International Journal of 'Umrānic Studies
Jurnal Antarabangsa Kajian 'Umrān
المجلة العالمية للدراسات العمرانية
Journal homepage: www.unissa.edu.bn/ijus

Pengetahuan dan Sikap Pelajar Institusi Pengajian Tinggi di Negara Brunei Darussalam Terhadap Aspek Keselamatan Siber: Perisian Aplikasi

Muhammad Haziq bin Haji Shahjahan[1], Adam bin Haji Jait[2], Anis Malik Thoha[3], Nurefnazahani binti Haji Durani[4]

[1,2, 3 & 4]Fakulti Pengurusan Pembangunan Islam, Universiti Islam Sultan Sharif Ali, Negara Brunei Darussalam

[1]haziq.shahjahan@outlook.com
[2]adamjait@yahoo.com
[3]malik.thoha@unissa.edu.bn
[4]nurefnazahani.durani@unissa.edu.bn

Vol. 7, Issue 1 | January 2024

KATA KUNCI

Keselamatan Siber, Pengetahuan, Sikap, Perisian Aplikasi.

ABSTRAK

Perkembangan pesat info-teknologi dan penggunaan internet masa kini bergerak secara pantas sehingga menimbulkan isu-isu terhadap keselamatan siber. Fenomena ini perlu diberi perhatian khususnya pelajar institusi pengajian tinggi disebabkan mereka didapati bersifat lalai dan menjadi sasaran jenayah siber. Maka kajian ini bertujuan meneliti tahap pengetahuan dan sikap pelajar institusi pengajian tinggi di Negara Brunei Darussalam terhadap penggunaan perisian aplikasi. Kajian ini menggunakan pendekatan kuantitatif yang berbentuk tinjauan. Instrumen kaji selidik dengan menetapkan skala Likert empat mata telah diedarkan kepada 580 orang pelajar tahun akhir di empat buah universiti awam Negara Brunei Darussalam, dengan menggunakan persampelan Bola Salji. Hasil kajian mendapati tahap pengetahuan responden terhadap penggunaan perisian aplikasi di tahap sederhana (min= 2.77); manakala tahap sikap responden pula ditahap tinggi (min =3.03). Dapatan ini menjelaskan sungguhpun pelajar mengamalkan sikap berhemah dalam menggunakan perisian aplikasi, tetapi masih terdapat lagi ruang bagi meningkatkan pengetahuan mereka ke tahap lebih baik. Ia turut menunjukkan jurang antara tahap sikap dan tahap pengetahuan pelajar yang memerlukan latihan agar pengetahuan mereka sejajar dengan sikap positif mereka.

PENGENALAN

Kemajuan dan perkembangan alat info-teknologi yang semakin pesat ini telah memudahkan seluruh masyarakat di dunia untuk menjalankan pelbagai urusan seperti komunikasi, pendidikan mahupun aspek kewangan. Kemajuan dan perkembangan ini sememangnya membawa kesan positif dan kesan negatif baik kepada negara, masyarakat dan para penggunanya. Isu-isu mengenai penggunaan internet juga kian meningkat terutama sekali mengenai kesannya yang memberi kemudharatan terhadap orang lain seperti buli siber ataupun serangan siber. Perkara-perkara tersebut sememangnya dilarang dalam syari'at Islam baik berupa perkataan ataupun perbuatan sebagaimana dalam hadith Rasulallāh Ṣallallāhu 'Alaihi Wasallam:

لا ضرر ولا ضرار

"*Tidak boleh melakukan sesuatu yang membahayakan diri sendiri ataupun orang lain*"[1]

Oleh itu, adalah menjadi keperluan terhadap setiap individu bagi mengetahui jenis-jenis serangan siber, bagaimana ia boleh berlaku dan tatacara melindungi dari menjadi mangsa siber yang lebih dikenali sebagai keselamatan siber. Maka kajian ini akan memfokuskan sasaran dan lokasi terhadap para pelajar tahun akhir program Sarjana Muda di institusi pengajian tinggi awam. Pemilihan ini adalah atas sebab tempat tersebut kian meningkat diserang siber. Kajian lepas juga mendapati bahawa para pelajar merupakan pengguna internet yang tertinggi dan pengaksesan internet secara terbuka.[2] Kesediaan mereka dalam mengambil langkah-langkah untuk melindungi diri dari diserang siber adalah tidak wujud seperti kurang kawalan alat keselamatan dalam komputer/ telefon pintar,[3] tidak mengemaskini perisian aplikasi, penggunaan kata laluan yang mudah diteka dan sebagainya. Apabila pelajar tidak peka dengan penjagaan perisian aplikasi, maka keselamatan maklumatnya akan mudah terjejas. Perkara ini sememangnya akan menimbulkan isu pencerobohan pada maklumat dirinya dan juga pada institusi pengajian.[4]

Kajian Zahidah Zulkifli et. al[5] telah mendapati bahawa pelajar meluangkan masa dengan internet selama 6.6 jam dalam sehari. Tambahan lagi pelajar gemar berkongsi dan mempamerkan maklumat peribadi, menayangkan gambar dan video melalui media sosial tanpa memikirkan risikonya.[6] Ini menunjukkan bahawa pelajar tidak begitu peduli dengan keselamatan maklumat peribadi mereka dari dicuri dan disalahgunakan. Walhal penjenayah siber boleh mencuri maklumat-maklumat tersebut dengan pelbagai cara seperti memuat turun, menggodam akaun dan seumpamanya. Ini dapat dikukuhkan lagi melalui laporan statistik dari pihak Brunei Computer Emergency Response Team (BruCERT); seramai 1, 536 responden telah terlibat dan 20% daripadanya terdiri dari golongan pelajar

[1] Ibn Majah, Abu Abdillah Muhammad Ibn Yazid al-Qazwaini, *Sunan Ibn Majah*, Vol. 1 (Riyadh: Darussalam, 2000). 784. Hadith No. 2341.

[2] Ali Farooq, et. al, "Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors". *14th IEEE International Conference on Trust, Security and Privacy in Computing Communication*. Helsinki: Finland. (2015): 352.

[3] Moti Zwilling et. al, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study", *Journal of Computer Information System* 62, no. 1 (January, 2022): 1.

[4] Wida Susanty Haji Suhaili, "Cabaran Keselamatan Siber Bagi Kesejahteraan Ummah", *Kertas Kerja Simposium Majlis Ilmu 2016*", Pusat Persidangan Antarabangsa Berakas, Negara Brunei Darussalam. (2016): 6.

[5] Zahidah Zulkifli et. al, "Cyber Security Awareness Among Secondary School Students in Malaysia", *Journal of Information Systems and Digital Technologies* 2, no. 2 (30th November 2020): 28.

[6] Mohd Azul Mohd Salleh et. al, "Kesedaran dan Pengetahuan Terhadap Keselamatan dan Privasi Melalui Media Sosial Dalam Kalangan Belia", *Journal of Social Sciences and Humanities* 12, no. 3 (2017): 5.

yang menyatakan pernah mengalami insiden buli siber dan kecurian maklumat peribadi.[7] Berdasarkan dari laporan tersebut, ia memaparkan kurangnya kesedaran mereka terhadap aspek keselamatan siber.

PENGETAHUAN DAN SIKAP TERHADAP PERISIAN APLIKASI

Aspek pengetahuan dan aspek sikap yang dibincangkan dalam kajian ini adalah bagaimana tatacara penggunaan perisian aplikasi yang betul dan selamat seperti mengubahsuai tetapan, menyekat dan sebagainya. Turut dibincangkan juga adalah mengenai penggunaan alat keselamatan yang terdapat pada komputer dan telefon pintar/peranti seperti penggunaan antivirus, *firewall*, penggunaan kata laluan dan seumpamanya.

Secara lazimnya, setiap peranti mengandungi perisian (*software*) bagi mengurus dan menyokong sistem-sistem serta aktiviti dalam memproses maklumat. Perisian boleh dibahagikan kepada dua bahagian iaitu:[8]

i. Perisian Sistem. Ia berfungsi untuk mengurus seluruh sistem yang terdapat pada peranti. Contohnya ialah Sistem Operasi (*Operating System*). Terdapat pelbagai jenis Sistem Operasi yang dibina pada komputer seperti *MacOS*, *Microsoft Windows*, *Ubuntu* dan lain-lain. Manakala Sistem Operasi bagi telefon pintar pula adalah *iOS* dan *Android*.
ii. Perisian Aplikasi. Ia berfungsi bagi membantu tugas-tugas peribadi dan terdiri dari program-program yang direka supaya pengguna lebih produktif, memudahkan proses komunikasi dan sebagainya. Contohnya ialah *Microsoft Office*, aplikasi antivirus, aplikasi permainan, media sosial dan sebagainya.

Di antara perisian aplikasi keselamatan siber yang mampu mencegah dari serangan virus adalah penggunaan antivirus dan *firewall*. Antivirus adalah sebuah perisian yang direka cipta bagi mengenal pasti dan menghapuskan virus pada peranti sebelum ia merebak dan memusnahkan sistem[9]; manakala *firewall* pula ialah perisian yang mengawas kemasukan dan pengeluaran segala rangkaian dari peranti.[10] Tugas utama kedua-dua jenis perisian aplikasi keselamatan ini ialah bagi mencegah virus dari memasuki sistem dan menghapuskannya. Virus juga boleh dikenali sebagai *malicious software* atau *malicious logic*. Terdapat pelbagai jenis virus yang telah dikesan pada masa kini, tetapi dua jenis virus yang amat popular pada masa sekarang ialah:[11]

i. *Trojan Horse*, sejenis virus yang mampu mengambil alih sistem pada sebuah peranti. Tujuan virus ini dicipta adalah bagi merosakkan sistem peranti dan mencuri maklumat peribadi mangsa. Virus ini dikategorikan merbahaya kerana penjenayah mampu mengesan apa yang ditulis oleh mangsa pada peranti.
ii. *Worm*, singkatan nama bagi '*write once, read many times*'. *Worm* ini sejenis virus yang mengeksploitasikan kelemahan yang terdapat pada sistem peranti. Peranti yang sentiasa terikat dengan rangkaian akan lebih mudah menjadikan virus ini membiak dan merebak. Virus ini juga mampu membuatkan penjenayah mencuri maklumat peribadi mangsa.

Kewujudan virus pada peranti boleh disebabkan dua perkara. Pertama, kecuaian pelajar kerana telah memuat turun sesuatu perisian aplikasi tanpa berhati-hati, dan; kedua, penjenayah siber telah menghantar

[7] BruCERT, "*Online Safety Awareness Survey 2021*" (Negara Brunei Darussalam: BruCERT, 2021) 4.

[8] Mohd Tarmizi bin Musa, "STID 1103 – Aplikasi Komputer Dalam Pengurusan", 2016, https://www.scribd.com/presentation/430207901/03-Perisian-Aplikasi.

[9] Federal Communications Commissions, "*Cyber Security Planning Guide*" (California: CreateSpace Independent Publishing Platform, 2014) CSG-1.

[10] Federal Communications Commissions, "*Cyber Security Planning Guide*", CSG-5.

[11] Federal Communications Commissions, "*Cyber Security Planning Guide*", CSG-9 – CSG-10.

kepada pelajar untuk menekan/memuat turun suatu pautan yang seakan-akan selamat digunakan. Jika pelajar telah melakukan salah satu diantara dua perkara berikut, maka perisian aplikasi mereka telah disahkan terjejas (*system compromise*). Peranti akan menjadi kurang cekap dan tidak efisien, mengalami kegagalan sewaktu log masuk, kerosakan pada sistem dan banyak lagi. Oleh itu, penggunaan antivirus dan *firewall* sahaja tidaklah memadai untuk melindungi peranti jika pelajar tiada pengetahuan yang asas mengenainya.

Selain itu, pelajar hendaklah juga memastikan bahawa setiap perisian aplikasi perlu dikemaskini dari semasa ke semasa. Ini kerana setiap penambahbaikan mempunyai komponen alat keselamatan yang terkini dan mampu mencegah virus dari menyerang peranti. Ia juga membuatkan peranti menjadi lebih berintegriti, utuh dan mapan. Tindakan pelajar yang tidak membuat penambahbaikan pada perisian aplikasi serta kurang pengetahuan dalam menetapkan langkah-langkah pada perisian aplikasi akan memudahkan kebocoran maklumat peribadi (*non-compliance activity*).[12] Tambahan lagi, ia akan memberi ruang yang mudah bagi para penggodam untuk cuba menceroboh dan mencuri maklumat-maklumat peribadi.

Menurut Wida Susanty Haji Suhaili[13], pencerobohan boleh dikategorikan kepada tiga peringkat iaitu manusia, proses dan teknologi. Di antara istilah nama-nama yang digunakan bagi merujuk kepada cubaan penggodaman atau pencerobohan ialah: *User Level* Intrusion, *Root Level* Intrusion, *Unsuccessful Hacking Attempt* atau *Unsuccessful Activity Attempt.* Peringkat manusia merupakan salah satu cabaran terbesar dalam isu pencerobohan disebabkan sifat cuai mereka yang tidak menukar kata laluan atau tidak mengukuhkan kawalan keselamatan peranti. Kebanyakkan pelajar hanya beranggapan bahawa mencipta kata laluan yang unik dan susah ataupun memuat turun perisian aplikasi antivirus dan *firewall* mampu melindungi mereka dari diserang siber dan kecurian maklumat peribadi.[14] Perbuatan tersebut sememangnya betul tetapi ia belum cukup memadai. Penjenayah siber pada sekarang sangat kreatif dan pintar dalam modus operandi mereka dengan berbekalkan kecanggihan teknologi pada masa sekarang.

Menggunakan kata laluan yang unik dan susah adalah menjadi satu kemestian kepada setiap pelajar. Penggunaan kata laluan hendaklah mengandungi huruf besar, huruf kecil, nombor dan simbol.[15] Selain itu, penggunaan Pengesahan Dua Faktor (*Two-Factor Authentication*) juga digalakkan kepada setiap pelajar bagi meningkatkan tahap kawalan peranti mereka. Menurut Amelia Mike, walaupun penggunaan Pengesahan Dua Faktor ini tidak menjamin sepenuhnya dari diserang siber, tetapi ia akan mengurangkan penjenayah siber dari berjaya menyerang dan menceroboh data pelajar.[16]

Antara perkara yang perlu diambil perhatian juga adalah mengenai penggunaan perisian aplikasi yang berstatus cetak rompak (*pirated*). Jika pelajar telah mengikuti saranan dan nasihat yang diberikan bagi melindungi perantinya tetapi ia telah menggunakan perisian aplikasi yang berstatus cetak rompak, maka ia hanyalah sia-sia belaka sahaja. Kesilapan ini masih akan memudahkan penjenayah siber mencerobohi peranti dan maklumat peribadi.[17] Oleh itu, adalah disarankan kepada pelajar agar menggunakan perisian aplikasi yang asal. Sungguhpun pelajar perlu membeli perisian aplikasi

[12] Chairman of The Joint Chiefs of Staff Manual, "*Cyber Incident Handling Program*" (USA, 10 July 2012), B-A-3.

[13] Wida Susanty Haji Suhaili, "*Cabaran Keselamatan Siber Bagi Kesejahteraan Ummah*", 6.

[14] Talal Alharbi and Asifa Tassaddiq, "Assessment of Cybersecurity Awareness among Students of Majmaah University", *Big Data Cognitive Computing* 5, no. 23 (10th May 2021): 1.

[15] BruCERT "*Cyber Attacks You Should Be Aware Of*" (Negara Brunei Darussalam: BruCERT, 11 March 2022).

[16] Amelia Mike, "*A Profound Guide on Cyber Security - Getting Protected at Ease as A Professional and A Beginner*" (Independently Published, 2021), 24.

[17] Wida Susanty Haji Suhaili, "*Cabaran Keselamatan Siber Bagi Kesejahteraan Ummah*", 7.

tersebut dan terpaksa mengeluarkan wang, akan tetapi keselamatan diri dan maklumat peribadi lebih berharga berbanding wang yang dikeluarkan untuk membelinya.

Pengetahuan terhadap pelayar web (*web browser*) secara asas juga memainkan peranan penting. Salah satu antaranya adalah dengan mengetahui akan kepentingan dan penggunaan Protokol Pemindahan Hiperteks Selamat (*Hypertext Transfer Protocol Secure* – HTTPS). Ia digunakan bagi menghalang penggodam dari memintas komunikasi. Walaupun penggunaan HTTPS ini agak perlahan sewaktu penimbalan (*buffering*), ini bererti rangkaian sedang dalam proses menjadi terlindung.[18] Jika laman sesawang menunjukkan HTTP, maka lebih baik dielakkan dari meneruskan melayarinya. Ini kerana berkemungkinan laman sesawang tersebut hanyalah dicipta bagi tujuan penggodaman ataupun serangan pancingan data sahaja. Cara paling mudah bagi pelajar untuk memastikan keselamatan web adalah dengan membezakan antara: perkataan '*https://*' bermaksud selamat digunakan, dan; perkataan '*http://*' bermaksud sebaliknya.

Selain itu, jika tujuan menggunakan internet tersebut dikehendaki untuk memasukkan kata laluan, adalah disarankan kepada pelajar untuk menggunakan pelayar web yang berbentuk *incognito*. Pelayar *incognito* ini tidak akan menyimpan mana-mana kata laluan, maklumat peribadi ataupun menjejak aktiviti sewaktu melayari internet. Tetapi, ia tidak menghalang dari diserang virus atau dikesan lokasi. Akhir sekali adalah penggunaan Rangkaian Peribadi Maya (*Virtual Private Network – VPN*) yang menambah kawalan keselamatan dan kerahsiaan kepada pelajar sewaktu mereka melayari internet. Secara asasnya, dengan menggunakan VPN ini, ia akan menyembunyikan identiti atau Alamat Protokol Internet (*Internet Protocol Address – IP Address*) dari dijejaki oleh penggodam.

METODOLOGI

Kajian ini adalah kajian deskriptif berbentuk tinjauan yang terkandung dalam pendekatan kuantitatif. Instrumen yang digunakan pula adalah kaji selidik. Item kaji selidik mengandungi tiga bahagian. Bahagian I merupakan latar belakang responden; Bahagian II mengenai pengetahuan responden terhadap penggunaan perisian aplikasi, dan; Bahagian III mengenai sikap responden terhadap penggunaan perisian aplikasi. Pengkaji telah menggunakan Skala Likert empat mata; responden dikehendaki memberi gerak balas dengan memilih satu jawapan daripada empat pilihan tanpa ada pilihan jawapan 'tidak pasti'. Ini kerana jawapan 'tidak pasti' itu tidak begitu diperlukan dan sukar di ukur walaupun pengkaji telah menetapkan nombor skala padanya.[19] Kajian lepas mendapati responden lebih memilih jawapan 'tidak pasti' disebabkan mengambil jalan mudah dan tidak ingin memikirkan secara mendalam terhadap item yang dikemukakan.[20] Menurut Deobold dalam Mohmad Zamri Ali et. al.,[21] penggunaan Skala Likert empat mata ini mudah ditadbir kepada jumlah yang luas, memberi kesenangan kepada pengkaji untuk menumpukan kepada subjek yang dikaji serta melancarkan proses penjadualan dan penganalisisan.

Dari aspek persampelan pula, responden adalah terdiri dari pelajar-pelajar tahun akhir/Tahun 4 yang sedang mengambil jurusan Sarjana Muda di institusi pengajian tinggi awam iaitu (i) Universiti Brunei Darussalam; (ii) Universiti Islam Sultan Sharif Ali; (iii) Universiti Teknologi Brunei, dan; (iv) Kolej Universiti Perguruan Ugama Seri

[18] BruCERT, "*Tips for a Secure Browsing Experience*" (Negara Brunei Darussalam: BruCERT, 2021).

[19] Gail M. Sullivan dan Anthony R. Artino Jr, "Analyzing and Interpreting Data from Likert-Type Scales", *Journal of Graduate Medical Education* 5, no. 4 (December, 2013): 541.

[20] Christine E. DeMars dan T. Dary Erwin, "Neutral or Unsure: Is There a Difference?", *Annual Meeting of the American Psychological Association*, Washington DC: 2.

[21] Mohmad Zamri Ali et. al, "Tahap Penghayatan Akhlak Tasawuf Dalam Kalangan Pelajar Bermasalah Disiplin Di Sekolah Aliran Agama Daerah Bachok, Kelantan", *International Journal of Education, Psychology and Counselling* 7, no. 46 (June 2022): 206.

Begawan. Jumlah populasi adalah sebanyak 1, 148 orang. Maka dengan merujuk kepada jadual Krejcie dan Morgan[22], seramai 580 orang sampel sahaja yang terlibat dalam kajian ini. Persampelan yang digunakan adalah persampelan Bola Salji (*Snowball sampling*) yang termasuk pada persampelan bukan kebarangkalian (*non-probability sampling*). Ia dilaksanakan dengan mengumpul data ke atas beberapa orang responden yang hendak dikaji, kemudian meminta bantuan kepada mereka untuk mengongsikan maklumat ke atas pelajar lain yang bersamaan ciri-cirinya dalam kajian ini. Pemilihan para pelajar yang sedang berada pada tahun akhir ini adalah disebabkan dua perkara iaitu:

i. Pelajar universiti merupakan sasaran yang semakin giat diserang siber (seperti serangan *phishing, scam, intrusion*) disebabkan sifat cuai mereka dan terlalu terdedah kepada dunia siber. Mereka dikategorikan sebagai pengguna aktif internet dan terlalu banyak bergantung kepada internet dalam pencarian maklumat serta penggunaan media sosial.[23]
ii. Setelah tamat pengajian nanti, pelajar-pelajar ini bakal memegang jawatan bertaraf Pegawai di tempat pekerjaan mereka. Mereka bakal memimpin dan menjadi contoh kepada orang bawahan dalam pelbagai aspek. Oleh itu, meningkatkan aspek keselamatan siber dalam diri adalah satu tindakan yang betul bagi kebaikan mereka di masa hadapan.

Bagi memudahkan pengutipan data ini kepada sampel yang lebih luas, pengkaji telah menggunakan pelayar web *Google* untuk membentuk kod QR dengan menggunakan laman sesawang khas iaitu https://www.qr-code-generator.com/. Setelah itu, pengkaji menjana kod QR tersendiri dengan memasukkan pautan instrumen kaji selidik kedalam kod QR tersebut. Kod QR serta pautan instrumen kaji selidik secara *softcopy* (dihantar melalui e-mel) dan *hardcopy* telah diserahkan kepada ketua bahagian Hal Ehwal Akademik pada setiap empat buah universiti. Pengkaji telah meminta bantuan kepada mereka untuk mengongsikan pautan tersebut kepada setiap fakulti, kemudian pihak fakulti mengongsikan pautan itu kepada para pelajar tahun akhir melalui e-mel universiti dan perisian aplikasi *WhatsApp*. Selain itu, pengkaji juga membuat perjumpaan bersama beberapa orang responden untuk mengisikan instrumen kaji selidik tersebut serta meminta bantuan kepada mereka untuk mengongsikan pautan tersebut kepada rakan sebaya mereka.

Data yang dikumpul telah dianalisis menggunakan perisian *Statistical Package for Social Sciences*. Analisis berbentuk deskriptif dilakukan ke atas demografi responden bagi mengetahui jumlah responden seperti jantina, tempat pengajian melalui teknik taburan kekerapan dan peratusan. Nilai min dan sisihan piawai pula digunakan pada soalan bahagian II dan III bagi menganalisa soalan yang berkaitan dengan faktor pengetahuan dan faktor sikap. pengkaji menggunakan interpretasi skor min yang telah digunapakai oleh Ghani Hj Taib dalam Mohmad Zamri Ali, et. al.[24] iaitu dengan menetapkan tiga peringkat; peringkat rendah, peringkat sederhana dan peringkat tinggi.

Jadual 1: Interpretasi Skor Min

Skala	**Tahap**
1.00 – 2.00	Rendah
2.01 – 3.00	Sederhana
3.01 – 4.00	Tinggi

[22] Robert V. Krejcie and Daryle W. Morgan, "Determining Sample Size for Research Activities", *Educational and Psychological Measuremenet* 30, no. 3 (Autumn 1970), 608.

[23] Safiek Mokhlis, "Buli Siber Dalam Kalangan Pelajar Sekolah Menengah: Satu Penerokaan Awal", *Jurnal Dunia Pendidikan* 1, no. 2 (2019): 8-9.

[24] Mohmad Zamri Ali et. al, "*Tahap Penghayatan Akhlak Tasawuf Dalam Kalangan Pelajar Bermasalah Disiplin Di Sekolah Aliran Agama Daerah Bachok, Kelantan*": 206.

Bagi menganggarkan kebolehpercayaan atau ketekalan dalaman item-item instrumen kaji selidik, maka pengkaji telah menjalankan kajian rintis dan menggunakan *Alpha Cronbach*. Kajian rintis adalah sangat penting bagi sesebuah kajian kerana ia boleh membantu pengkaji mengenal pasti tahap kebolehlaksanaan instrumen kajian, dapat mengetahui sejauhmana item-item yang dikemukakan itu sesuai dan difahami oleh responden dan dapat mengetahui item-item yang mengelirukan ataupun item yang kurang sesuai.[25]

Dalam kajian rintis ini, seramai 40 orang pelajar Sarjana Muda Tahun 3 dari empat buah universiti telah dipilih secara rawak bagi menjawab kajian rintis. Pemilihan 40 orang sampel secara rawak yang terdiri dari bukan sampel kajian adalah kerana mereka mempunyai ciri-ciri yang sama dengan populasi kajian yang sebenar. Mereka turut menggunakan kemudahan info-teknologi yang diberikan di universiti serta mereka juga kelak memimpin orang bawahan di alam pekerjaan nanti. Manakala pemilihan jumlah responden seramai 40 orang adalah dengan melihat pandangan Guadagnoli dan Velicer[26] yang mencadangkan seramai 50 orang dan melihat pandangan Isaac dan Michael[27] serta Hill[28] menyatakan jumlah sampel bagi kajian rintis adalah sebanyak 10 – 30 orang kerana mempunyai banyak kebaikan, seperti pengiraan yang mudah. Jadual 2 merupakan analisis laporan ujian kebolehpercayaan berdasarkan nilai *Alpha Cronbach* bagi setiap pembolehubah yang dikaji.

Jadual 2: Laporan Kajian Rintis

Pembolehubah	**Jumlah Item**	**Alpha Cronbach**
Pengetahuan	7	.795
Sikap	5	.703

Menerusi Jadual 2 ini, nilai kebolehpercayaan *Alpha Cronbach* yang telah didapati oleh pengkaji dalam kajian rintis ini telah menunjukkan bahawa 'Faktor Pengetahuan' mempunyai nilai sebanyak .795, dan; 'Faktor Sikap' mempunyai nilai sebanyak .703. Dalam kajian ini, pengkaji telah merujuk kepada tahap kebolehpercayaan *Alpha Cronbach* yang telah digariskan oleh Azizi Yahaya et. al:[29] nilai <0.50 rendah; nilai antara 0.60 – 0.70 kebolehpercayaan memadai; nilai antara 0.70 – 0.90 kebolehpercayaan tinggi, dan; nilai >0.90 kebolehpercayaan sempurna. Ini menunjukkan kesemua item dalam instrumen kaji selidik ini memenuhi kriteria kebolehpercayaan untuk dilaksanakan pada kajian sebenar.

DAPATAN KAJIAN

Jadual 3: Demografi Responden

Demografi (n=580)		**Frekuensi**	**Peratus**
Jantina	Lelaki	244	42.1
	Perempuan	336	57.9
Universiti	UBD	217	37.4
	UNISSA	152	26.2
	UTB	175	30.2
	KUPU SB	36	6.2

Profil demografi responden yang dianalisis secara deskriptif menunjukkan seramai 580

[25] Ahmad Mahdzan Ayob, "*Kaedah Penyelidikan Sosioekonomi*" (Kuala Lumpur: Dewan Bahasa dan Pustaka, 1992) 83.

[26] Guadagnoli Edward dan Velicer Wayne F, "Relation to Sample Size to the Stability of Component Patterns", *Psychological Bulletin* 103, no. 2 (1988): 265

[27] Isaac Stephen dan Michael William B, "*Handbook in Research and Evaluation*" (San Diego, California: Educational and Industrial Testing Services, 1995) 101.

[28] Robin Hill, "What Sample Size Is "Enough" in Internet Survey Research?", *Interpersonal Computing and Technology: An Electronic Journal for 21st Century* 6, no. 3-4 (July 1998): 11.

[29] Azizi Yahaya et. al, "*Menguasai SPSS Dengan Mudah*" (Universiti Islam Sultan Sharif Ali: UNISSA Press, 2016) 57.

orang responden telah menjawab instrumen kaji selidik yang terdiri dari 244 orang responden (43.1%) adalah lelaki dan 336 orang responden (57.9%) adalah perempuan. Manakala demografi seterusnya adalah mengenai tempat pengajian. Data melaporkan seramai 217 orang responden (37.4%) adalah dari Universiti Brunei Darussalam; 152 orang responden (26.2%) berasal dari Universiti Islam Sultan Sharif Ali; 175 orang responden (30.2%) dari Universiti Teknologi Brunei, dan; 36 orang responden (6.2%) dari Kolej Universiti Perguruan Ugama Seri Begawan.

Jadual 4: Faktor Pengetahuan

No	Item	Min
1	Istilah '*http://*' bererti selamat digunakan untuk melayari internet	2.56
2	Fungsi penyemak imbas hanyalah untuk memelihara kata laluan	2.51
3	Menggunakan antivirus adalah mencukupi bagi melindungi peranti	2.56
4	Saya menggunakan '*incognito web*' bagi mencegah serangan virus	2.26
5	Saya menghidupkan Pengesahan-Dua-Faktor bagi tujuan keselamatan.	3.21
6	Fungsi VPN adalah untuk melindungi aktiviti sewaktu melayari internet	3.09
7	Mengemaskini perisian aplikasi akan menjadikan peranti lebih mapan	3.22

Min Keseluruhan = 2.77

Jadual 4 memaparkan taburan nilai min mengenai pengetahuan para responden terhadap penggunaan perisian aplikasi. Berdasarkan dari Jadual 4 tersebut, item pertama adalah berada pada tahap sederhana dengan nilai min 2.56. Seramai 278 orang responden (47.9%) menyatakan tidak bersetuju bahawa penggunaan istilah '*http://*' adalah selamat digunakan bagi melayari internet, manakala seramai 302 orang responden (52.1%) pula menyatakan bersetuju mengenainya. Begitu juga item mengenai pengetahuan terhadap fungsi penyemak imbas hanya untuk memelihara kata laluan sahaja telah mendapat nilai min sebanyak 2.51 iaitu tahap sederhana. Sebilangan responden seramai 289 orang (49.8%) menyatakan tidak bersetuju dan sebilangan responden lagi seramai 291 orang (50.2%) menyatakan bersetuju.

Pengetahuan terhadap perisian aplikasi juga berkaitan dengan penggunaan antivirus bagi melindungi peranti. Item ini mendapat nilai min sebanyak 2.56 iaitu pada tahap sederhana. Sebilangan kecil responden seramai 280 orang (48.3%) menyatakan tidak bersetuju bahawa penggunaan antivirus adalah mencukupi bagi melindungi peranti. Melalui data ini, dapat dilihat bahawa seramai 300 orang responden (51.7%) pula menyatakan mereka bersetuju terhadap perkara tersebut. Selain itu, item mengenai penggunaan '*incognito web*' bagi mencegah peranti dari diserang virus pula mendapat nilai min 2.26, iaitu pada tahap sederhana. Sebilangan besar responden seramai 361 orang (62.3%) menyatakan tidak bersetuju bahawa penggunaan '*incognito web*' adalah bertujuan bagi mencegah peranti dari diserang virus. Manakala seramai 219 orang responden (37.7%) sahaja yang menyatakan bersetuju mengenainya.

Pengetahuan responden terhadap perisian aplikasi juga merangkumi fungsi Pengesahan-Dua-Faktor bagi tujuan keselamatan. Taburan nilai min menunjukkan 3.21 iaitu pada tahap tinggi. Taburan nilai kekerapan dan nilai peratusan pula menunjukkan sebahagian besar seramai 496 orang responden (85.5%) bersetuju bahawa menghidupkan Pengesahan-Dua-Faktor adalah bagi tujuan keselamatan. Manakala sebahagian kecil pula seramai 84 orang responden (14.5%) menyatakan tidak bersetuju. Tambahan lagi, pengetahuan terhadap fungsi *VPN* bagi melindungi aktiviti sewaktu melayari internet telah mendapat nilai min sebanyak 3.09 iaitu pada tahap tinggi. Sebahagian besar responden seramai 460 orang (79.3%) menyatakan bersetuju mengenai fungsi *VPN* tersebut. Manakala sebahagian kecil seramai 120 orang responden (20.7%) menyatakan tidak bersetuju bahawa fungsi *VPN* adalah bagi melindungi aktiviti mereka sewaktu menggunakan internet. Selain itu, item terakhir berada di tahap tinggi dengan nilai

min sebanyak 3.22. Taburan nilai kekerapan dan nilai peratusan menunjukkan bahawa seramai 497 orang responden (85.6%) mempunyai pengetahuan bahawa peranti mereka akan menjadi lebih mapan dengan mengemaskini perisian aplikasi. Oleh itu, data ini juga menunjukkan bahawa seramai 83 orang responden (14.3%) sahaja menyatakan tidak bersetuju mengenainya.

Secara kesimpulan, item mengenai pengetahuan responden terhadap pengemaskinian perisian aplikasi agar menjadi mapan merupakan item yang tertinggi dengan keputusan nilai min 3.22. Manakala data menunjukkan responden kurang pengetahuan terhadap fungsi penggunaan '*incognito web*', dengan mendapat nilai min terendah iaitu sebanyak 2.26. Dapatan kajian ini menunjukkan bahawa bahawa keseluruhan keputusan nilai min berada pada tahap 2.77, iaitu tahap sederhana. Nilai min 2.77 ini juga menunjukkan bahawa para responden perlu meningkatkan lagi ilmu pengetahuan mereka dalam aspek penggunaan perisian aplikasi terutama mengenai peranan '*incognito web*', fungsi penyemak imbas dan juga istilah '*http://*' sewaktu mereka melayari internet.

Jadual 5: Faktor Sikap

No	Item	Min
1	Saya hanya memberikan maklumat peribadi kepada organisasi yang diketahui	3.33
2	Saya tidak membuka pesanan e-mel kecuali dari sumber yang dipercayai	3.23
3	Saya mengemaskini kesemua perisian aplikasi	2.91
4	Saya memeriksa tetapan yang terdapat pada perisian aplikasi	2.75
5	Kata laluan saya mengandungi huruf besar, huruf kecil, nombor dan simbol	3.05
6	Saya tidak pernah menukar kata laluan	2.54

Min Keseluruhan = 3.03

Jadual 5 memaparkan taburan nilai min bagi setiap item yang mengukur faktor sikap responden dalam penggunaan perisian aplikasi. Berdasarkan dari Jadual 5 ini, sikap berhati-hati dengan memberikan maklumat peribadi kepada organisasi yang diketahui sahaja memperolehi nilai min 3.33 iaitu pada tahap tinggi. Sebahagian besar seramai 528 orang responden (91.0%) menyatakan mereka bersetuju untuk memberikan maklumat peribadi mereka kepada organisasi yang mereka ketahui sahaja. Manakala seramai 52 orang responden (9.0%) pula menyatakan mereka tidak bersetuju. Begitu juga item mengenai tidak membuka pesanan e-mel kecuali dari sumber yang dipercayai. Item ini mempunyai nilai min sebanyak 3.23 iaitu pada tahap tinggi. Seramai 499 orang responden (86.0%) memberikan jawapan bersetuju mengenai tindakan tersebut dan seramai 81 orang responden (14.0%) sahaja tidak bersetuju mengenai tindakan itu.

Selain berhati-hati dalam melindungi maklumat peribadi, aspek sikap dalam menjaga peranti juga ditekankan seperti kerap kali mengemaskini kesemua perisian aplikasi. Item ini mempunyai nilai min sebanyak 2.91 iaitu pada tahap sederhana. Seramai 173 orang responden (29.8%) menyatakan tidak bersetuju, iaitu mereka tidak mengemaskini perisian aplikasi mereka. Oleh itu, data ini menunjukkan bahawa seramai 407 orang responden (70.2%) menjaga peranti mereka dengan kerap kali mengemaskini perisian aplikasi. Aspek melindungi peranti juga meliputi sikap responden yang memeriksa tetapan yang pada perisian aplikasi. Item ini mempunyai nilai min 2.75 pada tahap sederhana. Seramai 221 orang responden (38.1%) tidak bersetuju, iaitu tidak memeriksa tetapan yang terdapat dalam perisian aplikasi mereka. Manakala seramai 359 orang responden (61.9%) pula bersetuju terhadap tindakan tersebut.

Aspek sikap responden juga merangkumi penggunaan kata laluan. Item tentang kata laluan yang mengandungi huruf besar, huruf kecil, nombor dan simbol adalah pada tahap tinggi dengan nilai min 3.05. Data menunjukkan sebilangan besar para responden seramai 450 orang (77.6%) bersetuju mengenai penggunaan kata laluan sedemikian. Manakala seramai 130 orang responden (22.4%) pula tidak menerapkan

sikap untuk menggunakan kata laluan sedemikian. Begitu juga dengan sikap responden yang tidak pernah menukar kata laluan. Item ini telah memperoleh nilai min sebanyak 2.54 iaitu pada tahap sederhana. Sebahagian responden seramai 301 orang (51.9%) bersetuju bahawa mereka tidak pernah menukar kata laluan mereka. Data ini mempamerkan bahawa hanya seramai 279 orang responden (48.1%) yang pernah menukar kata laluan mereka.

Secara kesimpulan, item mengenai sikap responden yang selalu memberikan maklumat peribadi kepada organisasi yang diketahui sahaja merupakan item yang tertinggi dengan nilai min 3.33. Manakala item mengenai responden mempunyai sikap yang kurang peka dengan tidak pernah menukar kata laluan mereka mendapat nilai min terendah iaitu sebanyak 2.54. Keseluruhan dapatan ini menunjukkan bahawa nilai min adalah berada pada tahap tinggi dengan nilai 3.03. Oleh itu, responden juga perlu meningkatkan dan mengubah sikap mereka agar selalu mengemaskini perisian aplikasi mereka, memeriksa tetapan serta menukar kata laluan mereka sekurang-kurangnya setiap enam bulan.

PERBINCANGAN

Secara keseluruhan, dapatan kajian menunjukkan para pelajar mempunyai pengetahuan yang minima dalam menggunakan dan mengendalikan perisian aplikasi. Ini boleh dilihat melalui nilai keseluruhan min yang diperolehi pada Jadual 4 sebanyak 2.77, iaitu tahap sederhana. Nilai sederhana tersebut mencerminkan pelajar hanya didapati mempunyai pengetahuan terhadap penggunaan Pengesahan-Dua-Faktor, menggunakan VPN dan pengemaskinian perisian aplikasi. Ketiga-tiga komponen ini sememangnya merupakan antara pengetahuan yang perlu wujud dalam tiap pelajar bagi menjaga perisian aplikasi mereka. Walau bagaimanapun, pengetahuan yang hanya tertumpu terhadap tiga komponen tersebut sahaja tidaklah memadai jika komponen-komponen lain diabaikan seperti fungsi penggunaan antivirus, penggunaan pelayar *incognito* dan sebagainya. Hal ini bertepatan sepertimana yang telah dibincangkan oleh Mohd Azul Mohammad Salleh et. al[30] bahawa sesetengah pelajar hanya memahami dan menguasai sebahagian konsep perisian aplikasi sahaja, tetapi tidak memahami konsep yang lain.

Dapatan ini disokong sebagaimana kajian Henriksson[31] yang berbentuk kualitatif dengan sampel seramai 10 orang, telah menemukan kesemua pelajar mengetahui mengenai penggunaan Pengesahan-Dua-Faktor. Tetapi, tidak semua responden menggunakannya. Ini menjelaskan perlunya inisiatif dari pihak institusi pengajian tinggi untuk mewujudkan program yang menggalakkan pelajar menggunakan Pengesahan-Dua-Faktor bagi perlindungan perisian aplikasi mereka. Selain itu, Sharma dan Kaur[32] turut mengkaji penggunaan VPN dikalangan pelajar universiti. Fungsi VPN adalah bagi melindungi privasi pelajar sewaktu berinteraksi dengan internet dengan menyembunyikan alamat protokol asal. Tetapi Xiong[33] mendapati seramai 350 orang pelajar dari Princeton University telah menggunakan VPN bagi tujuan mengakses laman sesawang yang disekat/terlarang , bukan bagi tujuan menyembunyikan alamat protokol mereka. Hal ini menggambarkan perlunya ditingkatkan kesedaran pelajar dalam aspek

[30] Mohd Azul Mohammad Salleh, et. al, "*Kesedaran dan Pengetahuan Terhadap Keselamatan dan Privasi Melalui Media Sosial Dalam Kalangan Belia*": 12.

[31] Adam Henriksson, "What are the Motivations and Barriers for Incorporating Multi-Factor Authentication among IT Students?" (Degree Project, University of Skövde, 2020), 11.

[32] Yogesh Kumar Sharma dan Chamandeep Kaur, "The Vital Role of Virtual Private Network (VPN) in Making Secure Connection Over Internet World", *International Journal of Recent Technology and Engineering* 8, no. 6 (March 2020): 2336-2337.

[33] Andre Xiong, "College Students' Perceptions and Usage of Virtual Private Network" (Undergraduate Senior Thesis, Princeton University, 2019), 6.

keselamatan siber agar mereka tidak menyalahgunakan ciri-ciri yang tersedia.

Sehubungan dengan itu, dapatan kajian ini bertentangan dengan kajian Araos, Damsa dan Gasevic.[34] Kajian yang menggunakan gabungan pendekatan kuantitatif dan kualitatif keatas 73 orang pelajar Sarjana Muda di empat buah universiti New Zealand ini mendapati pelajar tidak begitu peduli dengan mengemaskini perisian aplikasi. Ini memaparkan perlunya penekanan kepada pelajar agar memahami bagaimana mekanisme pengemaskinian perisian aplikasi berfungsi dan mampu untuk melindungi mereka sewaktu berada di alam siber.

Di sini, soal penggunaan perisian aplikasi berbalik semula pada sikap pelajar dalam menggunakan internet. Pelajar masih mampu untuk melindungi peranti mereka dengan baik jika mereka tidak sewenang-wenangnya membuka pesanan e-mel yang mencurigakan ataupun menggunakan kata laluan yang kompleks dan seumpamanya. Berdasarkan dari dapatan kajian pada Jadual 5 di atas memaparkan bahawa sikap pelajar dalam penggunaan perisian aplikasi adalah pada tahap tinggi dengan mencatatkan nilai keseluruhan min sebanyak 3.03. Nilai min tersebut menjelaskan sikap pelajar yang sentiasa berhati-hati dalam menerima pesanan e-mel, tidak memberikan maklumat mereka sewenang-wenangnya adalah satu tindakan yang bertepatan dalam menjaga perisian aplikasi mereka. Tambahan lagi pelajar telah sedia maklum dengan penggunaan kata laluan yang kompleks. Ini selaras dengan teori asas yang telah digariskan oleh *National Institute of Standard and Technology (NIST)* dalam Bhatnagar dan Pry[35] serta Cybersecurity and Infrastructure Agency[36] dalam PR.AC-1 Rangka Kerja Keselamatan Siber; yang menyatakan penggunaan kata laluan hendaklah diurus dengan betul bagi melindungi hak pengguna.

Walau bagaimanapun, terdapat kesan yang negatif terhadap keselamatan perisian aplikasi jika pelajar tidak menanamkan sikap untuk sentiasa mengubah kata laluan sekurang-kurangnya setiap 6 bulan. Sikap pelajar yang tidak begitu memuaskan dalam hal ini boleh membuka peluang kepada penjenayah untuk melakukan aktiviti penggodaman akaun, mencuri dan seumpamanya. Tambahan lagi pelajar didapati tidak begitu hirau dalam mengemaskini perisian aplikasi mereka. Sungguhpun mereka mengetahui tindakan mengemaskini perisian aplikasi tersebut akan menambah kawalan yang mapan terhadap perisian aplikasi, tetapi mereka tidak mengaplikasikan pengetahuan tersebut. Dalam hal ini, para pelajar seharusnya melahirkan rasa khawatir tentang keselamatan perisian aplikasi mereka dari dicerobohi.

Hasil kajian daripada 580 orang responden ini telah membantu dan memberikan perbincangan yang penting untuk mengetahui tahap pengetahuan dan sikap pelajar terhadap perisian aplikasi mereka. Segala maklumat dan dapatan yang telah diperolehi ini menjadi titik asas kepada kajian yang berbentuk keselamatan sosial agar dapat diterokai lagi kepada skop yang lebih besar pada masa hadapan.

LIMITASI DAN CADANGAN KAJIAN

Penemuan yang dipaparkan dalam kajian ini memberikan perkara penting untuk meningkatkan kemahiran yang perlu dikecapi dalam diri pelajar iaitu kemahiran dalam memahami konsep perisian aplikasi. Sungguhpun demikian, terdapat beberapa

[34] Andrés Araos, Crina Damsa dan Dragan Gasevic, "Browsing to Learn: How Computer and Software Engineering Students Use Online Platforms in Learning Activities", *Journal of Computer Assisted Learning* 39, (December 2022): 676.

[35] Neelima Bhatnagar dan Michael Pry "Student Attitudes, Awareness and Perceptions of Personal Privacy and Cybersecurity in the Use of Social Media: An Initial Study", *Information Systems Education Journal* 18, no. 1 (February 2020): 52.

[36] Cybersecurity and Infrastructure Security Agency, "*Commercial Facilities Sector – Cybersecurity Framework Implementation Guidance*", (United States of America: Department of Homeland Security, 2020) 30.

batasan yang perlu diketengahkan untuk menambah baik pada kajian-kajian di masa hadapan. Antaranya ialah:

i. Kajian lanjut perlu dijalankan ke atas populasi pelajar peringkat pasca-siswazah. Kajian ini hanya memfokuskan terhadap pelajar Sarjana Muda sahaja. Maka kajian akan datang boleh memfokuskan kepada populasi yang berlainan seperti pelajar di peringkat pasca-siswazah. Ini kerana pelbagai faktor yang boleh mempengaruhi tahap pengetahuan dan sikap pelajar dalam penggunaan perisian aplikasi seperti faktor umur, pengalaman dan juga kesedaran. Tambahan lagi, pelajar pasca-siswazah lazimnya terdiri dari golongan professional yang berkemungkinan mempunyai pengalaman kerja dan pelbagai kemahiran berbanding pelajar Sarjana Muda.
ii. Kajian ini hanya dijalankan ke atas pelajar-pelajar tahun akhir/Tahun 4 di empat buah universiti awam di Negara Brunei Darussalam, tetapi tidak melibatkan universiti swasta seperti Kolej Perdagangan Laksmana, Kolej Pengajian Siswazah Antarabangsa, Kolej Perdagangan dan Teknologi Cosmopolitan dan seumpamanya. Maka kajian akan datang bolehlah membuat perbandingan terhadap tahap pengetahuan dan sikap keselamatan siber antara pelajar universiti awam dan universiti swasta. Hasil dari dapatan kajian nanti akan dapat memberikan gambaran yang menyeluruh kepada pihak Kementerian Hal Ehwal Ugama, Kementerian Pendidikan dan Kementerian Pengangkutan dan Infokomunikasi untuk menggubal satu kurikulum atau program latihan keselamatan siber yang berkesan.
iii. Pihak institusi pengajian tinggi perlu berusaha dan bekerjasama dengan pihak-pihak yang berkenaan bagi menangani isu keselamatan siber dalam era Revolusi Industri 4.0 ini; untuk meningkatkan tahap pengetahuan dan sikap pelajar dalam penggunaan perisian aplikasi, konsep asas dan seumpamanya.
iv. Kaedah penyampaian dalam meningkatkan faktor pengetahuan dan faktor sikap pelajar hendaklah bersesuaian serta mampu memberikan kesan yang berpanjangan. Kajian Noor Hayani Abd Rahim[37] menunjukkan bahawa kaedah latihan berasaskan video memberikan impak yang positif terhadap para pelajar. Ini kerana setiap tindakan dan kesalahan yang mereka lakukan sama ada secara sedar mahupun tidak mampu dipantau melalui kamera.

KESIMPULAN

Setiap pelajar yang menggunakan internet tidak akan menyedari jika sistem peranti mereka telah diceroboh ataupun diserang. Ini kerana mereka tidak begitu mengetahui bagaimana tatacara perlindungan yang sebaiknya bagi mengelakkan menjadi mangsa siber. Oleh itu pelajar perlu mengikuti saranan dan nasihat yang telah ditunjukkan oleh agensi keselamatan siber sepertimana yang telah dinyatakan dari Cyber Security Brunei melalui segmen Radio Televisyen Brunei, jerayawara, seminar dan media sosial Instagram. Oleh sebab itu, pengetahuan adalah kunci bagi meningkatkan kawalan keselamatan perisian aplikasi serta bagi menyedari manakah perkara yang perlu dilakukan dan mana perkara yang perlu ditinggalkan. Dengan ilmu pengetahuan, ia boleh memajukan, membangunkan dan mampu beroleh kejayaan bagi diri sendiri, ugama, bangsa dan juga negara. Walhal agama Islam amat menggalakkan umatnya agar berusaha mencari ilmu dan ia adalah menjadi satu kewajipan terhadap diri sendiri sebagaimana sabda Rasulallāh Ṣallallāhu ‘Alaihi Wasallam:

[37] Noor Hayani Abd Rahim, “Assessment of Cybersecurity Awareness Program on Personal Data Protection among Youngsters in Malaysia”, *Malaysian Journal of Computer Science* 32, no. 3 (July 2019): 241.

عن أنس ابن مالك قال: قال رسول الله صلى الله عليه وسلم: طلب العلم فريضة على كل مسلم

"*Daripada Anas bin Malik ia berkata: Sabda Rasulallāh Ṣallallāhu 'Alaihi Wasallam: Menuntut ilmu adalah satu kefardhuan ke atas setiap muslim*"

BIBLIOGRAFI

Ahmad Mahdzan Ayob, *Kaedah Penyelidikan Sosioekonomi*. Kuala Lumpur: Dewan Bahasa dan Pustaka, 1992

Alharbi, Talal and Tassaddiq, Asifa, "Assessment of Cybersecurity Awareness Among Students of Majmaah University". *Big Data Cognitive Computing* 5, no. 23 (10th May 2021): 1-15. https://doi.org/10.3390/bdcc5020023.

Araos, Andres, Damsa, Crina dan Gasevic, Dragan, "Browsing to Learn: How Computer and Software Engineering Students Use Online Platforms in Learning Activities", *Journal of Computer Assisted Learning* 39 (December 2022): 676-693. https://doi.10.111/jcal.12774.

Azizi Yahaya, Dk Zainab Pg Hj Tuah, Baharudin Arus dan Ismail Ibrahim, *Menguasai SPSS Dengan Mudah*. Universiti Islam Sultan Sharif Ali: UNISSA Press, 2016.

Bhatnagar, Neelima dan Pry, Michael, "Student Attitudes, Awareness and Perceptions of Personal Privacy and Cybersecurity in The Use of Social Media: An Initial Study", *Information Systems Education Journal* 18, no. 1 (February 2020): 48-58.

BruCERT, *Cyber Attacks You Should Be Aware Of*. Negara Brunei Darussalam: BruCERT, 2022.

BruCERT, Tips for a Secure Browsing Experience. Negara Brunei Darussalam: BruCERT, 2022.

Chairman of The Joint Chiefs of Staff Manual, *Cyber Incident Handling Program*. United States, 10 July, 2012.

Cybersecurity and Infrastructure Security Agency, *Commercial Facilities Sector – Cybersecurity Framework Implementation Guidance*. United States of America: Department of Homeland Security, 2020

DeMars, Christine E dan Erwin, T. Dary, "Neutral or Unsure?: Is There a Difference?", *Annual Meeting of the American Psychological Association*, Washington DC.

Farooq, Ali et. al, "Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors", *14th IEEE International Conference on Trust, Security and Privacy in Computing Communication*. Helsinki: Finland, 2015.

Federal Communications Commissions, *Cyber Security Planning Guide*. California: CreateSpace Independent Publishing Platform, 2014.

Guadagnoli, Edward dan Velicer, Wayne F, "Relation to Sample Size to the Stability of Component Patterns", *Psychological Bulletin* 10, no. 2 (1988): 265-275. https://doi.org/10.1037/0039-2909.103.2.265.

Henrikson, Adam, "What are the Motivations and Barriers for Incorporating Multi-Factor Authentication among IT Students?" Degreee Project, University of Skövde, 2020.

Hill, Robin, "What Sample Size Is "Enough" in Internet Survey Research?', *Interpersonal Computing and Technology: An Electronic Journal for 21st Century* 6, no. 3-4 (July 1998): 1-10.

Isaac, Stephen dan Michael, William B. *Handbook in Research and Evaluation*. San Diego, California: Educational and Industrial Testing Services, 1995.

Krejcie, Robert V. dan Morgan, Daryle W, "Determining Sample Size for Research Activities". *Educational and Psychological Measurement* 30. No. 3 (Autumn 1970): 607-610. https://doi.org/10.1177/001316447003000308.

Mike, Amelia, *A Profound Guide on Cyber Security - Getting Protected at Ease as A Professional and A Beginner*. n. pl: Independently Published, 20211.

Mohd Azul Mohamad Salleh, Mohd Yusof Hj Abdullah, Ali Salman dan Ahmad Sauffiyan Hassan, "Kesedaran Dan Pengetahuan Terhadap Keselamatan Dan Privasi Melalui Media Sosial Dalam Kalangan Belia", *Journal of Social Sciences and Humanities* 12, no. 3 (2017): 1-15.

Mohd Tarmizi bin Musa, "STID 1103 – Aplikasi Komputer Dalam Pengurusan", 2016, https://www.scribd.com/presentation/430207901/03-Perisian-Aplikasi.

Mohmad Zamri Ali, Nawi @Mohd. Nawi Ismail dan Azizah Hussin, "Tahap Penghayatan Akhlak Tasawuf Dalam Kalangan Pelajar Bermasalah Disiplin Di Sekolah Aliran Agama Daerah Bachok, Kelantan", *International Journal of Education, Psychology and Counselling* 7, no. 46 (June 2022): 197-214. http://dx.doi.org/10.35631/IJEPC.746017.

Muhammad Adnan Pitchan, Siti Zobidah Omar, Jusang Bolong and Akhmar Hayati Ahmad Ghazali. "Analisis Keselamatan Siber Dari Perspektif Persekitaran Sosial: Kajian Terhadap Pengguna Internet Di Lembah Klang". *Journal of Social Sciences and Humanities* 12, no. 2 (2017): 16-29. ISSN 1823-884x.

Noor Hayani Abd. Rahim, Suraya Hamid dan Laila Mat Kiah, "Assessment of Cybersecurity Awareness Program on Personal Data Protection Among Youngsters in Malaysia", *Malaysian Journal of Computer* 32, no. 3 (31 July 2019). https://doi.org/10.22452/mjcs.vol32no3.4.

Safiek Mokhlis, "Buli Siber Dalam Kalangan Pelajar Sekolah Menengah: Satu Penerokaan Awal", *Jurnal Dunia Pendidikan* 1, no. 2 (2019): 7-18.

Sharma, Kyogesh Kumar dan Kaur, Chamandeep, "The Vital Role of Virtual Private Network (VPN) in Making Secure Connection Over Internet World", *International Journal of Recent Technology and Engineering* 8, no. 6 (March 2020). https://dx.doi.org/10.35940/ijrte.F8335.038620

Sullivan, Gail M. dan Artino, Anthony R Jr, "Analyzing and Interpreting Data from Likert-Type Scales", *Journal of Graduate Medical Education* 5, no. 4 (December 2013): 541-542). https://doi.org/10.4300%2FJGME-5-4-18.

Wida Susanty Haji Suhaili, "Cabaran Keselamatan Siber Bagi Kesejahteraan Ummah", *Kertas Kerja Simposium Majlis Ilmu 2016*" Pusat Persidangan Antarabangsa Berakas, Negara Brunei Darussalam, 23-25 Ogos 2016.

Xiong, Andre, "College Students' Perceptions and Usage of Virtual Private Network" Undergraduate Senior Thesis, Princeton University, 2019.

Zahidah Zulkifli, Nurul Nuha Abdul Molok, Nurul Hayani Abd Rahim dan Shuhaili Talib, "Cyber Security Awareness Among Secondary School Students in Malaysia", *Journal of Information Systems and Digital Technologies* 2, no. 2 (2020): 28-41. https://doi.org/10.31436/jisdt.v2i2.151.

Zwilling, Moti, Klien, Galit, Lesjak, Dusan, Wiechetek, Lukasz, Cetin, Fatih dan Basim, Nejat, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study", *Journal of Computer Information System* 62, no. 1 (January 2022): 82-97. http://dx.doi.org/10.1080/08874417.2020.1712269.