# A CONCEPTUAL MODEL FOR PREVENTION OF E-FINANCIAL CRIMES IN UAE: A REVIEW PAPER

**Sultan Khalifa Humaid Khalifa Alshamsi, Universiti Teknikal Malaysia Melaka**
**Nabil Hasan Saleh Al-Kumaim, Universiti Teknikal Malaysia Melaka**

## ABSTRACT

*E-crime is a criminal activity involving computer with the internet that distributes or damages electronics through viruses or cyber-attacks that lead to sensitive information leakage. E-crimes will cause a deny service to many authorized users through their computer functionality and breaches their security level. Thus, E-financial crimes are the act of obtaining financial gain through a profit-driven criminal activity focusing on stealing financial information. Businesses and consumers in the UAE suffered more than 617,347 phishing attacks during the Covid-19 stay-at-home measures. The data is then used to access important accounts and can result in identity theft and financial loss. UAE was ranked 9th after a higher number of phishing attacks on a bank. Therefore, individuals in economic and even non-financial organizations need to prevent these attacks from succeeding by developing an integrated model of e-crime awareness towards preventing e-crime in the UAE. Prevention of E-crimes is an essential element that creates awareness to the employees through well-equipped knowledge on human errors that tricks them through suspicious behavior.*

*Furthermore, cyber security leadership is tended sufficiently in organizational leadership and security mechanisms. This paper intends to review the previous and current e-financial crime factors and comprehensively discuss the prevention of e-financial crimes in the UAE. Besides, the present concerns and difficulties that emerge and how to resolve the scenarios will be accumulated. The research's primary conclusion focuses on developing an integrated model of e-crime awareness toward preventing e-financial crimes in the UAE.*

**Keywords**: E-Crime, Cyber Attack, Cybercrime, Technology, Financial Crimes, Prevention

## INTRODUCTION

The quickly growing digital nature that outcomes in a consistently developing issue of e-crime lead to the entanglements and risks that are continually associated and arranged through the anonymity and speed of the internet prompts steadily expanding cyber-criminal dilemma. Every year, cybercriminals arise with modern tactics and techniques intended to trick their possible victims (Kuru & Bayraktar, 2017). Thus, we desire to understand what sets of e-crimes aside from digital threats are encountered such as viruses, Trojans, spyware, and the targeted cybercriminals' activity using a computer (Herath, Yim, D'Arcy, Nam & Rao, 2018). The physical attack of e-crime can be categorised as a security breach circumvented where the individual does not have 100% protection in their online security. According to the United Nations Crime Trends for 2019, the UAE has been ranked at 36th place out of 180 countries for higher e-financial crime (United Nations Office on Drugs and Crime Report, 2019).

E-financial crimes is an activity that steals financial information, gaining access to financial accounts for unauthorised transactions attacked *via* malware injection, phishing, or bot for obtaining sensitive financial details, subsequently causing economic damage. According to Pavlidis & Satolias (2019), today's widely economically motivated crime generates wealth through insider information or another person's property by stealing their material benefit. Thus, organised criminals will increase their e-financial crimes for large-scale funds for their operations, involving more extensive and effective financial infrastructure (Gibbs, 2018).

Moreover, e-financial crimes can be categorised as money laundering, fraud, electronic crime, market abuse, and insider information stealing, leading to criminal activity and employing sophisticated techniques to manage their financial activities. Yet, emerging markets open their economies that increase the viable targets for e-financial crime activity.

One of the most e-financial severe crime effects is the transactions meant to conceal the proceeds of a crime beyond the reach of the law. E-financial crimes often use front companies, which involve abuse of trust or active manipulation through leaking sensitive data. Today's trend shows that organized criminal groups focus on the easy way to make money that targets wealthy organizations because a large amount of cash flows daily and contains sensitive information (Ratten, 2019). Moreover, the financial organization encounters cybercrimes problems through theft identity and phishing due to the complexity of technology (Nowacki & Willits, 2019). Thus, data breaches occur due to the digitization of data storage, storing private data and records, consisting of confidential information and financial progress (Weijer et al., 2020).

With the digitalization evolution of modern information systems, financial crime is an ever-growing concern for organizations. It is the effect of individuals changing behavior and leveraging towards societal phenomena and economic phenomena changes (Jayakrishnan, Mohamad & Yusof, 2020b). In the UAE, cyberattacks focus on phishing and identity theft that emphasize a rapidly growing online base (Ferguson, Renaud, Wilford & Irons, 2020). Furthermore, the financial services area is the most attacked businesses. In the UAE, relatively half of the organizations (56%) and a quarter of financial institutions (36%) announced obtaining phishing attacks (Kaspersky, 2019). Particularly in the current environment, where nature has become more digital due to the Covid-19 pandemic, phishing emails utilizing the pandemic as a topic expanded e-financial crime activities. Cybercriminals imitate an authentic financial organization to take individual's information or login credentials.

The UAE Police statistics showed that in 2019, there were 9046 complaints, with 1277 from email accounts that had been hacked (Zabyelina, 2019). Most of these cases were filed by women who belong to wealthy, educated, and government officers' families blackmailed through cyber-attacks dilemma (Mahdavi, 2019). Furthermore, the ascent of phishing attacks represents a critical threat to financial organizations. Thus, every financial institution should recognize probably the most well-known phishing attacks to protect their corporate information. Hence, cyber security awareness is still lacking in terms of prevention for a banking institution that becomes the victims of financial loss due to the identity theft of corporate information and financial information that generally incur the cost associated (Afifi, 2019). Therefore, developing the conceptual model of cyber-attack prevention factors and cyber security awareness can be used as guidance to prevent cyber-attacks dilemma within the banking context.

We conceptualize an integrated model of e-crime awareness toward the prevention of e-financial crimes in the UAE. The prevention knowledge and skills required today are evolving rapidly. Thus, financial organizations must provide cyber security leadership with practical training to their employees in characterizing the technological development rate of the UAE digitalization and technological adoption level of awareness and knowledge on how to defend against identity theft and phishing. Therefore, there is a need to study the role of skilled leaders in financial organizations in the UAE in preventing cyber attacks and investigate other human factors related to the individual in financial organizations in the UAE in preventing cyber-attacks.

## LITERATURE REVIEW

A decent comprehension of arising cyber security and technologies is not only for the information technology department but demand surplus to comprehend the chances and implications of working in a digital world and decrease the general danger. Cyber-attacks are an intensifying issue that can prompt a loss of money-related and individual data (Cymru, 2006). Online users are becoming anxious and cautious while working in computer applications

(Oksanen & Keipi, 2013). The idea of intrigue is people's daily patterns of routine activities on the internet that increase the potential for cyber-attacks. To converse the threat and endeavor the modern chances, we need to understand daily activity patterns that could clarify the rise in cyber-attack victims. Note that criminologists in the mid-1970s understood the significance of victimization studies that they recently positioned their focus on the criminal offender through routine activity (Cohen & Felson, 2003).

Cybercriminals attack every organization because there are some critical assets that the criminals may seek to exploit. Cybercriminals involve in crimes for personal gains that motivate them to perform an offending acts. Moreover, they choose the right individual as their victims for cash or financial data. On different occasions, it might be the individual data of customers and staff or even the organization foundation. According to Cohen & Felson (1979), the motivated offender must exist for the crime to happen. Besides, a suitable target is necessary for the offence to occur. Thus, the absence of a capable guardian makes a straightforward way for criminals to target their victims. The UAE has the most profoundly internet-connected population in the whole Middle East, with 85% of the community using online. According to Al-Ali & Al-Nemrat (2017), most web users in the UAE have been a victim of cyber-attacks. Furthermore, these cyber-attacks are hard to prove, and criminals typically focus on the UAE residents because the overall economic status has a very high pace in utilising digital devices.

According to the Global web index (2018), mobile banking is 60%, making mobile payments is 29%, purchasing items online using a mobile phone is 55%, and crypto currency is 5.2% in the UAE. Therefore, the UAE faces malicious email attacks and is impacted by phishing activities. Thus, scammers posing as bank agents ask the victim's bank details due to credit card overcharge or blocked, where scammers can use this information to access the account's money. Besides, the massive increment in the utilization of online payment and e-services has urged cybercriminals to target victims because low risk and high money stimulate cybercriminals to participate in cyber-attacks. Cyber-attacks raise complex issues with new technologies that brought unprecedented threats to social dilemmas for UAE (ElYacoubi, 2020). Cyber-attacks have significant impacts on a wide variety of public safety, reducing confidence in personal identity and computer security (Kuru & Bayraktar, 2017), national security impact through reduction on economic strength (Lemieux, 2018), and human security that creates danger and fear for an individual (Barrera, 2019).

Therefore, we conducted a literature review to identify the most relevant prevention factors of e-financial crimes in the UAE. The literature review is a method that focuses on strategising the body of literature for research that needs to be reviewed and aggregated their specified indicators for the study. Conducting a literature review critically examines the research problems and summarise the solution clearly for the research study (Jayakrishnan, Mohamad & Abdullah, 2019). Moreover, it identifies the indicators that require further investigation for the research study. Yet, the literature review divides the workload through the planning phase that determines the model's interaction and development. Moreover, the motivation of this study is to develop a prevention model of e-crimes in the UAE. Therefore, we have identified that Protection Motivation Theory (PMT) as one of the most relevant theoretical backgrounds toward preventing e-financial crimes hinges on the literature review, as shown in Table 1.

**Table 1**
**PROTECTION MOTIVATION THEORY (PMT) TOWARDS THE PREVENTION OF E-FINANCIAL CRIMES. THREAT APPRAISAL**

| Threat Appraisal | | | | |
|---|---|---|---|---|
| **No** | **References** | **Perceived severity** | **Perceived vulnerability** | **Indicators** |
| 1 | (Briggs et al., 2017) | √ | | An organization's perception of the seriousness of a cyber-attack is left untreated. |
| 2 | (Vrhovec & Mihelič, 2021) | √ | | |
| 3 | (Bada et al., 2019) | | √ | An organization's perception of risk contracting in a |

| | | | | | |
|---|---|---|---|---|---|
| 4 | (Choi & Young, 2021) | | √ | cyber-attack condition. | |
| **Coping Appraisal** | | | | | |
| **No** | **References** | **Self-efficacy** | **Response efficacy** | **Response costs** | **Indicators** |
| 5 | (Li, Xu, He, Chen & Chen, 2016) | √ | | | Confidence to continue the cybersecurity behaviour and overcome temptations. |
| 6 | (Salehi, 2021) | √ | | | |
| 7 | (White, 2017) | | √ | | The perceived effectiveness of taking action to improve cybersecurity. |
| 8 | (Bada et al., 2019) | | √ | | |
| 9 | (Briggs et al., 2017) | | | √ | The perceived impediments to taking action to improve a cybersecurity condition. |
| 10 | (Vrhovec & Mihelič, 2021) | | | √ | |

Based on Table 1, we have identified the Protection Motivation Theory (PMT) toward the prevention of e-financial crimes. Protection Motivation Theory (PMT) explains the health avoidance behaviour related to the perception of risks and self-efficacy capacity to take effective action to avoid risks (Rogers, 1975). Yet, it has been used to explain an individual's propensity to engage in voluntary, secure behaviours (Rogers, 1983). Therefore, Protection Motivation Theory (PMT) can be practised to cybersecurity behaviours by focusing on the threat itself and the capacity to move against that threat in the economic context. It has five main components: "threat appraisal" that comprises perceived severity and perceived vulnerability, followed by "coping appraisal", which contains response costs, self-efficacy, and response efficacy.

In threat appraisal, the perception assesses the different elements that will probably impact one to engage in a potential cyberattack behaviour. Perceived severity is estimated in the condition of selecting from the response received through rear arousal (Vrhovec & Mihelič, 2021). The individual can be asked how they perceive the prospect of being a cyberattack victim, generating responses like "not stressed" and "restless" that are pointers of the degree of fear concerning a threat. Perceived vulnerability is the individual's belief that he/she is susceptible to a potential cyberattack threat (Choi & Young, 2021). For instance, the person might be requested to provide personal details and banking information through an email posing as a legitimate institution to lure individuals.

The coping appraisal assesses the different variables that guarantee a recommended response in a preventive nature (Li et al., 2016). There are three arrangements of convictions included, which is: (1) self-efficacy manages the conviction that one has the necessary capacity to participate in a cyber-attack behavior that deliberate by reactions proclamation (Salehi, 2021), (2) response efficacy is the conviction that engages in specific conduct will outcome in a decreased cyber-attack threat (White, 2017), and (3) response costs manage with the costs that one appends to the exhibition of a cyber-attack behavior (Briggs et al., 2017). Therefore, adopting the Protection Motivation Theory (PMT) for this study will indicate the severe threat in a financial organization and can viably diminish the threat by engaging the prevention behavior that alerts the cyber-attacks dilemma.

Furthermore, we conduct the narrative review to obtain the cyber attack prevention factors. A narrative review is to identify the described problem of interest in a specified search solution strategy (Jayakrishnan, Mohamad & Yusof, 2020a). This narrative review captures a subset of recently advanced cyber-attack prevention factors for e-financial crimes in the UAE. Perhaps the most professional approach to secure against cyber-attacks and a wide range of information breaches is preparing and alerting financial organization representatives on cyber-attack prevention and educating them regarding present cyber-attacks (McCrohan et al., 2010). Cybercriminals desire to drop false emails mimicking somebody in a financial organization and demand one requesting individual particulars or approach positive documents (Rajan et al., 2017). Connections regularly appear authentic to a normal eye, and it is not difficult to fall into the trap. Subsequently, workforce awareness is imperative for a financial organization. We have

tabulated the component of cyber-attack prevention factors suitable for a financial institution, as shown in Table 2.

**Table 2**
**COMPONENT OF CYBER-ATTACK PREVENTION FACTORS**

| Cyber-attack Prevention Factors | | | | |
|---|---|---|---|---|
| **No** | **References** | **Organization Frequent Training** | **Government Frequent Alerting** | **Indicators** |
| 1 | (McCrohan et al., 2010) | √ | | Cybersecurity training helps employees protecting themselves and the organisation from cyber-attacks and threats. |
| 2 | (Amer, Abdulrahim, Juma, Rajan & Ahamed, 2013) | √ | | |
| 3 | (Bada, Maria, Angela M. Sasse, 2019) | √ | | |
| 4 | (Tsagourias, 2012) | | √ | Government offers a variety of information for users in cyber-attacks and alerts them. |
| 5 | (Chandra & Snowe, 2020) | | √ | |
| 6 | (Islam, Farah & Stafford, 2018) | | √ | |

Based on Table 2, cyber-attack prevention factors can contribute to creating cyber security awareness in a banking environment. Organization frequent training will make the employees identify and eliminate cyber threats and protect their essential resources (McCrohan et al., 2010). Thus, employees can effectively identify and prevent security breaches by noticing the threat level as spams, malware, and phishing that commonly occurs in the organization context. Moreover, the government's frequent alerting will make people aware of recent and actual cyber-threats affecting their daily security infrastructure (Tsagourias, 2012). Thus, it establishes basic security controls, where people can protect themselves from such attacks. From an organization's perspective, cyber security leadership is needed to secure their systems and protect their information and financial details. Therefore, we can conclude that the theoretical framework of Protection Motivation Theory (PMT) is mapped with the relationship between cyber-attack prevention factors. Yet, the theory indicates two (2) criteria when making a decision under threat, which is (1) threat appraisal that ensures security instructions are realistic and perceived for the organisational environment and (2) coping appraisal that ensures threat information is accompanied by practical information in delaying it, which is suitable for this study context in a banking environment.

## FRAMEWORK DEVELOPMENT

Cyber-attacks, especially counting the Internet, speak to increased criminal behavior near-unique illegal activities (Ryder & Reid, 2012). Yet, most cyber-attacks is an attack on information about governments, organization's, or people. Even though the attacks don't happen on a physical body, they occur on the corporate or individual basic build, which is the course of action qualities defining personal and foundations on the web (Gupta et al., 2018). In other words, our primary characters are fundamental segments of customary daily presence in the digital era. There is a load of identifiers and numbers in different computer data sets moved by enterprises and governments. Cyber-attack highlights the balance of networked computers in our lives, similarly to the weakness of such solid factors as personal identity.

This study is conducted in the UAE, considering very few criminological landscape studies have been implemented on evaluating and identifying cyber security awareness. It is significant for the UAE that cyber security awareness can significantly improve economic growth with technology. Moreover, cyber-attacks have become a crucial matter among developed countries

globally and developing countries like UAE (Halbouni et al., 2016). Organised criminal groups are gradually moving towards damaging the business's reputation by hacking the networks containing business-sensitive information, which may cost more significant losses to the business performance (Malik & Islam, 2019). Moreover, this dilemma occurs due to the adoption of modern technology consisting of information flow, which has no boundary and is difficult to monitor (La Torre et al., 2018). Furthermore, borderless technology transfer is exposed to new theft methods in the data breach that negatively affect the organization (Arewa, 2018).

Cyber-attack prevention factors significantly impact the perception of social and moral values in the business context. However, the causes behind cyber-attacks are complicated to be eliminated because they are mapped to electronic criminality that keeps on growing (Koziarski & Lee, 2020). Moreover, the cyber-attack negatively impacts the business context because unauthorized access consists of many possibilities of a data breach due to complex technology (Shah et al., 2019). Many organizations are still struggling to make cyber security a proactive part of their daily operation (Chandra & Snowe, 2020). Cyber security is a phrase situated at the center and front of numerous personalities while harm from malicious assaults keeps on aggregating. Despite the possibility for unfortunate outcomes, numerous pacific organization's strive to deal with cyber security like a business organizations that concern on how to prevent financial threat.

Today's financial organization leaders must embed cyber security throughout their organization's operations that respond to cyber-attacks. They must be able to lead by hiring security executives that can develop skills to prevent cyber-attacks. Moreover, the financial organization needs cyber security leadership, particularly Chief Information Security Officers, who take a strategic and more decisive role within their economic organization. Furthermore, a cyber-security framework is required for the business, where leaders must spur cyber security success (Amer et al., 2013). Yet prioritizing cyber security and awareness to mitigate potential cyber-attacks for future threats need to be strategized. Cyber security leadership is now required to move beyond compliance monitors and work towards shared risk ownership. For this reason, we conducted a systematic literature review on the initial selection of primary sources for the moderator effects through checking the inclusion or exclusion criteria of cyber security leadership by reviewing full research papers. Table 3 indicates the components of cyber security leadership that can be utilized as a moderator in developing the conceptual model of cyber-attack prevention factors and cyber security awareness.

**Table 3**
**COMPONENT OF CYBER SECURITY LEADERSHIP**

| **Cyber Security Leadership** | | | | | |
|---|---|---|---|---|---|
| **No** | **References** | **Setting the Cyber Security Strategy.** | **Positioning the Cyber Security Functions.** | **Implementing the Cyber Security Activity.** | **Indicators** |
| 1 | (Hathaway, 2012) | √ | | | Building the cyber security strategy that protects the business and provides less risk exposure in their operational activities. |
| 2 | (Amer et al., 2013) | √ | | | |
| 3 | (Islam et al., 2018) | | √ | | Slotting cyber security within the Information Technology function through the operations and digital infrastructure that prevents cyber-attacks. |
| 4 | (Tsagourias, 2012) | | √ | | |
| 5 | (McCrohan et al., 2010) | | | √ | Prioritizing cyber security technical skills that improve the organization's digital structure and secure the data breach from the cyber attackers in their daily operations. |
| 6 | (Hathaway, 2012) | | | √ | |

Based on Table 3, the component of cyber security leadership is one of the most thought-provoking criteria that have been emphasized in the cyber security awareness context. Cyber security leadership must take more decisive and more strategic leadership roles within their business during crisis environments (Hathaway, 2012). Thus, cyber security leadership has not been tended sufficiently in terms of technology but primarily in organizational policy and leadership details. In this study, the cyber security leadership will move as a moderator in finding the connection between cyber-attack prevention factors and cyber security awareness. Moreover, cyber security leadership will view cyber security liability and influence effects to adjust the requirements for data security and viable security, ensuring against future and current cyber threats.

Besides, cyber security leadership needs to be well equipped with critical knowledge of emerging cybercrime trends and the cyber security environment. Therefore, the study contains 12 hypotheses for creating cyber security awareness, which scrutinizes the cyber-attack prevention factors towards cyber security awareness. Utilizing innovations alongside tackling technology capacities, organizations are reproducing regular encounters for users and the UAE government, making it more customized, consistent, productive, and significant. UAE governments must incorporate security with their innovations and technologies (Aloul, 2010). Users must remain careful from a broad scope of cyber threats because monetisable information is the primary objective for cyber attackers. The Middle East sees a flood in political and strategic hacking.

The greater worth of this information on the darknet composes this financial organization an appealing objective for cybercriminals. Moreover, advances in online banking, instant payments, and mobile apps complete the desire for modern technology that increases the financial organization's attack on new vulnerabilities. This has made it more challenging for the leadership to maintain a balance and ensure the safety of their economic organisation and informational assets with online transactions. Therefore, the daunting challenge for the administration is to protect the financial organisation's digital assets and infrastructure while ensuring operations without interruption. Consequently, we have developed and designed an integrated model of e-crime awareness toward preventing e-financial crimes in the UAE, as shown in Figure 1.

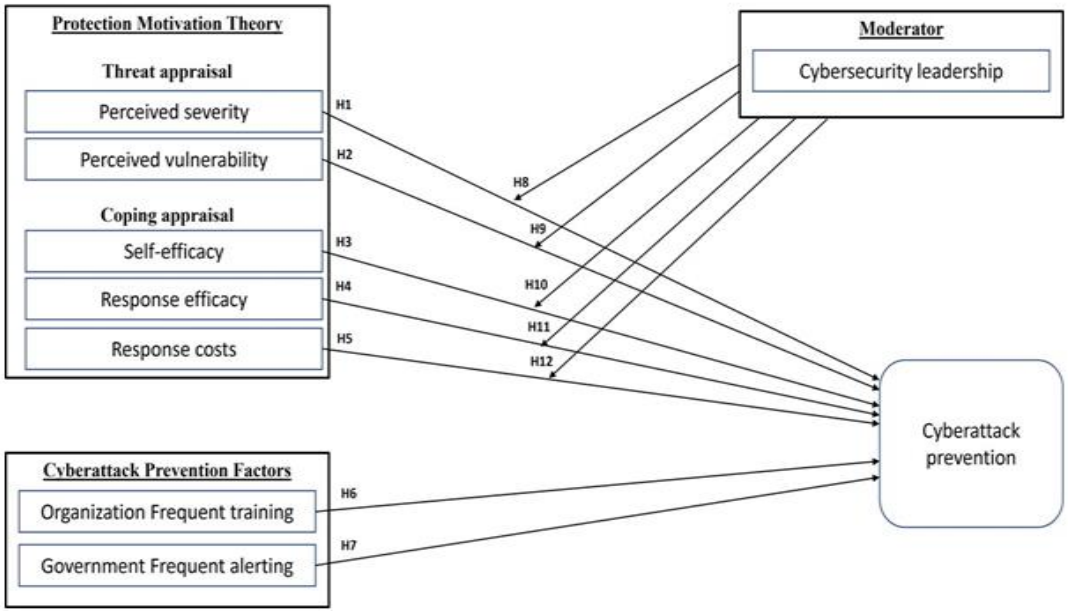


**FIGURE 1**
**CONCEPTUAL MODEL OF E-CRIME AWARENESS TOWARD THE PREVENTION OF E-FINANCIAL CRIMES**

Based on Figure 1, the conceptual model of e-crime awareness toward preventing e-financial crimes shows the factors in Protection Motivation Theory (PMT) and cyber-attack prevention as the independent variable with the moderator variable on cyber-security leadership. Therefore, we have defined our dependent variable for cyber-attack prevention. The investigation of the relationship between cyber-attack prevention and cyber-security awareness was framed within the Protection Motivation Theory (PMT). Therefore, the principal dispute for the theoretical proposition about this study is gaunt from Protection Motivation Theory (PMT), which guides the understanding of the impact on progress, social change, and development.

## CONCLUSION

UAE is one of the highest cyber-attack cases in the world. Therefore, this study becomes even more significant when it focuses on cyber-attack prevention and cyber-security awareness in the UAE. The dilemma of cyber-attacks within the UAE has started from many technological advances that involve everyday communications and commercial activities using online. Due to the enormity of the dilemma, it has become compulsory to utilize all techniques to prevent cyber-attacks. At the same time, cyber-security enhances in-depth technical support that creates opportunities to perfect the skills of technology-based ideas. Therefore, this study brings new insights into the relevance of cyber-security skills under these conditions. Furthermore, these matters have not been investigated or undertaken in any past research of UAE, so this assembles the study's specialty, mainly because the cyber-attack prevention factors play a significant aspect in creating cyber-security awareness that conveys technology safety into the local market by empowering the knowledge economy. This assures more efficiency and encourages the secure digital process, strategizing modern technology that creates cyber-security awareness.

## REFERENCES


Afifi, M.A. (2019). Ethical responsibilities for assessment of techniques and legal framework to minimise IT crimes in UAE.

Al-Ali, A.A.H., & Al-Nemrat, A. (2017). Cyber victimization: UAE as a case study. In 2017 Cybersecurity and Cyberforensics Conference (CCC) (pp. 19–24). IEEE. https://doi.org/10.1109/CCC.2017.14

Aloul, F.A. (2010). Information security awareness in UAE: A survey paper. In 2010 International conference for internet technology and secured transactions, 1–6, IEEE.

Amer, F., Abdulrahim, H., Juma, S., Rajan, A.V., & Ahamed, J. (2013). Shopping online securely in UAE. In 2013 International Conference on Current Trends in Information Technology (CTIT), 153–160, IEEE. https://doi.org/10.1109/CTIT.2013.6749494

Arewa, A. (2018). Border-less crimes and digital forensic: Nigerian perspectives. *Journal of Financial Crime*, 00–00. https://doi.org/10.1108/JFC-12-2016-0079

Maria, B., Sasse, A.M., & J.R.N. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv.

Barrera, D.J.S. (2019). Doing dialogical narrative analysis: *Implications for narrative criminology*. In The Emerald Handbook of Narrative Criminology, 367–388, Emerald Publishing Limited. https://doi.org/10.1108/978-1-78769-005-920191031

Briggs, P., Jeske, D., & Coventry, L. (2017). Behavior change interventions for cybersecurity. *In behavior change research and theory*, 115–136, Elsevier. https://doi.org/10.1016/B978-0-12-802690-8.00004-9

Chandra, A., & Snowe, M.J. (2020). A taxonomy of cybercrime: Theory and design. *International Journal of Accounting Information Systems*, 100467. https://doi.org/10.1016/j.accinf.2020.100467

Choi, H., & Young, K.J. (2021). Practical approach of security enhancement method based on the Protection Motivation Theory (PMT). *In 2021 21st ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD-Winter), 96–97, IEEE*. https://doi.org/10.1109/SNPDWinter52325.2021.00028

Cohen, L.E., & Felson, M. (2003). Routine activity theory. Criminological theory: Past to Present (Essential Readings). (C. Francis Cullen, Robert Agnew. Los Angeles, Ed.).

ElYacoubi, D. (2020). Challenges in customer due diligence for banks in the UAE. *Journal of Money Laundering Control*, (ahead-of-print). https://doi.org/10.1108/JMLC-08-2019-0065

Ferguson, R.I., Renaud, K., Wilford, S., & Irons, A. (2020). PRECEPT: A framework for ethical digital forensics investigations. *Journal of Intellectual Capital*, (ahead-of-print). https://doi.org/10.1108/JIC-05-2019-0097

Gibbs, T. (2018). Making sure crime does not pay. *Journal of Money Laundering Control, 21*(4), 555–566. https://doi.org/10.1108/JMLC-10-2017-0060

Gupta, B.B., Arachchilage, N.A.G., & Psannis, K.E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems, 67*(2), 247–267. https://doi.org/10.1007/s11235-017-0334-z

Halbouni, S.S., Obeid, N., & Garbou, A. (2016). Corporate governance and information technology in fraud prevention and detection. *Managerial Auditing Journal, 31*(6/7), 589–628. https://doi.org/10.1108/MAJ-02-2015-1163

Hathaway, M.E. (2012). Leadership and responsibility for cybersecurity. *Georgetown Journal of International Affairs*, 71–80.

Herath, T., Yim, M.S., D'Arcy, J., Nam, K., & Rao, H.R. (2018). Examining employee security violations: Moral disengagement and its environmental influences. *Information Technology & People, 31*(6), 1135–1162. https://doi.org/10.1108/ITP-10-2017-0322

Islam, M.S., Farah, N., & Stafford, T.F. (2018). Factors associated with security/cybersecurity audit by internal audit function. *Managerial Auditing Journal, 33*(4), 377–409. https://doi.org/10.1108/MAJ-07-2017-1595

Jayakrishnan, M., Mohamad, A.K., & Abdullah, A. (2019). A systematic literature review in enterprise architecture for railway supply chain of Malaysia transportation industry. *International Journal of Engineering Research and Technology, 12*(12), 2473–2478.

Jayakrishnan, M., Mohamad, A.K., & Yusof, M.M. (2020a). Business architecture model in strategic information system management for effective railway supply chain perspective. *International Journal of Engineering Research and Technology, 13*(11), 3927–3933.

Jayakrishnan, M., Mohamad, A.K., & Yusof, M.M. (2020b). digitalization railway supply chain 4.0: Enterprise architecture perspective. *International Journal of Advanced Trends in computer science and engineering, 9*(5), 9056–9063. https://doi.org/10.30534/ijatcse/2020/310952020

Kaspersky. (2019). Spam and phishing in Q3 2019. Retrieved from https://securelist.com/spam-report-q3-2019/95177/.

Koziarski, J., & Lee, J.R. (2020). Connecting evidence-based policing and cybercrime. *Policing: An International Journal*, (ahead-of-print). https://doi.org/10.1108/PIJPSM-07-2019-0107

Kuru, D., & Bayraktar, S. (2017). The effect of cyber-risk insurance to social welfare. *Journal of Financial Crime, 24*(2), 329–346. https://doi.org/10.1108/JFC-05-2016-0035

La Torre, M., Dumay, J., & Rea, M.A. (2018). Breaching intellectual capital: Critical reflections on Big Data security. *Meditari Accountancy Research, 26*

(3), 463–482. https://doi.org/10.1108/MEDAR-06-2017-0154

Lemieux, F. (2018). Criminal intelligence. In intelligence and state surveillance in modern societies (95–119). Emerald Publishing Limited. https://doi.org/10.1108/978-1-78769-171-120181005

Li, L., Xu, L., He, W., Chen, Y., & Chen, H. (2016). Cyber security awareness and its impact on employee's behavior, 103–111, https://doi.org/10.1007/978-3-319-49944-4_8

Mahdavi, P. (2019). The personal politics of private life in the United Arab Emirates (UAE): sexualities, space, migration and identity politics in motion. *Culture, Health & Sexuality, 21*(12), 1381–1393.

Malik, M.S., & Islam, U. (2019). Cybercrime: an emerging threat to the banking sector of Pakistan. *Journal of Financial Crime, 26*(1), 50–60. https://doi.org/10.1108/JFC-11-2017-0118

McCrohan, K.F., Engel, K., & Harvey, J.W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce, 9*(1), 23–41. https://doi.org/10.1080/15332861.2010.487415

Nowacki, J., & Willits, D. (2019). An organisational approach to understanding police response to cybercrime. Policing: *An International Journal*, (ahead-of-print). https://doi.org/10.1108/PIJPSM-07-2019-0117

Oksanen, A., & Keipi, T. (2013). Young people as victims of crime on the internet: A population-based study in Finland. *Vulnerable Children and Youth Studies, 8*(4), 298–309. https://doi.org/10.1080/17450128.2012.752119

Pavlidis, G., & Satolias, K. (2019). Tracing, freezing and confiscating the proceeds of crime in Cyprus. *Journal of Money Laundering Control, 22*(3), 434–441. https://doi.org/10.1108/JMLC-07-2018-0049

Rajan, A.V., Ravikumar, R., & Shaer, M.A. (2017). UAE cybercrime law and cybercrimes — An analysis. *In 2017 International Conference on Cyber Security And Protection Of Digital Services* (Cyber Security), 1–6, IEEE. https://doi.org/10.1109/CyberSecPODS.2017.8074858

Ratten, V. (2019). The effect of cybercrime on open innovation policies in technology firms. *Information Technology & People, 32*(5), 1301–1317. https://doi.org/10.1108/ITP-03-2018-0119

Rogers, R.W. (1975). A Protection Motivation Theory (PMT) of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114.

Rogers, R.W. (1983). Cognitive and psychological processes in fear appeals and attitude change: *A revised theory of protection motivation. Social psychophysiology*: A sourcebook.

Ryder, N., & Reid, A.S. (2012). *E- Crime. Information & Communications Technology Law, 21*(3), 203–206. https://doi.org/10.1080/13600834.2012.744219

Salehi, S. (2021). Analysis of environmental behaviors of rural people by applying protection motivation theory (PMT). *Journal of Rural Research, 11*(4), 662–673. https://doi.org/10.22059/jrur.2020.300437.1489

Shah, M.H., Jones, P., & Choudrie, J. (2019). Cybercrimes prevention: Promising organisational practices. *Information Technology & People, 32*(5), 1125–1129. https://doi.org/10.1108/ITP-10-2019-564

Team Cymru. (2006). Cybercrime. *Queue, 4*(9), 24–35. https://doi.org/10.1145/1180176.1180190

Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law, 17*(2), 229–244. https://doi.org/10.1093/jcsl/krs019

van de Weijer, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimisation: determinants, motives, and previous experiences. Policing: *An International Journal, (ahead-of-print).* https://doi.org/10.1108/PIJPSM-07-2019-0122

Vrhovec, S., & Mihelič, A. (2021). Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. Computers & Security, 106, 102309. https://doi.org/10.1016/j.cose.2021.102309

White, J.K. (2017). *Impact of Protection Motivation Theory (PMT) and general deterrence theory on the behavioral intention to implement and misuse active cyber defense*. Capella University.

Zabyelina, Y. (2019). The role of major intergovernmental organizations and international agencies in combating transnational crime. International and transnational crime and justice.