APEC Women Empowerment through Cybercrime-Free Workshop for Secure Online Trading in the 4th Industrial Revolution

Kuala Lumpur, Malaysia | 12 - 13 September 2023

APEC Policy Partnership on Women and the Economy

February 2024

Asia-Pacific
Economic Cooperation

Asia-Pacific
Economic Cooperation

APEC Women Empowerment through Cybercrime-Free Workshop for Secure Online Trading in the 4th Industrial Revolution

Kuala Lumpur, Malaysia | 12 - 13 September 2023

APEC Policy Partnership on Women and the Economy

February 2024

APEC Project: PPWE 02 2022A

Produced by

Project Overseer
Universiti Kebangsaan Malaysia
Website: www.ukm.edu.my

Ministry of Women, Family and Community Development, Malaysia
Website: www.kpwkm.gov.my

FSKTM Technovation Sdn Bhd
Website: https://www.technovations.com.my/

For
Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

APEC#224-PP-01.3

Table of content

1. Executive Summary

In the era of IR4.0, women, particularly those working in business, aggressively embrace the application of smart technology. The growing usage of smart technology has facilitated online commerce for small and medium-sized firms (SMEs). As a result, it is critical to incorporate the community's digital well-being as an intrinsic component of long-term economic development. Cyber and ICT crimes such as digital harassment, financial fraud, phishing, e-commerce fraud, and love scams regularly target women as victims. Addressing these difficulties is critical for establishing a secure digital environment and assuring the economy's overall success.

Based on the study conducted by APEC in 2019, digital harassment or stalking has been severely experienced by young women aged 18 to 24. While in another part of Europe, more than 20 million women have experienced digital harassment at the early age of 15. It was also stated that 0.6% to 3.5% of the population in Europe is reported to be the victims of online purchasing fraud every year. In Indonesia, the cyber and ICT crime index has reached 0.62, higher than the global average (0.54), based on the survey reports (Widiasari & Thalib, 2022).

To address these challenges, the APEC Women Empowerment Free Cybercrime Workshop was developed and organized to empower women and enhance their entrepreneurial capabilities in the digital arena. The project intends to raise cyber and ICT crime knowledge among women to promote safe online trading, in line with the La Serena Roadmap for Inclusive Growth. This project supported APEC women's participation in the digital economy and innovation through capacity-building activities, including networking, mentoring, and developing technical skills to ensure secure online trading.

A preliminary study was conducted to assess the cyber and ICT crime awareness level among potential participants in the workshop. This initial effort also gained a deeper insight into the cyber and ICT crime issues in online trading activities. On 4 July, the preliminary study was conducted, participated by twenty-five participants, mostly women. The findings of the preliminary study were analyzed to find the correlation of the workshop modules with the participant level of cyber and ICT crime awareness.

The findings were analyzed using a one-sample t-test through SPSS analysis. The results showed that each indicator (topic) in the modules has significant differences, which can improve the participants’s awareness of cyber and ICT crimes. This can be justified when most respondents showed moderate and excellent knowledge of cyber and ICT crime awareness; however, some respondents were unaware of common preventive measures to avoid becoming victims of cyber and ICT crimes.

The APEC Women Empowerment Free Cybercrime Workshop was held on 12 – 13 September 2023 at Cititel Mid Valley Hotel, Kuala Lumpur. The event drew 80 participants, comprising 92% women and 8% men. The workshop comprised diverse activities, including forum discussions, session sharing, practical exercises,

presentations on case studies, and pre- and post-test assessments. The sessions provided in-depth discussions on securing online trading and covered topics such as cyber and ICT crime and threats, cyber laws, online attack demonstration, preventive measures, incident and emotion handling, and sharing of best practices.

The workshop began with a forum discussion featuring cyber and ICT crime experts entitled "**Secure Our Online Trading in the 4IR Era**". The forum discussed several topics related to why cyber and ICT crime is still ongoing despite having a bunch of methods to prevent cyber and ICT crime from occurring and suggestions for individuals to protect themselves. An expert from the Taiwan Academy of Banking and Finance, Chinese Taipei shared his opinions on the supply and demand for scam threats. The correlation between scam price and technical sophistication cyber threat level depends on the type of economy. For example, developing economies have less sophisticated levels of cyber-attacks. However, they may have a high volume of cyber-attacks due to the low skills of labourers.

The Assistant General Manager of the Security Incident Response Team from TM Tech Ltd Company shared a variety of real-life cyber and ICT crime situations. She explained that TM Network often encountered spam, fraud, spoofs, Wangiri scams, and short message service (SMS) phishing. Those who blindly trust these cyber and ICT crimes will easily be the victims. The Cybercrime Officer from the United Nations Office on Drugs and Crime later explained the involvement of ransomware as malware from crypto virology that affects virtual assets (cryptocurrency). The cyber and ICT crimes impact the individual and the whole economy. An Associate Professor at the University of Melbourne under the School of Computing and Information Systems also emphasized his concern and suggested adequate cybersecurity technological investments are needed to secure online trading.

Following the forum, module presentations and practical sessions were conducted. The participants were also engaged in interactive activities using the Slido application during the module presentations (Adnan et al., 2023). The first session for module presentation was the Cybercrime and Threat module. The presenter introduced several types of cyber and ICT crimes that occur frequently, such as Denial of Service (DOS) attacks, Internet bots, Brute Forde attacks, cross-site scripting, SQL injection, spamming, cyberbullying, phishing, malware, and human error. The participants were also aware as the presenter showed how love scams, type allocation codes (TAC), one-time passwords (OTP), and investment scams work worldwide. A police officer also shared several real case studies on love scams, e-wallet account hacking, and tele-fraud.

The second session of module presentations was on the Best Practice module. The participants learned about one of the best secure online trading practices, security hardening. The presenter also shared the steps on how to apply security hardening, which is by using a secure e-commerce platform, implementing a Secure-Socket Layer (SSL), applying multi-factor authentication (MFA), avoiding public Wi-Fi and public computers or using Virtual Private Network (VPN), implementing data privacy

protection, and educating the employees and clients. To be more aware of cyber and ICT crime, the session continued with the Cyber Law Awareness module. Consumer Protection Law is important to be notable. The participants learned four things to be aware of for the Consumer Protection Law: warranty, fair treatment, correct information, and valid advertisement.

Understanding the online attack narrative or modus operandi has helped the participants to be more concerned about everything, including the small details of the online attack. An online attack that had been demonstrated was juice jacking. Nowadays, many public places provide charging devices in case of emergency state. However, with their adversary in mind, the perpetrators of cyber and ICT crimes use public charging devices to perform their wrongdoings. They attack using the USB charging port when other people use public charging devices. The participants become more aware of this threatening issue of using public charging devices.

Besides the technical method, the participants also learned about the affective aspect. Handling emotions from a spiritual and rejuvenating perspective is the simplest way for anyone to try. Observing nature can ease the mind of the victim. Practising effective breathing techniques can improve blood circulation and help think in peace, especially for cyber and ICT crime victims. The victim, who has been scammed, just felt very sad and depressed. Through this module, the participants learned how to cope with negative emotions. After that, the participants learned about incident handling. As the victim can manage their emotion perfectly, they can have good incident handling. The presenter also highlighted the types of data extraction techniques that can easily be applied through mobile phones: manual, logical, and physical data extractions. These techniques can help the cyber and ICT crime victims have their justice. They can have enough evidence to report the perpetrator.

During the practical session, the participants learnt several preventive measures to protect and secure digital assets and business activities. Simple preventive measures are often to be neglected. Therefore, this module provided preventive measures such as determining authentic websites and securing their shopping and social media accounts. The participants become more aware of these simple preventive measures, and they will practice them in their daily lives.

To evaluate the impact, pre-and post-test assessments were conducted in the workshop to measure the level of cyber and ICT crime awareness among participants. The findings from these tests have shown a significant improvement in cyber and ICT crime awareness by the end of the workshop. In a nutshell, each module contributed to increasing participants' awareness of cyber and ICT crime. The improvement observed in the pre- to post-test assessments indicates that participants increased their knowledge and awareness of cyber and ICT crime. These modules are deemed essential for anyone to apply daily, serving as crucial tools to prevent falling victim to cyber and ICT crime.

2. Introduction

2.1 Background

Women are consistently depicted as the victims of cyber and ICT crime. This trend is particularly concerning, especially given the ongoing advancements in high-technology gadgets. According to Lazarus et al. (2022), online fraud occurs when someone gains financial advantage through deception, impersonation, manipulation, counterfeiting, forgery, or Internet use. The environment of online fraud is compelling, making cyber and ICT crime victims fall into the trap. From the survey by Ghani & Ghazali (2020), 34 of 150 young women have the experience of becoming cyber and ICT crime victims. These women were scammed when engaging on e-commerce platforms or dating applications.

Cyber and ICT crimes include telecommunication crimes (Macau scams), love scams, parcel scams, online fraud, non-existent loans, and phishing. Lack of information security awareness applied to social media users is the cause of most cyber and ICT crime cases (Saizan & Singh, 2018). This proportion concludes that women must enhance their cyber and ICT crime awareness. A study by (Saad et al. 2018) explained that those with fewer computer skills and low cyber and ICT crime awareness would easily fall victim to cyber romance fraud. According to (Al-Nasrawi, 2020), more than 70% of women and girls are exposed to cyber violence, and most of these cases are not reported worldwide.

This project is an extension of the Malaysia Women Free Cybercrime (Sibernita) Workshop held in 2021 through the Zoom platform (Yusof, M.S.B. et al, 2022) (Mohd et al., 2021). The positive contribution of participants from the Sibernita workshop motivates the continuity of the awareness program. Previously, the Sibernita workshop only delivered four workshop modules: i. Recognizing Cyber and ICT crime and threat, ii. Cyber and ICT crime Prevention, ICT Software and Tools, iii. Best Practices in Handling Cyber and ICT crime, and iv. Reflection. Based on these extant modules, this project has improved them to be more specific in online trading aspects, such as the demonstration of online trading attacks, the explanation of specific cyber and ICT laws related to online trading, or the emotional and incident handling module for the current victims.

Figure 1 shows the phases of the project implementation. Based on the Sibernita modules, the module developer has enhanced the new workshop modules following the project objectives. The new workshop modules were tested in the preliminary study to be improved before the actual workshop. With the improved workshop modules, the APEC Women Empowerment Free Cybercrime Workshop was held on the 12 – 13 September 2023 at Cititel Hotel, Mid Valley, Kuala Lumpur. Later, the pre- and post-survey workshop findings are assessed and analyzed to determine the effectiveness of the cyber and ICT crime awareness program on online trading. Lastly, the project contractor wrote a report summarising the workshop findings. More information on the workshop can be found on the website: https://awfreecybercrime.com/ .

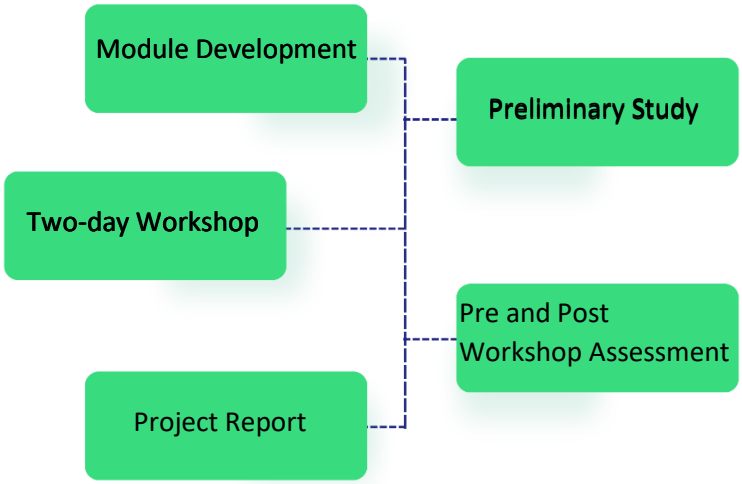


Figure 1: Phases of project implementation

2.2 Project Objectives

This project aims to empower women with the essential cyber skillsets to safeguard during online trading. Hence, the specific objectives are:

a) To be familiar with cyber and ICT crime and threats in the online trading environment,
b) To understand Law and Best Practices related to information security and
c) To apply hands-on information security preventive measures for secure online trading.

3. Preliminary Study

3.1 Introduction

This preliminary study aims to identify areas for improvement in the developed modules and the specific needs of the expected participants. The preliminary study measured five sub-modules:

a) Module 1 explained the vulnerabilities, threats, and risks of online trading for female participants, including the case studies related to scammers. The objective of module 1 is to discuss the cyber and ICT crime trends and security risks associated with online transactions, e-commerce, and data privacy for social media, mobile devices, and the Internet of Things (IoT).

b) Module 2 highlighted the cyber law, and data privacy that protects participants from cyber and ICT crimes. The participants understand the importance of applying security best practices in the online business environment, systems hardening techniques to secure online business environments, and data privacy protection for clients.

c) Module 3 advocated that participants identify suspicious trading websites/social media accounts and the Secure Sockets Layer (SSL) certificates in online selling platforms. This module introduces techniques to protect online trading

accounts (as a seller) and helps students understand the strategy to prevent the Internet from cyber and ICT crime.

d) Module 4 guided participants on managing depression and practising the systematic reflection method for maintaining a calm mind to avoid overreacting emotions that can deter participants' rational thinking after facing a cyber and ICT crime event.

e) Module 5 explained the evidence-handling process of acquisition, collection, and preservation based on the application and the device (PC, tablet, smartphone) acting as a first responder while conducting digital forensics.

3.2 Results of Preliminary Study

The study showed that the participants gained knowledge after attending the workshop. Based on Figure 1, every indicator representing module topics has shown an increased awareness of cyber and ICT crime. The indicators represent topics of

i. Cyber and ICT crime and threat
- VTR (Vulnerabilities, Threats, and Risks)
- SP (Scammers: Phone)
- SE (Scammers: Email)
- SW (Scammers: Ewallet)

ii. Cyber Law and Best Practices
- CL (Cyber and ICT Law)
- DP (Data Privacy)
- CR (Consumer Right)
- A (Alert on suspicious actions and react accordingly)
- H (System hardening produces a secure online trading environment)

v. Preventive Measures
- R (Responsible on customers' PII)
- I (Identify suspicious trading websites/social media accounts/other platforms)
- SSL (Identify the Secure Sockets Layer certificates in the online selling platform)
- E (Identify suspicious email)
- AI (Android/IOS)

vi. Emotion Handling
- WCR (Women cyber and ICT crime Reflection)
- M (Mindset to react)

vii. Incident Handling
- AC (Acquisition)
- C (Collection)
- P (Preservation)

viii. Cyber and ICT crime Awareness (CA)

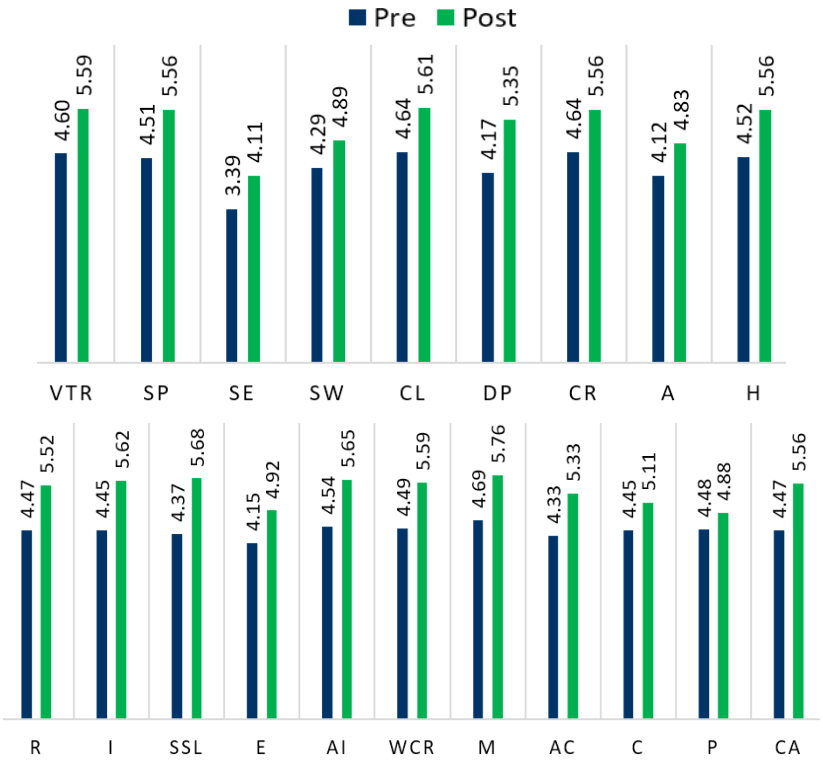


Figure 2: The mean difference between results of pre and post-survey for preliminary study.

As shown in Figure 2, the post-test results show some improvement compared to the pre-test for each module component. This early improvement explains that the participants knew the importance of the APEC Women Free Cybercrime Workshop module and the possibilities of cyber and ICT crime incidents. However, the participants needed further exposure to handle the cyber and ICT crime situation rationally.

3.4 Gap Analysis and Future Directions

The preliminary study of the APEC Women Cyber and ICT crime-Free with initially developed modules has identified several limitations that require improvement as follows:

a) Module 1 - The functions and processes involved in each online trading stage must be explained so the participants can understand how online trading works. The features of secure online trading must also be justified to highlight the economic aspects of online trading commencement within a secure system.

b) Module 2 - Demonstration of the preventive measures must incorporate practical activities for effective comprehension.

c) Module 3 - A detailed explanation regarding money laundering AMLA by sharing a real case study, elaborating on personal data, taxation, and the Jurisdiction of the cyber law, including contracts, privacy, rights, and liability.

d) Module 4 - To include the Window log activities and the importance of VPN for security purposes by creating a scenario that illustrates the process of removing cookies, provides a general overview of browser exercise, addresses cross-site tracking, emphasizes password strength checking, and evaluates URL validity can instantly raise awareness among the audience.

e) Module 5 - Explanation of the effect of cyber and ICT crime attacks such as digital harassment, digital espionage, and pornography. Additionally, it is important to provide information on the Digital Wellness Compliance /Counseling Approach. The integration of active learning sessions helps participants engage with the module contents.

The preliminary study shows its significance in empowering cyber and ICT crime awareness among women and men, especially online trading. This workshop module taught the participants the technical and emotional parts of handling cyber and ICT crime. Conclusively, the participants gained insight into the tactics applied by scammers, such as love scams or job scams, and how to encounter this cyber and ICT crime situation properly. A full study report is in Annex 1.

4. Workshop

4.1 Introduction

The two-day workshop was held on 12 – 13 September 2023 (Agenda Annex 2) in Kuala Lumpur to spread awareness of cyber and ICT crime related to online trading. The workshop was attended by a total of 80 participants, including representatives from APEC economies, government officials, women entrepreneurs, non-governmental organizations (NGOs), and academicians. The workshop included several sessions with expert sharing and presentations, interactive sessions to engage with participants through the Slido application, and breakout sessions to maximize learning and knowledge retention. In a nutshell, the workshop objectives are as follows:

- To ensure the participants understand recent women's cyber and ICT crime modus operandi
- To identify the preventive or countermeasure elements to sustain women's cyber and ICT crime-free community
- To determine the awareness level of cyber law and best practices among women involved in digital trading.

4.2 Workshop Sessions

The photos of the workshop activities are shown in Annex 3.

4.2.1 Welcoming Remarks

In partnership with Universiti Kebangsaan Malaysia (UKM) and the Ministry of Women, Family, and Community Development (KPWKM) and with the full support of the Asia-

Pacific Economic Cooperation (APEC), two distinguished figures have been invited to deliver welcoming remarks. They were Her Excellency Dato' Sri Hajah Nancy Shukri, the Minister of Women, Family, and Community Development, and Ms. Chantelle Stratford, the Policy Partnership on Women and the Economy Chair.

Her Excellency Dato' Sri Hajah Nancy Shukri expressed gratitude to Universiti Kebangsaan Malaysia and FSKTM Technovation for coordinating the workshop. She encouraged participants to actively engage in the module's activities, emphasizing the importance of acquiring valuable knowledge during the workshop. Highlighting the significant digital threats faced by Malaysia, she underscored the government's commitment to enhancing public education in digital literacy and reinforcing law enforcement measures.

In response to the escalating cyber and ICT challenges, the government has established the National Scam Response Centre (NSRC) in collaboration with key stakeholders, including Bank Negara Malaysia, private banks, the Malaysian Communications and Multimedia Commission, and the police. These entities are working together to assist cyber and ICT crime victims, aiming to minimize losses and prevent further incidents.

Utilizing a pre-recorded video for the event titled "Advancing Women's Economic Empowerment in APEC | APEC", Ms. Chantelle Stratford delivered a speech addressing the goal of achieving a gender-equal society and economy. In her presentation, she highlighted APEC's commitment to enhancing women's skills and providing training opportunities to enable women to participate actively in both economies and society. Ms. Chantelle Stratford conveyed her speech on gender equality in society and the economy. She also stated that APEC focused on amplifying women's skills and the training that could help women to participate in the economy and society.

4.2.2 Forum

A forum entitled "**Secure Our Online Trading in the 4IR Era**" was moderated by Dr. Raja Jamilah Raja Yusof, a senior lecturer from Universiti Malaya who is also a member of IEEE Women in Engineering (WIE) and the International Muslim Women Union (IMWU) Malaysia Branch. Esteemed forum panelists representing diverse organizations are Dr. Atif Nisar Ahmad from the University of Melbourne, Australia, Mr. David Stinson from the Taiwan Academy of Banking and Finance (TABF), Chinese Taipei, Ms. Daniela Dora Eilberg from the United Nations Office on Drug and Crime, and Ms. Patrina Nasiron from Telekom Malaysia.

Representing the TABF, Chinese Taipei, Mr. David Stinson, responsible for managing international partnerships in financial training, explained the relation of information security to financial fraud and how it differs between advanced economies and the developing world. Mr. David explained the supply and demand for scam threats, where the demand refers to the willingness to pay. The scam price corresponds to the technical sophistication level of digital-attacks. He also stated that developing economies can easily be attacked by using only social engineering instead of a higher

sophistication level of digital-attacks such as hacking (as shown in Figure 3). Unlike developed economies, a high number of less skilled laborers in developing economies may escalate the volume of digital-attacks.

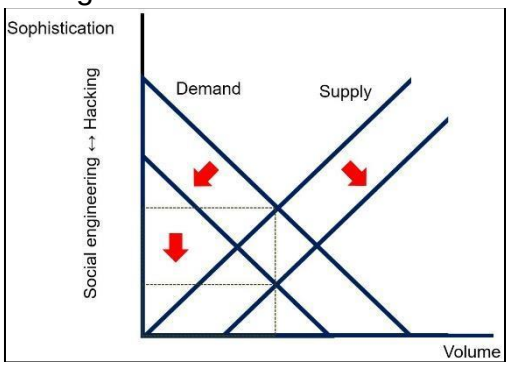


Figure 3: Developing economies have less demand and more supply, leading to less sophistication in attack types, but not necessarily less volume of attacks

Then, Mr. David shared that the information security threat landscape will evolve over the foreseeable future. He justified supply and demand under technological innovation. New technologies generally open new markets and increase demand and supply. “Technologies” can include market development as well as programming innovations. Ransomware is when the attackers lock and/or exfiltrate victims’ files. Ransomware as a Service (RaaS) markets for active breaches are a source of secondary market demand. This form of market development helps justify using economic analysis in information security. Large Language Models (LLMs) such as ChatGPT can engage in logical conversation, and regulations and safeguards are unlikely to be effective against organized threats. Fine-tuning by model developers is easily evaded by users, and open-source pre-trained models can be self-hosted. In the longer term, restricting the training process will also be difficult.

As a second panelist, Mrs. Patrina Nasiron, the Assistant General Manager for the Security Incident Response Team in TM Tech Sdn Bhd, shared Telekom Malaysia's efforts in combating online fraud and scams. Mrs. Patrina also shared the real-life scenarios encountered by the TM Network, such as spam calls, scam calls, fraud calls, spoof calls, Wangiri (a scam where the caller makes a call to mobile numbers and then hangs up, anticipating that the victim will be curious enough to call back) and short message service (SMS) phishing.

Mrs. Patrina informed the audience that TM had played a major role in combating telecommunication fraud with 24/7 proactive monitoring and blocking suspicious call attempts through the TM network. TM, Malaysian Communications and Multimedia Commission (MCMC), and other telecommunication organizations have formed the Telecommunications Fraud Task Force to combat fraud effectively. TM also provided nationwide fraud awareness to PABX/IP PABX customers.

Mrs. Patrina then explained actions that need to be taken to avoid being scammed and what action to take if we get scammed. For example, if the participants encounter a Macau Scam situation, they must first not panic and contact the Malaysia Bank

hotline at 1-300-88-5465. The participants can also check the phone or account number given by the scammer using https://semakmule.rmp.gov.my, an application developed by the Commercial Crime Investigation Department of Royal Malaysia Police. She also stated that if financial scammers victimized the participants, they should immediately call the bank's scam hotline of the Malaysia Scam Response Centre at 997 and lodge a police report.

Next, Dr Raja Jamilah asked Ms. Daniela to briefly explain cryptocurrencies and what needs to be raised attention to secure online lives. Ms. Daniela Dora Eilberg, the Cybercrime Programme Officer at the United Nations Office on Drugs and Crime, explained that ransomware attacks are cyber and ICT crimes related to virtual assets (cryptocurrency). She defined ransomware as malware from crypto virology that threatens to publish or delete people's data. The money that the perpetrator received will be used for any criminal activity. She also highlighted that cryptocurrency is an increasingly popular scenario. Regulation plays an important role in protection, as shared by Ms. Daniela. Correct protection, standards for the latest industry, how to detect and prevent cyber and ICT crime, determining systems of security protocols, information security control, and periodically reporting staff compliance are some essential checklists that any organization needs to keep in mind.

Ms. Daneila also explained types of scams such as email, phone, finance, impersonation, romance, clickbait, text/SMS, and many more. She also explained how modus operandi shopping scams work and shared technical tips to tighten our security. Firstly, stay aware and know that scams, phishing, and identity theft exist. Then think before clicking any link, verify a site's security, check your online accounts regularly, keep your browser up to date, use a firewall, be aware of pop-ups, never give out personal information online, use antivirus software, and lastly, use two-factor authentication (2FA).

The discussion continued with Dr. Atif Nisar Ahmad, an Associate Professor at the University of Melbourne under the School of Computing & Information Systems. He shared regarding the impacts of critical cyber incidents on organizations. He highlighted that the most obvious impact upon detecting an ICT incident involves financial costs related to digital response, particularly for technical investigation and handling customers affected by the incident. Furthermore, managing public relations, especially when the business requires the public to know or needs to know, will lead to additional costs for remediation and legal fees.

In addition, Dr. Atif also emphasized a critical concern: the potential disruption to business operations caused by the prolonged unavailability of Information and Technology (IT) services that subsequently will increase costs to the organization. The significant consequences for organizations are obvious reputation and intellectual property. The devaluation of a brand name affects customers' trust and relationships. Regaining trust proves challenging, plus it affects market share, thereby increasing competitive disadvantages.

Dr. Atif was asked to share his opinion on what organizations could do now to avoid the severe impacts of digital-attacks. Dr. Atif explained that to secure online trading, adequate investment in information security technological solutions needs to be considered. He advised users to consider fundamental aspects such as identifying information or IT assets critical to their business, assessing the impact on customer relationships, and developing a comprehensive business continuity plan (BCP) to address various attack types. These collective proactive actions prevent organizations from investing in expensive technical solutions (opportunity cost) that might worsen their business situation.

As the forum concluded, Dr. Raja Jamilah emphasized that we should be more concerned about frauds that relate to social aspects rather than focusing too much on the most sophisticated ones. The community needs to be vigilant and aware of current media news to avoid becoming victims of such activities and not just rely on government agencies such as TELEKOM, Cyber Security Malaysia (CSM), Royal Malaysia Police (RMP), and Ministry of Communication and Multimedia Commission (MCMC). Additionally, she encouraged participants to take an active role in educating and sharing information regarding voice/online fraud among family members, especially older people, to mitigate the risk of falling into scams.

4.2.3 Modules Presentation

a. Cyber and ICT crime and Threats

The Cyber and ICT crime and Threats module was presented by Prof. Dr Madihah Mohd Saudi, a professor from Universiti Sains Islam Malaysia (USIM) and ASP Siti Baizura Mohd Yusof, Royal Malaysia Police (RMP). Relating to her expertise, which is Malware and Mobile, Prof. Dr. Madihah started the presentation by introducing different types of cyber and ICT crimes, such as Denial of Service (DOS) attacks, Internet bots, Brute Forde attacks, cross-site scripting, SQL injection, spamming, Internet-bullying, phishing, malware, and human error. The number of cyber and ICT crime victims continues to rise as perpetrators get smarter at exploiting victims' weaknesses. Prof. Dr. Madihah shared three situations on how love, Type Allocation Code (TAC) or One-Time-Password (OTP), and investment scams work worldwide. She also shared steps to take when encountering an early digital-attack situation. These include refraining from sending compromising pictures, avoiding disclosing excessive personal information, refraining from physical meetings with unfamiliar individuals, taking caution from believing information from strangers, refusing to accept money from someone they have not met, and adhering to various other precautionary measures.

Next, ASP Siti Baizura described real case studies on love scams, e-wallet account hacking, and tele-fraud. The purpose of sharing the real case studies is to inform the participants that such cyber and ICT crimes occur daily (Ismail et al., 2018). Related to the outcome of this module, which is to help participants explain the cyber and ICT crime trends and security risks associated with online trading to accelerate their

knowledge and capability to respond correctly based on the case studies, she concludes that cyber and ICT crime is a growing threat that involves criminal activities using digital technologies or the internet. It can cause significant financial losses and reputational damage. The key takeaway is to approach situations logically, recognizing that nothing is free or easily gained. Maintaining vigilance, awareness, sensitivity, and verification attitude before taking action is crucial.

b. Best Practices

Assoc. Prof. Dr. Normaziah Abdul Aziz from International Islamic University Malaysia shared her insightful knowledge on the best practices to avoid becoming a cyber and ICT crime victim. Her specialization is digital forensics, related to the module outcome on delivering security best practices in the online business environment. She included explaining the systems hardening to secure the online business environment and data privacy protection for clients. She started with an introduction to the front end and back end of the online business processes that involve payment activities.

She defined a payment gateway (PG) as an online service that allows businesses and individuals to accept customer payments (debit/credit card, digital wallet) through their websites or mobile applications. PG bridges securely between the customer's payment and the merchant's bank account. She shared a few steps that can be applied by online business operators for security hardening, such as using a secure e-commerce platform, implementing a Secure-Socket Layer (SSL), applying multi-factor authentication (MFA), avoiding public Wi-Fi and public computers or using Virtual Private Network (VPN), implementing data privacy protection, and educating the employees and clients.

c. Cyber Law Awareness

Leveraging her legal expertise, Prof. Dr. Nazura Abdul Manap from Universiti Kebangsaan Malaysia presented a Cyber Law Awareness module. The objective was to disseminate crucial information about cyber and ICT law that may be overlooked by the community in Malaysia and other economies, covering aspects such as data privacy and related acts enforced globally. The outcome of this module was to help the participants identify the laws relating to cyber laws and online trading, to relate between the issues in online trading and the laws, and to equip themselves to adhere to the applicable laws.

She shared four things to be aware of regarding Consumer Protection Law: (1) warranty, (2) fair treatment, (3) correct information, and (4) valid advertisement. Suppose there are issues related to personal information, such as someone reusing personal data for unrelated purposes without the consumer's consent. In that case, it will fall under the Data Protection and Privacy Law.

There are several ways to address data privacy issues in e-commerce where businesses should prioritize publishing a clear and comprehensive privacy policy. This policy should outline how businesses handle customer-sensitive information after

making a transaction and data collection and retention details. Moreover, businesses should use the most trusted and secure platforms for payment authorization to mitigate any potential breaches of information related to payment details. In conclusion, all e-commerce websites should ensure they provide the following information to their customers: clear and detailed information about the product, delivery information, and exchange and refund policies.

d. Online Attack/Threat Demonstration

Ts. Dr. Ahmad Firdaus Bin Zainal Abidin from Universiti Malaysia Pahang Al-Sultan Abdullah specialized in research areas of Mobile Security, Artificial Intelligence, Blockchain, and Intrusion Detection Systems. Dr. Ahmad Firdaus emphasized that the module aims to help participants understand the attack mechanism by the perpetrators and ways to counter it. He demonstrated the cyber and ICT crime attack in several situations, such as cracking Wi-Fi passwords, Wi-Fi attacks, getting access to the victim's machine, access attacks, phishing attacks, conducting phishing from Facebook, and illustrating attacks from USB charging ports (juice jacking).

Dr. Ahmad Firdaus demonstrated and deliberated three impacts on online trading that adhere to Wi-Fi password cracking: man-in-the-middle attacks, network sniffing, and executing dangerous malicious actions. The Man-in-the-Middle attacks will also lead to IT system compromise and data theft activity. Next, he demonstrated how perpetrators easily access the victim's machine using the Server Message Block (SMB) service. SMB is a network file-sharing protocol that allows devices and systems to share files, printers, and other resources over a local network or the internet. Lastly, he showcased an attack using a USB charging port called juice jacking. Juice jacking involves hacking into smartphones or other smart devices via a compromised USB charging port, typically encountered when charging devices in public spaces like airports, hospitals, coffee shops, or other public charging booths.

e. Preventive Measures

Assoc. Prof. Dr. Zulaiha Ali Othman from Universiti Kebangsaan Malaysia (UKM) and facilitators from Special Interest Group (SIG) Cyberhack and Ethics conducted practical sessions on preventive measures. The participants were divided into two groups based on their mobile phone operating system: the IOS and Android groups. This module aims to help participants identify suspicious trading websites or social media. The contents of this module were on (i) Securing communication, (ii) Android and IOS, (iii) eWallet, (iv) eCommerce-Shoppee, (v) eCommerce-Social Media, (vi) Windows 10, and (vii) browsers.

Starting with the topic of securing communication, facilitators explained how to use public Wi-Fi securely. With the latest version of Wi-Fi Protected Access (WPA), participants were guided on assessing their password strength through the Password Strength Test. The session also covered skills such as identifying fake websites, configuring a VPN for enhanced security, and logging out.

Then, facilitators shared how to strengthen the security of operating systems (Android and IOS). Android users were instructed to restrict application access to One Drive, activate Google Play Protect, manage pop-up notifications, implement screen lock and application lock passwords, clear cookies, and leverage additional safety features on Google. Meanwhile, iOS users were guided through setting up data privacy measures, including user consent, application tracking transparency, private browsing, cookie removal, location and autofill password disabling, and physical privacy measures such as two-factor authentication, facial recognition/fingerprint/passcode, restricting **Siri & Search access** when the iPhone is locked, and activating the Find My application.

For preventive measures to secure the eWallet application, the participants learned how to set the eWallet lock, configure security questions, enable two-factor or multi-factor authentication, and restrict the top-up amount of the eWallet. Afterwards, facilitators shared a beginner guide to privacy and security settings on Shopee, an e-commerce platform for recognizing authentic websites, tips to prevent scams, techniques to verify trusted Shopee shops, and keeping Shopee accounts more secure. The facilitators also explained e-commerce on Social Media platforms, including the ways to shop safely on Facebook, privacy settings for Facebook, how to shop safely on TikTok and privacy settings on TikTok.

f. Emotion and Incident Handling

Assoc. Prof. Dr. ‘Adawiyah Ismail from the Faculty of Islamic Studies, UKM, addressed emotional handling from the spiritual and rejuvenating perspective by observing nature flora and fauna, such as sea or river breezes. Another reflection activity presented by Dr. Azianura Hani Shaari from the Faculty of Social Sciences and Humanities is an effective breathing technique to calm the mind instantly. This module provides psychotherapy and behavioral approaches to help the cyber and ICT crime victim emotionally recover.

Assoc. Prof. Dr. Khairul Akram Zainol Ariffin from the Center for Cyber Security, Universiti Kebangsaan Malaysia, explained best practices for handling cyber and ICT crime evidence. He described methods to extract data from a smartphone, understand the application's features, examine email headers, and manage evidence if the participants use social media and online shopping platforms. Dr. Khairul Akram highlighted three types of data extraction techniques on mobile devices: manual data extraction, logical data extraction, and physical data extraction. The participants need to understand the application features, such as email. The headers contain significant information such as message sent time, unique identifying numbers, and the IP address of the sending server, which are important evidence to be reported. For online shopping platforms such as Shopee, the participants can identify and screenshot the important information such as Chat, Profile, or Purchase log to be kept as evidence.

Cyber and ICT crime generally evolves rapidly according to the borderless community's knowledge, skills, and attitudes. Knowing human errors are the weakest point, at the end of the program, Associate Professor Dr Siti Norul Huda Sheikh Abdullah, the APEC project overseer, encouraged the participants to be consistently

well equipped with recent essential skill sets in keeping pace with the secure cyberspace ecosystem at the 4IR era. For example, Universiti Kebangsaan Malaysia offers a Professional Certification in Cyber Protection course to raise awareness about the current threat landscape in the digital world. This course is conducted practically and interactively, covering various proactive preventive measures that can be taken to enhance human safety.

Associate Professor Dr. Mohd Ridzwan Yaakub, Deputy Dean of Industry and Community Partnerships, Faculty of Information Science and Technology (FTSM), UKM, also appreciated the workshop's organizers and attendees. To conclude the two-day course, he emphasized the Centre for Cyber Security, a prominent institution within FTSM, UKM, that has offered innovative solutions to protect communities and organizations from the ever-changing digital threat scenario through rigorous research, education, and consultation.

5. Pre and Post Workshop Assessment

5.1 Introduction

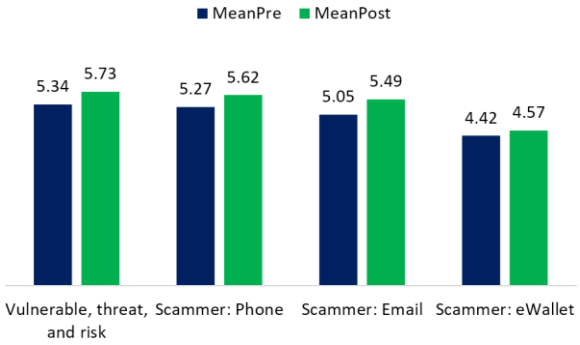
The pre and post workshop assessments were conducted to measure participants' understanding, knowledge, and level of information security awareness before and after they attended the workshop using the 6-Likert scale. The 6-Likert scale consists of (1) Very Not Satisfied, (2) Not Satisfied, (3) Moderately Not Satisfied, (4) Moderately Satisfied, (5) Satisfied, and (6) Very Satisfied.

The questionnaire comprises 79 questions, each addressing specific subtopics covered in the workshop modules. The same questions were asked for the post-test to measure the difference in participants' cyber and ICT crime awareness levels.

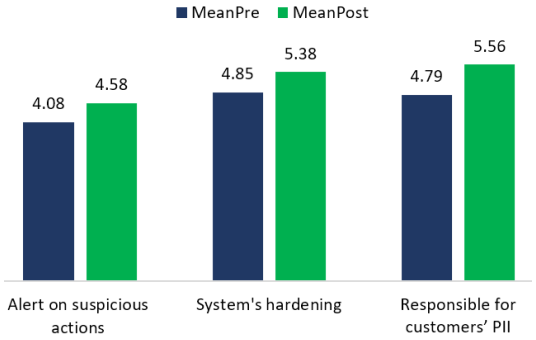
5.2 Result and Discussion

Based on the findings on demography, 42% of participants engage in online trading as buyers, 38% do not use online platforms for trading, and 18% participate in online trading as both buyer and seller, while only 1% act as sellers. This distribution describes that most participants have online trading experience. Concern about potential scams victimizing them may influence the 38% who do not use online platforms for trading.

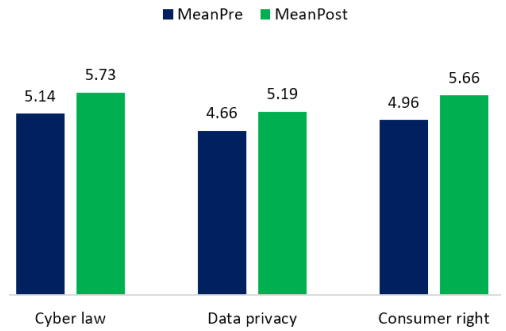
Regarding operating systems, 59% of participants use Android, while 41% use IOS. Android is more susceptible to malware attacks than IOS, which justifies the importance of having information security knowledge to avoid becoming the victim of cyber and ICT crime. The findings of the pre-and post-workshop assessments are explained below.



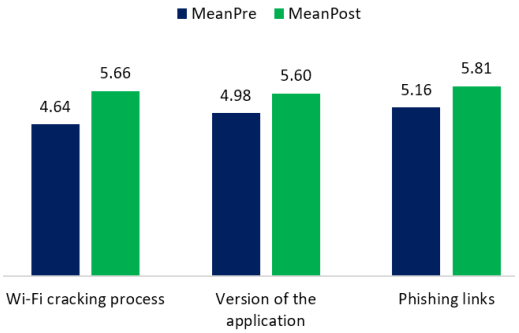
(a) Cyber and ICT crime and Threat Module



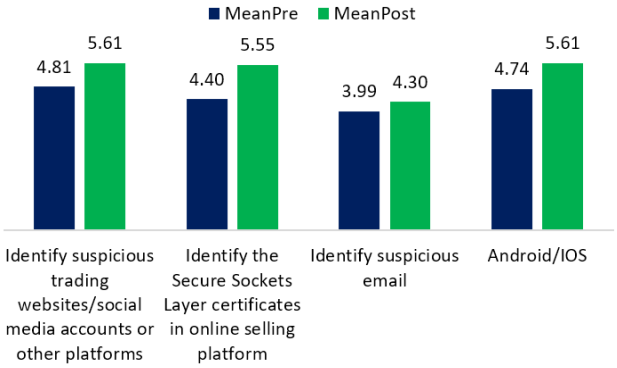
(b) Best Practices Module



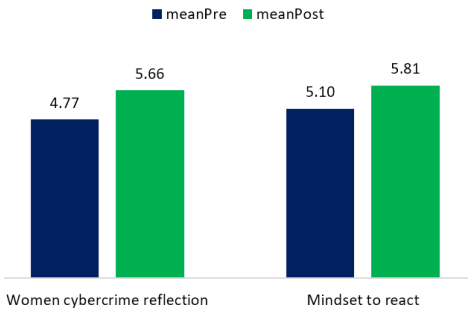
(c) Cyber and ICT Law Awareness Module



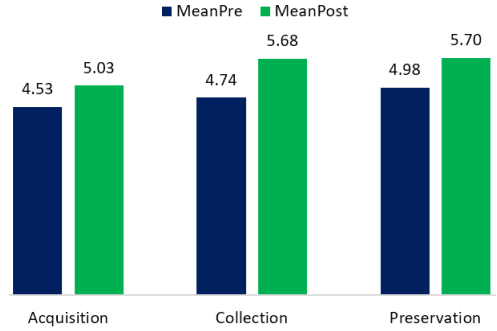
(d) Online Trading Threat/Attack Demonstration Module



(e) Preventive Measure Module



(f) Emotion Handling Sub Module



(g) Incident Handling Sub Module

Figure 4: Mean difference of pre and post-survey for (a) Cyber and ICT crime and Threats, (b) Best Practices, (c) Cyber and ICT Law Awareness, (d) Online Trading Threats/Attacks Demonstration, (e) Preventive Measure, (f) Emotion and (g) Incident Handling Modules.

5.2.1 Cyber and ICT crime and Threat

In this module, the participants are exposed to four components, which are Vulnerabilities, Threats, and Risks (VTR), Scammers: Phone (SP), Scammers: Email (SE), and Scammers: Ewallet (SW). As shown in Figure 4(a), the mean value of post-VTR is higher than pre-VTR, with values of 5.73 and 5.34, respectively. Similar upward trends are observed for SP (5.27 to 5.62), SE (5.05 to 5.49), and SW (4.42 to 4.57) components, indicating increased participants' understanding of cyber and ICT crime and threats. Improvement was shown from pre-VTR to post-VTR results; the participants understood the vulnerability of the human weakness that can easily be persuaded to trust anyone, the threats of cyber and ICT crimes occurring in online trading, and the cyber and ICT crime risks that arise from any online platform that they have. The participants were aware that scamming could also occur through phone calls (SP component). Furthermore, cyber and ICT crime victims easily trust when the so-called ‘authorities’ ask for their private information because they are afraid they might get a penalty or maybe jail.

The increase in the mean score of pre-SE to post-SE is attributed to the participants’ higher awareness of identifying scams like love, job, investment, reward, and predatorial publication through email. This increased awareness, resulting from attending the workshop, has consequently contributed to lowering the risk of email scams. Any fraudulent behaviour involving the unlawful use of a person's digital wallet to make unauthorized transactions is called an e-wallet scam (SW component). This misbehaviour can also include using stolen credit card information or creating fake digital wallets to trick people into submitting payment information. In conclusion, the module on cyber and ICT crime and threats significantly contributes to improving societal cyber and ICT crime awareness.

5.2.2 Best Practices

Three components of Best Practices were explained in this module: i. Alert on suspicious actions (A), ii. System’s hardening (H), and iii. Responsible for customers’ PII (CST). Based on Figure 4(b), the mean value for each component shows increasing value from pre- to post-results; the mean score for pre-A and post-A is 4.08 and 4.58, respectively, which shows an improvement by the participants. Same with the H component (mean score for pre-H is 4.85 and post-H is 5.38) and the CST component (mean score for pre-CST is 4.79 and post-CST is 5.56).

From this module, the participants learned to be alert of suspicious communication or actions that may implicate the business, know the appropriate steps to address it and get professional advice, if necessary (A component). The participants also acknowledge the need for security hardening (H component), such as implementing Secure Socket Layer certificates for secure transactions, applying multi-factor authentication, and, most importantly, avoiding public Wi-Fi to perform any money transactions. When dealing with customers' data, the participants understand that there is Personal Identifiable Information (PII) such as name, birthdate, address, bank

account, or phone number, which must not be exposed (CST component) and can be penalized under Personal Data Protection Act (PDPA).

5.2.3 Cyber Law Awareness

This module explained cyber law (CL), data privacy (DP), and consumer rights (CR). As shown in Figure 4(c), the mean score for all components of Cyber and ICT law Awareness elevated from pre- to post-results. The mean score for post-CL is higher than pre-CL, with 5.73 and 5.14, respectively. The mean score for pre-DP is 4.66, and post-DP is 5.19, which also shows improvement. Similarly, the mean score for pre-CR is 4.96, and post-CR is 5.66, which also shows the progress of the participant's understanding of the CR component.

The increment in mean score shows that participants have increased their awareness of cyber law on data protection and privacy, intellectual property, taxation, criminal-related laws, and the procedures for dispute resolution. This module provides a comprehensive understanding of the contractual obligations to help the participants prevent legal disputes.

5.2.4 Online Trading Threat / Attack Demonstration

Three components, namely the Wi-Fi cracking process (W), version of the application (VP), and phishing links (PL), are the gist of this module. Based on Figure 4(d), the mean score for pre-W, pre-VP, and pre-PL are 4.64, 4.98, and 5.16, respectively. The number inclined for post-W, post-VP, and post-PL was 5.66, 5.60, and 5.81, respectively. The increasing mean score for these three components shows that the participants understand the danger of online trading threats.

The demonstration of cyber and ICT attacks served as an eye-opener for participants. From the result, it can be explained that the participants were previously unaware of the potential risks, such as attacks in the context of cyber and ICT crime incidents. For example: Man-in-the-Middle attacks, Network sniffing, and other dangerous malicious actions by the perpetrators. This module empowers users to make informed decisions, protect sensitive information, and maintain a secure online trading environment.

5.2.5 Preventive Measures

During breakout sessions, the participants learned to identify suspicious trading websites/social media accounts or other platforms (I), identify the Secure Sockets Layer certificates in online selling platforms (SSL), identify suspicious emails (E), and security of Android/IOS (AI). Based on Figure 4(e), this practical session helps the participants actively engage in the activity, allowing them to apply the knowledge to strengthen their security. The participants were also reminded to avoid automatically saving bank card details to prevent their personal information from being stolen if they accidentally downloaded malware to their mobile phones.

The higher average scores for every component clarified why the participants responded positively to the module's presentation. For instance, the participants'

mean score for identifying suspicious trading websites/social media accounts or other platforms at pre-I is 4.81 while post-I is 5.61, which shows improvement from pre- to post-result. The mean scores for identifying SSL during online selling platforms with pre-SSL (4.40) and post-SSL (5.55) also show a positive difference. The mean score for identifying suspicious email (E) inclines from pre-E to post-E with values of 3.99 and 4.30, respectively. Lastly, the mean score for Security of Android/IOS pre-AI (4.74) rises positively to post-AI (5.61). In a nutshell, the participants gained more knowledge and understanding about the essential skill of preventive measures.

5.2.6 Emotion and Incident Handling

This module encompassed two subtopics, namely Emotion Handling consists of women's cyber and ICT crime reflection (WCR) and mindset to react (M), while Incident Handling covers the correct way for acquisition (AC), collection (C), and preservation (P). Based on Figure 4(f) and 4(g), there is a substantial difference in the mean score of pre and post-results for emotion and incident handling. Based on Figure 4(f), the mean score of pre-WCR is 4.77 and post-WCR is 5.66. While, pre-M is 5.10 and post-M is 5.81. Based on the results, it is verified that the participants understand the suitable method to handle emotion in distress situations.

From the Incident Handling module, the mean Acquisition (AC) pre-AC score is 4.53 and post-AC, it is 5.03. Meanwhile, for Collection (C), the value for pre-C is 4.74, post-C is 5.68, and Preservation (P). The value for pre-P is 4.98 and post-P is 5.70. The participants learned about data extraction techniques such as manual data extraction, logical data extraction, and physical data extraction. As the presenter explained, logical data extraction techniques extract the data on the mobile phone by interacting with the operating system and accessing the file system. The participants were also taught that physical extraction is a process to obtain the exact bit-by-bit image of the device. Compared to logical extraction, physical extraction is an exact copy of the device's memory and includes more information, such as slack or unallocated space.

During the explanation on online platforms, the participants are now aware to preserve the evidence by taking screenshots (with standard time) to identify the important features for potential evidence such as Chat, Profile, or Purchase log. The improvement in the emotion and incident handling module explained that the participants better understood how to react to cyber and ICT crime situations and the correct methods to store evidence and report cyber and ICT crime incidents.

5.2.7 Overall Cyber and ICT crime Awareness

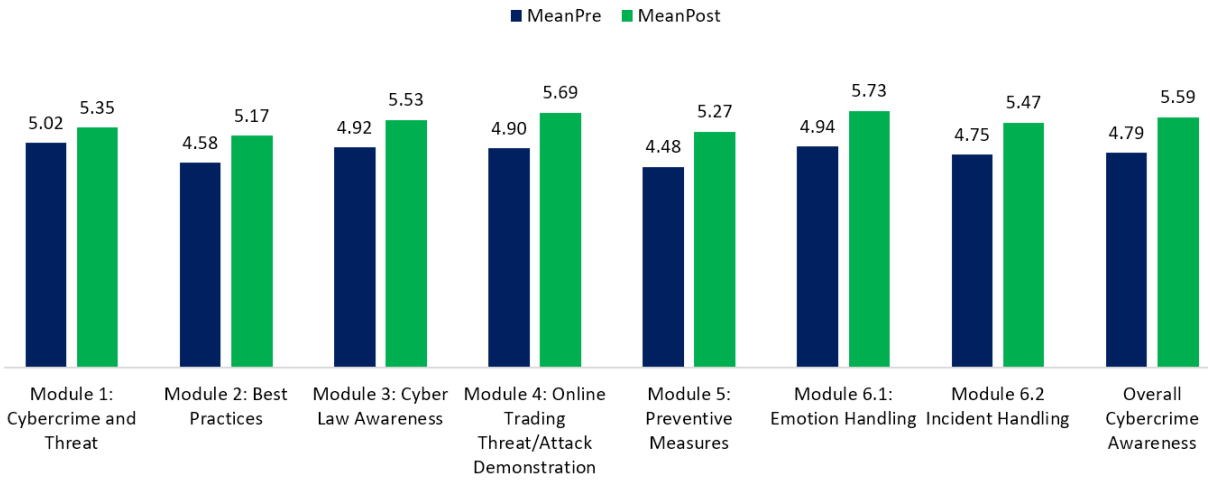


Figure 5: Mean difference between six modules and overall Cyber and ICT crime Awareness Level before and after the workshop

In general, each module showed a positive and significant interest to the participant based on the mean score as shown in Fig.5. Module 6.1, Emotion Handling, visualized the highest mean score, followed by Module 4, Online Trading Threat/Attack Demonstration, and Module 6.2, Incident Handling consecutively. Even though the organizer allocated most of the time to practical sessions on Module 5: Preventive Measures, the participant seemed to struggle to grasp them as the mean score showed the lowest value. Furthermore, the cyber and ICT crime awareness level greatly increased from 4.79 to 5.59. This inclination justified the participants' gaining more knowledge of overall cyber and ICT crime awareness after attending the workshop. In conclusion, all the workshop modules elevated cyber and ICT crime awareness and assisted the participants in becoming aware of cyber and ICT crime attempts.

6. Post Workshop

6.1 Introduction

The purpose of the post-workshop survey was to collect feedback on the workshop, the satisfaction of participants with the workshop's activities, and other recommendations. In this survey, the participants were asked to give their permission and consent for the media publication.

6.2 Results of the Workshop Survey

A total of 57 participants answered the post-workshop survey. The satisfaction score is measured using the 6-Likert scale (1) Very Not Satisfied, (2) Not Satisfied, (3) Moderately Not Satisfied, (4) Moderately Satisfied, (5) Satisfied, and (6) Very Satisfied. The mean score of the post-workshop survey is as follows: Committee - 5, workshop's suitability - 5, workshop's content - 4, workshop's effectiveness to the participant- 4,

Flow of workshop - 5, Achievement of the objectives - 4. Therefore, it can be concluded that the participants enjoyed and benefitted from the workshop. The participants also shared their feedback and recommendations in the post-workshop survey. They expressed that the topics presented were interesting and eye-opening. The participants also understand the importance of awareness regarding cyber and ICT crime and its threats. They would be more careful in handling unpleasant situations related to cyber and ICT crime. The participants also suggested incorporating more technical and theoretical aspects, along with hands-on activities.

7. Recommendations

The following recommendations were proposed through the observations and surveys.

Individual/Community/Education Institution perspective

- Conduct cyber and ICT crime awareness in other communities, such as the elderly and the younger generation, by organizing periodical workshops.
- Disseminate good practices of spreading cyber and ICT crime awareness through private or government social media.
- Establish a self-learning platform through professional certificate courses in Universiti Kebangsaan Malaysia for long-term awareness programs.

Government and Policy Makers

- Advocate the community in developing online small and enterprise (SME) business policies
- Improvise laws and regulations for client-customer data privacy protection to alleviate unethical selling of business data.
- Empower digital courts with competent talents, providing digital evidence permissible by laws.

List of References

Adnan, N., Abdullah, S. N. H. S., Raja Yusof, R. J., Zainal, N. F. A., Qamar, F., & Yadegaridehkordi, E. (2023). A Systematic Literature Review in Robotics Experiential Learning With Computational and Adversarial Thinking. IEEE Access, 11(May), 44806–44827. https://doi.org/10.1109/ACCESS.2023.3249761

Al-Nasrawi, S. (2020). Combating Cyber Violence Against Women and Girls: An Overview of the Legislative and Policy Reforms in the Arab Region. *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, 493–512. https://doi.org/https://doi.org/10.1108/978-1-83982-848-520211037

Ghani, N. M., & Ghazali, S. (2020). *The Vulnerability Of Young Women To Cybercrime: A Case Study In Penang*. 443–455. https://doi.org/10.15405/epsbs.2020.10.02.40

Ismail, A., Ab Rahman, Z., Sheikh Abdullah, S. N. H., Sudin, M. N., Shaari, A. H., & Sarnon @ Kusenin, N. (2018). Relationship Between Personal Empowerment and Self-Identity Development among Adolescents in Malaysia. Asia-Pacific Journal of Information Technology and Multimedia, 07(02(02)), 43–51. https://doi.org/10.17576/apjitm-2018-0702(02)-04

Lazarus, S., Button, M., & Kapend, R. (2022). Exploring the value of feminist theory in

understanding digital crimes: Gender and cybercrime types. *Howard Journal of Crime and Justice*, *61*(3), 381–398. https://doi.org/10.1111/hojo.12485

Mohd, M., Abdullah, S. N. H. S., Paizi@Fauzi, W. F. W., Yusof, S. B. M., & Kadri, A. (2021). Pemerkasan Wanita Melalui Program Wanita Malaysia Revolusi Industri (IR4.0) Bebas Jenayah Siber. International Journal for Studies on Children, Women, Elderly and Disabled, 14, 84–94.

Saad, M. E., Abdullah, S. N. H. S., & Murah, M. Z. (2018). Cyber romance scam victimization analysis using Routine Activity Theory versus apriori algorithm. *International Journal of Advanced Computer Science and Applications*, *9*(12), 479–485. https://doi.org/https://doi.org/10.14569/IJACSA.2018.091267

Saizan, Z., & Singh, D. (2018). Cyber Security Awareness among Social Media Users: Case Study in German-Malaysian Institute (GMI). *Asia-Pacific Journal of Information Technology & Multimedia*, *07*(02), 111–127. https://doi.org/https://doi.org/10.17576/apjitm-2018-0702(02)-10

Widiasari, N. K. N., & Thalib, E. F. (2022). The Impact of Information Technology Development on Cybercrime Rate in Indonesia. *Journal of Digital Law and Policy*, *1*(2), 73–86. https://doi.org/10.58982/jdlp.v1i2.165

Yusof, S.B.M, Abdullah, S.N.H.S. Mohd, M., Adnan, N. Yusof, R.J.R., Mokhtar, U.A., Norman, A.A., Fauzi, W.F., "The effectiveness of Women 4IR Cyber 3A #Aware, Avoid, Act Program in Malaysia," 2022 International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 2022, pp. 1-5, doi: 10.1109/ICCR56254.2022.9995864.

Annex 1 – Preliminary study results

PRELIMINARY STUDY
(Pre-gap Analysis)

APEC Women Empowerment through Cybercrime-Free Workshop for Secure Online Trading in the 4th Industrial Revolution (PPWE 02 2022A)

Organizer: Universiti Kebangsaan Malaysia
Event held under APEC Project: PPWE 02 2022A – APEC Women Empowerment through Cyber crime-Free Workshop for Secure Online Trading in the 4th Industrial Revolution
Proposing Economy / Project Overseer: Malaysia
Co-sponsoring APEC economies: Indonesia; Papua New Guinea; Peru; Viet Nam
Funded by: ASF Sub-Fund on Digital Innovation

TABLE OF CONTENT

Page

List of Tables **Page**

List of Figures **Page**

APEC Women Free Cybercrime Workshop 2023 (Pilot Study)

Date: 4 July 2023
Time: 9.00 am – 6.00 pm (Malaysia time)
Venue: Meeting Room 1, Block B, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia.

1. INTRODUCTION

From day to day, women are constantly being portrayed as the victims of cyber and ICT crime. This is one worrying issue, especially with the high-technology gadgets that keep developing (Yusof, M.S.B. et al, 2022). According to (Lazarus et al., 2022), online fraud occurs when someone gains financial advantage through deception, impersonation, manipulation, counterfeiting, forgery, or Internet use. The environment of online fraud is compelling, making cyber and ICT crime victims fall into the trap. From the survey by Ghani & Ghazali (2020), 34 of 150 young women have the experience of becoming cyber and ICT crime victims. These women were scammed when they went to e-commerce platforms or dating applications. This justification concludes that cyber and ICT crime awareness among women needs to be further enhanced.

APEC Women Free Cybercrime Workshop 2023 aims to empower women in cyber and ICT crime issues. Four modules will be presented to help women handle the cyber and ICT crime situation or give solutions for women who have experienced becoming victims of cyber and ICT crime. The justification of the modules is shown in Table 1. The APEC Women Free Cybercrime Workshop 2023 will be held on 12 – 13 September 2023. Accordingly, a pilot study was carried out before the event to identify the strengths and weaknesses of the workshop.

Table 1: Modules of APEC Women Free Cybercrime Workshop 2023

Name of module	Content of module	Objective of module
Module 1: Cyber and ICT crimes and Threats in Online Trading	Overview of online trading processes and the threats identification and cyber and ICT crimes related to online trading.	Discuss the cyber and ICT crime trends, security risks associated with online transactions, e-commerce, and data privacy for social media, mobile devices and the Internet of Things (IoT).
Module 2: Cyber Law and Best Practices	Explanation of cyber law in Malaysia and other economies, data privacy, and related acts enforced across the globe.	Understand on: ● The need to apply security best practices in the online business environment. ● System hardening to secure online business environment. ● Data privacy protection for clients
Module 3: Preventive Measures	Identify suspicious trading websites or social media accounts and other platforms.	● Protecting your online trading accounts (as a seller) ● Understand the strategy to prevent Cybernet from Cyber and ICT crime.

Module 4: Emotion handling	Practical activity on handling depression and mind-calming practices.	To avoid overrating our emotions, which can deter our rational thinking.
Module 5: Incident handling	Brief theory on evidence handling process.	To educate the evidence-handling process (Acquisition, Collection, and preservation). - Based on the application - Based on the device (PC, tablet, smartphone)

2. METHODOLOGY

2.1 Sample size

Based on (Economies Around The World, 2023) and (World and Regional Statistics, World Data Atlas, Maps, Rankings, 2023), the working women population in 11 APEC economies has been identified, as shown in Table 2.

Table 2: Population of women in the working group

APEC economy	Population of women in working group
Chile	4, 823, 563
China	422, 583, 484
Indonesia	64, 252, 660
Malaysia	8, 752, 620
Mexico	29, 807, 812
Papua New Guinea	2, 288, 589
The Philippines	29, 985, 344
Peru	11, 364, 203
Russia	42, 535, 679
Thailand	21, 670, 678
Viet Nam	34, 330, 641

Sample size can be determined from the total population of women involved in working groups. Studies with insufficient sample sizes may not provide accurate estimates, which causes inaccurate information on the treatment effect (Kang, 2021). Using the working women population of 672,395,273, the sample size is calculated using the formula (Adam, 2020) as shown below, leading to the final sample size, which is 385 women.

$$n = \frac{N}{1+N\varepsilon^2}$$

where,

n = minimum of sample size
N = size of population
ε = adjust margin of error

2.2 Participant of Pilot Study

On 4 July 2023, a pilot study of APEC Women Free Cybercrime Workshop 2023 (AWFreeCybercrime) was held. The pilot study occurred in Meeting Room 1, Block B, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia. As for the pilot study, around 25 participants participated in the workshop. The participants were undergraduate students of Universiti Kebangsaan Malaysia, and all of them were in Malaysia's economy. Based on the demography, 80% of the participants were female (20 people), and the other 20% were male (5 people). Most participants are around 21 to 30 (76%), and the other 24% are less than 20. The participants were stated to be unemployed as they are students and have less than USD500 (Less than MYR2333.50) monthly earnings.

The participants are Faculty of Technology and Information Science students who explained their IT background. Only one person was not from an IT background. The operation systems used in participants' mobile phones were IOS (15 people) and Android (10 people). This usage shows that most participants use IOS as their operation system (60%). English was the most used language on the participants' mobile phones. Lastly, most participants are buyers of online trading (e-commerce), with around 21 participants. The demography of the participants is portrayed in Table 3.

Table 3: Demography of participants

Demography		**Number of participants**
Gender	Female	20
	Male	5
Age	21 – 30 years old	19
	Less than 20 years old	6
Economy	Malaysia	25
Level of education	Bachelor Degree	24
	High School	1
Type of occupation	Unemployed	25
Monthly earning	Less than USD500 (Less than MYR2333.50)	25
IT Background	IT	24
	Non – IT	1
Operation system (mobile phone)	IOS	15
	Android	10
Language use (mobile phone)	English	24
	Non – English	1
Trade online as	Buyer	21
	Both	4

As shown in Table 4, the module developers constructed the module contents. In module 1, the vulnerabilities, threats, and risks of online trading towards women were explained, including the case studies related to scammers. In module 2, the developer highlighted the cyber and ICT law protecting people from cyber and ICT crimes. Data privacy was also taught in module 2. Next, module 3 helped identify suspicious trading websites/social media accounts and the Secure Sockets Layer (SSL) certificates in online selling platforms. For module 4, participants learned to encounter depression and practised the correct method for mind-calming to have a rational mind if they face any cyber and ICT crime situation. The workshop ended with module 5, which provides the correct method of handling the cyber and ICT crime evidence.

Table 4: Contents of modules

Module	Indicator	Topics
Module 1: Cyber and ICT crime and Threats in Online Trading	VTR	Vulnerabilities, Threats, and Risks
	SP	Scammers: Introduction and Case Study (Phone)
	SE	Scammers: Introduction and Case Study (Email)
	SW	Scammers: Introduction and Case Study (Ewallet)
Module 2: Cyber Law and Best Practices	CL	Cyber and ICT law
	DP	Data Privacy
	CR	Consumer right
	A	Alert on suspicious actions and react accordingly.
	H	System hardening produces a secure online trading environment.
Module 3: Preventive Measures	R	Responsible for customers' PII
	I	Identify suspicious trading websites/social media accounts/other platforms
	SSL	Identify the Secure Sockets Layer (SSL) certificates in the online selling platform.
	E	Identify suspicious email
	AI	Android/IOS
Module 4: Emotion and Incident Handling	WCR	Women Cyber and ICT crime Reflection
	M	Mindset To React
Module 5: Incident Handling	AC	Acquisition
	C	Collection
	P	Preservation
Participant's Awareness	CA	Cyber and ICT Crime Awareness

3. RESULTS AND DISCUSSION

3.1 Reliability Test

Table 5 shows the reliability test results of the module component. The Cronbach' Alpha of all components is higher than 0.05, which explains the accuracy of the items of the modules toward participant's comprehension of online trading cyber and ICT crime situations and their knowledge of facing the situations.

Table 5: Reliability test results

Indicator	Number of Item	Cronbach's Alpha
VTR	3	0.959
SP	3	0.923
SE	3	0.598
SW	3	0.512
CL	3	0.981
DP	3	0.766
CR	3	0.982
A	3	0.692
H	3	0.871
R	3	0.901
I	3	0.961
SSL	3	0.950
E	3	0.570
AI	9	0.959
WCR	3	0.949
M	3	0.950
AC	3	0.817
C	3	0.979
P	3	0.935
CA	3	0.916

3.2 Correlation

Pearson correlation has been applied to analyze the correlation between the components. This is the most prevalent correlation technique. It is the covariance between two variables divided by the product of their standard deviations (Makowski et al., 2020). Based on Figure 1, all components show a positive correlation, which justifies the importance of these components in the APEC Women Free Cybercrime Workshop 2023 modules.

Figure 1: Pearson correlation between the components

Correlations

		VTR	SP	SE	SW	CL	DP	CR	A	H	R	I	SSL	E	AI	WCR	M	AC	C	P	CA
VTR	Pearson Correlation	1	.909**	.370	.831**	.938**	.747**	.942**	.737**	.859**	.931**	.925**	.840**	.830**	.806**	.888**	.858**	.841**	.758**	.756**	.808**
	Sig. (2-tailed)		<.001	.068	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
SP	Pearson Correlation	.909**	1	.459*	.751**	.877**	.723**	.859**	.748**	.860**	.942**	.938**	.918**	.864**	.802**	.926**	.864**	.798**	.728**	.721**	.731**
	Sig. (2-tailed)	<.001		.021	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
SE	Pearson Correlation	.370	.459*	1	.690**	.325	.527**	.314	.635**	.426*	.407*	.352	.457*	.631**	.442*	.415*	.415*	.347	.126	.115	.146
	Sig. (2-tailed)	.068	.021		<.001	.113	.007	.126	<.001	.034	.044	.085	.022	<.001	.027	.039	.039	.090	.550	.585	.486
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
SW	Pearson Correlation	.831**	.751**	.690**	1	.793**	.787**	.789**	.778**	.709**	.750**	.736**	.694**	.867**	.773**	.758**	.792**	.718**	.563**	.580**	.611**
	Sig. (2-tailed)	<.001	<.001	<.001		<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	.003	.002	.001
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
CL	Pearson Correlation	.938**	.877**	.325	.793**	1	.794**	.962**	.676**	.875**	.886**	.937**	.835**	.837**	.797**	.915**	.881**	.874**	.809**	.828**	.826**
	Sig. (2-tailed)	<.001	<.001	.113	<.001		<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
DP	Pearson Correlation	.747**	.723**	.527**	.787**	.794**	1	.773**	.809**	.867**	.775**	.759**	.706**	.731**	.764**	.773**	.826**	.865**	.656**	.625**	.649**
	Sig. (2-tailed)	<.001	<.001	.007	<.001	<.001		<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
CR	Pearson Correlation	.942**	.859**	.314	.789**	.962**	.773**	1	.695**	.876**	.911**	.934**	.882**	.829**	.770**	.907**	.889**	.850**	.806**	.815**	.807**
	Sig. (2-tailed)	<.001	<.001	.126	<.001	<.001	<.001		<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
A	Pearson Correlation	.737**	.748**	.635**	.778**	.676**	.809**	.695**	1	.830**	.824**	.736**	.688**	.808**	.798**	.729**	.819**	.742**	.542**	.465*	.522**
	Sig. (2-tailed)	<.001	<.001	<.001	<.001	<.001	<.001	<.001		<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	.005	.019	.007
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
H	Pearson Correlation	.859**	.860**	.426*	.709**	.875**	.867**	.876**	.830**	1	.908**	.902**	.839**	.773**	.740**	.864**	.856**	.899**	.727**	.676**	.698**
	Sig. (2-tailed)	<.001	<.001	.034	<.001	<.001	<.001	<.001	<.001		<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
R	Pearson Correlation	.931**	.942**	.407*	.750**	.886**	.775**	.911**	.824**	.908**	1	.954**	.920**	.856**	.834**	.930**	.888**	.854**	.767**	.725**	.780**
	Sig. (2-tailed)	<.001	<.001	.044	<.001	<.001	<.001	<.001	<.001	<.001		<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
I	Pearson Correlation	.925**	.938**	.352	.736**	.937**	.759**	.934**	.736**	.902**	.954**	1	.891**	.857**	.783**	.935**	.852**	.866**	.789**	.760**	.775**
	Sig. (2-tailed)	<.001	<.001	.085	<.001	<.001	<.001	<.001	<.001	<.001	<.001		<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
SSL	Pearson Correlation	.840**	.918**	.457*	.694**	.835**	.706**	.882**	.688**	.839**	.920**	.891**	1	.847**	.704**	.895**	.846**	.740**	.726**	.722**	.714**
	Sig. (2-tailed)	<.001	<.001	.022	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001		<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
E	Pearson Correlation	.830**	.864**	.631**	.867**	.837**	.731**	.829**	.808**	.773**	.856**	.857**	.847**	1	.822**	.893**	.867**	.740**	.690**	.682**	.666**
	Sig. (2-tailed)	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001		<.001	<.001	<.001	<.001	<.001	<.001	<.001
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
AI	Pearson Correlation	.806**	.802**	.442*	.773**	.797**	.764**	.770**	.798**	.740**	.834**	.783**	.704**	.822**	1	.892**	.905**	.804**	.716**	.725**	.748**
	Sig. (2-tailed)	<.001	<.001	.027	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001		<.001	<.001	<.001	<.001	<.001	<.001
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
WCR	Pearson Correlation	.888**	.926**	.415*	.758**	.915**	.773**	.907**	.729**	.864**	.930**	.935**	.895**	.893**	.892**	1	.919**	.882**	.833**	.838**	.811**
	Sig. (2-tailed)	<.001	<.001	.039	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001		<.001	<.001	<.001	<.001	<.001
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
M	Pearson Correlation	.858**	.864**	.415*	.792**	.881**	.826**	.889**	.819**	.856**	.888**	.852**	.846**	.867**	.905**	.919**	1	.854**	.789**	.811**	.766**
	Sig. (2-tailed)	<.001	<.001	.039	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001		<.001	<.001	<.001	<.001
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
AC	Pearson Correlation	.841**	.798**	.347	.718**	.874**	.865**	.850**	.742**	.899**	.854**	.866**	.740**	.740**	.804**	.882**	.854**	1	.881**	.834**	.843**
	Sig. (2-tailed)	<.001	<.001	.090	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001		<.001	<.001	<.001
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
C	Pearson Correlation	.758**	.728**	.126	.563**	.809**	.656**	.806**	.542**	.727**	.767**	.789**	.726**	.690**	.716**	.833**	.789**	.881**	1	.947**	.946**
	Sig. (2-tailed)	<.001	<.001	.550	.003	<.001	<.001	<.001	.005	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001		<.001	<.001
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
P	Pearson Correlation	.756**	.721**	.115	.580**	.828**	.625**	.815**	.465*	.676**	.725**	.760**	.722**	.682**	.725**	.838**	.811**	.834**	.947**	1	.912**
	Sig. (2-tailed)	<.001	<.001	.585	.002	<.001	<.001	<.001	.019	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001		<.001
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
CA	Pearson Correlation	.808**	.731**	.146	.611**	.826**	.649**	.807**	.522**	.698**	.780**	.775**	.714**	.666**	.748**	.811**	.766**	.843**	.946**	.912**	1
	Sig. (2-tailed)	<.001	<.001	.486	.001	<.001	<.001	<.001	.007	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	
	N	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

3.3 Relationship between the module component and cybercrime awareness.

The pilot study showed that the participants gained knowledge after attending the workshop. The sample, N, is slightly different for the pre-test and post-test due to the time constraint of the participants. One-sample t-test was done using SPSS to analyze the pre and post-survey findings. Based on Table 5, every indicator (topic) in the four modules improves participants' awareness of cyber and ICT crime. Each indicator significantly affects the participant's cyber and ICT crime awareness, as the p-value for each indicator is less than 0.05. This explains that the participants understand the importance of each learning topic of the APEC Women Free Cybercrime Workshop 2023 module and are aware of the possibilities of cyber and ICT crime.

One of the external factors that help the participants may come from their IT background. Since most participants have an IT background, they are more aware of cyber and ICT crime issues. However, they might not know how to handle the cyber and ICT crime situation emotionally. Indicators WCR and M are two topics in Module 4: Emotion Handling, while indicators AC, C, and P are three topics from Module 5: Incident Handling that explains

emotion management. Based on Table 6, the post-test results show an increase in understanding compared to the pre-test. This increment justifies the APEC Women Free Cybercrime Workshop 2023, which benefits women and men in improving their cyber and ICT crime awareness. The conceptual diagram of the Women Free Cybercrime Model has been developed based on the analysis, as shown in Figure 2.

Table 6: One-sample T Test

Indicator	N		Mean		Std. Deviation		Sig. (2-tailed)	
	Pre-test	Post Test	Pre-test	Post Test	Pre-test	Post Test	Pre-test	Post Test
VTR	25	22	4.604	5.591	.293	.149	.000	.000
SP	25	22	4.507	5.561	1.324	.792	.000	.000
SE	25	22	3.388	4.107	1.249	1.533	.000	.000
SW	25	22	4.293	4.892	.211	.169	.000	.000
CL	25	22	4.640	5.606	1.487	.774	.000	.000
DP	25	22	4.173	5.348	1.463	.794	.000	.000
CR	25	22	4.639	5.561	1.478	.723	.000	.000
A	25	22	4.119	4.832	1.269	1.112	.000	.000
H	25	22	4.520	5.561	1.285	.751	.000	.000
R	25	22	4.466	5.515	1.388	.821	.000	.000
I	25	22	4.454	5.621	1.407	.637	.000	.000
SSL	25	22	4.374	5.682	1.431	.604	.000	.000
E	25	22	4.146	4.924	1.175	.992	.000	.000
AI	25	22	4.543	5.646	1.306	.543	.000	.000
WCR	25	22	4.493	5.591	1.375	.682	.000	.000
M	25	22	4.694	5.758	1.364	.463	.000	.000
AC	25	22	4.333	5.334	1.368	.810	.000	.000
C	25	22	4.453	5.106	1.434	1.245	.000	.000
P	25	22	4.480	4.879	1.365	1.237	.000	.000
CA	25	22	4.467	5.561	1.329	.806	.000	.000

*sig.diff = .05

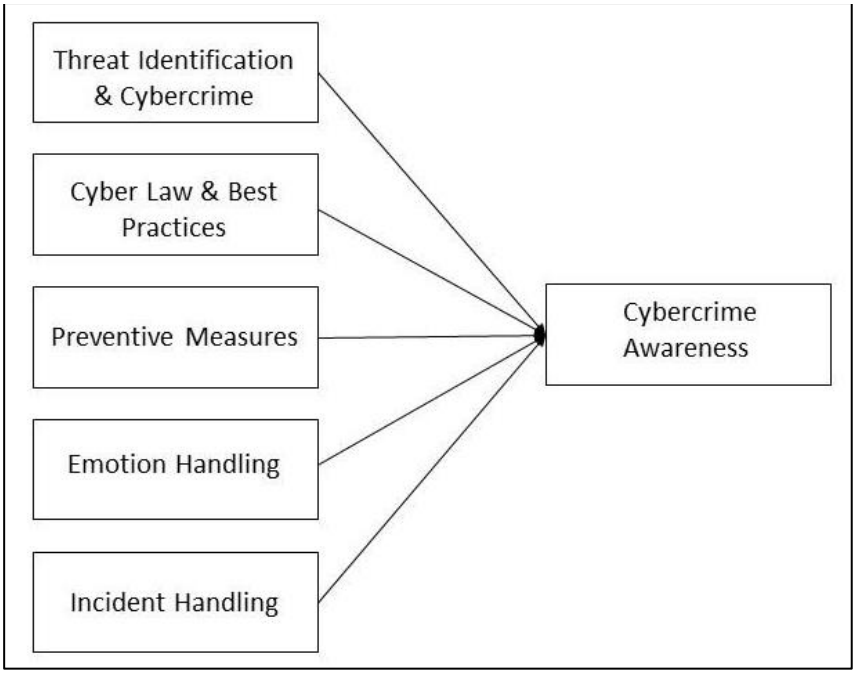


Figure 2: Conceptual model of Women Free Cybercrime Model

4. GAP ANALYSIS AND FUTURE DIRECTION

From the pilot study of the APEC Women Free Cybercrime module, we identified several limitations that need to be improved. For module 1, two sessions were done. The first session was the Overview of Online Trading, and the second was Threat Identification and Cyber and ICT crime. There were only brief explanations of online trading previously. The functions and processes involved at each stage of online trading must be explained so the participants can understand how online trading works. The features of secure online trading also need to be justified to highlight the focus of the workshop, which is the people involved in online trading who can use the system securely. The improvement of the presentation is to reduce the time frame for the videos and add active learning activities between the module presentations.

Next, for module 2 (Preventive Measures), the demonstration of the preventive measures needs to be explained using practical activity. The module's content needs to be clear and understandable, for example, increase the QR code size during the practical activity. An explanation of the verified seller and the methods of preventive measures needs to be discussed during the practical activity of module 2. Module 3, Cyber Law and Best Practices has to improve by highlighting the important keywords such as SSL, PDPA, Payment Gateway, and Trustee CA. The participants must also understand how money laundering works, AMLA, and the real case study in module 3. The justification of personal data, taxation and the jurisdiction of the cyber law need to be explained to the participants. Another important aspect of cyber law is the cloud, including contracts, privacy, rights, and liability.

For module 4, the participants have learned about securing the devices and e-wallets, which is more of a practical activity. The method for the initial settings button on Android and iOS needs to be specified in the module activity. The contents of the Android or IOS have to be re-arranged. The facilitators must frequently check on the audience to ensure the participant understands the information. The module content must also include the Window log activities and the importance of VPN for security. Giving an example by creating a scenario on removing

cookies, generalizing the browser exercise, cross-site tracking, password strength checking, and URL validity can instantly give awareness to the audience.

Module 5 is divided into two sections: emotion and incident handling. For emotion handling, the activity should be started with drama roleplay to show the example of emotions if they are the cyber and ICT crime victims. Provide the video for the cooling down method and give an example of handling panic attacks for the cyber and ICT crime situations such as digital harassment, digital espionage, and photography. It is also important to explain the effects, such as micro-sleep, and provide information on the Digital Wellness Compliance /Counseling Approach. As for incident handling, the image authentication methods need to be justified. The module activity should explain the authorisation on the identified IP log. For the overall modules, it is encouraging for all the modules to include active learning sessions to improve the participants' understanding of the module contents. Table 7 portrays demography, and reviews have been summarized in Table 8.

Table 7: Demographic of experts

Expert	**Occupation**	**Year of experiences in IT field**	**IT expertise**
Expert 1	Lecturer	More than 10 years	Information System
Expert 2	Lecturer	More than 10 years	Artificial Intelligence
Expert 3	Royal Malaysian Police	More than 10 years	Forensic Analyst
Expert 4	Cybersecurity Malaysia	More than 10 years	Digital Forensic Specialist
Expert 5	Lecturer	More than 10 years	Software Engineering

Table 8: Expert reviews on the pilot study

No.	**Slot**	**Continuous Improvement Items**
1	Module 1: Overview of Online Trading Processes	- Explain the functions and processes involved at each stage of online trading. - Explain the vulnerabilities, threats, and risks briefly. - Justify secure online trading features (to highlight the focus of the WORKSHOP is on the PEOPLE part – using the system securely).
2.	Module 1: Threat Identification & Cyber and ICT Crime	- The time frame must be reduced if there is too much video. - Add active learning activities in between the presentations. - Introduce at least ten cyber and ICT crime types related to secure online trading.

3.	Module 2: Prevention Measures	- This session will be run after Module 1: Threat Identification and Cyber and ICT Crime. - Demonstration of the preventive measures. - Compare between obsolete policy or otherwise. - QR code too small for the practical activity - Justify the Good and Best Rights and Choices - Improve the text, and check the option, unsubscribe easy or difficult - Explain the verified seller - real or not seller - Variety of methods of preventive measures. - Justify the halal and haram of crypto-trading. - Give the example of cross-siting. - Explain the steps to check: 1) check fake URL 2) chatgpt 3) phishing link 4) tools to check the password
4.	Module 3A: Secure Online Trading Best Practice	- Add animation to improve the understanding of the process on best practices for the laymen. - Highlight important keywords SSL, PDPA, Payment Gateway, and Trustee CA.
5.	Module 3B: Cyber Law	- Money Laundering, AMLA, real case study - Personal Data - Taxation - ROB - Jurisdiction- Tribunal, Online Trading, Agreement to Government - Two Jurisdiction - for any dispute B2B, C2C explain - Cloud - contract, privacy, right, liability
6.	Module 4: Securing your devices and e-wallets	- Present the method for the initial settings button Android and iOS. - More to practical activities. - Arrange the contents for the Android/IOS. - Check the audience to grab the information. -Explain on the Window log activities. -Explain the importance of VPN. - Rearrange module - Create checklist - Create a scenario to remove cookies - Remove adds cookies - Exercise before and after implementing functions - Generalize browser exercise - Cross-site tracking - Bottom- sub-topic title/icon - Password strength checking - Check URL validity

7.	Module 5A: Emotion Handling	- Starting with drama roleplay to show the example of emotions if they are the cyber and ICT crime victims. - Show video for cooling down method - Give examples of how to handle panic attacks - such as cyber digital, digital espionage, pornography - Provide the effect such as micro-sleep - Do practical activity - Translate some Arabic Word to English Word - Show video of different emotions - Digital Wellness Compliance /Counseling Approach
8.	Module 5B: Incident Handling	- Focus Practical Approach - First Responder based on case study - Add animations - Teach the hash technology - Explain the image authentication methods - Explain about the authorization on the identified IP log - Justify the Google image match - Give an example of simple data recovery
9.	Active Learning using Slido	All modules must prepare active learning activities to adopt the digital thinking model.

5. CONCLUSION

The APEC Women Free Cybercrime Workshop 2023 (pilot study) shows its significance in empowering women and men in cyber and ICT crime awareness. The comparison of the pre- and post-surveys showed an improvement in the participants' understanding of cyber and ICT crime, especially in online trading. These workshop modules taught the participants the technical and emotional aspects of cyber and ICT crime. Conclusively, the participants learned the methods applied to scammers, such as love or job scams, and how to properly encounter this cyber and ICT crime situation.

6. REFERENCES

Adam, A. M. (2020). Sample Size Determination in Survey Research. *Journal of Scientific Research and Reports*, *26*(5), 90–97. https://doi.org/10.9734/jsrr/2020/v26i530263

Ghani, N. M., & Ghazali, S. (2020). *The Vulnerability Of Young Women To Cybercrime: A Case Study In Penang*. 443–455. https://doi.org/10.15405/epsbs.2020.10.02.40

Kang, H. (2021). Sample size determination and power analysis using the G*Power software. *Journal of Educational Evaluation for Health Professions*, *18*, 1–12. https://doi.org/10.3352/JEEHP.2021.18.17

Lazarus, S., Button, M., & Kapend, R. (2022). Exploring the value of feminist theory in

understanding digital crimes: Gender and cybercrime types. *Howard Journal of Crime and Justice*, *61*(3), 381–398. https://doi.org/10.1111/hojo.12485

Makowski, D., Ben-Shachar, M., Patil, I., & Lüdecke, D. (2020). Methods and Algorithms for Correlation Analysis in R. *Journal of Open Source Software*, *5*(51), 2306. https://doi.org/10.21105/joss.02306

World and Regional Statistics, World Data Atlas, Maps, Rankings. Knoema. (2023). https://knoema.com/atlas

Yusof, S.B.M, Abdullah, S.N.H.S. Mohd, M., Adnan, N. Yusof, R.J.R., Mokhtar, U.A., Norman, A.A., Fauzi, W.F., "The effectiveness of Women 4IR Cyber 3A #Aware, Avoid, Act Program in Malaysia," 2022 International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 2022, pp. 1-5, DOI: 10.1109/ICCR56254.2022.9995864.

Prepared by,

Assoc. Prof. Dr. Azah Anir Norman

Project Contractor,

APEC Women Cybercrime-Free Workshop 2023.

Annex 2 - Agenda of the workshop

AGENDA

APEC WOMEN FREE CYBERCRIME WORKSHOP FOR SECURE ONLINE TRADING

IN THE 4TH INDUSTRIAL REVOLUTION

Cititel Mid Valley Hotel, Kuala Lumpur

Date: 12 - 13 September 2023

Time zone: UTC/GMT+8

https://awfreecybercrime.com/

12 September 2023	
08:30-09:00	**Arrival and Registration**
09:00–10:00	**Welcoming Remarks** ● Minister of Women, Family and Community Development ● APEC Representative
10:00 – 10:30	**Break and Hotel Security Talk**
10:30–12:30	**Forum** "Secure Our Online Trading in 4IR Era" **Moderator:** Dr. Raja Jamilah Raja Yusof, Universiti Malaya and International Muslim Women Union **Speaker:** Mr. David Stinson, Taiwan Academy of Banking & Finance (Sub-topic 1: Financial Fraud in Business) **Speaker:** Mrs Patrina Nasiron, Telekom Malaysia (Sub-topic 2: Business Telecommunication Risk & Fraud) **Speaker:** Ms. Daneila Dora Eilberg, United Nations Office on Drug and Crime (Sub-topic 3: Secure Online Trading Best Practises) **Speaker:** Dr. Atif Ahmed, University of Melbourne (Sub-topic 4: Online Business Incident Handling)
12:30–14:00	**Break**
14:00–15:30	**Session 1: Cyber and ICT crime and Threats (Interactive Talk)** The session will focus on an overview of online trading processes and the threats identification and cyber and ICT crimes related to online trading. **Speakers:**

	• Mr. Saravanan Kulanthaivelu, Standard Chartered Bank Global Business Services • Professor Ts. Dr. Madihah Mohd Saudi, Universiti Sains Islam Malaysia • ASP Siti Baizura Mohd Yusof, Royal Malaysian Police
15:30 – 16:00	**Break**
16:00 – 16:30	**Session 2: Best Practises (Interactive Talk)** This session will focus on the best practices for secure online trading. **Speaker:** Associate Professor Dr. Normaziah Abdul Aziz, International Islamic University Malaysia
16:30 - 17:30	**Session 3: Cyber Law Awareness (Interactive Talk)** This session will focus on cyber and ICT law for secure online trading. **Speaker:** Professor Dr. Nazura Abdul Manap, Universiti Kebangsaan Malaysia
13 September 2023	
09:00 – 09:45	**Session 4: Online Trading Threat/Attack Demonstration** This session will demonstrate online trading threats and attacks. **Speaker:** Ts. Dr. Ahmad Firdaus Zainal Abidin, Universiti Malaysia Pahang Al-Sultan Abdullah (UMPSA)
09:45 – 11:00	**Breakout Session 1 - Prevention Measures: Mobile Devices and Communication (Hands-on training)** This session will focus on securing mobile devices and communication. **Speaker:** Associate Professor Dr. Zulaiha Ali Othman, Universiti Kebangsaan Malaysia
11:00 – 11:30	**Break**
11:30 – 13:00	**Breakout Session 2 - Prevention Measures: Online Trading Platforms (Hands-on training)** This session will focus on securing your shopping platforms, social media and e-wallets. **Speaker:** Associate Professor Dr. Zulaiha Ali Othman, Universiti Kebangsaan Malaysia
13:00 – 14:00	**Break**
14:00 – 15:00	**Breakout Session 3 – Prevention Measures: Browsers and Windows** This session will focus on securing your browsers and windows. **Speaker:** Associate Professor Dr. Zulaiha Ali Othman, Universiti Kebangsaan Malaysia

15:00 – 16:00	**Breakout Session 4 - Emotional Handling (Hands-on training)** This session will focus on practical activities or immersive simulations/scenarios. **Speakers:** ● Associate Professor Dr. A'dawiyah Ismail, Universiti Kebangsaan Malaysia ● Dr. Azianura Hani Shaari, Universiti Kebangsaan Malaysia
16:00 – 16:45	**Breakout Session 4 - Incident Handling** (Hands-on training) This session will focus on hands-on walkthrough acquisition and collection of evidence (from buyer's and seller's perspectives). **Speaker:** Associate Professor Dr. Khairul Akram Zainol Arrifin, Universiti Kebangsaan Malaysia Mrs. Sarah Khadijah Taylor, Cybersecurity Malaysia
16:45 – 17:00	**Break**
17:00 – 17:30	**<u>Closing Remarks</u>** ● Deputy-vice Chancellor (Industry, Network, Alumni dan Community) Universiti Kebangsaan Malaysia ● APEC Representative

Asia-Pacific Economic Cooperation

Universiti Kebangsaan Malaysia
The National University of Malaysia

WOMEN FREE Cybercrime

WOMEN FREE CYBERCRIME

Workshop For Secure Online Trading In 4IR Era

APEC | Aware | Avoid | Act

https://www.awfreecybercrime.com/

Agenda 2023

12 September

DAY 1

Welcoming Remarks 08:30 AM – 09:30 AM
by H.E. Dato' Sri Hajah Nancy Shukri
Minister of Women, Family and Community Development Malaysia

Forum 09:45 AM – 11:30 AM
Secure Our Online Trading in 4IR Era

Session 1 11:30 AM – 01:00 PM
Cybercrime and Threats (Interactive Talk)

Session 2 02:30 PM – 03:00 PM
Best Practises (Interactive Talk)

Session 3 03:45 PM – 04:15 PM
Online Trading Threat/Attack Demonstration

Session 4 04:15 PM – 05:30 PM
Cyber Law Awareness (Interactive Talk)

13 September

DAY 2

Breakout Session 1 09:00 AM – 11:00 AM
Prevention Measures Part 1
(Hands-on training)

Breakout Session 2 11:15 AM – 12:30 PM
Prevention Measures Part 2
(Hands-on training)

Breakout Session 3 02:00 PM – 03:00 PM
Emotional Handling (Hands-on training)

Breakout Session 4 03:15 PM – 04:30 PM
Emotional Handling (Hands-on training)

Closing Remarks 05:00 PM – 05:45 PM
by Prof. Dato' Dr. Norazah Mohd Nordin
Deputy Vice-Chancellor (Industry Network, Alumni & Community) UKM

FREE ADMISSION

SPONSORS

KEMENTERIAN PEMBANGUNAN WANITA KELUARGA DAN MASYARAKAT

CSAM CYBER SECURITY ACADEMIA MALAYSIA

IEEE Women in Engineering We

CyberSecurity MALAYSIA

Annex 3 - Workshop's activities

Workshop's Activities - Day 1 (12 September 2023)

Image : Opening speech by Assoc. Prof. Ts. Dr. Abdul Hadi Abd Rahman, Deputy Dean (Research and Innovation), Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia.

Image 2: Opening speech by Her Excellency Dato' Sri Hajah Nancy Shukri, Minister of Women, Family and Community Development of Malaysia.

Image 3: Token-giving ceremony to the ceremony official.

Image 4: Silat performance during opening ceremony.

Image 5: Forum “Secure Our Online Trading in the 4IR Era” that was moderated by Dr. Raja Jamilah Raja Yusof, a senior lecturer from Universiti Malaya with esteemed forum panelists representing diverse organizations are Dr. Atif Nisar Ahmad from the University of Melbourne, Australia, Mr. David Stinson from the TABF, Chinese Taipei, Ms. Daniela Dora Eilberg from the United Nations Office on Drug and Crime, and Ms. Patrina Nasiron from Telekom Malaysia.

Image 6: Forum discussion session.

Image 7: Cyber and ICT Crime and Threat module, presented by Prof. Dr. Madihah Mohd Saudi, a professor from Universiti Sains Islam Malaysia (USIM) for the first session.

Image 8: Cyber and ICT Crime and Threat module presented by Prof. Dr. Madihah Mohd Saudi, a professor from Universiti Sains Islam Malaysia (USIM), for the first session.

Image 9: Cyber and ICT Crime and Threat module presented by ASP. Siti Baizura Mohd Yusof, Royal Malaysia Police (RMP) for the second session.

Image 10: Cyber and ICT Crime and Threat module presented by ASP Siti Baizura Mohd Yusof, Royal Malaysia Police (RMP) for the second session.

Image 11: Best Practice module presented by Assoc. Prof. Dr. Normaziah Abdul Aziz from International Islamic University Malaysia.

Image 12: Best Practice module presented by Assoc. Prof. Dr. Normaziah Abdul Aziz from International Islamic University Malaysia.

Image 13: Cyber Law Awareness module presented by Prof. Dr. Nazura Abdul Manap from Universiti Kebangsaan Malaysia.

Image 14: Cyber Law Awareness module presented by Prof. Dr. Nazura Abdul Manap from Universiti Kebangsaan Malaysia.

Workshop's Activities - Day 2 (13 September 2023)

Image 15: Online Trading Threat/Attack Demonstration module presented by Ts. Dr. Ahmad Firdaus Bin Zainal Abidin from Universiti Malaysia Pahang Al-Sultan Abdullah.

Image 16: Online Trading Threat/Attack Demonstration module presented by Ts. Dr. Ahmad Firdaus Bin Zainal Abidin from Universiti Malaysia Pahang Al-Sultan Abdullah.

Image 17: Preventive Measures module (practical session) presented by Assoc. Prof. Dr. Zulaiha Ali Othman with facilitators from Special Interest Group (SIG) Cyberhack and Ethics, Universiti Kebangsaan Malaysia.

Image 18: Preventive Measures module (practical session) presented by Assoc. Prof. Dr. Zulaiha Ali Othman with facilitators from Special Interest Group (SIG) Cyberhack and Ethics, Universiti Kebangsaan Malaysia.

Image 19: Emotion Handling module presented by Dr. Azianura Hani Shaari from the Faculty of Social Sciences and Humanities, Universiti Kebangsaan Malaysia.

Image 20: Emotion Handling module presented by Dr. Azianura Hani Shaari from the Faculty of Social Sciences and Humanities, Universiti Kebangsaan Malaysia.

Image 21: Emotion Handling module presented by Assoc. Prof. Dr. ‘Adawiyah Ismail from the Faculty of Islamic Studies, Universiti Kebangsaan Malaysia.

Image 22: Emotion Handling module presented by Assoc. Prof. Dr. ‘Adawiyah Ismail from the Faculty of Islamic Studies, Universiti Kebangsaan Malaysia.

Image 23: Incident Handling module presented by Assoc. Prof. Dr. Khairul Akram Zainol Ariffin from Center for Cyber Security, Universiti Kebangsaan Malaysia.

Image 24: Closing speech by Associate Professor Dr Siti Norul Huda Sheikh Abdullah, the APEC project overseer.

Image 25: Closing speech by Associate Professor Dr Ridzwan Yaakub, Deputy Dean of Industry and Community Partnership, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia.

Image 26: Token-giving ceremony to the ceremony official.