SIKAP TERHADAP KESELAMATAN SIBER: KAJIAN TERHADAP PELAJAR INSTITUSI PENGAJIAN TINGGI

Muhammad Haziq Bin Haji Shahjahan
Nurefnazahani Binti Haji Durani

Universiti Islam Sultan Sharif Ali, Negara Brunei Darussalam
Universiti Islam Sultan Sharif Ali, Negara Brunei Darussalam

haziq.shahjahan@outlook.com
nurefnazahani.durani@unissa.edu.bn

Abstrak

Perubahan dunia yang semakin berkembang dengan kepesatan teknologi telah menimbulkan kekhuatiran terhadap seluruh negara khususnya aspek keselamatan siber. Malahan ia telah membuka ruang kepada penjenayah siber untuk melancarkan pelbagai ancaman dan serangan. Adapun sasaran yang semakin mendapat perhatian dikalangan penjenayah siber adalah para pelajar di institusi pengajian tinggi disebabkan tempat tersebut merupakan pengguna siber yang tertinggi dan pengaksesan internet secara terbuka. Sikap pelajar merupakan salah satu teras utama dalam konteks keselamatan siber. Dengan meningkatkan kewaspadaan terhadap perlindungan peranti dan maklumat peribadi, ia mampu mengurangi risiko pelajar dalam alam siber. Oleh itu, kajian ini bertujuan meneliti sikap pelajar dalam perlindungan peranti dan maklumat peribadi sewaktu menggunakan internet. Kajian berbentuk kuantitatif ini telah dijalankan ke atas 580 orang pelajar institusi pengajian tinggi dan analisis deskriptif telah digunakan bagi menjawab objektif kajian. Hasil kajian mendapati sikap pelajar terhadap perlindungan peranti dan maklumat peribadi berada di tahap sederhana (min = 2.92). Tambahan lagi, para pelajar didapati mengamalkan sikap yang kurang memuaskan dalam aspek keselamatan siber seperti tidak mengubah tetapan menjadi tertutup, menekan pautan dan memuat turun dokumen dari sumber yang tidak dikenali.

Kata Kunci: Sikap, Pelajar, Keselamatan Siber

Abstract

The ever-expanding changes in the world with the advancement of technology have caused concern to the whole world, especially in the aspect of cybersecurity. In fact, it has opened space for cybercriminals to launch various threats and attacks. The students of higher education institutions have gained attention and became the target of cybercriminals because they are among the highest cyber users, and they can access the internet without restrictions. Students' attitudes are the main core in the context of cybersecurity. By increasing awareness of protecting the students' personal information, the students can reduce the risk of exposing their personal information on the cyberspace. Therefore, this study aims to examine the students' attitudes in protecting their devices and personal information while using the internet. A quantitative approach using a descriptive analysis was conducted to 580 students at the higher education institutions to answer the objectives of the study. The results of the study found that the students' attitudes towards protecting their devices and personal information was at a moderate level (min = 2.92). Furthermore, the students were found to practice unsatisfactory attitudes in cyber security aspects such as not changing the privacy settings to private, clicking on links and downloading documents from unknown sources.

Keywords: *Attitudes, Students, Cyber Security*

PENDAHULUAN

Isu serangan siber pada masa kini menjadi salah satu isu yang mendapat perhatian dikalangan sektor kerajaan, sektor swasta mahupun para akademik. Ini kerana pelbagai bentuk serangan siber telah direkodkan seperti penggodaman, pencurian, pembulian dan seumpamanya. Walhal serangan pancingan data merupakan serangan tertinggi yang direkodkan pada tahun 2022 dengan aduan sebanyak 300, 469 (Federal Bureau of Investigation, 2022). Serangan tersebut tidak hanya tertumpu kepada golongan orang tua, bahkan kanak-kanak, pelajar sekolah menengah dan pelajar universiti. Malahan pelajar universiti merupakan sasaran utama bagi penggodam untuk melancarkan berbagai-bagai bentuk serangan siber pada abad ke-21 ini disebabkan universiti penuh dengan penyimpanan maklumat-maklumat peribadi (Richardson, M. et. al., 2020). Maka artikel ini memfokuskan sasaran kajian kepada para pelajar universiti.

Isu serangan siber ini tidak boleh dipandang ringan kerana ia berpunca dari kesilapan pelajar sendiri (Alharbi, T. dan Tassaddiq, A., 2021). Sungguhpun pelbagai program dan intervensi telah dibangunkan bagi meningkatkan pengetahuan pelajar terhadap aspek keselamatan siber, tetapi sikap mereka masih kerap dibincangkan terutama sekali sewaktu menggunakan media sosial (Zwilling, M. et. al, 2020). Kes-kes seperti buli siber, penyebaran fitnah, intipan, peras ugut dan pornografi semakin lazim dilaporkan. Ini kerana pelajar tidak begitu peka akan risiko siber dan tidak mengetahui sikap yang harus diaplikasikan sewaktu melayari internet (Bada, M. dan Sasse, A., 2014). Ini dibuktikan melalui kajian Fariza Khalid et. al. (2018) bahawa sungguhpun pelajar mempunyai kesedaran terhadap aspek keselamatan siber, tetapi sikap mereka masih tidak memuaskan; kerana pelajar tidak mengamalkan tatacara perlindungan peranti dan maklumat peribadi yang disarankan serta melakukan perkara yang kurang elok seperti melayari pornografi.

Selain itu, segala nasihat yang disampaikan dari pihak berkepentingan adalah bertujuan untuk menjaga peranti dan maklumat peribadi pelajar dari diserang dan disalahgunakan. Ianya tidak lain hanya untuk kemashlahatan pelajar sendiri. Dengan erti kata lain menyelamatkan diri dari kemusnahan. Hal ini bertepatan dengan ayat Al-Quran dalam surah Al-Baqarah ayat 195:

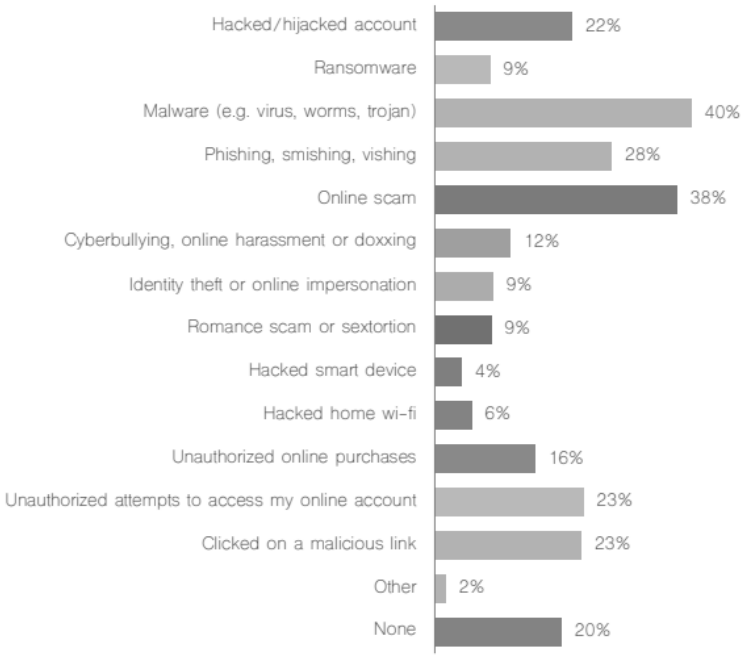
… وَلَا تُلْقُوا بِأَيْدِيكُمْ إِلَى التَّهْلُكَةِ …

"… Dan janganlah kamu sengaja menjerumuskan diri kamu sendiri ke dalam kebinasaan …"

Latar Belakang Kajian

Media sosial mula hangat digunapakai pada sekitar tahun 2008 setelah kewujudan *Friendster*, *Facebook*, *MySpace*, *YouTube* dan sebagainya. Perkembangan media sosial dari tahun 2008 sehingga tahun 2020 ini telah banyak membantu urusan harian. Kehebatan media sosial yang mampu menghubungkan sesama orang pada jarak yang jauh telah menarik hati pada setiap pengguna. Selain daripada itu, media sosial juga memberikan suatu maklumat dan khabar berita dalam jangka masa yang amat cepat. Menurut laporan digital *We Are Social* tahun 2020, seramai 3.80 bilion di dunia ini merupakan pengguna aktif media sosial. Manakala lima jenis media sosial yang menduduki di tangga teratas adalah *Facebook*, *YouTube*, *WhatsApp*, *Facebook Messenger* dan *WeChat*. Di Negara Brunei Darussalam pula, pengguna aktif media sosial adalah terdiri dari kalangan pelajar berumur 18 – 29 tahun (BruCERT, 2021). Tidak dinafikan bahawa pada setiap jenis media sosial ini mempunyai fungsi dan kelebihannya yang tersendiri serta menarik minat kepada para pelajar, tetapi tujuan utamanya hanyalah untuk berkomunikasi sesama pengguna media sosial.

Akan tetapi, sejauh manakah para pelajar mengurus tahap kawalan yang terkandung di dalam akaun mereka agar terlindung dari ancaman dan serangan siber? Adakah para pelajar memikirkan risiko sebelum mereka berkongsi maklumat di dalam akaun mereka? Aspek keselamatan siber ini perlu ditekankan dan dititikberatkan bagi menghindarkan diri dari menjadi mangsa jenayah siber. Rajah 1 menunjukkan laporan insiden serangan siber pada tahun 2021.



Rajah 1: Insiden Serangan Siber Di Negara Brunei Darussalam Tahun 2021

Berdasarkan dari Rajah 1 tersebut, dapat dilihat bahawa serangan virus, penipuan dan pancingan data (*phishing*) adalah tiga bentuk serangan tertinggi direkodkan. Akibat serangan itu, peranti dan maklumat peribadi setentunya akan terjejas dan berisiko tinggi terdedah serta disalahgunakan. Serangan yang dilakukan oleh penggodam ini boleh berada di mana-mana, baik dalam negara mahupun luar negara, sama ada dari jarak dekat ataupun jauh. Di antara tujuan utama serangan yang dilakukan adalah bagi mendapatkan keuntungan serta menjadikan maklumat yang telah dicuri itu sebagai tebusan; maklumat yang dicuri itu juga boleh dijual di laman sesawang terlarang seperti *Dark Web* (Alharbi, T. dan Tassaddiq, A., 2021). Berdasarkan kepada serangan siber yang sedang semakin meningkat ini, para pelajar perlu menyedari akan kepentingan menjaga peranti dan maklumat peribadi.

Faktor Sikap

Dalam agama Islam, kita di anjurkan untuk sentiasa menjaga dan menjamin keselamatan diri sendiri dan orang sekeliling. Hal ini telah termasuk dalam tuntutan Maqāṣid Syari'ah yang meliputi semua aspek iaitu bagi perlindungan agama (*Hifz al-Din*), perlindungan nyawa (*Hifz al-Nafs*), perlindungan akal (*Hifz al-'Aql*), perlindungan keturunan (*Hifz al-Nasl*) dan perlindungan harta (*Hifz al-Māl*) (Abdul Nasir & Ayatul Suhadah, 2011). Peranan Maqāṣid Syari'ah ini adalah bagi menegah pelajar dari terjerumus kepada pemikiran dan akhlak yang menyimpang (Aiman Jibrin Juwaylis, 2014). Bagi sikap yang betul, ia dinamakan sebagai *al-Suluk al-Sawi*, iaitu perbuatan yang sejajar dengan ajaran agama Islam apabila berhadapan dengan suatu keadaan. Ini boleh dilihat melalui firman Allāh Subḥānahu wa Ta'āla dalam surah Al-'Imran ayat 135.:

وَالَّذِينَ إِذَا فَعَلُوا فَاحِشَةً أَوْ ظَلَمُوا أَنْفُسَهُمْ ذَكَرُوا اللَّهَ فَاسْتَغْفَرُوا لِذُنُوبِهِمْ وَمَنْ يَغْفِرُ الذُّنُوبَ إِلَّا اللَّهُ وَلَمْ يُصِرُّوا عَلَى مَا فَعَلُوا وَهُمْ يَعْلَمُونَ

Terjemahannya:

"Dan orang-orang yang apabila melakukan perbuatan keji atau menganiaya diri mereka sendiri, mereka segera ingat kepada Allah lalu memohon ampun terhadap dosa-dosa mereka. Dan sememangnya tidak ada sesiapa yang dapat mengampunkan dosa-dosa selain Allah. Dan mereka juga tidak meneruskan perbuatan keji yang mereka telah lakukan itu sedang mereka mengetahui (akibatnya)."

Maka sikap yang dimaksudkan disini merujuk kepada sikap pelajar terhadap penggunaan peranti dan melindungi maklumat peribadi bagi mencegah serangan siber sepertimana yang difokuskan dalam kajian ini iaitu: virus, penipuan secara atas talian dan serangan pancingan data.

Bagi menghindar virus ini menjangkiti peranti dan maklumat peribadi, pelajar hendaklah memastikan bahawa peranti yang digunakan hendaklah mempunyai perisian aplikasi antivirus. Perisian aplikasi antivirus ini berfungsi untuk melindungi pelajar dari memuat turun dan menekan pautan laman sesawang yang mengandungi virus. Perisian aplikasi antivirus ini boleh didapati secara percuma ataupun memuat turun melalui laman sesawang yang sahih. Akan tetapi, penggunaan perisian aplikasi antivirus sahaja tidaklah memadai jika tidak diselaraskan dengan penggunaan *firewall*. Pelajar juga perlu mengaktifkan *firewall* pada peranti, kerana ia bertindak sebagai pengukuhan kepada perisian aplikasi antivirus dan mencegah virus sewaktu pelajar melayari internet. Kajian Alharbi, T. dan Tassaddiq, A. (2021) mendapati lebih 30% pelajar universiti tidak menggunakan perisian aplikasi antivirus disebabkan berasa tidak memerlukan perlindungan; mereka juga tidak mengetahui tentang *firewall* serta tidak tahu bagaimana untuk mengaktifkannya.

Selain itu, setiap perisian aplikasi perlu dikemaskini dari semasa ke semasa. Ini kerana setiap penambahbaikan tersebut mempunyai komponen alat keselamatan yang terkini dan mampu mencegah virus dari membiak. Ia juga membuatkan peranti menjadi lebih berintegriti, utuh dan mapan. Tindakan pelajar yang menghiraukan penambahbaikan pada perisian aplikasi akan memudahkan kebocoran maklumat peribadi yang disimpan pada peranti (Chairman of The Joint Chiefs of Staff Manual, 2012). Tambahan lagi, ia akan memberi ruang yang mudah bagi para penggodam untuk cuba mencuri maklumat-maklumat peribadi. Alharbi, T. dan Tassaddiq, A. (2021) menyatakan seramai 17.6% pelajar tidak mengemaskini perisian aplikasi mereka.

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 peranti tetapi pelajar menggunakan perisian aplikasi cetak rompak, maka ia hanyalah sia-sia belaka sahaja. Kesilapan ini masih akan memudahkan penjenayah siber mencerobohi peranti dan maklumat peribadi (Wida Susanty, 2016). Oleh itu, adalah disarankan kepada pelajar agar menggunakan perisian aplikasi yang asal. Sungguhpun pelajar perlu membeli perisian aplikasi tersebut dan terpaksa mengeluarkan wang, akan tetapi keselamatan diri dan maklumat peribadi lebih berharga berbanding wang yang dikeluarkan untuk membelinya.

Seterusnya bagi menghindarkan pelajar menjadi mangsa penipuan secara atas talian pula, salah satunya adalah dengan membuat tapisan terhadap akaun orang lain di media sosial. Penjenayah siber pada masa kini boleh berada dimana-mana sahaja termasuk menjadi senarai golongan rakan pada akaun diri sendiri. Laporan DeLiema, M. et. al. (2019) memaparkan sebanyak 91% penipuan secara atas talian ini bermula dari media sosial, iaitu bermula pada fasa penerimaan/penolakkan akaun yang tidak dikenali. Oleh itu, memilih keputusan untuk menerima atau menolak akaun yang tidak dikenali adalah perlu difikirkan kesan baik dan buruknya. Kajian Alharbi, T dan Tassaddiq, A. (2021) turut mendapati bahawa pelajar tidak begitu menghiraukan tentang konsep penerimaan atau penolakan dalam senarai rakan terhadap orang yang tidak dikenali; ini menunjukkan sikap pelajar tidak begitu memuaskan dalam aspek perlindungan maklumat peribadi.

Selain itu, pelajar juga hendaklah tidak sesekali berkongsi akaun mereka sesama orang lain mahupun memberikan butiran peribadi kepada orang tidak diketahui tanpa menjalankan sebarang pemeriksaan. Apa yang mengejutkan ialah Kovačević, A. et. al. (2020) mendapati seramai 54.4% pelajar dalam kajiannya berkongsi akaun; manakala majoriti pengguna internet akan menyerahkan maklumat peribadi mereka begitu sahaja apabila diminta dari orang yang tidak dikenali.

Tambahan lagi, pelajar perlu mengubahsuai tetapan pada media sosial agar menjadi tertutup/*private* supaya individu lain tidak dapat mengintip (Mohd. Azul Mohamad Salleh, et. al., 2017). Akan tetapi, pelajar didapati gemar memuat naik gambar/video tanpa mengubahsuai sebarang sekatan pada tetapan (*settings*). Disebabkan sikap tidak peka ini, ia telah membuka jalan yang mudah kepada orang yang berniat jahat untuk mengintip dan mencuri segala maklumat peribadi. Moallem, A. (2019) mendapati pelajar tidak begitu menghiraukan maklumat peribadi mereka walaupun mereka menyedari segala aktiviti mereka di alam siber mudah diawasi oleh orang lain. Ini memaparkan pelajar tidak mempunyai sikap yang begitu memuaskan.

Akhir sekali adalah mengenai serangan pancingan data. Pelajar perlu mengambil langkah berjaga-jaga dalam aspek keselamatan siber agar tidak terdedah privasi mereka dan terjejas peranti yang digunakan. Ini termasuklah penggunaan kata laluan yang kompleks; iaitu mengandungi huruf besar, huruf kecil, nombor dan simbol, tidak menggunakan kata laluan yang sama pada akaun media sosial yang lain dan kerap mengubah kata laluan sekurang-kurangnya tiap enam bulan (BruCERT, 2022). Banyak kajian seperti kajian Stainbrook, M. dan Caporusso, N. (2019) mendapati bahawa para pelajar lebih gemar menggunakan kata laluan yang mudah diteka seperti nama mereka, tarikh lahir ataupun nombor telefon. Sesetengah pelajar sebanyak 60.7% merasakan kata laluan yang teguh dan panjang adalah menyusahkan (Alharbi, T. dan Tassaddiq, A., 2021). Perkara ini akan menjadi masalah besar apabila pelajar menggunakan kata laluan yang sama pada pelbagai akaun media sosial yang lain kerana; jika satu akaun digodam, besar kemungkinan penggodam akan mencuba taktik yang sama pada jenis akaun yang lain. Ini memaparkan sikap pelajar yang tidak endah akan kebocoran maklumat peribadi mereka.

Pelajar juga hendaklah 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 (BruCERT, 2022). Jika laman sesawang menunjukkan HTTP, maka lebih baik dielakkan dari meneruskan melayarinya. Ini kerana besar kemungkinan laman sesawang tersebut hanyalah dicipta bagi tujuan penggodaman sahaja. Cara paling mudah bagi setiap individu untuk memastikan keselamatan web adalah dengan membezakan antara: perkataan '*https://*' bermaksud selamat digunakan, dan; perkataan '*http://*' bermaksud sebaliknya. Kajian Kovačević, A. et. al. (2020) memaparkan hanya 10.9% pelajar sahaja mengetahui mengenai perkara ini. Ini menunjukkan perlunya ditingkatkan kewaspadaan pelajar dalam aspek serangan pancingan data.

Selain itu, pelajar perlu menerapkan sifat berhati-hati seperti membuat kesahihan terhadap suatu perkara. Ini kerana serangan pancingan data menggunakan taktik penipuan dengan pelbagai agenda seperti: penyamaran dari institusi kewangan, wakil dari sektor kerajaan dan swasta dan seumpamanya. Lazimnya serangan pancingan data ini dilancarkan melalui pesanan e-mel, disertakan dengan lampiran dan pautan laman sesawang untuk di isikan oleh pelajar. Jika sekiranya pelajar telah mengenal pasti kandungan pesanan e-mel tersebut adalah palsu, maka segeralah membuangnya atau tidak memedulinya. Akan tetapi kajian mendapati majoriti pelajar menekan pautan dari pesanan e-mel tersebut dan memuat turun lampiran yang diberikan (Cain, A. A., et. al., 2018). Tindakan tersebut akan membuatkan peranti sekaligus dijangkiti virus dan besar kemungkinan peranti akan gagal berfungsi dengan baik.

METODOLOGI

Kajian ini mengaplikasikan kaedah kuantitatif untuk meneliti sikap pelajar terhadap perlindungan peranti dan maklumat peribadi sewaktu mereka menggunakan internet. Teknik persampelan bola salji telah digunakan berdasarkan jadual penentuan saiz sampel Krejcie & Morgan (1970) bagi mendapatkan responden kajian. Saiz sampel yang telah diambil adalah sebanyak 580 orang pelajar Tahun 4 daripada empat buah universiti Negara Brunei Darussalam iaitu: Universiti Brunei Darussalam, Universiti Islam Sultan Sharif Ali, Universiti Teknologi Brunei dan Kolej Universiti Perguruan Ugama Seri Begawan.

Instrumen kaji selidik yang mengandungi 2 bahagian telah diedarkan kepada responden untuk dijawab. Bahagian A adalah mengenai maklumat demografi responden dan Bahagian B mengenai sikap responden terhadap perlindungan peranti dan maklumat peribadi sewaktu menggunakan internet. Kaedah analisis yang digunakan adalah dengan mengira nilai min bagi jawapan yang diberikan oleh para responden. Nilai min akan dirujuk kepada interpretasi yang telah ditetapkan oleh Moidunny (2009).

Jadual 1: Interpretasi Skor Min

Skala	Tahap
1.00 – 1.80	Tahap Sangat Rendah
1.81 – 2.60	Tahap Rendah
2.61 – 3.20	Tahap Sederhana
3.21 – 4.20	Tahap Tinggi
4.21 – 5.00	Tahap Sangat Tinggi

Sebelum memulakan kajian sebenar, satu kajian rintis telah dijalankan bagi menentukan nilai kebolehpercayaan instrumen kaji selidik. Kajian rintis ini melibatkan 40 orang responden secara rawak yang terdiri dari pelajar Tahun 3 dari setiap universiti. 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, E. dan Velicer, W. F. (1988) yang mencadangkan seramai 50 orang dan melihat pandangan Isaac, S. dan Michael, W. B., (1995) serta Hill, R., (1998) menyatakan jumlah sampel bagi kajian rintis adalah sebanyak 10 – 30 orang kerana mempunyai banyak kebaikan, seperti pengiraan yang mudah. Oleh yang demikian, pengkaji telah memilih sebanyak 40 orang sampel.

Jadual 2: Indeks Nilai Kebolehpercayaan Alpha Cronbach Bagi Instrumen Kaji Selidik

Pembolehubah	Bilangan Item	*Alpha Cronbach*
Sikap Terhadap Perlindungan Peranti dan Maklumat Peribadi	11	.809

Menurut Azizi Yahaya et. al. (2016), 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. Berdasarkan dari Jadual 1 tersebut memaparkan bahawa nilai *Alpha Cronbach* yang diperolehi adalah pada tahap tinggi dan sempurna.

HASIL DAPATAN KAJIAN

Jadual 3: Analisis Deskriptif Bagi Demografi Responden

Demografi Responden (n = 580)		Frekuensi (f)	Peratus (%)
Jantina	Lelaki	274	47.2
	Perempuan	306	52.8
Tempat Pengajian	UBD	217	37.4
	UNISSA	152	26.2
	UTB	175	30.2
	KUPU SB	36	6.2

Data menunjukkan seramai 274 orang lelaki (47.2%) dan 306 orang perempuan (52.8) yang terlibat dalam kajian ini. Dari segi tempat pengajian pula, responden dari Universiti Brunei Darussalam adalah seramai 217 orang (37.4%). Responden dari Universiti Islam Sultan Sharif Ali pula adalah seramai 152 orang (26.2%). Responden dari Universiti Teknologi Brunei adalah seramai 175 orang (30.2%), dan responden dari Kolej Universiti Perguruan Ugama Seri Begawan adalah seramai 36 orang (6.2%).

Jadual 4: Sikap Responden Terhadap Perlindungan Peranti Dan Maklumat Peribadi

Bil.	**Item**	**STK (%)**	**TK (%)**	**KK (%)**	**K (%)**	**SK (%)**	**Skor Min**	**Interpretasi Skor Min**
1	Saya merasa susah dengan kata laluan yang unik.	74 12.8 %	100 17.2 %	98 6.9%	155 26.7 %	153 26.4 %	3.37	Tinggi
2	Saya menekan pautan yang diberikan dari e-mel yang tidak dikenali.	114 19.7 %	143 24.7 %	134 23.1 %	105 18.1 %	84 14.5 %	2.83	Sederhana
3	Saya memuat turun dokumen dari e-mel yang tidak dikenali.	90 5.5%	101 17.4 %	147 25.3 %	123 21.2 %	19 20.5 %	3.14	Sederhana
4	Saya mengubah tetapan media sosial menjadi tertutup.	96 16.6 %	120 20.7 %	147 25.3 %	130 22.4 %	87 5.0%	2.99	Sederhana
5	Saya menggunakan kata laluan yang berbeza pada akaun media sosial yang lain.	156	185	111	67	61	2.47	Rendah

		26.9 %	31.9 %	19.1 %	11.6 %	10.5 %		
6	Saya menerima akaun orang lain untuk menjadi teman saya.	113 19.5 %	109 18.8 %	80 13.8 %	139 24.0 %	139 24.0 %	3.14	Sederhana
7	Saya berkongsi akaun dengan rakan saya.	133 22.9 %	177 30.5 %	116 20.0 %	96 16.6 %	58 10.0 %	2.60	Rendah
8	Saya mengemaskini kesemua perisian aplikasi.	185 31.9 %	186 32.1 %	88 15.2 %	66 11.4 %	55 9.5%	2.34	Rendah
9	Saya mengubah kata laluan saya setiap 6 bulan.	186 32.1 %	155 26.7 %	84 14.5 %	78 13.4 %	77 13.3 %	2.49	Rendah
10	Saya meneruskan melayari internet yang memaparkan istilah '*http://*'.	94 16.2 %	95 16.4 %	110 19.0 %	165 28.4 %	116 20.0 %	3.20	Sederhana
11	Saya mengimbas peranti saya untuk mengesan virus.	44 7.6%	85 14.7 %	157 27.1 %	161 27.8 %	133 22.9 %	3.44	Tinggi

Min Keseluruhan	2.92 (Sederhana)

Jadual 4 memaparkan taburan nilai kekerapan, nilai peratusan dan nilai min bagi setiap item yang mengukur sikap responden terhadap perisian aplikasi dan maklumat peribadi. Berdasarkan dari Jadual 4 ini, sikap merasa susah dengan kata laluan yang unik mendapat nilai min sebanyak 3.37 iaitu pada tahap tinggi. Hanya 174 orang responden (30.0%) sahaja seringkali berasa tidak susah untuk mencipta kata laluan yang unik. Tetapi seramai 308 orang responden (53.1%) kerap berasa susah mengenainya; hanya 98 orang responden (16.9%) sahaja kadangkala berasa demikian. Selain itu, item mengenai menekan pautan dari e-mel yang tidak dikenali mendapat nilai min sebanyak 2.83 iaitu tahap sederhana. Seramai 257 orang responden (44.4%) seringkali tidak menekan pautan yang diberikan dari e-mel yang tidak dikenali, hanya 189 orang responden (32.6%) sahaja kerap menekan pautan yang diterima dari sumber e-mel yang tidak dikenali, dan; hanya 134 orang responden (23.1%) lagi kadangkala berbuat demikian.

Tambahan lagi, item mengenai memuat turun dokumen dari e-mel yang tidak dikenali berada pada tahap sederhana dengan nilai min 3.14. Seramai 191 orang responden (32.9%) menyatakan tidak kerap, iaitu bermaksud mereka tidak memuat turun dokumen dari e-mel yang tidak dikenali; hanya 242 orang responden (41.7%) sahaja seringkali berbuat sebaliknya; data selebihnya seramai 147 orang responden (25.3%) memberikan jawapan kadangkala. Selain itu, item tentang menukar tetapan media sosial menjadi tertutup berada pada tahap sederhana dengan nilai min 2.99. Seramai 216 orang responden (37.3%) tidak kerap mengubah tetapan mereka menjadi tertutup dalam media sosial. Ini menunjukkan seramai 217 orang responden (37.4%) lagi kerap mengubah tetapan menjadi tertutup; hanya 147 orang responden (25.3%) menjawab kadangkala.

Item tentang penggunaan kata laluan yang berbeza pada akaun media sosial yang lain pula mendapat nilai min sebanyak 2.47 iaitu ditahap rendah. Lebih sebahagian responden seramai 341 orang (58.8%) lazim menggunakan kata laluan yang sama pada akaun media sosial yang lain; hanya 128 orang responden (22.1%) sahaja kerap menggunakan kata laluan yang berbeza pada berlainan akaun, dan; seramai 111 orang responden (19.1%) pula kadangkala berbuat demikian. Selain itu, penerimaan akaun orang lain untuk menjadi rakan media sosial mendapat nilai min sebanyak 3.14 ditahap sederhana. Seramai 222 orang responden (38.3%) menyatakan mereka tidak bersetuju, iaitu menolak akaun orang lain untuk menjadi rakan di media sosial; seramai 278 orang responden (48.0%) kerap menerima akaun orang lain yang ingin menjadi rakan di media sosial, dan; seramai 80 orang responden (13.8%)

memberikan jawapan kadangkala. Di samping itu, item mengenai berkongsi akaun dengan rakan berada di tahap rendah dengan nilai min 2.60. Sejumlah besar responden seramai 310 orang (53.4%) tidak kerap berkongsi akaun sesama rakan mereka; hanya 154 orang responden (26.6%) sahaja berkongsi akaun mereka sesama rakan, dan; seramai 116 orang responden (20.0%) menyatakan kadangkala.

Sementara itu, sikap dalam meningkatkan kawalan peranti dan maklumat peribadi juga perlu diberi penekanan seperti mengemaskini kesemua perisian aplikasi. Item ini mendapat nilai min sebanyak 2.34 ditahap rendah. Sebilangan besar responden seramai 371 orang (64.0%) tidak kerap mengemaskini perisian aplikasi mereka; hanya seramai 121 orang responden (20.9%) pula sebaliknya, dan; hanya 88 orang responden (15.2%) kadang-kadang mengemaskini perisian aplikasi mereka dan kadang-kadang sebaliknya. Begitu juga dengan meningkatkan tahap kawalan peranti dan maklumat peribadi seperti mengubah kata laluan setiap 6 bulan. Item ini mendapat nilai min sebanyak 2.49 iaitu pada tahap rendah. Sebilangan besar responden seramai 341 orang (58.8%) menyatakan tidak kerap mengubah kata laluan mereka tiap 6 bulan. Manakala seramai 155 orang responden (26.7%) sahaja yang kerap mengubahnya. Data selebihnya seramai 84 orang responden (14.5%) menyatakan kadangkala.

Seterusnya item mengenai meneruskan melayari internet yang memaparkan istilah '*http://*' mendapat nilai min sebanyak 3.20 di tahap sederhana. Hanya 189 orang responden (32.6%) sahaja memberikan jawapan tidak kerap; manakala seramai 281 orang responden (48.4%) pula menyatakan kerap, dan; seramai 110 orang responden (19.0%) memberikan jawapan kadangkala. Akhir sekali adalah item mengenai mengimbas peranti bagi mengesan virus. Item ini berada ditahap tinggi dengan nilai min sebanyak 3.44. Seramai 129 orang responden (22.3%) tidak kerap mengimbas peranti mereka bagi mengesan virus, hanya 294 orang responden (50.7%) sahaja bersikap sebaliknya. Data selebihnya seramai 157 orang responden (27.1%) memberikan jawapan kadangkala berbuat demikian.

Perbincangan Kajian

Kajian ini bertujuan untuk meneliti sikap pelajar terhadap perlindungan peranti dan maklumat peribadi sewaktu mereka menggunakan internet. Memandangkan kajian ini memfokuskan kepada serangan virus, penipuan atas talian dan serangan pancingan data, maka perbincangan kajian adalah tertumpu kepada tiga serangan tersebut. Berdasarkan dari dapatan kajian yang telah diperolehi, sikap pelajar berada pada tahap sederhana dengan memaparkan nilai keseluruhan min sebanyak 2.92. Nilai min ini telah dirujuk kepada Moidunny (2009) seperti yang telah diterangkan. Secara keseluruhan, pelajar mempunyai sikap untuk mengimbas peranti jika sekiranya telah dijangkiti virus ataupun tidak. Item ini mempunyai nilai min sebanyak 3.44. Nilai min ini menunjukkan bahawa majoriti responden seramai 294 orang (50.7%) kerap mengamalkan sikap untuk mengimbas peranti mereka bagi tujuan pengesanan virus. Tambahan lagi, ia turut berfungsi sebagai pemberi ingatan kepada pelajar jika berlakunya aktiviti yang mencurigakan pada peranti seperti pemuatan turun virus secara sendirinya.

Manakala item mengenai pengemaskinian perisian aplikasi merupakan item yang mendapat nilai min terendah sebanyak 2.34. Sebahagian besar responden seramai 371 orang (64.0%) seringkali mengabaikan peranti mereka untuk tidak dikemaskini. Hasil dapatan pengkaji ini berbeza sebagaimana dapatan kajian Zwilling, M. et. al. (2020). Kajian mereka mendapati sebanyak 56% pelajar menerapkan sikap dalam mengemaskini perisian aplikasi. Pengkaji berpendapat perbezaan ini terjadi disebabkan lokasi dan sampel kajian. Kajian Zwilling, M. et. al ini telah dijalankan di empat buah negara iaitu Slovenia, Poland, Turkey dan Israel dan sampel mereka adalah terdiri dari para pelajar Sarjana Muda dan pelajar pascasiswazah yang hanya berada dalam program *Management and/or Business Administration* sahaja. Tambahan lagi, bahasa pengantar yang digunakan pada instrumen kaji selidik di Turkey adalah dengan menggunakan bahasa asal mereka iaitu Kurdish dan Arab. Maka adalah menjadi satu kesulitan bagi beberapa orang pelajar antarabangsa (*international students*) untuk menjawab borang kaji selidik tersebut. Justeru dapatan kajian yang diperolehi itu boleh memberikan sedikit kesan pada penganalisisan data disebabkan bahasa pengantar yang digunakan pada borang kaji selidik.

Manakala serangan penipuan atas talian pula boleh dilihat melalui dari sikap pelajar dalam penggunaan media sosial. Ia boleh dirujuk kepada dua perkara iaitu (1) tidak mengubah tetapan media sosial menjadi tertutup iaitu sebanyak 37.3%; dan (2) penerimaan akaun orang sewenang-wenangnya iaitu sebanyak 48.0%. Penggunaan media sosial yang berhemah seperti menjadikan tetapan tertutup dan tidak menerima akaun orang lain sewenang-wenangnya merupakan sikap yang selamat dan digalakkan. Tambahan lagi, faktor kepercayaan adalah salah satu faktor utama yang membuatkan pelajar sentiasa berhati-hati apabila berada di alam siber (Mohammed Daffalla Elradi, et. al., 2020). Justeru adalah wajar peningkatan terhadap sikap dan tindakan pelajar dalam media sosial; kerana segala apa yang dipaparkan di internet tidak boleh dipercayai.

1. Mengubah tetapan media sosial menjadi tertutup boleh mengurangkan dari terjadinya serangan siber keatas pelajar. Ini kerana penjenayah siber pada masa kini seringkali menjalankan operasi mereka melalui media sosial dengan memantau akaun yang terbuka seperti pencurian identiti, pengintipan dan seumpamanya. Kesan dari serangan tersebut bukan sahaja akan mengakibatkan kehilangan data, malah boleh menjadikan pelajar kemurungan dan tertekan serta hilang keyakinan diri apabila maklumat peribadi mereka disalahgunakan (Rustam,

H. et. al., 2023). Justeru, adalah ditekankan kepada pelajar agar meluangkan lebih masa untuk memeriksa tetapan pada media sosial kerana tetapan asal adalah bersifat terbuka.

2. Dari sudut penerimaan akaun orang lain pula turut berisiko kepada pelajar menjadi mangsa siber. Pada masa kini, pencurian identiti semakin meningkat terutama dikalangan akaun pelajar berumur 18-24 tahun (BruCERT, 2022). Perkara ini selaras dengan laporan BruCERT (2022) yang menyatakan kes ini mencatatkan sebanyak 9% dan penipuan pula mencatatkan sebanyak 38%. DeLiema, M. et. al. (2019) menyatakan bahawa jenayah penipuan siber adalah bermula pada fasa penerimaan/penolakkan akaun yang tidak dikenali. Penjenayah siber boleh berpura-pura menjadi teman pelajar dan melakukan penipuan. Zarei, K. (2022) pula berpendapat perkara ini terjadi disebabkan kewujudan media sosial mendorong pengguna internet untuk berbuat jahat disebabkan oleh perkara-perkara tertentu seperti marah, dendam mahupun terdesak (Kovačević, A. et. al., 2020).

Akhir sekali adalah serangan pancingan data. Serangan pancingan data dalam internet lazimnya mengarahkan pelajar untuk menekan pautan laman sesawang dengan menawarkan pelbagai agenda seperti hadiah, perkhidmatan dan seumpamanya. Selain itu, serangan ini juga seringkali disusuli dengan penyediaan dokumen sama ada berbentuk '.docx' mahupun '.pdf'. Pautan laman sesawang dan dokumen ini mengandungi virus yang boleh menjejaskan peranti pelajar sebaik sahaja mereka menekan atau memuat turunnya. Berdasarkan dari dapatan kajian, boleh dilihat bahawa sebanyak 32.6% orang pelajar kerap menekan pautan yang diterima dari sumber e-mel yang tidak dikenali dan sebanyak 41.7% orang pelajar pula kerap memuat turun dokumen dari e-mel yang tidak dikenali. BruCERT (2022) menjelaskan bahawa antara faktor yang menyebabkan pelajar menjadi mangsa serangan pancingan data adalah disebabkan:

1. Pelajar memberikan tindakbalas menentang kerana seringkali menerimanya.
2. Perasaan ingin tahu apa yang terkandung pada dokumen/pautan laman sesawang.
3. Kurang pengetahuan tentang aspek keselamatan siber.

KESIMPULAN

Oleh itu, pelajar tidak perlu menjadi pakar info-teknologi bagi mencegah diri dari serangan siber. Apa yang perlu hanyalah mengikuti saranan dan nasihat yang telah ditunjukkan oleh agensi keselamatan siber serta menerapkan etika yang berpatutan sewaktu menggunakan internet. Sikap pelajar adalah kunci bagi meningkatkan aspek keselamatan siber dan juga bagi menyedari manakah perkara yang perlu dilakukan dan mana perkara yang perlu ditinggalkan, sesuai bagi perlindungan di dunia dan di akhirat.

DAFTAR PUSTAKA

Mushaf Brunei Darussalam dan Terjemahannya. (2014). Negara Brunei Darussalam: Pusat Dakwah Islamiah.

Abdul Nasir bin Haji Abdul Rani dan Ayatul Suhadah binti Haji Sijom. (2011). Maqasid Al-Shari'ah Dalam Undang-Undang Hudud: Tinjauan Umum Terhadap Keberkesanan Undang-Undang Islam. *Seminar Isu-Isu Kontemporari Dalam Syariah dan Undang-Undang*. Fakulti Syariah dan Undang-Undang, Universiti Islam Sultan Sharif Ali.

Aiman Jibrin Juwaylis. (2014). Al-Dhawbit al-Syari'yyah li Istikhdam Wasail al-Tasawul al-Hadithah. *Kertas Kerja Pembentangan Mukhtamar Wasail al-Tasawul al-Hadithah wa Atharuha 'ala al-Mujtama'*. Jami'ah al-Najah al-Wataniah, Nablus: Palestin.

Alharbi, T. dan Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness Among Students of Majmaah University. *Big Data Cognitive Computing*. Vol. 5(23).

Azizi Yahaya et. al. (2016). *Menguasai SPSS Dengan Mudah*. Universiti Islam Sultan Sharif Ali: UNISSA Press.

Bada, M. dan Sasse, A. (2014). *Cyber Security Awareness Campaign: Why Do They Fail to Change Behavior?* Global Cyber Security Capacity Centre. United Kingdom: University of Oxford.

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

BruCERT. (2021). *Online Safety Awareness Survey 2021*. Negara Brunei Darussalam: BruCERT.

Cain, A. A. et. al. (2018). An Exploratory Study of Cyber Hygiene Behaviors and Knowledge. *Journal of Information Security and Applications*. Vol. 42.

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

DeLiema, M. et. al. (2019). *Exposed to Scams – What Separates Victims from Non-Victims?* United States of America: FINRA.

Fariza Khalid, et. al. (2018). *A*n Investigation of University Students' Awareness on Cyber Security. *International Journal of Engineering & Technology*. Vol. 7(4.21).

Federal Burau of Investigation. (2022). *Federal Burau of Investigation Internet Crime Report 2022*. United States of America: Department of Justice.

Guadagnoli, E. dan Velicer, W. F. (1988). Relation to Sample Size to the Stability of Component Patterns. *Psychological Bulletin*. Vol. 103(2).

Hill, R. (1998). What Sample Size Is "Enough" in Internet Survey Research? *Interpersonal Computing and Technology: An Electronic Journal for 21st Century*. Vol. 6(3-4).

Isaac, S. dan Michael, W. B. (1995). *Handbook in Research and Evaluation*. San Diego, California: Educational and Industrial Testing Services.

Kovačević, A. et. al. (2020). Factors Related to Cyber Security Behavior. *Institute of Electrical and Electronic Engineers Journal*. Vol. 8.

Krejcie, R. V. dan Morgan, D. W. (1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement*. Vol. 30.

Moallem, A. (2019). Cyber Security Awareness Among College Students. Ahram, T. dan Nicholson, D. (ed.). *International Conference on Applied Human Factors and Ergonomics*. USA.

Mohammed Daffalla Elradi, et. al. (2020). Cyber Security Awareness among Students and Faculty Members in a Sudanese College. *Electrical Science & Engineering*. Vol. 2(2).

Mohd Azul Mohamad Salleh et. al. (2017). Kesedaran Dan Pengetahuan Terhadap Keselamatan Dan Privasi Melalui Media Sosial Dalam Kalangan Belia. *Journal of Social Sciences and Humanities*. Vol. 12(3).

Moidunny, K. (2009). The Effectiveness of The National Professional Qualification for Educational Learners (NPQEL). Doctoral Dissertation. Bangi: The National University of Malaya.

Richardson, M. et. al. (2020). Planning for Cyber Security in Schools: The Human Factors. *Educational Planning*. Vol 27(2).

Rustam, H. et. al. (2023). Social Media Impact on Human Behavior. *Global Sociological Review*. Vol 3(2).

Stainbrook, M. dan Caporusso, N. (2019). Convenience or Strength? Aiding Optimal Strategies in Password Generation. Ahram, T. dan Nicholson, D. (ed.). *International Conference on Applied Human Factors and Ergonomics*. USA.

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

Zarei, K. (2022). Fake Identity & Fake Activity Detection in Social Media Networks Based on Transfer Learning. Tesis Doktor Falsafah. Computation and Language: Institut Polytechnique de Paris.

Zwilling, M., et. al. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information System*. Vol. 62(1).