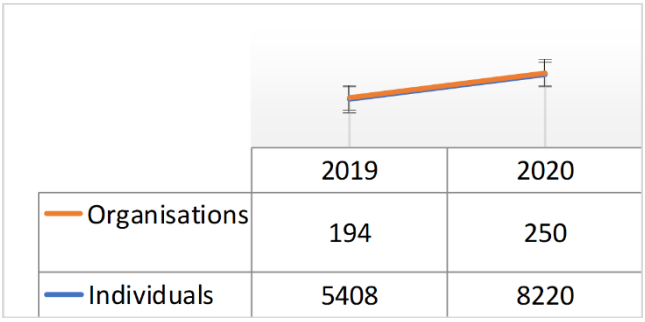
The rest of this paper is organized as follows: the second section discusses the phishing campaigns proliferated during COVID-19 pandemic including the online fraud and phishing emails. The third section discusses the COVID-19 impact on financial fraud covering the

dependency on online payment services given cybersecurity attackers' opportunity to perform financial fraud. The fourth section approaches the social engineering attacks during the pandemic that manipulated human emotions during COVID-19 lockdown. The fifth section is about the risky employee behaviors; this section will discuss the insider threats during the pandemic as the employee works remotely, which created challenges related to implementing cybersecurity controls like surveillance systems. The paper will then end with a conclusion and future remarks.

2. Phishing Campaigns During COVID-19 Pandemic

A phishing campaign is considered one of the most used cyber-attacks because of the ease of doing it from an attacker's perspective while causing significant damage within the targeted organizations. This is due to the reason that human is considered the weakest point of the cybersecurity chain. During the pandemic, there was a significant surge in phishing attacks targeting organizations (Abukari & Bankas, 2020).

Moreover, one important aspect of the lockdown was that many criminals could not perform their fraud and crimes that they used to do physically (Buil-Gil et al., 2020). Therefore, there was a shift in their crimes to be done through the cyber ecosystem. As a result, the number of traditional crimes decreased while cybercrimes were noticeably increased. For example, comparing cybersecurity attacks in the year 2019 and year 2020, there was a significant increase in online fraud in the United Kingdom (UK) due to the lockdown, refer to Figure 1 (Buil-Gil et al., 2020).



	2019	2020
Organisations	194	250
Individuals	5408	8220

Figure 1. The reported online fraud cases to UK police, including phishing email victims.

As a result of the pandemic and the devastating situation of hospitals and healthcare sectors, many spear-phishing targeting healthcare providers with subjects concerning COVID-19 or impersonating healthcare officials. Unfortunately, many incidents were confirmed as a result of that (Saudi NCA, 2020). Also, state-sponsored attacks targeting healthcare sectors in order to take advantage of the vaccine were substantial during the pandemic with the main objective of stealing the vaccine's intellectual property using phishing attacks (Curran, 2020). furthermore, based on the Saudi National Cybersecurity Authority report, 9 out of 10 COVID-19 websites are malicious due to phishing tools' availability. Additionally, the top cybersecurity threats that phishing email could be injected with malware, account hijacking, targeted attack, exploiting a vulnerability, and malicious spam, refer to Figure 2 (Saudi NCA, 2020).

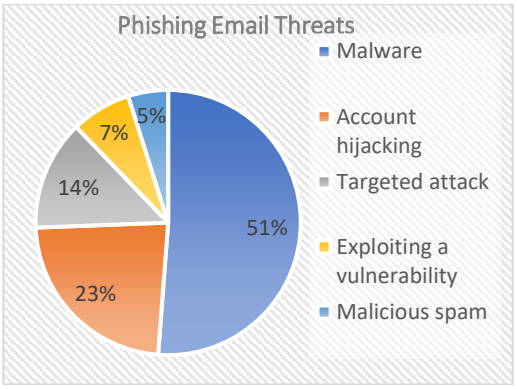


Figure 2. The top cybersecurity threats that can comes from phishing emails.

It is highly recommended to implement several security controls in order to mitigate the cybersecurity standardize it either cybersecurity or cybersecurity risks associated with phishing attacks. One of the most important security measures is to start with the human by raising employee awareness in order to identify phishing emails. Also, adequate access controls measures must be implemented. For example, multi-factor authentications must be enforced in order to add another step that lowers the probability of the risk of accounts being compromised (Hui & Yi-Ling, 2020). Finally, organizations should capitalize on continuous monitoring, detection, and resilience. This will ensure that any possible unauthorized access is detected in a timely manner, and further action is performed to contain it (Hui & Yi-Ling, 2020).

3. COVID-19 Impact on Financial Fraud

COVID-19 implications on financial transactions, online behaviors, and related cyber risks were substantial. The reduction of cash transactions and shifting to mobile money and online payments was already trending before COVID-19 (Jakhiya et al., 2020; Engert et al., 2020).

However, the pandemic has accelerated this trend significantly; this includes mobile banking, mobile payments, and mobile microfinance (Jakhiya et al., 2020). In the "Cash Alternative Survey" which was conducted in Canada in April 2020, 35% of respondents stated that they had decreased their cash usage due to reports highlighting the risk of virus transmission via cash notes (Engert et al., 2020). The percentage of already cashless Canadians increased from 10% in 2019 to 19% in 2020 (Engert et al., 2020). Similarly, Kingdom of Saudi Arabia (KSA) has an existing target to transform 70% of all payments to digital means part of the government 2030 vision; however, the transition during COVID-19 has exceeded the government's expectations and predictions, as mobile payment shares of overall Point of Sale (POS) payments jumped from 8% in Sep 2019 to 25% in Sep 2020 (Alshowmer, 2020).

2.1 Financial Fraud Trend

The accelerated trend towards digital payments and online financial transactions has also fostered financial fraud activities, which were classified under Cyber-enabled crime according to Lallie et al. (2021); this study analyzed 43 cybersecurity COVID-19-related incidents between Jan and May 2020. It was found that 34% of the attacks were categorized as financial fraud. The researchers also highlighted that most of the remaining 28 attacks' ultimate aim was most probably to achieve financial fraud too. Buil-Gil et al. studied the increase in cybercrime in the UK during the COVID-19 pandemic (Buil-Gil et al., 2020). The study indicated that the financial fraud rate increased by 50.95% in May 2020 compared to the same month in 2019. They also highlighted that cybercrime attacks were concentrated in the months when strict lockdown and precautionary measures were applied since online activities rapidly increased during this period (Buil-Gil et al., 2020).

2.2 Financial Fraud Examples

Financial fraud occurs in multiple forms. Attackers use calls, SMS, WhatsApp, or emails to deceive victims and direct them to enter fraudulent websites that appear legitimate to steal individuals' data (Jakhiya et al., 2020; Lallie et al., 2020). In one of the attacks that exploited people's goodwill, an email was broadcasted claiming to be from Centers for Disease Control and Prevention (CDC), which politely requested Bitcoin donations in order to develop a COVID-19 vaccine; the following message was sent: "Funding of the above project is quite a huge cost, and we plead for your goodwill donation, nothing is too small" (Lallie et al., 2020). Furthermore, in another fraud case, people were manipulated to invest in medical firms claiming the development of promising cures to COVID-19 (Lallie et al., 2020). Moreover, it is worth noting that crowdfunding platforms' growth during the pandemic has further facilitated fraud activities since fraudsters can easily hide their identities on these websites (Karpoff, 2020).

2.3 Solutions

In order to address the exceptional surge of financial fraud, the following solutions were proposed. Jakhiya et al. (2020) emphasized ensuring that a proper KYC (Know Your Customer) process is in place to provide financial services only to legitimate customers and entities. Also, AI methods could minimize financial fraud by detecting suspicious transactions, even in milliseconds for real-time transactions, which is applied in Paypal for example (Jakhiya et al., 2020). Bandyopadhyay and Dutta proposed a method based on recurrent neural networks to detect suspicious mobile money transactions during the exceptional lockdown period. According to the experiment, this approach achieved a success rate of 99.87% (Bandyopadhyay & Dutta, 2020).

4. Social Engineering Attacks During COVID-19 Pandemic

Social engineering is among the types of attacks that exploit vulnerabilities within the human being. Therefore, attackers have already started to take advantage of the pandemic and use it for their favors. Thus, there was a spike in social engineering attacks. For example, many hospitals and healthcare providers suffered from security breaches resulting from impersonating other healthcare officials. Based on statistics recently revealed by the US Federal Bureau of Investigation (FBI), more than 600% increase in successful cyber-attacks within the US happened during the pandemic and almost 300% increase globally (Malecki, 2020).

Since cybersecurity is dynamic and associated with constant changes, it is highly recommended to continuously identify and assess new cybersecurity risks and identify proper mitigation controls proactively. This is vital since human beings depend on technology more than any time before due to the lockdown enforced in more than half of the world. In addition, the impact of risk will be greater than before as well (Borkovich, 2020).

It is also highly recommended to enterprises to subscribe to the government Computer Emergency Response Team (CERTs) and other cybersecurity advisories in order to react to any possible mass wave of attacks and implement recommended controls proposed by them (Saudi NCA, 2020). Besides, conduct continues awareness to users in order to be vigilant from being a victim without their knowledge.

5. Risk Employees Behavior (Working from Home During COVID-19)

Despite the fact, that working from home lowers the risk of human exposure to the COVID-19 and complies with local authorities of lockdown enforcement; it introduced several cybersecurity risks.

One of the risks that were introduced is insider threats. High-risk employees who work from home are able to target their organizations away from the office. Correspondingly, having the company's assets at home increases the probability of stealing or misusing those data compared to employees who are physically located at the company's premises surrounded by other colleagues. Also, working within abnormal office hours will make anomaly detection extremely challenging to Security Operation Centers within the organizations and eventually make it less effective (Saudi NCA, 2020).

Another risk that might occur is the inability to physically protect companies' assets while connected remotely. Therefore, in this scenario unauthorized users might obtain access to companies' data (Borkovich, 2020).

It is highly recommended to reexamine the threat cases that were implemented before the COVID-19 pandemic and add new ones considering the major changes in the environment that was introduced (Saudi NCA, 2020). In addition, the level of access needs to be assessed to ensure the least required privileges are granted to users (Abukari & Bankas, 2020). Also, users should be aware of the risks associated with accessing remotely and should comply with cybersecurity policies at home to protect their organizations.

6. Conclusion

In summary, the world before the COVID-19 pandemic is not the same during and after the pandemic. Therefore, considering performing things remotely has become the new normal life, which requires a paradigm shift in how to tackle cybersecurity risks, especially considering the significant environmental changes and enormous dependencies on technologies. Without adequate security measures, greater risks will occur that varies from causing financial loss to put human life in danger. The success factor of this will start from individuals as the first layer of defense. As Islam encourages human to protect themself and others from all harm including cybersecurity risk. Also, awareness and sharing the knowledge they all what Islam value is advice at such time that cyber threats spread everywhere.

References

Abukari, A. M., & Bankas, E. K. (2020). Some cyber security hygienic protocols for teleworkers in COVID-19 pandemic period and beyond. International Journal of Scientific & Engineering Research, 11(4), 1401-1407.

Alshowmer, S. (2020). Remarkable success of mobile and contactless payments through near field communication 'NFC' technology boosting the aim of a less dependent on cash society within the Kingdom of Saudi Arabia," BusinessWire, Nov. 10, 2020. [Online]. Available: https://www.businesswire.com/news/home/20201110005684/en/Remarkable-Success-of-Mobile-and-Contactless-Payments-Through-Near-Field-Communication-%E2%80%9CNFC%E2%80%9D-Technology-Boosting-the-Aim-of-a-Less-Dependent-on-Cash-Society-Within-the-Kingdom-of-Saudi-Arabia (Accessed Dec. 07, 2020).

Bandyopadhyay S. & Dutta, S. Detection of fraud transactions using recurrent neural network during COVID-19, Preprints, Jun. 2020.

Borkovich, D. B. and Skovira, R. J. (2020). Working from home: cybersecurity in the age of

COVID-19. Issues in Information Systems, 21(4)234-246.
Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. European Societies, 23:sup1, S47-S59.
Chen, H., Engert, W., Huynh, K., Nicholls, G., Nicholson, M. and Zhu, J. (2020). Cash and COVID-19: The impact of the pandemic on demand for and use of cash, Bank of Canada, Staff discussion papers, 2020-6. Jul. 2020, [Online]. Available: https://www.bankofcanada.ca/wp-content/uploads/2020/07/sdp2020-6.pdf
Curran, K. (2020). Cyber security and the remote workforce. Computer Fraud & Security, 2020(6), 11-12.
Hui, J. Y., & Yi-Ling, T. (2020). Pandemic and beyond: phishing in a larger pond, Global health security: COVID-19 and its impacts.
Jakhiya, M. M. Bishnoi, & H. Purohit. (2020). Emergence and growth of mobile money in modern India: a study on the effect of mobile money, in 2020 Advances in science and engineering technology international conferences (ASET), 2020, pp. 1–10.
Karpoff, J. M. (2020). "The future of financial fraud," Journal of Corporate Finance, Jul. 2020.
Lallie, H. S., Shepherd, L. A., Nurse, J. R. C, Erola, A., Epiphaniou, G., Maple, C, & Bellekens, X. (2021). Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic, Computers & Security, Vol. 105.
Malecki, F. (2020). Overcoming the security risks of remote working. Computer Fraud & Security, 2020(7):10-12.
Saudi National Cybersecurity Authority. (2020). NCA Cybersecurity Quarterly, Available at https://nca.gov.sa/

Biodata

	Arwa M. Al-Romaih is a master's student in Cybersecurity at the college of IT, University of Bahrain. She is specialized in IT Security, and she also works at John Hopkins Aramco Healthcare company as an IT Security Analyst. Her research interests include information security governance and risk management, cybersecurity awareness and training, artificial intelligence in cybersecurity, cybersecurity capability maturity models.
	Abdulrahman Khaled Abdulwahab is a Master student in Cybersecurity at the college of IT, University of Bahrain. He is specialized in Network Security. He works at Batelco Bahrain as Head of IT Infrastructure.
	Ahmed M. Zeki is an assistant professor at the department of Information Systems, University of Bahrain. He holds a PhD in Computer Science, and specialized in Artificial Intelligence and Machine Learning. He has given a number of workshops in data mining, published many research papers in international journals and international conferences, and received several awards.

Abstract in Arabic

تأثير جائحة COVID-19 في تصاعد مخاطر الأمن السيبراني، مع تصور إسلامي

أروى الرميح[1]، عبد الرحمن خالد عبد الوهاب[2]، أحمد محمد زكي[3]

[1،2،3] قسم أنظمة المعلومات، كلية تقنية المعلومات، جامعة البحرين، مملكة البحرين

20190266@stu.uob.edu.bh[1]

202000050@stu.uob.edu.bh[2]

amzeki@uob.edu.bh[3]

الخلاصة. أثَّرت جائحة كورونا COVID-19 على جوانب عديدة من سلوك الناس، ما دفعهم إلى تبني أسلوبَ حياةٍ يتَّسمُ بالحذر الشديد. ومن الناحية التقنية، تتمثل هذه الآثار بزيادة مطردّة في الخدمات الرقمية عبر الإنترنت، وزيادة ملحوظة في تحويل الأموال عن طريق الهاتف المحمول، وتقليل المعاملات النقدية، فضلًا عن تحول المنظمات إلى العمل من المنزل. كل هذه التغيّرات وغيرها، زادت من المخاطر الإلكترونية ذات الصلة. تستعرض هذه الورقة أربعة من أكثر مخاطر الأمن السيبراني شيوعًا والتي برزت أثناء فترة انتشار الجائحة حول العالم، وهي: حملات التصيد الاحتيالي، والاحتيال المالي، والهندسة الاجتماعية، والمخاطر المرتبطة بسلوك الموظفين العاملين من المنازل. تشير هذه الدراسة أيضًا إلى بعض الأمثلة لبعض البلدان حيث قارنت تحديات مخاطر الأمن السيبراني قبل وبعد COVID-19 مثل المملكة العربية السعودية والمملكة المتحدة. بالإضافة إلى ذلك، يوصي هذا البحث ببعض من أفضل الممارسات التدابير للتغلب على مخاطر الأمن السيبراني المذكورة. إلى جانب ذلك، تتناول هذه الورقة هذه القضايا والحلول المقترحة من منظور إسلامي.

الكلمات الجوهرية. كوفيد-19، التصيد الاحتيالي، الاحتيال المالي، الهندسة الاجتماعية.