

PEMERKASAAN WANITA MELALUI PROGRAM WANITA MALAYSIA REVOLUSI INDUSTRI (IR4.0) BEBAS JENAYAH SIBER

Masnizah Mohd
Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia, 43600 Kuala Lumpur, Malaysia
Emel: masnizah.mohd@ukm.edu.my

Siti Norul Huda Sheikh Abdullah
Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia, 43600 Kuala Lumpur, Malaysia
Emel: snhsabdullah@ukm.edu.my

Wan Fariza Paizi@Fauzi
Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia, 43600 Kuala Lumpur, Malaysia
Emel: fariza.fauzi@ukm.edu.my

Siti Baizura Mohd Yusof
Jabatan Siasatan Jenayah Komersial Bukit Aman
Polis Diraja Malaysia, Aras 33, Menara 238
Jalan Tun Razak, 50400 Kuala Lumpur
Emel: baizura@rmp.gov.my

Atikah Kadri
International Muslim Women Union
No 30 Jalan Selasih U12/18e
Cahaya Alam, Seksyen U12
40150 Shah Alam, Selangor
Emel: atikahkadri@gmail.com

ABSTRAK

Pembangunan negara yang mampan perlu mengambikira kesejahteraan siber penduduk khususnya memperkasa golongan wanita yang sering menjadi mangsa. Pelbagai isu jenayah siber seperti gangguan siber, buli siber, hendap siber dan menakutkan secara jenayah, di bawah skop keganasan berdasarkan jantina, secara dalam talian telah banyak melibatkan wanita sebagai mangsa utama. Ketidakseimbangan kuasa jantina yang wujud dalam masyarakat di mana kebiasaannya, lelaki dianggap sebagai jantina yang dominan, manakala wanita dianggap sebagai jantina yang submisif. Ini telah memotivasikan keperluan membangunkan satu bentuk program latihan yang memfokus kepada kesaksamaan jantina dan pemerkasaan wanita dalam keselamatan siber. Justeru, kajian ini bertujuan membangunkan program latihan keselamatan siber yang dinamakan sebagai Bengkel Wanita Malaysia Revolusi Industri (IR4.0) Bebas Jenayah Siber (Sibernita). Ia bermatlamat meningkatkan kesedaran mengenai jenayah siber di kalangan wanita Malaysia yang sering menjadi pemangsa atau penjenayah tanpa sedar. Terdapat empat modul dibangunkan iaitu Kenali Ancaman dan Jenayah Siber, Amalan Terbaik Mengendali Jenayah Siber, Kaedah Pencegahan Jenayah Siber, dan Aktiviti Refleksi Bebas Jenayah Siber. Kandungan modul direka bentuk dan dibangunkan dengan pendekatan Analisis, Reka bentuk, Pembangunan, Implementasi dan Penilaian (ADDIE). Program Sibernita ini dijalankan dalam dua sesi yang memfokuskan kepada wanita sebagai peserta sasaran. Analisis dari soal selidik yang diedarkan di awal dan di akhir program mendapati peserta kini celik dan cakna mengenai jenis-jenis jenayah siber melibatkan wanita, yang berlaku di organisasi dan komuniti. Malah satu program Sijil Profesional Perlindungan Siber turut dihasilkan. Program-program ini yang dianjurkan tepat pada masanya dan dapat mengelakkan lebih ramai lagi wanita daripada menjadi mangsa jenayah siber. Kesimpulannya, pelaksanaan program Sibernita dan penawaran pensijilan profesional ini dilihat sebagai satu amalan terbaik dalam memperkasa penduduk wanita khususnya ke arah kesejahteraan siber di Malaysia.

Kata kunci: Wanita, keselamatan siber, sijil profesional

PENGENALAN

Aktiviti bekerja dari rumah serta penggunaan media sosial yang lebih tinggi berbanding biasa mengakibatkan ramai menjadi sasaran penjenayah siber. Walaupun secara keseluruhannya kes jenayah semakin menurun namun kes jenayah indeks siber pula semakin membimbangkan. Isu ini adalah sangat membimbangkan. Jadual 1 menunjukkan perbandingan modus operandi jenayah siber bagi tahun 2020 dan 2021 berdasarkan bilangan kes dan jumlah kerugian. Secara amnya didapati bilangan kes dan jumlah kerugian menunjukkan peningkatan yang amat membimbangkan.

Jadual 1: Perbandingan modus operandi jenayah siber

Modus Operandi	Bilangan Kes		Kerugian (RM)	
	2020	*2021	2020	*2021
PENIPUAN TELEKOMUNIKASI (TALIAN/SISTEM PESANAN RINGKAS)	4408	4398	210,427,340.38	127,192,048.95
E-DAGANG (BELIAN DALAM TALIAN)	4141	6499	28,820,272.63	41,947,303.52
419 SCAM (PENIPUAN ASMAR/CINTA)	1126	1076	39,727,961.99	36,302,022.27
PENIPUAN KEWANGAN DALAM TALIAN	485	659	19,370,791.25	44,162,938.97
BAHAN LUCAH (SEK 292 KANUN KESEKSAAN)	34	21	0	400.00
SEKSYEN 233 AKTA KOMUNIKASI DAN MULTIMEDIA (MEDIA SOSIAL)	33	15	15,702.48	3,540.00
HARTA INTELEK (CD/VCD/DVD)	11	10	0	0
PERLINDUNGAN DATA PERIBADI	10	37	439,847.70	383,965.79
BERITA PALSU	0	0	0	0
JUMLAH	10,248	12,715	298,803,316.43	250,043,788.52

*sehingga 1 September 2021

Semasa Pandemik Covid19 ini, CyberSecurity Malaysia menerusi Cyber999 telah melaporkan peningkatan 82.5% atau sejumlah 838 insiden bermula dari tempoh perintah kawalan 18 Mac hingga 7 April 2020 berbanding hanya sahaja pada tempoh sama bagi tahun 2019. Dari jumlah tersebut, 18% atau 152 kes melibatkan syarikat tempatan dan selebihnya adalah dari pengguna rumah dan lain-lain. Antara kes-kes jenayah siber yang terlibat adalah penipuan, penembusan dan buli siber. PDRM turut menyokong bahawa statistik jenayah siber iaitu penipuan cinta siber telah merekodkan kerugian negara sebanyak 63.05 juta sehingga 100.92 juta pada tahun 2015 dan 2016 masing-masing (PDRM, 2017). Selangor, Kuala Lumpur, Pulau Pinang dan Johor merekodkan penipuan siber cinta sejumlah melebihi 2 juta seperti di Jadual 2.

Jadual 2: Statistik penipuan cinta tahun 2015 sehingga 2017 (PDRM, 2017)

Negeri	2015		2016		2017*	
	Bil. Kes	Kerugian (RM)	Bil. Kes	Kerugian (RM)	Bil. Kes	Kerugian (RM)
PERLIS	17	407,810	14	685,330	4	61,900
KEDAH	75	3.35 juta	136	1.93 juta	15	194,240
PULAU PINANG	110	4.93 juta	200	9.41 juta	22	2.37 juta
PERAK	145	2.49 juta	173	3.80 juta	10	270,130
SELANGOR	435	15.15 juta	607	26.61 juta	39	4.59 juta
KUALA LUMPUR	256	15.18 juta	360	24.34 juta	29	704,470
NEGERI SEMBILAN	86	1.16 juta	107	2.09 juta	15	411,050
MELAKA	110	5.30 juta	140	4.22 juta	12	298,875
JOHOR	265	4.94 juta	333	7.98 juta	34	1.12 juta
PAHANG	69	1.49 juta	98	6.03 juta	9	226,600
TERENGGANU	48	762,648	66	1.50 juta	4	268,538
KELANTAN	59	1.09 juta	59	1.75 juta	9	659,658
SABAH	89	2.54 juta	93	5.48 juta	5	60,600
SARAWAK	76	4.22 juta	122	5.05 juta	8	69,066
JUMLAH	1,840	63,05 juta	2,508	100,92 juta	215	11.32 juta

Maka kajian ini bertujuan merekabentuk dan membangunkan program latihan keselamatan siber bagi meningkatkan kesedaran mengenai jenayah siber di kalangan wanita Malaysia sebagai pemangsa atau penjenayah tanpa sedar.

KAJIAN LITERATUR

Kajian Wan Noor Hamiza et al (2021a, 2021b) menyatakan selain isu buli siber yang semakin membimbangkan, isu penipuan dalam talian juga turut membimbangkan. Ini disokong oleh kajian Ezry dan Abdullah (2019) yang menyiasat faktor-faktor kecenderungan pemangsa penipuan cinta siber di Malaysia di kalangan individu yang telah menjadi mangsa penipuan cinta siber

dan membuat laporan polis di negeri Selangor, Malaysia. Berdasarkan Teori Aktiviti Rutin, kajian ini menemui bahawa mereka yang berusia di antara 25 tahun hingga 45 tahun, cenderung menjadi mangsa penipuan cinta siber di Malaysia. Majoriti mangsa adalah yang berpendidikan dengan majoriti memiliki Diploma. Selain itu, Ezry dan Abdullah (2019) mendapati bahawa wanita bujang dan wanita yang telah berkahwin lebih kerap menjadi mangsa dalam penipuan cinta siber berbanding lelaki. Sasaran mangsa juga merupakan wanita berumur 25 tahun ke atas, tidak mengira status pekerjaan si mangsa mahupun tidak bekerja sama sekali. Kajian lain pula iaitu Abdullah dan Mohd (2019) turut mengkaji berkenaan jenayah penipuan siber bernama pancingan data spesifik (*spear phishing*) yang biasanya merujuk kepada mencuri kata nama dan kata laluan bagi menembusi sistem tertentu. Beberapa ujian simulasi yang telah dijalankan pada 2018 dan 2019 terhadap pekerja sektor telekomunikasi dan pertahanan mendapati bahawa dari 39 emel yang telah dihantar, sebanyak 12 responden telah memberi respon kepada kandungan emel dan jenayah pancingan data berjaya menembusi serta membuktikan bahawa kesedaran 31% dari pekerja terdedah kepada ancaman jenayah pancingan data spesifik sektor telekomunikasi dan pertahanan. Satu ujian simulasi pancingan data yang dijalankan kepada pengurusan Institut Pengajian Tinggi Awam (IPTA) pula menunjukkan bahawa peningkatan bilangan respon antara bidang Sains & Teknologi (S&T) mendahului bidang bukan-S&T sebanyak 205 bagi tahun 2019 berbanding 198 bagi tahun 2018. Pemangsa pula terdiri dari golongan wanita iaitu dua kali ganda berbanding lelaki. Secara amnya, program kesedaran dan kemahiran swa-pencegahan jenayah siber perlu aktif dijalankan di kalangan masyarakat bagi membendung penipuan yang berleluasa yang menyebabkan kerugian kepada bangsa dan negara. Justeru Siti Norul Huda Sheikh Abdullah et al (2018) telah melaksanakan membangunkan Modul Swa-Pencegahan Jenayah Remaja yang telah dilaksanakan di beberapa sekolah bagi meningkatkan kesedaran mengenai jenayah siber di kalangan remaja.

Pengguna Internet semakin terdedah kepada penjenayah siber yang sentiasa mengambil peluang dan kesempatan. Dunia tanpa sempadan kini merupakan lubuk kepada penjenayah siber bagi melancarkan agenda mereka kepada pengguna yang leka dan tidak berhati-hati khususnya golongan wanita. Wanita merupakan salah satu tonggak pembangunan negara yang paling penting bukan sahaja bagi aspek sosial, politik dan ekonomi, malah merangkumi segala aspek pembangunan negara. Dapatan kajian menjangkakan bahawa pertambahan penyertaan 30% wanita dalam pasaran buruh Malaysia, mampu meningkatkan GDP (Keluaran Dalam Negara Kasar) negara antara 7% hingga 12% setahun. Malah kerajaan menerusi Majlis Keselamatan Negara turut memandang serius agenda pemerksaan wanita di Malaysia dengan memperkenalkan Strategi Keselamatan Siber Malaysia 2020-2024 merangkumi 12 strategi, 35 pelan tindakan dan 113 program.

KAEDAH PEMBANGUNAN PROGRAM PEMERKASAAN WANITA DI MALAYSIA

Kajian ini membangunkan dua cadangan program pemerksaan wanita di Malaysia dengan membangunkan program bengkel “Wanita Malaysia Revolusi Industri (IR4.0) Bebas Jenayah Siber” (SiberNita) dan Sijil Profesional Perlindungan Siber yang merupakan kesinambungan dari program SiberNita. Kandungan kedua-dua program ini dibangunkan menggunakan pendekatan Analisis, Reka bentuk, Pembangunan, Implementasi dan Penilaian (ADDIE).

Fasa	Aktiviti
1. Analisis	Keperluan program dikenalpasti dengan merujuk dokumen seperti Pelan Strategik Kementerian Pembangunan Wanita, Keluarga dan Masyarakat (2021-2025), Pelan Strategik Kementerian Dalam Negeri (2015-2020), Strategi Keselamatan Siber Malaysia 2020-2024 dan program Sarjana Keselamatan Siber di Universiti Kebangsaan Malaysia. Fasa ini penting dalam mengenalpasti inisiatif sedia ada, serta konsep atau tema yang diketengahkan. Analisis mendapati Malaysia masih kekurangan program atau inisiatif yang komprehensif dan bersepadu iaitu mengambilkira tiga kitaran penting iaitu sebelum (mencegah), semasa (menangani) dan selepas (melaporkan). Malah berlaku juga isu kesinambungan di mana program yang diwujudkan bersifat sementara dan jangka masa pendek. Ini telah memotivasikan kajian ini untuk menerapkan aspek komprehensif, bersepadu dan jangka masa panjang dalam pembangunan program pemerksaan wanita dalam keselamatan siber.
2. Reka bentuk	Dua program cadangan direka bentuk melalui pemetaan setiap modul mengikut kitaran dan aspek yang telah dikenalpasti dari fasa analisis (Jadual 3).

Jadual 3: Pemetaan kitaran, modul dan aspek

Kitaran	Modul	Aspek
SEBELUM (MENCEGAH)	• Modul Pengenalan: Malaysia Revolusi Industri 4.0 (IR4.0) Bebas Jenayah Siber	Komprehensif
SEMASA (MENANGANI)	• Modul 1: Jenayah Siber • Modul 2: Risiko, Tanggungjawab, Amalan Terbaik • Modul 3: Pra-Jenayah Siber: Kaedah Pencegahan	Bersepadu
SELEPAS (MELAPORKAN)	• Modul 4: Pasca-Jenayah Siber: Panduan dan Sokongan Mangsa	Jangka masa panjang

3. Pembangunan	Pembangunan program SiberNita adalah berbentuk dua siri bengkel yang diperincikan di seksyen Bengkel Wanita Malaysia Revolusi Industri (IR4.0) Bebas Jenayah Siber (Sibernita). Manakala Sijil Profesional Perlindungan Siber dibangunkan sebagai pensijilan profesional UKM dan diperincikan di seksyen Sijil Profesional Perlindungan Siber.
4. Implementasi	<p>Pelaksanaan program SiberNita dibuat dengan kerjasama antara Fakulti Teknologi dan Sains Maklumat (FTSM) UKM, Kementerian Pembangunan Wanita, Keluarga dan Masyarakat, <i>International Muslim Women Union</i> (IMWU), CyberSecurity Academia Malaysia (CSAM), Universiti Malaya (UM), Polis Diraja Malaysia (PDRM), CyberSecurity Malaysia (CSM) dan <i>IEEE Women in Engineering</i> (WIE). Program ini juga turut melibatkan <i>Special Interest Group CyberHack and Ethics</i> di FTSM sebagai jurus setia. Pembabitatan pelajar prasiswazah dilihat sebagai satu latihan dan pendedahan dalam menguruskan aktiviti luar dan rasmi.</p> <p>Manakala Sijil Profesional Perlindungan Siber diimplementasi menggunakan platform pembelajaran dalam talian iaitu <i>OpenLearning</i> (OL) di mana pembelajaran sendiri secara dalam talian (<i>online self-learning</i>) dilaksana.</p>
5. Penilaian	<p>Keberkesanan cadangan program SiberNita ini diukur melalui soal selidik yang diedarkan kepada peserta bengkel iaitu sebelum dan selepas bengkel. Perbandingan tahap kesedaran peserta dianalisis bagi memastikan pengisian bengkel ini bermanfaat seterusnya meningkatkan kesedaran mereka mengenai jenayah siber.</p> <p>Penilaian pensijilan pula ialah peserta perlu menyelesaikan bahan bacaan dan tugas kesemua modul (100% <i>Progress Completion</i>) untuk memenuhi syarat menduduki penilaian. Peserta perlu menduduki penilaian dalam tempoh kursus tersebut selama satu bulan. Penilaian adalah secara dalam talian dan terdiri daripada 40 soalan multi-pilihan (<i>multiple choice question</i>) di mana tempoh penilaian adalah 2 jam. Terdapat 3 slot penilaian disediakan dan peserta boleh memilih satu slot yang sesuai. Taklimat selama 15 minit diberikan sebelum sesi penilaian dalam talian dalam tempoh 2 jam.</p>

BENGGEL WANITA MALAYSIA REVOLUSI INDUSTRI (IR4.0) BEBAS JENAYAH SIBER (SIBERNITA)

Bengkel Wanita Malaysia Revolusi Industri (IR4.0) Bebas Jenayah Siber (Sibernita) ini yang bertemakan “Cegah, Celik, Cakna” adalah anjuran bersama antara Fakulti Teknologi dan Sains Maklumat UKM, Kementerian Pembangunan Wanita, Keluarga dan Masyarakat, *International Muslim Women Union* (IMWU), CyberSecurity Academia Malaysia (CSAM), Universiti Malaya (UM), Polis Diraja Malaysia (PDRM), CyberSecurity Malaysia (CSM) dan *IEEE Women in Engineering* (WIE). Ia dianjurkan dalam 2 sesi (Julai dan September 2021) secara dalam talian bagi memastikan berlaku kesinambungan. Peserta sasaran terdiri daripada wanita yang bekerja di sektor awam dan swasta, wanita yang mempunyai perniagaan dalam talian, suri rumah sepenuh masa, dan wanita yang masih belajar iaitu berjumlah seramai 200 peserta setiap sesi. Bengkel ini dirasmikan oleh Datuk Seri Rina Mohd Harun, Menteri Pembangunan Wanita, Keluarga dan Masyarakat.



BENKEL WANITA MALAYSIA REVOLUSI INDUSTRI (IR4.0) BEBAS JENAYAH SIBER

7 & 8 JULAI 2021
8.00pg - 1.00ptg.

PLATFORM
ZOOM ONLINE

PENGAJUR UTAMA



PENGAJUR BERSAMA



RM 10
PESERTA DALAM
TALIAN

RM 150
SIJIL PROFESIONAL
UKM

PERCUMA
RM 15
BAUCAR
Grab
dengan setiap penyertaan



Rajah 1: Bengkel wanita Malaysia revolusi industri (IR4.0) bebas jenayah siber

Objektif utama penganjuran program bengkel Wanita Malaysia Revolusi Industri (IR4.0) Bebas Jenayah Siber adalah untuk mengurangkan jenayah siber di kalangan wanita Malaysia sebagai pemangsa atau penjenayah tanpa sedar. Manakala berikut adalah sub-objektif program:

1. Memperkenalkan faedah peralatan IR4.0 yang berkait hubungan rangkaian bagi meningkat kualiti hidup dalam organisasi dan komuniti.
2. Untuk memberi kesedaran kepada jenis-jenis jenayah siber melibatkan wanita yang berlaku di organisasi dan komuniti.
3. Memberi garis panduan dan langkah-langkah pencegahan kepada peserta berkenaan ancaman jenayah siber di kalangan wanita.
4. Mengajar teknik-teknik dan alatan yang sesuai untuk melindungi daripada ancaman serangan jenayah siber di kalangan wanita.
5. Mengajar amalan terbaik sebelum, semasa dan selepas berlaku ancaman jenayah siber dari aspek organisasi dan komuniti.

Rajah 2 menunjukkan ahli panel bagi Forum Jenayah Siber Wanita Katakan Tidak.

FORUM JENAYAH SIBER WANITA KATAKAN TIDAK

AHLI PANEL

- ACP MUHAMAD TARMIZI BIN AWANG**
Penolong Pengarah
Bahagian Siasatan Jenayah Korporat/
Persatuan/Syarikat,
Jab. Siasatan Jen. Komersil, Bukit Aman
- PUAN SARAH KHADIJAH TAYLOR**
CyberSecurity Malaysia (CSM)
- DR. AZAH ANIR NORMAN**
Setiausaha, Pertubuhan Akademia
Keselamatan Siber Malaysia (CSAM)
- Moderator
DR. ATIKAH KADRI**
Presiden, International Women
Muslim Union (IMWU), Malaysia

7 JULAI 2021
8.25pg - 9.55pg.

SECARA LANGSUNG DI
ZOOM ONLINE

LIVE www.facebook.com/Sibernita

maklumat lanjut sila layari www.ftsm.ukm.my/sibernita

PENGAJUR UTAMA

PENGAJUR BERSAMA

Rajah 2: Forum jenayah siber wanita katakan tidak

Peserta wanita yang menyertai program forum dan bengkel ini akan mendapat faedah seperti memperolehi pengetahuan berkenaan ancaman jenayah siber wanita di kalangan komuniti setempat dan antarbangsa, memperolehi kemahiran sendiri yang meliputi jenayah siber Teknologi Maklumat Komunikasi, Internet Pelbagai Benda (IoT), gajet dan alatan komunikasi bagi pemerkasaan swa-pencegahan jenayah siber wanita, memperolehi kemahiran membangunkan polisi, prosedur, garis panduan dan amalan terbaik bagi melindungi dari ancaman jenayah siber. Laman web dan media sosial khusus dibangunkan untuk tujuan kesedaran, promosi dan kaunseling berterusan. Kesimpulannya, program Wanita Malaysia Revolusi Industri (IR4.0) Bebas Jenayah Siber merupakan satu program yang dianjurkan tepat pada masanya dan manfaat dari program ini dapat mengelakkan lebih ramai lagi wanita dari menjadi mangsa jenayah siber. Melalui bengkel seperti ini, pengetahuan dan kesedaran berkenaan jenayah siber dapat disebarluaskan kepada masyarakat secara amnya dan pekerja wanita secara khususnya.

SIJIL PROFESIONAL PERLINDUNGAN SIBER

Jumlah jenayah siber makin meningkat. Individu, keluarga termasuk kanak-kanak turut menjadi mangsa jenayah siber. Kursus Sijil Profesional Perlindungan Siber bertujuan untuk memberi kesedaran mengenai landskap ancaman semasa di dunia siber, serta memberikan sesi praktikal dan interaktif mengenai pelbagai langkah proaktif dan pencegahan yang dapat diambil untuk mengukuhkan keselamatan manusia. Kursus Sijil Profesional Perlindungan Siber ini membolehkan peserta meningkatkan pengetahuan asas dan praktikal dalam disiplin Keselamatan Siber agar berupaya melindungi diri dan keluarga daripada pelbagai ancaman siber yang berleluasa dan makin meningkat. Ia juga merupakan mekanisme penajaan kewangan melalui penawaran kursus ke agensi luar yang berminat untuk mendapatkan latihan di UKM. Platform sijil ini menggunakan Open Learning dan boleh dipaut di <https://www.openlearning.com/courses/sijil-profesional-perlindungan-siber>. Kursus ini merangkumi empat (4) modul iaitu Modul 1 Jenayah Siber, Modul 2 Perundangan, Risiko, dan Amalan Terbaik, Modul 3 Pra-Jenayah Siber: Kaedah Pencegahan, dan Modul 4 Pasca-Jenayah: Panduan dan Sokongan Mangsa. Terdapat 2 hasil pembelajaran kursus iaitu mengenal pasti jenayah siber, risiko, tanggungjawab, dan amalan terbaik keselamatan siber bagi memastikan keselamatan dalam persekitaran digital dan mengaplikasi pelbagai alat dan teknik semasa situasi pra- dan pasca-jenayah siber.

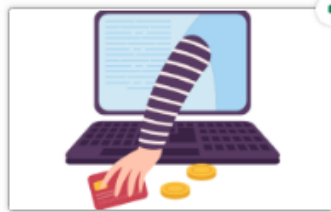


Modul 1: Jenayah Siber

Completed: 1 of 5



1.0 Pengenalan



1.1 Mendefinisi Jenayah Siber



1.2 Membincangkan Tren Jenayah Siber



1.3 Menganalisis Kaedah Menangani Jenayah Siber



Kuiz Modul 1

Modul 2: Perundangan, Risiko, dan Amalan Terbaik

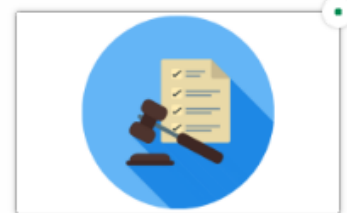
Completed: 0 of 5



2.0 Pengenalan



2.1 Ancaman Siber terhadap Wanita: Kes di Malaysia



2.2 Kerangka Perundangan dan Hak Kemanusiaan

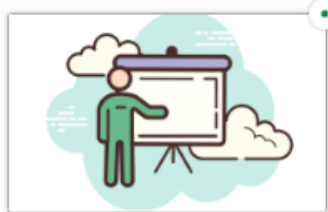


2.3 Strategi Keselamatan Siber dan Risiko



Kuiz Modul 2

▼ Modul 3: Pra-Jenayah Siber: Kaedah Pencegahan Completed: 0 of 6



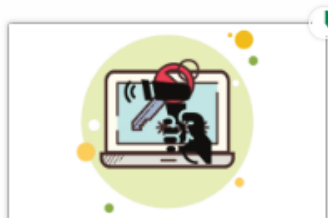
3.0 Pengenalan



3.1 Langkah Pencegahan Telefon Pintar



3.2 Langkah Pencegahan Akaun Media Sosial



3.3 Pengurusan Kata Laluan



3.4 Alat Pengesan Penipuan



Kuiz Modul 3

▼ Modul 4: Pasca-Jenayah Siber: Panduan dan Sokongan Mangsa Completed: 0 of 7



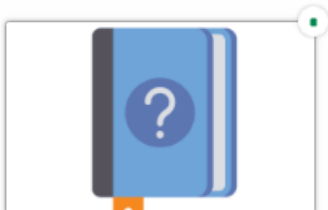
4.0 Pengenalan



4.1 Aspek Psikologi, Faktor dan Kesan



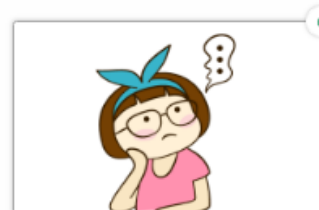
4.2 Pendekatan Psiko-spiritual



4.3 Panduan Mangsa



4.4 Senarai Semak / Talian Bantuan



Aktiviti Refleksi Modul 4



Kuiz Modul 4

Rajah 3: Modul dalam sijil profesional perlindungan siber

Jumlah kredit bagi kursus Sijil Profesional Perlindungan Siber adalah sebanyak 1 kredit (40 jam). Kursus ini mengandungi 5 modul (termasuk Modul Pengenalan) seperti di Jadual 4.

Jadual 4: Jumlah kredit sijil profesional perlindungan siber

Modul	Tempoh (Hari)	Jam
Modul Pengenalan: Malaysia Revolusi Industri 4.0 (IR4.0) Bebas Jenayah Siber		
Sinopsis: Modul ini memperkenalkan peserta dengan pengetahuan asas dan praktikal perlindungan siber pada era Revolusi Perindustrian ke-4 di mana manusia dan peranti saling berkaitan.	1	8
Modul 1: Jenayah Siber		
Sinopsis: Modul ini memperkenalkan konsep utama berkaitan dengan jenayah siber, apakah jenayah siber, Internet, penggunaan teknologi dan tren jenayah siber. Ia juga membincangkan topik mengenai cabaran teknikal, undang-undang, etika, dan operasi yang berkaitan dengan jenayah siber dan pencegahannya. Akhirnya modul ini mengkaji secara kritikal mengenai strategi, dasar dan program untuk meningkat kesedaran bagi pencegahan jenayah siber.	1	8
Modul 2: Risiko, Tanggungjawab, Amalan Terbaik		
Sinopsis: Modul ini memperkenalkan peserta kepada risiko, tanggungjawab, dan amalan terbaik dalam menangani dan menjaga keselamatan siber dan privasi data.	1	8
Modul 3: Pra-Jenayah Siber: Kaedah Pencegahan		
Sinopsis: Modul ini memperkenalkan peserta kepada alat dan tetapan yang terdapat dalam peranti serta platform web yang boleh menjaga keselamatan siber dan privasi data.	1	8
Modul 4: Pasca-Jenayah Siber: Panduan dan Sokongan Mangsa		
Sinopsis: Modul ini memperkenalkan peserta kepada konsep maqasid syariah sebagai satu kaedah untuk menangani psikologi negatif mangsa jenayah untuk membangunkan diri dan mengelak daripada menjadi mangsa lagi serta langkah-langkah pemulihan untuk mengawal keadaan.	1	8
Jumlah	5	40

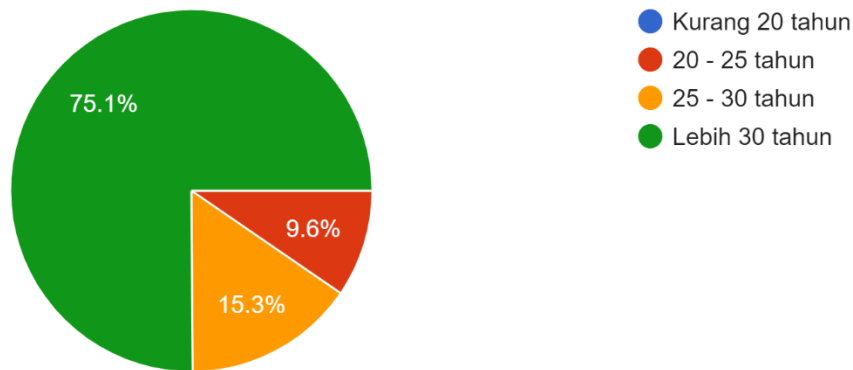
Pelaksanaan kursus ini bermula dengan modul pengenalan bertajuk Malaysia Revolusi Industri (IR4.0) Bebas Jenayah Siber yang dilaksana secara dalam talian melalui kaedah forum dan bengkel praktikal. Peserta yang menyelesaikan sesi pengenalan ini diberi sijil kehadiran dan bagi pensijilan profesional, para peserta perlu mengikuti empat (4) modul tambahan secara dalam talian (segerak dan tidak segerak). Setelah selesai semua modul, para peserta menduduki penilaian dalam talian dan akhirnya peserta diberi sijil tamat jika lulus penilaian tersebut.

ANALISIS

Analisis dibuat terhadap dua program pemerksaan wanita di Malaysia iaitu program bengkel Wanita Malaysia Revolusi Industri (IR4.0) Bebas Jenayah Siber (SiberNita) dan Sijil Profesional Perlindungan Siber

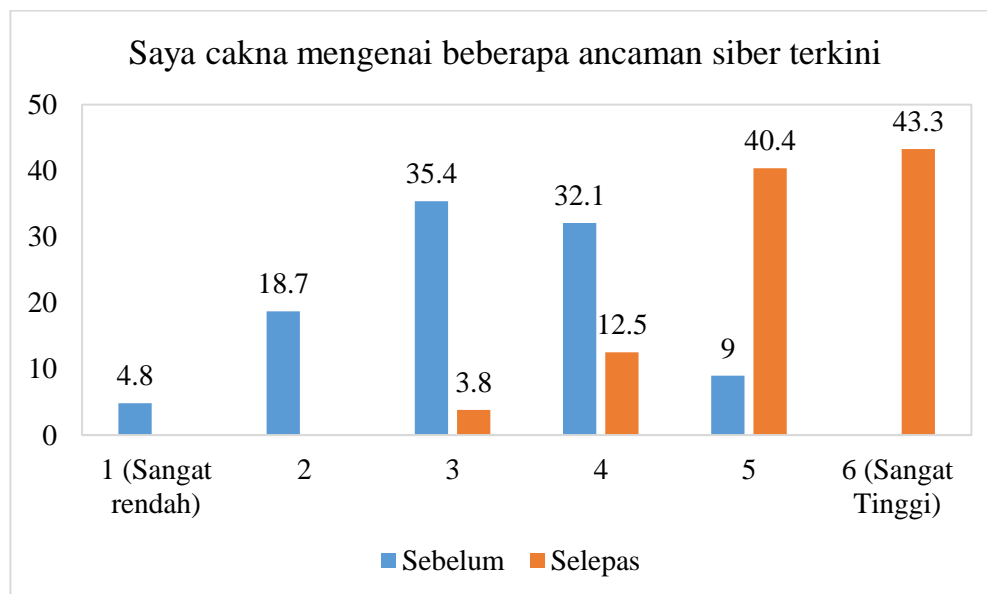
Penilaian Bengkel Wanita Malaysia Revolusi Industri (IR4.0) Bebas Jenayah Siber (Sibernita)

Analisis demografik peserta program SiberNita mendapati 100% pesertanya ialah wanita dengan 97.6% pesertanya dari kaum Melayu dan 2.4% kaum Cina. Manakala peratusan taburan umur peserta ialah seperti di Rajah 4.



Rajah 4: Peratusan taburan umur peserta program SiberNita

Analisis bagi mengukur tahap kesedaran peserta terhadap beberapa ancaman siber terkini mendapati peserta kini lebih cakna berdasarkan peratusan skala tahap kesedaran peserta sebelum dan selepas program seperti di Rajah 5. Skala tertinggi kesedaran peserta sebelum program ialah pada skala 3 (Sederhana) iaitu 35.4%. Menariknya kesedaran peserta didapati meningkat selepas program dengan skala tertinggi iaitu skala 6 (Sangat Tinggi) iaitu 43.3%. Peningkatan ini menunjukkan program SiberNita didapati berjaya meningkatkan tahap kesedaran peserta dengan memberi pendedahan mengenai beberapa ancaman siber terkini seperti penipuan telekomunikasi, cinta, kewangan dan e-komers serta modus operandinya. Menariknya tiada tahap kesedaran bagi skala 1 (Sangat Rendah) dan skala 2 (Rendah) di kalangan peserta selepas program.



Rajah 5: Perbandingan peratusan tahap kesedaran ancaman siber sebelum dan selepas program SiberNita

Penilaian Sijil Profesional Perlindungan Siber

Penilaian Sijil Profesional Perlindungan Siber pada 15 September 2021 melibatkan 20 peserta. Peserta perlu menyelesaikan bahan bacaan dan tugas kesemua modul dalam tempoh satu bulan untuk memenuhi syarat menduduki penilaian. Format penilaian adalah secara dalam talian dan terdiri daripada 40 soalan multi-pilihan di mana tempoh penilaian adalah dua jam. Keputusan akhir penilaian mendapati terdapat 17 peserta (85%) yang lulus. Ini merupakan indikator yang baik bagi menilai pemahaman dan prestasi peserta sijil profesional.

KESIMPULAN

Ruang Siber adalah suatu persekitaran yang kompleks di mana interaksi antara manusia, perisian dan perkhidmatan di Internet melalui teknologi dan rangkaian yang berhubung dengan persekitaran yang tidak wujud dalam bentuk fizikal tetapi dalam bentuk maya. Penggunaan dan pengembangan ICT telah mendedahkan Malaysia kepada ancaman keselamatan yang lebih luas dan tidak lagi terhad kepada tiga dimensi konvensional iaitu darat, udara dan laut tetapi turut melibatkan dimensi baharu iaitu ruang siber.

Kini ruang siber turut perlu dilindungi berikutan ancaman diruang siber adalah lebih kompleks dan kritikal untuk ditangani dengan bijak. Penyalahgunaan ruang siber jelas memberikan kesan kepada integriti, kebolehdapatan dan kerahsiaan maklumat yang memberi impak negatif terhadap individu, masyarakat, organisasi dan kerajaan. Peningkatan tren ancaman siber berskala besar berupaya melumpuhkan komponen utama Infrastruktur Maklumat Kritikal Negara yang boleh menjejaskan keselamatan negara, kesejahteraan sosial, dan pembangunan ekonomi. Pendekatan program pendidikan, latihan dan kesedaran merupakan satu mekanisme efektif dalam memperkasakan komuniti khususnya wanita agar bersedia siaga bagi menangani cabaran ruang siber yang wujud pada masa kini dan masa hadapan. Justeru program intervensi seperti SiberNita dan Sijil Profesional Perlindungan Siber boleh dianggap sebagai antara inisiatif terbaik untuk meningkatkan kesedaran dan pendidikan pencegahan mengenai jenayah siber. Program Wanita Malaysia Revolusi Industri (IR4.0) Bebas Jenayah Siber dan Sijil Profesional Perlindungan Siber merupakan satu program yang dianjurkan tepat pada masanya dan manfaat dari program ini dapat mengelakkan lebih ramai lagi wanita dari menjadi mangsa jenayah siber. Malah, pengetahuan dan kesedaran berkenaan jenayah siber dapat disebarluaskan kepada masyarakat secara amnya dan golongan wanita secara khususnya. Semoga lebih banyak program dan inisiatif seperti ini dapat disebarluaskan di Malaysia.

RUJUKAN

- Azianura Hani Shaari, Mohammad Rahim Kamaluddin, Fariza Fauzi, Masnizah Mohd. (2019). Online-Dating Romance Scam in Malaysia: An Analysis of Online Conversations between Scammers and Victims GEMA Online® Journal of Language Studies 19 (1).
- Mohd Ezri Saad, Siti Norul Huda Sheikh Abdullah and Mohd Zamri Murah. (2018). Cyber Romance Scam Victimization Analysis using Routine Activity Theory Versus Apriori Algorithm. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 9(12).
- Wan Noor Hamiza Wan Ali, Masnizah Mohd, Fariza Fauzi, Kiyooki Shirai, Muhammad Junaidi Mahamad Noor. (2021a). Implementation Of Hyperparameter Optimisation And Over-Sampling In Detecting Cyberbullying Using Machine Learning Approach. *Malaysian Journal of Computer Science*, 78-100. Retrieved from <http://mojes.um.edu.my/index.php/MJCS/article/view/34401>
- Wan Noor Hamiza Wan Ali, Masnizah Mohd, Fariza Fauzi. (2018). Cyberbullying Detection: An Overview. *2018 Cyber Resilience Conference (CRC)*, 1-3
- Wan Noor Hamiza Wan Ali, Masnizah Mohd, Fariza Fauzi. (2021b). Cyberbullying Predictive Model: Implementation of Machine Learning Approach," *2021 Fifth International Conference on Information Retrieval and Knowledge Management (CAMP)*, 2021, 65-69, doi: 10.1109/CAMP51653.2021.9497932.
- Siti Norul Huda Sheikh Abdullah, Wan Fariza Fauzi, Muhammad Nuruddin Sudin, Nurul Nadhirah Zahari, Zaizul Ab Rahman, A Dawiyah Ismail, Nur Riza Mohd Suradi, Azmin Sham Rambely, Norulhuda Sarnon Kusenin, Azianura Hani Shaari, Samruhaizad Samian, Norhana Arsad, Mohamad Hanif Md Saad, Masnizah Mohd, Masri Ayob, Kok Ven Jyn, Khairul Akram Zainol Ariffin, Mohd Zakree Ahmad Nazri, Mohd Ridzwan Yaakub. (2018). Assessment of Self-Identity among Teens towards Self-Crime Prevention Program. *2018 Cyber Resilience Conference (CRC)*, 1-4, doi: 10.1109/CR.2018.8626870.