EVALUATING CYBER SECURITY AWARENESS LEVELS FOR EMPLOYEES IN DRB-HICOM AUTO SOLUTIONS

MOHD FADLI BIN KASIM

OPEN UNIVERSITY MALAYSIA

2021

EVALUATING CYBER SECURITY AWARENESS LEVELS FOR EMPLOYEES IN DRB-HICOM AUTO SOLUTIONS

MOHD FADLI BIN KASIM

A Master's Project submitted in fulfilment of the requirements for the degree of Master of Information Technology

Faculty of Applied Sciences

Open University Malaysia

2021

DECLARATION

Name : MOHD FADLI KASIM

Number : CGS00750403

I hereby declare that this final year project is the result of my own work, except for quotations and summaries which has been duly acknowledged.

Signature Date : 2th December 2021

EVALUATING CYBER SECURITY AWARENESS LEVEL FOR EMPLOYEES OF DRB-HICOM AUTO SOLUTIONS

ABSTRACT

The Internet is becoming increasingly connected to people in the daily life of many individuals, organisations and nations. It has benefit many people and gives a positive effect on the way people communicate. It has also introduced new avenues for business and has offered nations an opportunity to be involved in an online business. Although cyberspace offers a borderless list of services and opportunities, it is also accompanied by many risks. One of these risks is cyber attack. In an organisation, most of the cyber-attacks are email phishing, ransomware and data leaking. As concluded by many researchers that those use the Internet are not aware of such threats. In view of this, there is a need for an effective of cyber security awareness training that is custom-made according to the level of user knowledge. In this context, the primary research objective of this study is to understand the level of awareness and propose a training model to the organisation. Respondents were required to feedback their level of awareness for email phishing, cyber fraud, ransomware, social engineering and data leak. The total of 108 respondents were involved in this study and the finding shows that the awareness level is quite low for social engineering and cyber fraud attacks for almost all group age, job category and length of service.

Keywords: Cyber security, awareness level, email phishing, cyber fraud, social engineering, ransomware, data leaking.

PENILAIAN TAHAP KESEDARAN KESELAMATAN SIBER BAGI PEKERJA DI DRB-HICOM AUTO SOLUTIONS

ABSTRAK

Didalam kehidupan seharian Internet semakin banyak diguna pakai oleh ramai individu, organisasi dan negara. Ia memberi banyak manfaat kepada orang ramai dan memberi kesan yang positif kepada cara mereka berkomunikasi. Ia juga telah membuka jalan untuk peluang perniagaan yang baru dan dapat menawarkan peluang kepada orang ramai serta organisasi untuk terlibat didalam perniagaan atas talian. Walau pun ruang siber boleh menawarkan pelbagai perkhidmatan tanpa sempadan, ia juga mempunyai banyak risiko. Salah satu risiko nya ialah serangan siber. Didalam sesebuah organisasi, kebanyakan serangan siber yang dikenal pasti adalah pancingan data melalui e-mel, tebusan data dan kebocoran data. Ramai penyelidik telah membuat kesimpulan bahawa mereka yang menggunakan Internet tidak menyedari ancaman tersebut. Sehubungan dengan itu, terdapat keperluan untuk latihan kesedaran berkenaan keselamatan siber yang berkesan dan sesuai dengan tahap pengetahuan pengguna. Dalam konteks ini, objektif kajian utama kajian ini adalah untuk memahami tahap kesedaran dan mencadangkan model latihan kepada organisasi. Responden dikehendaki memberi maklum balas tentang tahap kesedaran mereka untuk pancingan data e-mel, penipuan siber, perisian tebusan, kejuruteraan sosial dan kebocoran data. Seramai 108 orang responden terlibat didalam kajian ini dan hasil kajian menunjukkan tahap kesedaran agak rendah terhadap serangan kejuruteraan sosial dan penipuan siber bagi hampir kesemua categori umur, kategori pekerjaan dan pengalaman pekerjaan.

Kata Kunci: Keselamtan siber, tahap kesedaran, pancingan data emel, penipuan siber, kejuruteraan sosial, tebusan perisian, kebocoran data.

ACKNOWLEDGEMENT

I would like to express my gratitude and my warmest thanks to Mrs Jaspal Kaur for her guidance, support, patience and most of all her advice for the completion of this literature.

Apart from that, I would also like to sincerely thank all my peers and colleagues from whom I had help also with the discussions and pointers as well as all staff of my company for their cooperation and support especially for filling up the questionnaires.

Last but not least, I would like to also thank my family for being supportive, understanding and for giving me the courage needed to complete this project.

THANK YOU.

MOHD FADLI KASIM
2 Dec, 2021

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

5G	5th Generation Network
AI	Artificial Intellegence
CBU	Completely Built Up
CKD	Completely Knocked Down
DHAS	DRB-HICOM Auto Solutions
DNS	Domain Name System
EDI	Electronic Data Interchange
IOT	Internet of Things
KPMG	Klynveld Peat Marwick Goerdeler
RAT	Remote Access Trojans
SFTP	Secured File Transfer Protocol

CHAPTER 1

INTRODUCTION

1.1 Research Introduction

The automotive industry has many segments or chains, from manufacturing, assembling, distribution and servicing of vehicles. In Malaysia, there are two types of passenger vehicle in the local market named as Completely Built Up (CBU) and Completely Knocked Down (CKD). For CBU, the vehicles are completely imported from the origin country. Unlike CKD, the vehicles are assembly locally where components or parts of the vehicle are imported from the brand or principle country.

The importer has the direct communication with the principle in term of parts ordering and billing as well as communication with shipper or sea liner for delivery and shipment of the components. Amongst the countries that the importer are communicating are Germany, South Africa, Mexico, China, Japan and Indonesia. Normally the communications are via email or phone calls.

On top of that, there are system interfaces and integrations between the importer and the principle. For the Europe countries, the method of interface is using Electronic Data Interchange (EDI) which is a standard method for all automotive countries in Europe. Other countries, the interface is using Secured File Transfer Protocol (SFTP).

As the communications are borderless and involve many parties in the automotive industries with different countries, the cyber security risk need to be addressed efficiency and effectively. The individuals with low level of cyber security knowledge may be exposed to the cyber-attack.

1.2 Background to the study

The technique of securing computers, servers, mobile devices, electronic systems, networks, and data from hostile intrusions is known as cyber security. It's also known as electronic information security or information technology security. The term applies to a wide range of situations, from commercial to mobile computing, and is separated into a few areas, including network, application, information, and operational security. The impact of emerging technologies such as artificial intelligence, 5G, and quantum computing, as well as evolving technologies such as the Internet of Things (IoT) that move autonomous vehicles and mobile phones, as well as the emerging global cyber war, will increase targeted and profitable ransomware attacks.. There is very important role that the people play in cybersecurity and what to do about the cybersecurity skills shortage. (Gil Press, 2019).

According to IT security firm Barracuda Network, more than 70 state and municipal governments across the United States were victims of ransomware attacks in 2019.

We foresee an increase in voice phishing scams in 2020 due to the developments in deep fake speech technology, in which employees are duped into paying money to criminals or divulging critical information. If recordings of you speaking are available online, whether on social media, YouTube, or an employer's website, there could be an unspoken war for control of your voice going on without you even realising it.(Thomas Brewster, 2021)

As the availability and reliability of 5G slowly rolls out, new cybersecurity challenges will emerge as opportunistic hackers look to profit off of the proliferation of IOT data. With 5G, data, location, and identity could all pose serious privacy concerns from the user's standpoint.

Before installing most smart phone applications, the subscriber's personal information is required.. (Ijaz et al., 2017)

RATs, banking Trojans, crypto miners, adware, and even ransomware are all examples of current mobile malware. Adware is the most frequent sort of mobile spyware, and it can be found on big software stores such as Google Play and the App Store. Ransomware asaults have continued to be prevalent in 2019, but with one major distinction. The dissemination of ransomware has changed from a numbers game to a more targeted technique known as "big game hunting," in which advanced threat actors discover or purchase their way into specified target organisations. They've been able to encrypt critical infrastructure and demand large ransom payments as a result of this. ("Cyber Security Report", 2020).

One of the factor that contribute to the attacks are mainly due to the rapid development and changes in the digital technology world. Now, it is the critical time to hold and add cyber security training annual company training plans. Data will become more important than ever before in 2021 as digitalisation continues. Information that may have seemed unimportant to the average consumer will become extremely valuable to stakeholders and hackers across the board.

1.3 History of cyber security

Cyber security has a long history, perhaps as long as the Internet itself. Criminals have been exploiting the World Wide Web since its inception as a mainstream resource. In the early 1980s, one of the earliest cases of this type of crime occurred. The 414s were apprehended after breaking into around 60 separate computers. These devices ranged from those at the Memorial Sloan-Kettering Cancer Center to those at the Los Alamos National Laboratory. (Ryan, 2019)

In 1997, another case of hacking that harmed the general public occurred. Yahoo! was the target of the attack. On Christmas Day, hackers claimed, a "logic bomb" would be launched on any PC utilising Yahoo! The claim, however, was irrelevant.

1.4 Awareness program.

Based on the 2017 edition of "The Definition of Security Awareness." Four phases of security awareness can be identified:

- Determining the present situation
- Developing and creating a security awareness program
- Disseminating the program to employees
- Measuring and updating the program as needed

To note on the important of the cyber awareness program, a cyber awareness program has been conducted in UK to influence businesses and individuals to adopt simple secure online behavior to help protect themselves from cyber criminals. The importance of security awareness in an information security program is sometimes overlooked. While businesses invest in modern security technologies and continue to train their security personnel, nothing is done to raise security awareness among ordinary users, making them the weakest link in any organisation..(Fadi A. Aloul, 2014)

Organisations increase their risk of attack if their degree of information security awareness on the current strategies utilised by social engineering is not kept up to date. Because social engineering assaults are meant to progress in tandem with emerging technology and security measures, more specialised training is required to establish and evolve the knowledge base against these threats.

The fundamental goal of information security training and awareness program is to help employees build abilities in detecting, disabling, and reporting hostile social engineering attempts. The absence of a training budget is one of the most significant

issues that businesses encounter when it comes to offering training and awareness program. (Hussain, 2019).

The security awareness among Malaysian is moderate. The most popular countermeasure practiced is scan PC even though users know that never share password is the most efficient countermeasure. This phenomena shows that although education on security awareness is important, convenient and easy to tool is important in encouraging users to practice what they have learnt. (Eu, 2021).

1.5 Problem statement

Although organisations have not adopted a common method of delivering security awareness program, an effective program should include information on data, networks, user behaviour, social media, mobile device use, email phishing, social engineering, and other sorts of viruses and malware. The successful employee security awareness program should make it obvious that IT security is the responsibility of everyone in the organisations.

According to (Steven, 2019), there are 4 categories of users with different level of cyber security awareness or training requirements as described below:

1.5.1 Personal Users.

They must be able to protect their personal data and use the connected technology (devices and services) safely. They must also understand why such protection is necessary.

1.5.2 Workplace Users.

Other than the reason currently pertains to the necessity to protect workplace systems and data, in which they may not feel as intimately invested as personal users.

1.5.3 Technical Specialists.

Those in charge of creating, developing, implementing, and maintaining technology

systems. There is an obvious requirement for them to comprehend where security is necessary and how to provide it.

1.5.4 Security Professionals:

Must have a certain set of security skills, which can be defined and backed up by specialised academic studies and professional certifications.

Ideally everyone in the above categories must at least meet the above requirements. However, even though there are training and awareness programs conducted, the level of awareness still an issue. For this study, we will only focus to the category of people or staff which is workplace users. The reason for this approach is to specifically identify the level of that category cyber security awareness level and ultimately to plan the awareness program customised according to the group.

One of the most essential and extensively used ways in combating cyber-attacks is workplace user education. Many organisations have undertaken public awareness efforts to teach people how to spot cyber security threats. Based on the study conducted by (Maria et al., 2016) in U.K and Soth Africa, there are many awareness program failed to meet the objective due to:

(1) The awareness program must be properly organsied with all the necessary equipment.

(2) People willing to take risk, thus threatening them will not work

(3) The awareness program is not about sharing information but it must be in interactive method.

(4) The awareness program must be continued from time to time and to be conducted regularly in order to sustain the people knowledge.

(5) When developing cyber security awareness programs, diverse cultural settings

and characteristics must be considered (Maria et al., 2016)

Meanwhile, businesses may presume that their staff have already gained some level of generic cybersecurity awareness from somewhere else. While this effectively absolves the organisation of accountability, it is frequently an untenable position. As a result, one of the most important criteria is for all parties involved to understand and accept their responsibilities.

In response to this problem, this study is to identify the level of awareness among the DHAS employees and to take actions to improve the awareness (if any) in order to prevent on any loss to the company.

1.6 Objectives of the study

There are many factors that we could talk about on this research title, but here is what the researcher feels is important for the awareness level of employees of DRB_HICOM Auto Solutions.

Below are some following points for study: -

i. To determine the factors and relationship between a training and knowledge of cyber security attack.
ii. To develop an instrument to determine the relationship between demographic variables and cyber security attack knowledge.
iii. To evaluate the instrument and propose a best practice framework of cybersecurity awareness training to be implemented at DRB-HICOM Auto Solutions.

1.7 Research questions

Following are the research questions that this study will hopes to address:

i) Do demographical variables such as gender, age, and length of service in the current organisation contribute to level of awareness?

ii) Does the quantity and quality of conducted awareness program has a positive impact to the user?

iii) Does the awareness program increased the users' awareness level?

1.8 Significance of the study

Philippsohn Crawfords Berwald Solicitors, London highlighted that the United Kingdom pointed out that the number of Internet users has exploded in recent years. The number of individuals utilising the internet is growing at a rate of one million each day around the world. When compared to January 2018 statistics, the following increases can be seen:

- Internet users increased by 9 percent (366 million)
- Unique mobile users has increased by 2 percent (100 million users)
- Social media users growing by 9 percent (288 million)
- Social media on mobile devices growth by 10 percent (297 million)

In UK, around 6% of the GDP is generated by the Internet and is set to grow - making it a larger sector than either utilities or agriculture. However, as our reliance on digital technologies has grown, so have the risks. Every month, over 20,000 malicious emails are sent through government networks, with 1,000 of them being specifically targeted.

There are many ways of stealing customers' data. The main methods are phishing emails, scam texts and the theft of mail from external mail boxes and multi-occupancy

buildings.

Over 50% of all frauds committed in the first half of 2017 were cybercrimes. “Web-based fraud is rising dramatically, accounting for two thirds of all the fraud cases it investigated for its business members ”. Philippsohn Crawfords Berwald Solicitors, London, UK

(Bernama, 2019) reported that in Malaysia, cyber-rime involving losses of RM67.6 million in 2,207 cases was reported in the first three months of 2019. The three most common types of cyber-rime were cheating via telephone calls (773 cases totaling RM26.8 million in losses), cheating in online purchases (811 cases totaling RM4.2 million), and the 'African Scam' (371 cases totaling RM14.9 million), while E-financial fraud recorded 212 cases totaling RM21.5 million in losses.

Furthermore, an average of three cyber-rime cases are reported daily in Penang. For the first seven months of the year, there were 731 cases involving losses totaling RM20.63 million. Cyber-rime cases, such as the Macau scam, love scam, e-financial fraud, and e-purchase online, were a concerning and growing trend. (Audrey, 2019).

According to statistics from the Malaysia Computer Emergency Response Team (MyCERT) under Cyber Security Malaysia (CSM), since 2008, cyber fraud has accounted for the highest number of incidents reported each year compared to other cybercrimes, indicating that awareness of the issue among internet users in the country remains low. Between January and July of this year, MyCERT received reports of 3,127 cases of cyber fraud. In 2018, cyber fraud cases topped the list again, with 5,123 incidents reported, along with 1,805 intrusions and 1,700 reports of malicious code. (Cyber Security Malaysia, 2019).

According to CyberSecurity Malaysia's Cyber999 Incident Statistics 2021, there were 4,729 cases reported between January and July 2021, compared to 3,127 cases reported between January and July 2019 and 319 identity theft cases reported in Malaysia between January and August 2021.

Despite technological advancements, cybercriminals have found it easier to gain unauthorised access. The number of successful attacks will continue to rise, as will the average cost to the victim organisation per successful attack, and the pattern will repeat itself. With so many new and exciting technologies to choose from, IT security fundamentals are boring. (Cyber Security Asean, 2021a)

According to the findings of this year's independent survey of 3,600 IT managers and remote employees at small and medium-sized businesses in 18 countries around the world, 53 percent of global companies have a false sense of security when it comes to supply chain attacks.(Cyber Security Asean, 2021b)

That’s why it’s important to study the level of employee awareness that will help the organisation to improve the cyber security knowledge at all levels of employees so that they are better equipped to work in the office systems as well as applications on their devices.

Cyber Security Malaysia recently conducted a cyber security awareness programme for entrepreneurs in July 2021. The program aimed to provide MARA entrepreneurs with exposure and understanding of the Malaysian cyber security landscape.

1.9 Assumptions of the study

There are a number of assumptions that are done in this research paper to facilitate the

results of the statistics collected. The statistical model that is being used is of quantitative research designs and are accompanied with assumptions. . In view of the fact that this research is only confined to the users currently working in the private sector.

Here are the following assumptions that were made concerning this research:

i) The respondents of the questionnaires would respond to the questions with honesty and integrity

ii) The respondents possessed the knowledge and understanding of themselves enough to respond to the questionnaire truthfully

1.10 Scope of the study

First and foremost, as far as the primary data is concerned, the accuracy of the data is very much based on the quality of the respondents as well as the background of the respondents. As this is a statistics on the awareness level for all level of employees, the level may be differs. The data that is being collected is solely based on only one company. Apart form that the research is only based on a company located in Malaysia only. No other data was collected from other country to facilitate this research. The research had to accept the data given by the respondent at face value, which means that the research has to assume that the data provided by the respondent is correct and valid. With regards to the secondary data, literature review that was conducted on published journals and websites, is presented in Chapter 2.

1.11 Outline of the study

This research is being presented is formatted into 5 chapters, which contributes to this study in the following ways:

Chapter 1: The introduction chapter presents the summary and the focus of the

entire research, in addition to presenting the value that hopes to offer to the academia.

Chapter 2: This chapter sets the context for the research through explaining the definition of awareness level and its impact to a company. This chapter also provides literature review on users awareness level, the awareness program conducted by companies and, being the main focus of this research.

Chapter 3: This chapter describes the research methodology of this research. It delineates the research hypothesis and justifying the underlying research methods.

Chapter 4: This chapter analyses the finding of the research in the context of the literature reviewed in Chapter 2 and the methodology applied in Chapter 3.

Chapter 5: This chapter provides summarisation and discusses the key findings and their importance to the research. In addition, it also put forward the research's limitation. Direction for future research, conclusion and recommendations are also identified and presented.

REFERENCES

Abbas Moallem, 2019, Cyber security awareness among students and faculty. Retrieved from https://books.google.com.my › books

Adams, P. (2013) Technology talent shortage: Is the solution education, immigration or recruiting women? Retrieved from http://www.rockiesventureclub.org/2013/07/technology-talent-shortage-is-the-solution-education-immigration-or-recruiting-women/

Adedayo Solomon Williams, Folakeakinbohun and Olusegun Mathew Awotunde,OlojidoJoseph Bamikole, 2019 September. An Empirical Investigation into the Relationship betweenMotivational Factors and Threats Consciousness amongsome Malaysian Postgraduate Students. Retrieved from https://www.researchgate.net/publication/336830314_An_2019_An_Empirical_Investigation_into_the_Relationship_between_Motivational_Factors_and_Threats_Consciousness_among_Some_Malaysian_Postgraduate_Students

Afrozulla Khan Z, Vaishnavi Rajesh Thakur, and Arjun, 2018 May. Cyber Crime Awareness among Msw Students, School Of Social Work, Mangaluru. (PDF) Cyber Crime Awareness among Msw Students, School Of Social Work, Mangaluru. Retrieved from https://www.researchgate.net/publication/333408476_Cyber_Crime_Awareness_among_Msw_Students_School_Of_Social_Work_Mangaluru

Allan Brill 2018, special report - MBA courses start offering digital security skills. Retrieved from https://www.ft.com/content/7b3cbe46-537e-11e8-84f4-43d65af59d43

Arwa A. Al Shamsi, 2009 August.Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE. Retrieved from https://www.researchgate.net/publication/342887888_Effectiveness_of_Cyber_Security_Awareness_Program_for_young_children_A_Case_Study_in_UAE/link/5f0c14fa299bf1881619832d/download

ATD Research, (2017, December). 2017-state-of-the-industry. Retrieved from https://www.td.org/research-reports/2017-state-of-the-industry

Audrey Dermawan, 2019 August 15, Cyber crime cases in Penang 'worrying': State police [Press Release]. Retrieved from https://www.nst.com.my/news/crime-courts/2019/08/513003/cyber-crime-cases-penang-worrying-state-police

Avast. (n.d). Test your basic cybersecurity knowledge. Retrieved from https://www.avast.com/en-my/business/resources/cybersecurity-quiz#pc

Bayisa Kune Mamade1;_ and Diriba Mangasha Dabala, 2021, June 14, Exploring The Correlation between Cyber Security Awareness, Protection Measures and the State of

Victimhood: The Case Study of Ambo University's Academic Staffs retrieved from https://www.researchgate.net/publication/285906588_Information_security_activities_of_college_students_An_exploratory_study/citations cited on S. Mensch and L. Wilkie, "Information Security Activities of College Students: An Exploratory Study Scott Mensch, Indiana University of Pennsylvania."

Bernama, 2019. Retrieved from https://www.kkmm.gov.my/public/latest-news/14896-bernama-23-april-2019-rm67-6-mln-lost-to-cyber-crimes-in-first-quarter-this-year
Corinne Bernstein , 2013 February 28. IT Skills Shortage: The other critical cliff facing enterprises. Retrieved from https://www.eweek.com/it-management/it-skills-shortage-the-other-critical-cliff-facing-enterprises/

Check Point Research, 2019, Cyber Attack Trends:2019. Retrieved from https://www.ispin.ch/fileadmin/user_upload/partner/pdf/CP-mid-year-report-2019.pdf

Check Point Research, 2020. Cyber Software Security Report 2020. Retrieved from https://www.ntsc.org/assets/pdfs/cyber-security-report-2020

Check Point Research,2021. Cyber Security Report 2021. Retrieve from https://www.checkpoint.com/downloads/resources/cyber-security-report-2021.pdf?mkt_tok=NzUwLURRSC01MjgAAAGAjgSeN98NIxWNyH1Dt7fGiqBCSP2ye7YihhjIhlJQXnn-Qyx0aKOA6x-5ec4GyQFGRZuEyXsWaQJbZ9CkURLlqz68lk-7L1kcPXp6vJMvEWtZU08

Cyber-edge, 2021. Cyberthreat Defense Report. Retrieved from https://cyber-edge.com/wp-content/uploads/2021/04/CyberEdge-2021-CDR-Report-v1.1-1.pdf

Cyber Security Asean , 2021a October 25, Cybersecurity Trends Forecast for 2022 and Beyond by BeyondTrust [Press release] retrieved from http:// cybersecurityasean.com/news-press-releases cybersecurity-trends-forecast-2022-and-beyond- beyondtrust

Cyber Security Report, 2020. Retrieved from https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf

Dodge, R. C., Carver, C. and Ferguson, A., 2007 February. Phishing for user security awareness. Computers & Security, 26(1), pg 73. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404806001581?via%3Dihub
Dr. Walid Tohme, Jeremy Lindeyer, Imad Harb , n.d Cyber security in Middle East. Retrieved from https://www.strategyand.pwc.com/m1/en/reports/cyber-security-in-the-middle-east.pdf

DSP Mahfuz, (n.d).Cybercrime Malaysia. Retrieved from https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/DSP-Mahfuz-Majid-Cybercrime-Malaysia.pdf

Eu Z. H., Lim S. B., Chong K. S., Ting T. T, Tan L. P., 2021 October 27. Information Security Awareness: A Further Study on Users' Preference, Practice and Knowledge. Retrieved from https://www.researchgate.net/publication/355663812_Information_Security_Awareness

Experian, 2021 September 20. Experian & CyberSecurity Malaysia: Growth in Digital Transactions Increases Risk of Identity Theft. Retrieved from https://www.cybersecurity.my/data/content_files/44/2216.pdf

Gil Press, 2019 December 3. 141 Cybersecurity Predictions For 2020. Retrieved from https://www.forbes.com/sites/gilpress/2019/12/03/141-cybersecurity-predictions-for-2020/?sh=6649f7dd1bc5

Hussain aldawood , geoffrey Skinner, 2019 May 8. Challenges of Implementing Training and Awareness Programs Targeting Cyber Security Social Engineering, retrieved from https://www.researchgate.net/publication/330661200_Challenges_of_Implementing_Training_and_Awareness_Programs_Targeting_Cyber_Security_Social_Engineering

Ijaz Ahmad_, Tanesh Kumary, Madhusanka Liyanagez, Jude Okwuibex, Mika Ylianttila{, Andrei Gurtov, 2017, September. 5G Security: Analysis of Threats and Solutions. Retrieved from https://www.researchgate.net/publication/318223878_5G_Security_Analysis_of_Threats_and_Solutions

Internet World Stats, 2021. Retrieved from http://www.internetworldstats.com/stats.html

IT Expert, 2019 Oct 3,Stay safe this National Cyber Security Awareness Month. Retrieved from https://www.itproportal.com/features/stay-safe-this-national-cyber-security-awareness-month/

Jemal Abawajy, 2012 Feb. User preference of cyber security awareness delivery methods. Retrieved from https://www.researchgate.net/publication/254220699_User_preference_of_cyber_security_awareness_delivery_methods

Joanne Martin, 2014 October 1, Cybersecurity Awareness Is About Both 'Knowing' and 'Doing'. Retrieved from https://securityintelligence.com/cybersecurity-awareness-is-about-both-knowing-and-doing/

Joseph Kaos Jr, 2021 June 28. Cybercrime increasing as more people rely on digital tech during pandemic, says PM. Retrieved from https://www.thestar.com.my/news/nation/2021/06/28/cybercrime-increasing-as-more-people-rely-on-digital-tech-during-pandemic-says-pm

Ken Taylor.(2020,June 12). Training Spend During the COVID-19 Pandemic. Retrieved from https://trainingindustry.com/articles/outsourcing/training-spend-during-the-covid-19-pandemic/

KPMG, 2015 May. Cyber security: a failure of imagination by CEOs. Retrieved from https://assets.kpmg/content/dam/kpmg/pdf/2015/12/cyber-ceo-report.pdf

Kotoritechnologies.(n.d). 10 Questions to Test Your Employee's Cybersecurity Awareness. Retrived from https://kotoritechnologies.com/test-cyber-security-awareness-in-10/

Li, L. X., He, W., Xu, L. D., Ash, I. K., Anwar, M., and Yuan, X. 2019. "Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behavior," Retrieved from https://www.researchgate.net/publication/332121058_Investigating_the_impact_of_cybersecurity_policy_awareness_on_employees%27_cybersecurity_behavior

Louisville.(n.d). Information Security User Awareness Assessment. Retrieved from https://louisville.edu/security/files/user-awareness-questionnaire-pdf

Malaysia Cyber Security Strategy 2020-2021, nd. Retrieved from https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf

Marthie Grobler, Joey Jansen van Vuuren and Jannie Zaaiman2, 2013 April. Evaluating cyber security awareness in South Africa. Retrieved from https://www.researchgate.net/publication/228501727_Evaluating_cyber_security_awareness_in_South_Africa

Maria Bada, Angela M. Sasse, Jason R. C. Nurse, 2016 Jan 9. Cyber Security Awareness Campaigns: Why do they fail to change behaviour? Retrieved from https://www.researchgate.net/publication/274663655_Cyber_Security_Awareness_Campaigns_Why_do_they_fail_to_change_behaviour

Mimecast,2021. The state of email security report 2021. Retrieved from https://www.mimecast.com/globalassets/documents/ebook/state-of-email-security-report-2021.pdf

Mohamed Basyir, 2021 July 16. Malaysians suffered RM2.23 billion losses from cyber-crime frauds. Retrieved from https://www.nst.com.my/news/crime-courts/2021/07/708911/malaysians-suffered-rm223-billion-losses-cyber-crime-frauds

Mohd Shamir b Hashim, 2011, July 1.Malaysia's National Cyber Security Policy. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5978782
Nir Kshetri Bryan, 2019 April 9. Cybercrime and Cybersecurity in Africa. Retrieved from https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1603527

Norhayati Sarmoen, Haliyana Khalid, Siti Zaleha Abd Rasid, Shathees A/L Baskaran& Rohaida Basiruddin, 2019 Aug 16. Retrieved from https://www.researchgate.net/publication/335206163_Understanding_Human_Behaviour_in_Information_Security_Policy_Compliance_in_a_Malaysian_Local_Authority_Organization

Okenyi, P.O. and Owens, T. J., (2007). On the anatomy of human hacking. Information Systems Security. Retrieved from https://www.researchgate.net/publication/233431373_On_the_Anatomy_of_Human_Hacking

Pratapsingh Rathod, Ashutosh B Potdar, Study of Awareness of Cyber-Security among Medical Students, 2019 January. Retrieved from https://www.researchgate.net/publication/330978587_Study_of_Awareness_of_Cyber-Security_among_Medical_Students

Predrag TASEVSKI, 2015, IT and Cyber Security Awareness – raising Campaigns. Retrieved from https://www.researchgate.net/publication/297738173_IT_and_Cyber_Security_Awareness_-_Raising_Campaigns

Proprof. (n.d). Cyber security quiz. Retrieved from https://www.proprofs.com/quiz-school/topic/cyber-security

Ryan Fahey, 2019, Infosec Institute : Security Awareness Training. Retrieved from https://resources.infosecinstitute.com/category/enterprise/securityawareness/#gref

Samaher Al-Janabi, Ibrahim AlShourbaji, 2016 February. A Study of Cyber Security Awareness in Educational Environment in the Middle East. Retrieved from https://www.researchgate.net/publication/292672963_A_Study_of_Cyber_Security_Awareness_in_Educational_Environment_in_the_Middle_East

Sam Goundar, Chapter 3 - Research Methodology and Research Method, 2012 March, Retrieved from https://www.researchgate.net/publication/333015026_Chapter_3_-_Research_Methodology_and_Research_Method

Samuel J. Stratton, 2021 July 21. Population Research: Convenience Sampling Strategies, Retrieved from https://www.cambridge.org/core/services/aop-cambridge-core/content/view/B0D519269C76DB5BFFBFB84ED7031267/S1049023X21000649a.pdf/population-research-convenience-sampling-strategies.pdf

Sarrah Mullay 12 jul 2018, special report - MBA courses start offering digital security skills. Retrieved from https://www.ft.com/content/7b3cbe46-537e-11e8-84f4-43d65af59d43

Sedgwick Philip, 2013 October. Convenience sampling. Retrieved from https://www.researchgate.net/publication/291161903_Convenience_sampling/link/569e722408ae4af5254463e1/download

Sharique Ahmad, Saeeda Wasim, Sumaiya Irfan, Sudarshana Gogoi, Anshika Srivastava, Zarina Farheen, 2019 October. Qualitative v/s. Quantitative Research. Retrieved from https://www.researchgate.net/publication/337101789
Software Management: Security Imperative, Business Opportunity, 2018 June. Retrieved from https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf

Statista Research Department, (2020, Dec 15). Hours of training per employee in the training industry in the United States from 2017 to 2020, by company size. Retrieved from https://www.statista.com/statistics/795813/hours-of-training-per-employee-by-company-size-us/

Steven M. Furnell (University of Plymouth, UK and Edith Cowan University, Australia) and Ismini Vasileiou (University of Plymouth, UK), A Holistic View of Cybersecurity Education Requirements. Retrieved from https://www.researchgate.net/publication/332082965_A_Holistic_View_of_Cybersecurity_Education_Requirements

Singer, P. W., and Friedman, A. 2014. Cybersecurity: What Everyone Needs to Know. Oxford University Press. Retrieved from https://www.researchgate.net/publication/346865414_Cybersecurity_and_Cyberwar_What_Everyone_Needs_to_KnowRWhat_Everyone_Needs_to_KnowR

Stephen J. DeCanio • Catherine Dibble • Keyvan Amir-Atefi, 2014 May 14. The Importance of Organizational Structure For The Adoption of Innovations retrieved from https://www.researchgate.net/publication/227447261_The_Importance_of_Organizational_Structure_for_the_Adoption_of_Innovations

The definition of security awareness, 2017, July 6. Retrieved from https://resources.infosecinstitute.com/topic/security-awareness-definition-history-types/

Thomas Brewster, 2021, October 14. AI voice cloning is used in a huge heist being investigated by Dubai investigators, amidst warnings about cybercriminal use of the new technology retrieved from https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=7e59ad227559

Thomson M.E and R. Von Solms (1998), Information Security Awareness: Educating Your Users Effectively. Information Management & Computer Security, 6(4), 167-173. Retrieved from https://doi.org/10.1108/09685229810227649

Tomas Foltýn 1 Oct 2019, Cyber Security Awareness Month starts today!. Retrieved from https://www.welivesecurity.com/2019/10/01/cyber-security-awareness-month-starts/

Wejdan Aljohni, Nazar Elfadil, Mutsam Jarajreh, 2021. Cybersecurity Awareness Level: The Case of Saudi Arabia University Students. Retrieved from https://thesai.org/Downloads/Volume12No3/Paper_34-Cybersecurity_Awareness_Level.pdf.

Wolfgang Reinhardt, Peter B. Sloep & Hendrik Drachsler, 2012 September. Retrieved from https://www.researchgate.net/publication/230640624_Understanding_the_Meaning_of_Awareness_in_Research_Networks/link/55a6445408aeb00df23222e5/download

Yogesh Meena,Mahipal Singh Sankhla,Shriyash Mohril,Rajeev Kumar, 2020 October Cybercrime: youth awareness survey in Delhi NCR, India. Retrieved from https://medcraveonline.com/FRCIJ/FRCIJ-08-00325.pdf

Yogesh Shelokar, 2020 June 6. Cyber Security Awareness System. Retrieved from https://www.researchgate.net/publication/351541988_Cyber_Security_Awarenesss_System/link/609ca517a6fdcc9aa7ddbbcc/download

Yuen Meikeng, 2021 Sepember 19. Online threats continue to spike. Retrieved from https://www.thestar.com.my/news/focus/2021/09/19/online-threats-continue-to-spike