Borneo International Journal eISSN 2636-9826; Vol. 6 (3); 2023; 7-15
Published by *Majmuah Enterprise*
www.majmuah.com

The Rising Threat of Social Engineering in the Post COVID-19 Remote Work Era

MOHD HAFIZ ALI MOHD ANUAR, RAVISANKAR A/L MADHVAN AND MOHAMAD FADLI BIN ZOLKIPLI
School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah Darul Aman, MALAYSIA
Email:hafiz_ali@usm.my, ravisankar1097@gmail.com, m.fadli.zolkipli@uum.edu.my
Tel: +60125318364 , +601136047745 | +60177247779 |

Received: July 16, 2023
Accepted: July 26, 2023
Online Published: Sept 01, 2023

Abstract

Since the COVID-19 pandemic, when people started working from home, the cybersecurity scene has changed in a big way. This paper gives an in-depth look at how social engineering methods are becoming a bigger threat and how they affect the three pillars of cybersecurity: confidentiality, integrity, and availability (CIA). We look at the unique risks and challenges that come with remote work by showing examples of current threats. We look into how well the current preventive steps work, consider possible future threats, and suggest possible countermeasures. Lastly, we point out the holes in the present research and talk about where future research in the field of remote work cybersecurity could go. This study aims to add a new point of view to the ongoing discussion about cybersecurity and help companies navigate and deal with the complex network of threats in the remote work world after COVID-19.

Keywords: Social Engineering, Remote Work, Cybersecurity, Post Pandemic, Work from Home

1. Introduction

The global COVID-19 pandemic has sped up the digital transformation seen in all industries. This has caused a basic shift from traditional office spaces to remote work environments. Even though this change was unavoidable and mostly good, it has brought a new set of cybersecurity challenges. Most of all, the broad use of digital platforms has made it easy for social engineering threats to thrive. Social engineering is a part of cybersecurity that takes advantage of human mistakes and manipulation. In this situation, it is very important to understand, predict, and deal with these changing risks. The goal of this study is to look into the growing number of threats, with a focus on the risks that come with remote work and how they affect the Confidentiality, Integrity, and Availability (CIA) Cybersecurity triad(Hussain, Mohamed, & Razali, 2020). Because of the COVID-19 pandemic, more people are working from home. This has changed not only how companies work, but also how cybersecurity works. People who work from home often use their own networks or networks with less security(Prasad, 2021). This gives bad people more ways to get in and makes it more likely that social engineering attacks will work. Also, threat actors have used the COVID-19 pandemic to lure victims into traps(Ferreira & Cruz-Correia, 2020). They do this by taking advantage of the general fear and confusion about COVID-19. This goes against the CIA triad.

This paper has more than one goal. First, we want to know how common and harmful different types of social engineering risks are, which have become more dangerous in the age of remote work. Second, we want to figure out how good the current safety measures are at reducing these kinds of threats. At the same time, because cyber threats are always changing, we look to the future and try to predict possible threats and remedies in the fields of remote work and cybersecurity. When we present this study, we try to give a detailed analysis that goes beyond the instant effects and talks about the need for constant vigilance and strategies that can change. By doing this, we hope to give organizations actionable tips on how to deal with this new terrain, as well as suggest areas for future study to advance the conversation in this important area. In the end, this study adds to the growing body of research on cybersecurity by focusing on the urgent problems and future possibilities of securing remote work after COVID-19 .

1 Literature Review

2.1 Impact of COVID-19 on Remote Work Culture and Cybersecurity

The impact of COVID-19 on remote work culture and cybersecurity has been extensively studied by researchers. Whereas the COVID-19 pandemic necessitated a rapid shift to remote work, presenting new challenges and vulnerabilities (Prasad, 2021), it also led to increased cybersecurity risks and social engineering attacks (Y. He,

Aliyu, Evans, & Luo, 2020);(Ferreira & Cruz-Correia, 2020). In addition to that, organizations had to understand the evolving remote work landscape and its impact on cybersecurity (Rahman & Arif, 2021).The sudden transition to remote work arrangements due to the pandemic presented organizations with new challenges and vulnerabilities. (Prasad, 2021) emphasizes the need to adapt to this evolving remote work culture in order to effectively address cybersecurity concerns. However, this shift to remote work also brought about an increase in cybersecurity risks and social engineering attacks. (Y. He et al., 2020) and (Ferreira & Cruz-Correia, 2020) highlight the heightened threats and attacks targeting remote workers. These attacks take advantage of the vulnerabilities in remote work setups, such as unsecured home networks and employees' lack of awareness. This presents a contrasting situation where the need for enhanced cybersecurity measures is essential to protect sensitive data and prevent security breaches.

In addition to the increased cybersecurity risks, understanding the evolving remote work landscape is crucial for organizations. (Rahman & Arif, 2021) emphasize the importance of studying and comprehending the changes brought about by remote work during the pandemic. This understanding enables organizations to develop appropriate strategies and policies to mitigate cybersecurity risks and ensure a secure remote work environment. Thus, it is essential to consider the evolving nature of remote work culture and its impact on cybersecurity. The COVID-19 pandemic prompted a rapid transition to remote work, which introduced new challenges and vulnerabilities. Whereas organizations had to adapt to the evolving remote work landscape, they also faced increased cybersecurity risks and social engineering attacks. In contrast to the traditional office setup, remote work necessitates enhanced cybersecurity measures to protect sensitive data and prevent security breaches. Understanding the evolving remote work culture is vital for organizations to develop effective strategies and policies to address cybersecurity concerns ((Prasad, 2021); (Y. He et al., 2020); (Ferreira & Cruz-Correia, 2020); (Rahman & Arif, 2021)).

2.2 Types of Social Engineering Attacks and their Relevance to Remote Work

In the context of remote work, several types of social engineering attacks have emerged as significant threats. These include phishing, baiting, pretexting, and impersonation. Phishing, for instance, involves sending deceptive emails or messages to trick individuals into revealing sensitive information or accessing malicious links (The 17 Most Common Online Scams Phishing, n.d.) (Duff, 2005). Baiting relies on offering enticing rewards or benefits to lure remote workers into performing specific actions, such as clicking on malicious attachments or links. Pretexting involves creating a false scenario to manipulate individuals into disclosing confidential information or granting unauthorized access. Impersonation occurs when attackers pose as legitimate individuals or organizations to deceive remote workers and gain unauthorized privileges (Aldawood & Skinner, 2020) (Li et al., 2019) . Remote workers are particularly susceptible to social engineering attacks due to their heavy reliance on digital communication tools and virtual collaboration platforms. The shift to remote work has increased the reliance on email, messaging apps, video conferencing tools, and file-sharing platforms, creating new avenues for social engineering attacks. Attackers exploit the trust and vulnerabilities inherent in these communication channels to trick remote workers into divulging sensitive information, clicking on malicious links, or performing unauthorized actions (Aldawood & Skinner, 2020) (Li et al., 2019) . To combat the rising threat of social engineering in remote work environments, awareness and training are crucial. Remote workers need to be educated about the various social engineering techniques employed by attackers and taught how to recognize and respond appropriately to suspicious communications or requests. This includes being vigilant for phishing emails, verifying the authenticity of requests before sharing sensitive information, and adopting best practices for secure remote work. Training programs should emphasize the importance of maintaining strong passwords, using multi-factor authentication, and staying updated on the latest security practices (W. He et al., 2019) (Oedekerk, 2022)

2.3 Preventive Measures and Solutions for Remote Workers

To ensure the security of remote workers, employee training programs on cybersecurity best practices are essential. These programs educate employees about the risks associated with social engineering and raise awareness of common tactics used by cybercriminals. According to (W. He et al., 2019), such training programs can significantly improve employees' ability to detect and mitigate potential security threats. Another important preventive measure is the implementation of two-factor authentication (2FA) and virtual private networks (VPNs) to enhance remote access security. 2FA adds an additional layer of protection by requiring users to provide a second form of verification, such as a code sent to their mobile device, in addition to their password. VPNs, as highlighted by (Wenzhen & Mingchang, 2020) and (Lee, Kim, Park, & Moon, 2006), establish encrypted connections between remote workers and their organization's network, ensuring secure communication and data

transmission. Securing home networks and devices is also crucial for remote workers. Regular software updates and patches should be applied to all devices to address known vulnerabilities. Additionally, strong passphrase authentication should be employed to protect access to routers and other devices. (Bhana & Flowerday, 2020) and (Piasecki, Urquhart, & McAuley, 2021) emphasize the importance of these measures in mitigating the risk of unauthorized access and potential compromises of home networks. Furthermore, the establishment and enforcement of cybersecurity policies and standards play a vital role in promoting secure remote work practices. By implementing clear guidelines and expectations, organizations can ensure that remote workers adhere to necessary security measures. (Li et al., 2019) emphasizes the significance of cybersecurity policies in creating a culture of security awareness and accountability among remote employees

2.4 Research and Future Directions in Remote Work Cybersecurity:

Ongoing research and proactive cybersecurity strategies are of paramount importance as remote work continues to evolve. (Buil-Gil, Lord, & Barrett, 2020) emphasize the need for continuous investigation and understanding of the evolving cybersecurity landscape to effectively mitigate potential risks and threats in remote work environments. This highlights the significance of staying updated and proactive in implementing measures such as regular security assessments, vulnerability management, and employee education on best practices for remote work security. Similarly, (Goode, 2019) stresses the importance of ongoing research in developing innovative solutions to address emerging cybersecurity challenges in remote work scenarios, particularly in terms of establishing trustworthy digital identities and secure authentication methods.To strengthen remote work cybersecurity, exploring new technologies and approaches is essential. (Wenzhen & Mingchang, 2020) propose the design of a border security defense system specifically for VPN networks in power enterprises. By focusing on enhancing the security and integrity of VPN infrastructures, this research contributes to strengthening remote work cybersecurity. Additionally, (Piasecki et al., 2021) highlight the significance of cybersecurity standards for smart home devices used in remote work environments. By establishing and following these standards, the privacy and security of remote work setups can be ensured. Considering new technologies and approaches, such as these defense systems and cybersecurity standards, becomes crucial in fortifying the overall security posture of remote work environments. Understanding the impact of cybersecurity policy awareness on employees' behavior in remote work settings is also essential. (Li et al., 2019) emphasize the influence of cybersecurity policy awareness on shaping employees' decision-making processes and adherence to secure practices. In remote work scenarios, employees need to be aware of the organization's cybersecurity policies and guidelines to effectively implement security measures. This knowledge contributes to a safer remote work environment by promoting secure practices and mitigating potential vulnerabilities. In conclusion, ongoing research, proactive cybersecurity strategies, and the exploration of new technologies and approaches are vital for strengthening remote work cybersecurity. Understanding the impact of cybersecurity policy awareness on employees' behavior further contributes to creating a secure remote work environment. These factors work together to address the evolving challenges and mitigate risks associated with remote work, ensuring the protection of sensitive data, and enhancing overall cybersecurity.

2 Social Engineering and CIA Triad

Social engineering was chosen as the focus of this study because it has a clear place in the age of online work. Unlike most cybersecurity threats, which take advantage of technical flaws, social engineering takes advantage of human weaknesses (Oedekerk, 2022), like trust and fear (Hadlington, 2017). This makes it especially relevant in the current environment. Traditional security perimeters have been widened by the move to remote work, putting workers in places that may be less safe. At the same time, the confusion around the COVID-19 pandemic gives threat actors a lot to work with, which shows how important it is to look at social engineering threats. Our study of cybersecurity is built around the Confidentiality, Integrity, and Availability (CIA) Triad (Figure 1). Its ideas are especially important in today's world of online work and pandemics. Confidentiality, the idea that only authorized people should be able to access information, is at risk when employees view sensitive data remotely on networks that might not be safe. Integrity, which means making sure that data is correct and reliable, is at risk when data is shared and communicated through many avenues that might not be secure. Availability is the certainty that data and resources can be accessed reliably and on time. Overloaded networks or denial-of-service attacks can hurt availability.

Figure 1 (Source: https://www.nist.gov/image/cia-triad)

When we look at social engineering dangers through the lens of the CIA Triad, we can see how complex these cybersecurity risks are. Confidentiality can be broken by social engineering techniques like phishing and impersonation (Hatfield, 2018), which trick people into giving up private information. When these breaches lead to illegal changes to data, integrity is at risk. Availability can also be broken if attackers take over systems or data and change rights or system settings. This way of looking at social engineering in terms of the CIA Triad gives a full picture of how it affects cybersecurity. It talks about how important it is to have cybersecurity plans that deal with both technology and human flaws. This protects our information systems in the ever-changing world of remote work. By looking at these threats in the context of COVID-19, we show how global disasters can be used for bad purposes. This shows how important it is to be ready for such situations (Ferreira & Cruz-Correia, 2020).

3 Examples of Social Engineering Threats

Social engineering is a broad group of bad things that are done to take advantage of human psychology rather than flaws in technology. Due to the COVID-19 pandemic, the way people work has changed a lot. As a result, the field of social engineering has grown by leaps and bounds. As the traditional boundaries of the office have become less clear, workers who work from different, and often less secure, network environments are easy targets for these attacks. In this situation, it's important to know how social engineering threats are changing and how common they are becoming in the age of online work. This knowledge is important for building effective defenses and keeping the strength of the cybersecurity triad, which is made up of Confidentiality, Integrity, and Availability (CIA).

Table 1, "Analysis of Social Engineering Threats During the COVID-19 Remote Work Era Based on the CIA Triad," gives you a full picture of how these threats are changing. This table shows some common social engineering techniques that are especially effective when people work from home. Some of these are phishing, spear phishing, pretexting, baiting, quid pro quo, bullying, and pretending to be someone else (Sadiku, Shadare, & Musa, 2016).

Type of Social Engineering Threat	Description	Impact During Covid-19 Remote Work Era	Confidentiality Impact	Integrity Impact	Availability Impact
Phishing	An attacker masquerades as a trusted entity to trick victims into disclosing sensitive information.	Increase in phishing emails related to Covid-19 information or stimulus checks.	Victim's sensitive information such as login credentials may be compromised.	Unauthorized access can lead to data manipulation.	Compromised accounts could be locked by attacker, disrupting availability.

Spear Phishing	Similar to phishing, but the attacker targets specific individuals or companies.	With more employees working remotely, targeted attacks on individuals increased due to potentially weaker home network security.	Personal or corporate sensitive data may be leaked.	Unauthorized access can lead to data manipulation.	Access to key corporate accounts or services could be disrupted.
Pretexting	The attacker creates a false narrative to get the victim to reveal information.	Attackers might pretend to need information to assist with pandemic-related issues or remote work IT help.	Sensitive information disclosed during the pretext could be compromised.	False information could be inserted into systems.	If access is gained, key services could be disrupted by the attacker.
Baiting	The attacker leaves a malware-infected physical device in a location where it's sure to be found.	Less relevant during remote work era, as this typically requires physical presence.	If bait is taken, malware could provide access to sensitive data.	Once infected, data can be manipulated by the attacker.	Malware could potentially disrupt systems or lock out users.
Quid Pro Quo	An attacker requests private information in return for something desirable.	Increase, as attackers offered 'free' pandemic related aid or tools useful for remote work in exchange for information.	The information provided in return for the 'service' is at risk.	Could potentially lead to unauthorized access and data manipulation.	Could potentially block access to systems or data.
Tailgating	The attacker seeks to enter a restricted area by following behind a legitimate user.	Less relevant during remote work era as this relies on physical presence.	If access is gained, sensitive data could be physically accessed.	Unauthorized physical access could lead to manipulation of data.	Physical disruption of systems could limit service availability.
Impersonation	An attacker pretends to be someone else, such as a co-worker or a trusted entity, to trick the victim into giving up sensitive information.	Increased during remote work era due to lack of face-to-face verification opportunities.	Confidential information could be revealed to the impersonator.	The impersonator could gain unauthorized access to systems or data.	The impersonator could potentially disrupt services by altering settings or permissions.

Table 1: Analysis of Social Engineering Threats During the COVID-19 Remote Work Era Based on the CIA Triad

In phishing and spear phishing, attackers pose as trusted entities to trick victims into giving up private information or taking actions that weaken system security. In a setting where people work from home, the greater use of digital communication tools has made it easier for these dishonest things to happen. During the COVID-19 pandemic, these threats got worse because attackers took advantage of the widespread fear and doubt by sending phishing emails that looked like they were about the pandemic. This broke the CIA Triad's Confidentiality principle. Pretexting and baiting, which involve setting up a fake situation or making an offer the target can't refuse to trick them, are also very dangerous. Even though these methods have been around for a long time, the shift to remote work and the pandemic have given them new life, allowing attackers to take advantage of the weaknesses in both the infrastructure for remote work and the way workers think and act. These methods can lead to serious problems with confidentiality and honesty.

Tailgating, also called "piggybacking," is when an unauthorized person follows an authorized person into a limited area. Even though tailgating may have gotten a little less common because more people work from home, it is still a risk in hybrid work settings.

In the age of remote work, impersonation, in which the attacker claims to be someone else to get access or information, has become more common. Since there aren't any face-to-face exchanges, it's hard to check someone's identity, which makes it easier for attackers to pose as trusted people. The results can be anything from data leaks that hurt Confidentiality and Integrity to big problems with system availability. The way these threats are broken down in Table 1 shows how broad and flexible social engineering methods are, especially in the context of COVID-19's remote work environment. As organizations continue to adjust to this new normal, it becomes important to understand these dangers in depth as the first step in strengthening cybersecurity infrastructure. In the next parts of this paper, we'll talk more about how to stop social engineering, how to fix it, and where it might go in the future. This will show how important it is to take a proactive, all-around approach to safety in the age of remote work.

4 Current Preventive Measure and Solution

The ways to stop and fix the social engineering problems listed in Table 1 can be put into three main groups: employee awareness and training, strong technical infrastructure, and clear organizational policies.

Employee Awareness and Training

Since social engineering attacks are based on people, giving workers information is a key line of defense. Regular training on how to spot different types of attacks, like phishing, spear phishing, pretexting, and impersonation, can make a big difference in how secure a company is. Simulations, like fake phishing efforts (Baslyman & Chiasson, 2016), can help people learn how to spot and deal with these threats in real life. A proactive cybersecurity culture can be built by asking workers to report any suspicious behavior. This method of teaching directly handles the weaknesses in people that social engineering attacks take advantage of, adding an important layer of protection (Jones & Moncur, 2018).

Robust Technical Infrastructure

Putting in place strong technical protection is also very important. Multi-factor authentication can stop threats like phishing and impersonation from getting in without permission. Firewalls and anti-malware software can keep people from getting into an organization's network without permission. In the context of remote work, the CIA Triad says that using secure work practices like Virtual Private Networks (VPNs), secure cloud services, encrypted messaging, and strong passwords can protect the confidentiality and integrity of data (Wenzhen & Mingchang, 2020).

Clear Organizational Policies

Threats like baiting and "quid pro quo" can be stopped by making and following clear rules about how to handle surprising physical or digital gifts. Tailgating could be a problem in hybrid work settings, so there should be strict physical security measures like secure access controls, visitor management systems, and ways to keep an eye on things. Because these threats come from many different directions, it takes a mix of the above steps to stop them. For example, to stop phishing threats that have been especially strong during the COVID-19 pandemic (as shown in Table 1), organizations might combine training for employees (so they can spot phishing attempts), strong technical infrastructure (like strong email filtering systems and multi-factor authentication), and clear organizational policies (about how to handle suspicious emails) (Henschke & Ford, 2017). But because these threats change over time, our strategies and answers for stopping them must also change over time. The best protection comes from a defense plan with many layers. This is often called "defense in depth." We can stay one step ahead of potential attackers and keep our cybersecurity strong in this increasingly remote work setting by making sure that our defensive measures are always changing along with the threat landscape.

5 Future Threats and Potential Countermeasure

The world of cybersecurity is always changing because of changes in technology and in the ways that bad people do things. As working from home becomes more common, even after COVID-19, the threat of social engineering is likely to become more complicated and sneakier. This part looks ahead to possible threats in the future and talks about what can be done to prevent these threats. As artificial intelligence (AI) and machine learning become more and more popular, we can expect social engineering attacks to become more sophisticated (Sarker, Furhad, & Nowrozy, 2021). In the future, AI could be used in phishing attacks to automatically make and send out fake messages that look and sound very real. This would make them even harder to spot. Deepfake technology, which uses AI to make fake audio or video that sounds or looks very real, could also be used for impersonation attacks, making it much harder to verify someone's

identity in remote work settings (Morel, 2011). The rise of Internet of Things (IoT) gadgets in remote work may also make it easier for social engineering attacks to happen (Umran, Lu, Abduljabbar, Zhu, & Wu, 2021). These devices often have weaker security measures, which makes them easy targets for hackers who want to get into a network or get their hands on private information without permission.

Also, as more companies move toward hybrid work models that combine remote and in-person work, real social engineering threats like tailgating could become more common again. Here, attackers could take advantage of weak physical security measures in office areas with fewer people.
When it comes to remedies, it will be most important to keep investing in education and training, especially as threats become more complex. This could include learning how to spot phishing efforts that are driven by AI or how to spot deepfakes. A powerful way to stop future social engineering attacks is to encourage a culture of vigilance and skepticism in the workplace, where workers feel free to question and report strange requests or activities. Threats will change over time, so technological answers will need to keep up. This could include stronger security measures for IoT devices or better AI-based security solutions that can find and stop AI-driven social engineering risks. As deepfakes become more common, it will be more important to invest in tools that can spot them.

For the possible return of physical social engineering risks, it will be important to strengthen physical security measures. This could mean making access controls stricter, making visitor management systems more careful, and putting more focus on training employees about physical security. In the end, it's important to be able to predict possible future threats and put in place the right remedies before they happen. This is especially true in a time when more and more people are working remotely. As technology changes and workspaces grow, a forward-thinking approach to safety is no longer just a nice thing to have, it's a must.

6 Future Research Opportunities

Social engineering has many different parts, and the way it works is changing all the time. This opens up a lot of study possibilities for the future. Even though there is more and more written about this topic, there are still some study gaps that, if filled, could help us understand and deal with social engineering threats in the remote work era much better. One big gap in research is that there aren't enough studies about how new technologies like artificial intelligence (AI) and the Internet of Things (IoT) affect the complexity and frequency of social engineering attacks. As was already said, these technologies could be used to make attacks more targeted and effective, which would make cybersecurity more difficult. But most of the study that has been done so far has been on traditional types of social engineering threats. So, more research is needed to figure out how these technologies might change the way social engineering works and what kinds of protections can be taken against these new threats.

Another area that hasn't been looked into much is how psychological and social factors might affect how vulnerable people are to social engineering attacks when they work from home. Even though past studies have found general human weaknesses, it is still not clear how these weaknesses may be made worse or better by remote work conditions. For example, an employee's ability to recognize and react to social engineering attacks may be affected by being alone, having more work to do, or having their communication patterns change. In-depth study on these factors could give valuable information that could be used to make training and awareness programs for remote workers that are more effective. These found gaps are good places to start doing study in the future. By focusing on these areas, we can get a more complete picture of social engineering threats in the age of online work and come up with better ways to stop them.

7 Conclusions

Due to the COVID-19 pandemic, people quickly switched to working from home. This has led to a big rise in social engineering risks. As we've talked about and shown in Table 1, these risks take advantage of weaknesses in people to break the Confidentiality, Integrity, and Availability (CIA) of information systems. Even though these threats pose problems, they can be stopped with a combination of employee knowledge and training, strong technical infrastructure, and clear organizational policies. But as we move further into the post-pandemic era, the field of social engineering is likely to change along with changes in technology and the way people work. The danger landscape of social engineering is expected to become more complicated due to the possible use of AI and IoT technologies and the shift to hybrid work models. So, it is very important to stay alert and change our prevention plans as needed.
When study gaps are found, they point to good ways to do more research. By looking at how new technologies affect social engineering and how psychological and social factors affect how vulnerable people are to these threats in a remote work setting, we can get a better idea of how the threat landscape is changing. This kind of study would help improve cybersecurity measures, especially ones that are made for working from home.

In the end, this paper shows how important it is to keep learning about and changing how we deal with social engineering threats in the remote work world after COVID-19. By staying on top of possible future threats, putting countermeasures in place ahead of time, and filling in study gaps, we can make sure that cybersecurity is strong in a world where digital and remote work are becoming more common. Our digital future will bring both challenges and chances, and we will need to stay alert and change as needed.

Acknowledgments

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of Ethical Hacking & Penetration Testing Research Project. This work was supported by Universiti Utara Malaysia.

References

Aldawood, H., & Skinner, G. (2020). Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions. *IEEE Access*, 8, 67321–67329.

Baslyman, M., & Chiasson, S. (2016). 'Smells Phishy?': An educational game about online phishing scams. *2016 APWG Symposium on Electronic Crime Research (ECrime)*, 1–11.

Bhana, B., & Flowerday, S. (2020). Passphrase and keystroke dynamics authentication: Usable security. *Comput. Secur.*, 96, 101925.

Buil-Gil, D., Lord, N., & Barrett, E. C. (2020). The Dynamics of Business, Cybersecurity and Cyber-Victimization: Foregrounding the Internal Guardian in Prevention. *Victims & Offenders*, 16, 286–315.

Duff, A. S. (2005). Social Engineering in the Information Age. *The Information Society*, 21, 67–71.

Ferreira, A., & Cruz-Correia, R. J. (2020). COVID-19 and Cybersecurity: Finally, an Opportunity to Disrupt? (Preprint).

Goode, A. (2019). Digital identity: solving the problem of trust. *Biometric Technology Today*, 2019(10), 5–8. Retrieved from https://doi.org/https://doi.org/10.1016/S0969-4765(19)30142-0

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3.

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Comput. Secur.*, 73, 102–113.

He, W., Ash, I., Anwar, M., Li, L. X., Yuan, X., Xu, L., & Tian, X. (2019). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital*, 21, 203–213.

He, Y., Aliyu, A., Evans, M. G., & Luo, C. (2020). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *Journal of Medical Internet Research*, 23.

Henschke, A., & Ford, S. B. (2017). Cybersecurity, trustworthiness and resilient systems: guiding values for policy.

Hussain, A., Mohamed, A., & Razali, S. (2020). A Review on Cybersecurity: Challenges & Emerging Threats. In *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*. New York, NY, USA: Association for Computing Machinery. Retrieved from https://doi.org/10.1145/3386723.3387847

Jones, H. S., & Moncur, W. (2018). The role of psychology in understanding online trust.

Lee, J.-A., Kim, J.-H., Park, J.-H., & Moon, K.-D. (2006). A Secure Wireless LAN Access Technique for Home Network. *2006 IEEE 63rd Vehicular Technology Conference*, 2, 818–822.

Li, L. X., He, W., Xu, L. D., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *Int. J. Inf. Manag.*, 45, 13–24.

Morel, B. (2011). Artificial Intelligence and the Future of Cybersecurity. In *Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence* (pp. 93–98). New York, NY, USA: Association for Computing Machinery. Retrieved from https://doi.org/10.1145/2046684.2046699

Oedekerk, J. G. (2022). *A STUDY OF SOCIAL ENGINEERING CONCEPTS WITHIN A DECEPTIVE DEFENSE*.

Piasecki, S., Urquhart, L. D., & McAuley, D. (2021). Defence against the dark artefacts: Smart home cybercrimes and cybersecurity standards. *Comput. Law Secur. Rev.*, 42, 105542.

Prasad, K. (2021). Remote Working Challenges and Opportunities During Covid-19 Pandemic. *Journal of Business Strategy Finance and Management*, 2(1–2), 01–03.

Rahman, K., & Arif, Md. Z. U. (2021). Working from Home during the COVID-19 Pandemic: Satisfaction, Challenges and Productivity of Employees. *International Journal of Trade and Commerce-IIARTC*, 9, 282–294. Retrieved from https://doi.org/10.46333/ijtc/9/2/3

Sadiku, M., Shadare, A., & Musa, S. (2016). Social Engineering: An Introducction. *The Journal of Scientific and Engineering Research*, 3, 64–66.

Sarker, I. H., Furhad, Md. H., & Nowrozy, R. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN Computer Science*, 2.

Umran, S. M., Lu, S., Abduljabbar, Z. A., Zhu, J., & Wu, J. (2021). Secure Data of Industrial Internet of Things in a Cement Factory Based on a Blockchain Technology. *Applied Sciences*.

Wenzhen, M., & Mingchang, X. (2020). Design of Border Security Defense System for VPN Network in Power Enterprises. *Journal of Physics: Conference Series*, 1617.