



INTERNATIONAL JOURNAL
OF LAW, GOVERNMENT
AND COMMUNICATION
(IJLGC)

www.gaexcellence.com/ijlgc



**TADBIR URUS KESELAMATAN SIBER BERPUSATKAN
RAKYAT: PERANAN PENGANTARAAN LITERASI
DIGITAL DALAM KALANGAN MANGSA PENIPUAN
SIBER DI MALAYSIA**

*CITIZEN-CENTRED CYBERSECURITY GOVERNANCE: THE MEDIATING
ROLE OF DIGITAL LITERACY AMONG CYBER-FRAUD VICTIMS IN
MALAYSIA*

Adi Sofuan Md Yusof¹, Mohd Sobhi Ishak^{2*}, Zafari Zulkifli³

¹Institut Kajian Etnik (KITA), Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia

 P153634@siswa.ukm.edu.my

 <https://orcid.org/0009-0001-8245-7594>

²Institut Kajian Etnik (KITA), Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia

 msobhi@ukm.edu.my

 <https://orcid.org/0000-0003-1516-5652>

³Institut Kajian Etnik (KITA), Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia

 zafari6688@gmail.com

 <https://orcid.org/0009-0002-4876-6884>

*Corresponding Author

Article Info:

Article history:

Received date: 21.07.2026

Revised date: 18.08.2026

Accepted date: 24.09.2026

Published date: 30.09.2026

Abstrak:

Pendigitalan perkhidmatan awam telah memperluas akses kepada maklumat rasmi, kempen kesedaran, saluran pelaporan dan mekanisme perlindungan keselamatan siber. Namun, peranan literasi digital dalam hubungan antara orientasi sosiobudaya dengan persepsi terhadap pelaksanaan dasar keselamatan siber masih belum jelas, khususnya dalam kalangan mangsa penipuan siber. Kajian ini menguji literasi digital sebagai pemboleh ubah pengantara dalam hubungan tersebut. Tinjauan keratan rentas dijalankan terhadap 500 warganegara Malaysia berumur 18 tahun ke atas yang pernah menjadi mangsa penipuan siber dan telah membuat laporan polis. Data dianalisis menggunakan pemodelan persamaan berstruktur kuasa dua terkecil separa (PLS-SEM). Orientasi sosiobudaya mempunyai hubungan negatif yang signifikan dengan literasi digital. Literasi digital pula mempunyai hubungan positif yang tinggi dengan persepsi terhadap pelaksanaan dasar ($\beta = 0.912$). Hubungan langsung antara orientasi sosiobudaya dengan persepsi terhadap pelaksanaan dasar tidak signifikan, manakala hubungan tidak langsung melalui literasi digital adalah signifikan ($\beta = -0.404$). Model

To cite this document:

Yusof, A. S. M., Ishak, M. S. & Zulkifli, Z. (2026). Tadbir Urus Keselamatan Siber Berpusatkan Rakyat: Peranan Pengantaraan Literasi Digital Dalam Kalangan Mangsa Penipuan Siber Di Malaysia. *International Journal of Law, Government and Communication*, 11(45), 862-887.

DOI: 10.35631/IJLGC.1145055

menerangkan 82.9 peratus varians persepsi terhadap pelaksanaan dasar dalam sampel kajian. Walau bagaimanapun, nilai HTMT sebanyak 0.952 menunjukkan kemungkinan pertindihan empirikal antara literasi digital dengan persepsi terhadap pelaksanaan dasar. Oleh itu, kekuatan hubungan antara kedua-duanya perlu ditafsir dengan berhati-hati. Dapatan ini menunjukkan bahawa literasi digital berkait rapat dengan cara mangsa menilai pelaksanaan dasar keselamatan siber. Komunikasi dasar yang jelas tentang tindakan yang perlu diambil, saluran pelaporan yang mudah digunakan dan latihan literasi digital berasaskan situasi sebenar wajar diberi perhatian dalam tadbir urus keselamatan siber.

Kata Kunci:

Jurang Digital; Kerajaan Digital; Literasi Digital; Pelaksanaan Dasar; Penipuan Siber; Tadbir Urus Keselamatan Siber

Abstract:

The digitalisation of public services has expanded access to official information, awareness campaigns, reporting channels and cybersecurity protection mechanisms. However, the role of digital literacy in the relationship between sociocultural orientation and perceptions of cybersecurity policy implementation remains unclear, particularly among cyber fraud victims. This study examines digital literacy as a mediating variable in that relationship. A cross-sectional survey was conducted with 500 Malaysian citizens aged 18 and above who had experienced cyber fraud and filed a police report. Data were analysed using partial least squares structural equation modelling (PLS-SEM). Sociocultural orientation had a significant negative association with digital literacy. Digital literacy, in turn, had a strong positive association with perceptions of policy implementation ($\beta = 0.912$). The direct association between sociocultural orientation and perceptions of policy implementation was not significant, whereas the indirect association through digital literacy was significant ($\beta = -0.404$). The model explained 82.9% of the variance in perceptions of policy implementation within the study sample. However, the HTMT value of 0.952 indicates possible empirical overlap between digital literacy and perceptions of policy implementation. The strength of the association between the two should therefore be interpreted with caution. The findings show that digital literacy is closely associated with how victims assess cybersecurity policy implementation. Policy communication that clearly explains what actions to take, accessible reporting channels and digital literacy training based on real-world scenarios warrant attention in cybersecurity governance.

Keywords:

Cyber Fraud; Cybersecurity Governance; Digital Divide; Digital Government; Digital Literacy; Policy Implementation



© The authors (2026). This is an Open Access article distributed under the terms of the Creative Commons Attribution (CC BY NC) (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited. For commercial re-use, please contact ijlgc@gaexcellence.com

Pengenalan

Transformasi digital telah mengubah hubungan antara rakyat dengan institusi kerajaan. Maklumat rasmi, perkhidmatan kewangan, amaran keselamatan, mekanisme aduan dan tindak balas kecemasan semakin banyak disampaikan melalui laman sesawang, aplikasi mudah alih, media sosial, aplikasi pemesejan dan pelbagai saluran digital. Dalam konteks Malaysia, pembangunan ekonomi digital turut meletakkan teknologi sebagai sebahagian daripada infrastruktur kehidupan masyarakat, penyampaian perkhidmatan awam dan penglibatan rakyat dalam aktiviti sosial serta ekonomi (Economic Planning Unit, 2021). Walaupun akses Internet dan penggunaan teknologi digital di Malaysia berada pada tahap yang meluas, akses tidak semestinya menunjukkan bahawa rakyat mempunyai keupayaan yang mencukupi untuk menilai risiko, melindungi data peribadi dan menggunakan mekanisme perlindungan kerajaan secara berkesan (Department of Statistics Malaysia, 2025). Perkembangan tersebut memperlihatkan perubahan jurang digital daripada persoalan pemilikan peranti dan akses Internet kepada persoalan kemahiran, kualiti penggunaan dan hasil penggunaan teknologi (van Deursen & van Dijk, 2014).

Penipuan siber merupakan contoh jelas tentang jurang antara akses digital dengan keupayaan menggunakan teknologi secara selamat. Penipu memanfaatkan platform digital, identiti institusi, bahasa rasmi, tekanan masa dan manipulasi emosi untuk menghasilkan komunikasi yang kelihatan meyakinkan. Mangsa boleh berhadapan dengan panggilan penyamaran, penipuan e-pembelian, pelaburan palsu, tawaran pekerjaan palsu, pinjaman tidak wujud dan bentuk penipuan lain yang berasaskan interaksi digital. Kejayaan sesuatu penipuan tidak hanya bergantung pada kelemahan teknikal. Penipuan siber turut bergantung pada cara manusia mentafsir maklumat, mempercayai sumber, bertindak balas terhadap autoriti dan membuat keputusan dalam keadaan tertekan (Abroshan et al., 2021; Hanoch & Wood, 2021). Oleh itu, penipuan siber perlu dilihat sebagai masalah tadbir urus awam yang memerlukan maklumat jelas, mekanisme semakin mudah dicapai, saluran pelaporan dipercayai dan tindak balas institusi yang pantas.

Malaysia mempunyai ekosistem perlindungan yang melibatkan agensi penguatkuasaan, institusi keselamatan siber, pengawal selia komunikasi, institusi kewangan dan mekanisme tindak balas terhadap penipuan. Intervensi yang dilaksanakan merangkumi kempen kesedaran, penyebaran amaran rasmi, semakan maklumat, tindakan penguatkuasaan, saluran pelaporan dan bantuan kepada mangsa. Walau bagaimanapun, kewujudan sesuatu kempen, program atau saluran pelaporan belum mencukupi untuk membuktikan bahawa dasar tersebut benar-benar berfungsi pada peringkat rakyat. Pelaksanaan dasar perlu dinilai berdasarkan kejelasan, kebolehcapaian, kebolehgunaan, kepercayaan dan keupayaannya membantu kumpulan sasaran dalam situasi sebenar (Dupont, 2019; Vedung, 1997). Seseorang mungkin mengetahui bahawa saluran pelaporan disediakan, tetapi tidak mengetahui saluran yang perlu dihubungi terlebih dahulu. Pengguna juga mungkin tidak memahami perbezaan antara saluran semakin, tindakan bank, bantuan kecemasan dan laporan polis. Dalam kes penipuan kewangan, kekeliruan dan kelewatan bertindak boleh mengurangkan peluang untuk menghalang pemindahan wang, mengesan transaksi atau mendapatkan bantuan institusi. Isu tersebut berkait rapat dengan pendekatan kerajaan digital berpusatkan rakyat. Kerangka Dasar Kerajaan Digital OECD menegaskan bahawa transformasi digital perlu dipandu oleh nilai awam, keperluan pengguna dan penyampaian perkhidmatan yang terselaraskan, bukannya sekadar penggunaan teknologi (OECD, 2020). Pertubuhan Bangsa-Bangsa Bersatu turut menghubungkan kerajaan digital

dengan keterangkuman, akses bermakna dan pembangunan keupayaan manusia (United Nations Department of Economic and Social Affairs, 2024).

Dalam konteks tadbir urus keselamatan siber, pendekatan berpusatkan rakyat menimbulkan persoalan sama ada masyarakat dapat memahami maklumat rasmi, mengenal pasti saluran institusi sebenar, membezakan komunikasi kerajaan daripada penyamaran, melindungi maklumat peribadi dan mendapatkan bantuan ketika berhadapan dengan insiden yang memerlukan tindakan segera. Literasi digital dalam konteks ini bukan sekadar kemahiran menggunakan peranti atau aplikasi. Literasi digital merupakan keupayaan yang membolehkan rakyat menterjemahkan maklumat dan mekanisme dasar kepada tindakan perlindungan. Keupayaan tersebut meliputi penilaian maklumat, pengesahan sumber, perlindungan privasi, penggunaan ciri keselamatan dan pengetahuan tentang saluran bantuan rasmi (Ng, 2012; Vuorikari et al., 2022). Kajian terdahulu yang dibincangkan dalam artikel ini menghubungkan literasi digital dengan risiko pemangsaan, tingkah laku perlindungan dan kesedaran keselamatan siber (Elrayah & Jamil, 2023; Graham & Triplett, 2017; Li et al., 2024; Thani et al., 2026). Hubungan tersebut belum dengan sendirinya menjelaskan bagaimana keupayaan digital berkait dengan penilaian rakyat terhadap maklumat, garis panduan, kempen dan saluran bantuan yang disediakan institusi. Persoalan yang diteliti di sini ialah sama ada literasi digital menjadi pengantara dalam hubungan antara orientasi sosiobudaya dengan persepsi terhadap pelaksanaan dasar keselamatan siber, khususnya dalam kalangan mangsa yang telah membuat laporan polis.

Artikel ini meneliti sebahagian daripada model kajian yang lebih luas mengenai mangsa penipuan siber di Malaysia. Objektifnya ialah menguji hubungan langsung antara orientasi sosiobudaya, literasi digital dan persepsi terhadap pelaksanaan dasar keselamatan siber, serta menganggarkan kesan tidak langsung melalui literasi digital. Sumbangan khususnya terletak pada penelitian pengalaman kumpulan yang pernah menggunakan saluran pelaporan rasmi dan pada penghubungan orientasi sosiobudaya dengan penilaian terhadap pelaksanaan dasar melalui keupayaan digital. Fokus ini memperluas perbincangan jurang digital kepada persoalan penggunaan perlindungan institusi, dengan mengambil kira batasan ukuran persepsi dan reka bentuk keratan rentas.

Sorotan Literatur

Tadbir Urus Keselamatan Siber Berpusatkan Rakyat

Kerajaan digital tidak hanya melibatkan pemindahan perkhidmatan awam daripada kaedah konvensional kepada platform dalam talian. Kerajaan digital turut melibatkan proses mereka bentuk semula perkhidmatan dan institusi berdasarkan keperluan pengguna, nilai awam dan pengalaman rakyat. Tadbir urus berpusatkan rakyat menuntut supaya sistem kerajaan mudah difahami, mudah dicapai, dipercayai dan responsif terhadap kepelbagaian pengguna. Prinsip ini amat penting dalam keselamatan siber kerana pengguna perlu membuat keputusan dengan segera dalam keadaan tidak pasti, berisiko dan tertekan. Dasar keselamatan siber dilaksanakan melalui pelbagai instrumen, termasuk perundangan, penguatkuasaan, komunikasi risiko, kempen kesedaran, sistem semakan, saluran pelaporan dan sokongan kepada mangsa. Walaupun sesuatu dasar mungkin kelihatan lengkap pada peringkat institusi, dasar tersebut masih boleh berada jauh daripada pengalaman rakyat. Apabila masyarakat tidak mengetahui saluran yang sesuai, tidak memahami prosedur atau tidak mempercayai tindak balas institusi, kapasiti formal kerajaan tidak semestinya diterjemahkan kepada perlindungan praktikal.

Dupont (2019) menegaskan keperluan memantau dasar pencegahan jenayah siber berdasarkan pengaruhnya terhadap tingkah laku dan pengalaman sebenar masyarakat. Vedung (1997) telah membezakan kewujudan sesuatu program daripada proses pelaksanaan, hasil dan kegunaannya kepada kumpulan sasaran.

Dalam konteks penipuan siber, persoalan penting bukan sekadar sama ada kempen atau saluran pelaporan telah diwujudkan. Persoalannya ialah sama ada rakyat mengetahui kewujudan mekanisme tersebut, memahami fungsinya dan boleh menggunakannya pada waktu yang kritikal. Kempen kesedaran menunjukkan perbezaan antara penyampaian maklumat dengan pembinaan keupayaan bertindak. Bada et al. (2019) menjelaskan bahawa kempen keselamatan siber sering gagal mengubah tingkah laku apabila mesej terlalu umum, teknikal atau tidak berkait dengan pengalaman harian pengguna. Kempen yang berkesan perlu menerangkan bukan sahaja bentuk ancaman, tetapi juga tindakan yang perlu dilakukan, urutan tindakan dan saluran yang perlu digunakan. Alshaikh et al. (2018) turut menegaskan bahawa kesedaran keselamatan hanya menjadi bermakna apabila komunikasi institusi disokong oleh latihan dan pengukuhan tingkah laku secara berterusan.

Kepercayaan terhadap institusi juga mempengaruhi pelaksanaan dasar. Rakyat menilai institusi berdasarkan pengalaman sendiri, pengalaman ahli keluarga, cerita komuniti, liputan media dan interaksi terdahulu dengan pihak berkuasa. Kepercayaan boleh menggalakkan pematuhan serta pelaporan. Namun, kepercayaan tanpa amalan pengesahan boleh dieksploitasi oleh penipu yang menyamar sebagai institusi kerajaan. Kajian terhadap pengguna pembayaran digital menunjukkan bahawa komitmen keselamatan siber negara dan petunjuk kebolepercayaan institusi boleh membentuk keyakinan terhadap sistem digital (Krishna et al., 2025). Literasi teknologi kewangan juga boleh mengukuhkan hubungan antara strategi keselamatan, kualiti perkhidmatan dan kepercayaan pengguna (Chishty et al., 2025). Oleh itu, cabaran tadbir urus bukan sekadar membina kepercayaan, tetapi membentuk kepercayaan termaklum yang disertai amalan pengesahan.

Orientasi Sosiobudaya dan Literasi Digital

Rakyat tidak membangunkan pengetahuan dan amalan digital dalam kekosongan sosial. Cara seseorang menggunakan teknologi, menilai maklumat dan bertindak balas terhadap risiko dipengaruhi oleh bahasa, keluarga, komuniti, pendidikan, tempat kerja dan pengalaman interaksi antara budaya. Penyelidikan rentas budaya menunjukkan bahawa bahasa boleh mempengaruhi persepsi risiko dan pemprosesan maklumat dalam talian (Alcántara-Pilar et al., 2013, 2018). Akses kepada maklumat dalam pelbagai bahasa juga penting dalam membentuk literasi maklumat digital dalam kalangan komuniti yang mempunyai latar bahasa dan budaya yang berbeza (Wu et al., 2023).

Teori Pembelajaran Sosial menjelaskan bahawa individu mempelajari tingkah laku melalui pemerhatian, pengalaman, peniruan dan pengukuhan sosial (Bandura, 1986). Dalam persekitaran digital, amalan seperti menyemak sumber, mengesahkan identiti, melindungi maklumat peribadi dan membuat laporan boleh dipelajari melalui keluarga, rakan, komuniti, institusi pendidikan serta kempen awam. Pengalaman komunikasi antara budaya dan penyertaan dalam aktiviti penciptaan serta verifikasi kandungan turut menyumbang kepada perkembangan literasi digital kritikal (Guermat & Boubekri, 2026; Satar et al., 2025). Walau bagaimanapun, pengaruh orientasi sosiobudaya terhadap literasi digital tidak semestinya berlaku dalam satu arah. Komuniti yang membudayakan semakan sumber, perbincangan risiko

dan penggunaan saluran rasmi boleh menjadi sumber pembelajaran serta perlindungan. Sebaliknya, jaringan sosial yang kukuh juga boleh menyebarkan maklumat tidak tepat apabila kepercayaan terhadap ahli komuniti menggantikan proses pengesahan. Oleh itu, hubungan tersebut perlu diuji tanpa menetapkan arah positif atau negatif.

H1: Orientasi sosiobudaya mempunyai hubungan yang signifikan dengan literasi digital.

Literasi Digital dan Persepsi terhadap Pelaksanaan Dasar Keselamatan Siber

Perbincangan mengenai jurang digital telah berkembang daripada isu akses fizikal kepada perbezaan dalam kemahiran, bentuk penggunaan dan hasil yang diperoleh daripada teknologi. van Deursen dan van Dijk (2014) menjelaskan bahawa jurang digital masa kini semakin berkait dengan kemampuan individu menggunakan teknologi secara produktif, kritikal dan selamat. Dalam masyarakat yang mempunyai kadar penggunaan Internet yang tinggi, persoalan utama bukan lagi sama ada seseorang memiliki telefon pintar atau akses Internet, tetapi sama ada pengguna mampu menilai maklumat, mengenal pasti manipulasi, melindungi data dan menggunakan perkhidmatan digital kerajaan dengan selamat.

Literasi digital merangkumi dimensi teknikal, kognitif dan sosial. Ng (2012) mentakrifkannya sebagai keupayaan mengendalikan teknologi, memahami maklumat digital dan menyertai persekitaran digital secara sesuai. Kerangka DigComp 2.2 turut merangkumi literasi maklumat dan data, komunikasi, penciptaan kandungan, keselamatan serta penyelesaian masalah (Vuorikari et al., 2022). Dalam konteks keselamatan siber, keupayaan tersebut membolehkan pengguna berhenti seketika sebelum bertindak, menyemak mesej atau laman sesawang, menggunakan ciri keselamatan dan mendapatkan pengesahan daripada sumber rasmi. Bukti empirikal menunjukkan bahawa literasi digital boleh mengurangkan risiko pemangsaaan dan meningkatkan tingkah laku perlindungan. Graham dan Triplett (2017) mendapati bahawa literasi digital berfungsi sebagai bentuk penjagaan berkeupayaan dalam mengurangkan pemangsaaan pancingan data. Li et al. (2024) pula menunjukkan bahawa literasi digital mengurangkan kemungkinan seseorang menjadi mangsa penipuan. Kajian lain turut menghubungkan pengetahuan digital, kesedaran keselamatan, motivasi perlindungan dan efikasi sendiri dengan amalan keselamatan siber yang lebih baik (de Kimpe et al., 2022; Elrayah & Jamil, 2023; Thani et al., 2026).

Dari perspektif pelaksanaan dasar, literasi digital menentukan sama ada mekanisme yang disediakan kerajaan dapat digunakan oleh rakyat. Sesuatu portal pelaporan mungkin telah tersedia, tetapi pengguna masih perlu mengetahui kewujudannya, mengenal pasti antara muka yang sah, memahami maklumat yang diperlukan dan mengikuti prosedur yang ditetapkan. Individu yang mempunyai literasi digital lebih tinggi dijangka lebih berupaya mengakses maklumat rasmi, memahami komunikasi risiko dan menggunakan saluran perlindungan yang disediakan. Oleh itu, literasi digital dijangka mempunyai hubungan positif dengan penilaian terhadap kebolegunaan dan keberkesanan pelaksanaan dasar keselamatan siber.

H2: Literasi digital mempunyai hubungan positif yang signifikan dengan persepsi terhadap pelaksanaan dasar keselamatan siber.

Orientasi Sosiobudaya dan Persepsi terhadap Pelaksanaan Dasar Keselamatan Siber

Teori Pembinaan Realiti Sosial menjelaskan bahawa makna mengenai institusi, autoriti dan tindakan yang dianggap sah dibentuk melalui bahasa, simbol dan interaksi sosial (Berger & Luckmann, 1966). Dalam konteks kerajaan digital, rakyat bukan sahaja menilai kandungan maklumat yang disampaikan, tetapi turut menilai bahasa yang digunakan, identiti penyampai, saluran komunikasi dan kesesuaiannya dengan pengalaman kehidupan mereka. Dalam masyarakat majmuk, komunikasi keselamatan siber yang disampaikan melalui satu bahasa teknikal atau saluran nasional yang seragam tidak semestinya menghasilkan tahap kefahaman dan penerimaan yang sama. Orientasi sosiobudaya boleh meningkatkan penerimaan dasar apabila maklumat kerajaan disokong oleh pemimpin komuniti, keluarga atau jaringan sosial yang dipercayai. Sebaliknya, orientasi yang terlalu bergantung pada sumber tidak rasmi boleh mengurangkan penggunaan saluran kerajaan atau menimbulkan keraguan terhadap tindak balas institusi. Orientasi sosiobudaya dalam kajian ini tidak dianggap sebagai ciri tetap sesuatu kumpulan etnik. Konstruk tersebut merujuk kepada sejauh mana nilai budaya, bahasa, maklumat komuniti dan amalan komunikasi mempengaruhi interaksi individu dalam ruang digital. Oleh sebab pengaruh tersebut boleh menghasilkan penerimaan atau penolakan yang berbeza, hubungan langsung antara orientasi sosiobudaya dengan persepsi terhadap pelaksanaan dasar keselamatan siber perlu diuji secara empirikal tanpa menetapkan arah tertentu.

H3: Orientasi sosiobudaya mempunyai hubungan yang signifikan dengan persepsi terhadap pelaksanaan dasar keselamatan siber.

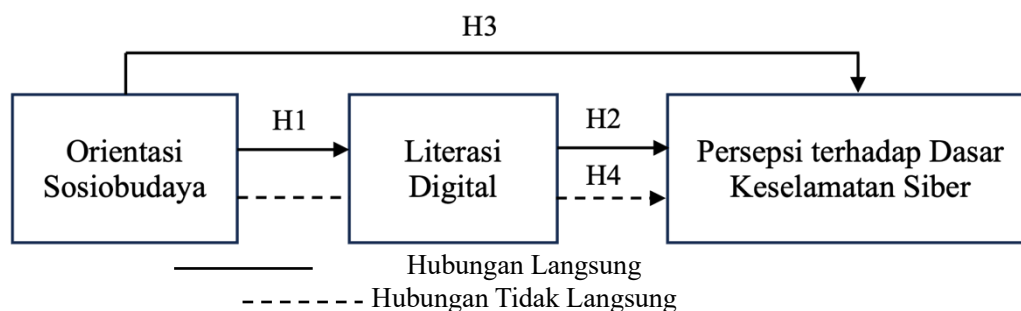
Peranan Pengantara Literasi Digital

Hubungan antara orientasi sosiobudaya dengan persepsi terhadap pelaksanaan dasar keselamatan siber mungkin tidak berlaku secara langsung sepenuhnya. Berdasarkan Teori Pembelajaran Sosial, konteks sosial dan budaya membentuk peluang individu mempelajari amalan digital, mendapatkan bantuan, menilai risiko dan memperoleh pengetahuan tentang mekanisme perlindungan. Keupayaan digital yang terbentuk daripada proses tersebut seterusnya menentukan sejauh mana seseorang dapat memahami dan menggunakan kempen, panduan keselamatan, sistem semakan serta saluran pelaporan kerajaan. Sebagai contoh, sokongan komuniti mungkin tidak secara langsung menyebabkan seseorang menilai pelaksanaan dasar secara positif. Sebaliknya, sokongan tersebut boleh membantu individu meningkatkan kemahiran mencari maklumat rasmi, mengenal pasti saluran yang sah dan memahami prosedur pelaporan. Literasi digital dengan itu berfungsi sebagai mekanisme yang menterjemahkan pengaruh sosiobudaya kepada pengalaman penggunaan dasar. Kajian terdahulu lebih banyak meneliti literasi digital sebagai faktor perlindungan daripada pemangsaan atau sebagai peramal tingkah laku keselamatan. Penjelasan tentang bagaimana literasi digital menghubungkan orientasi sosiobudaya dengan penilaian rakyat terhadap pelaksanaan dasar masih terhad, khususnya berdasarkan pengalaman individu yang pernah melalui proses pelaporan formal. Jurang ini mewajarkan pengujian literasi digital sebagai pemboleh ubah pengantara.

H4: Literasi digital menjadi pengantara yang signifikan dalam hubungan antara orientasi sosiobudaya dengan persepsi terhadap pelaksanaan dasar keselamatan siber.

Kerangka Konseptual Kajian

Kerangka konseptual kajian seperti ditunjukkan dalam Rajah 1, meletakkan orientasi sosiobudaya sebagai pemboleh ubah peramal, literasi digital sebagai pemboleh ubah pengantara dan persepsi terhadap pelaksanaan dasar keselamatan siber sebagai pemboleh ubah hasil. Tiga hubungan langsung diuji, iaitu orientasi sosiobudaya dengan literasi digital (H1), literasi digital dengan persepsi terhadap pelaksanaan dasar (H2), dan orientasi sosiobudaya dengan persepsi terhadap pelaksanaan dasar (H3). H4 menguji hubungan tidak langsung orientasi sosiobudaya terhadap persepsi tersebut melalui literasi digital. Susunan ini ialah spesifikasi model berasaskan teori dan tidak mengesahkan urutan temporal antara konstruk.



Rajah 1: Kerangka Konseptual Kajian

Metodologi

Reka Bentuk Kajian dan Responden

Kajian menggunakan pendekatan kuantitatif melalui reka bentuk tinjauan keratan rentas untuk menilai hubungan antara konstruk pada satu tempoh pengukuran (Creswell & Creswell, 2018). Kajian melibatkan 500 warganegara Malaysia berumur 18 tahun ke atas yang pernah menjadi mangsa penipuan siber dan telah membuat laporan polis. Teknik pensampelan bertujuan digunakan kerana kajian memerlukan responden yang mempunyai pengalaman pemangsaan dan pelaporan rasmi (Etikan et al., 2016). Akses kepada responden dipermudah melalui kerjasama rasmi dengan Jabatan Siasatan Jenayah Komersial, Polis Diraja Malaysia. Oleh sebab pensampelan bertujuan digunakan, dapatan perlu ditafsir dalam konteks 500 responden yang dikaji dan tidak boleh dianggap mewakili secara statistik semua mangsa yang membuat laporan polis atau seluruh rakyat Malaysia. Saiz sampel tersebut melebihi keperluan minimum bagi model PLS-SEM yang mempunyai dua peramal maksimum untuk sesuatu konstruk endogen dan memberikan ketepatan yang memadai bagi penganggaran laluan (Hair et al., 2022; Kock & Hadaya, 2018). Jadual 1 menunjukkan sampel terdiri daripada 256 orang perempuan (51.2%) dan 244 orang lelaki (48.8%). Responden Melayu membentuk 52.6 peratus daripada sampel, diikuti responden Cina sebanyak 29.8 peratus, India sebanyak 6.4 peratus dan kategori etnik lain sebanyak 11.2 peratus. Sebanyak 29.0 peratus responden bekerja dalam sektor kerajaan, manakala 30.8 peratus bekerja dalam sektor swasta.

Jadual 1: Profil Terpilih Responden

Ciri	Kategori	Kekerapan	Peratus
Jantina	Perempuan	256	51.2
	Lelaki	244	48.8
Etnik	Melayu	263	52.6
	Cina	149	29.8
	India	32	6.4
	Etnik lain	56	11.2
Pekerjaan	Sektor swasta	154	30.8
	Sektor kerajaan	145	29.0
	Tidak bekerja	92	18.4
	Kategori pekerjaan lain	109	21.8

Sumber: Data kajian. N = 500.

Pembangunan dan Pengesahan Instrumen

Instrumen kajian diadaptasi dan dikontekstualisasikan berdasarkan objektif kajian, sorotan literatur dan kerangka konseptual kajian berkaitan orientasi sosiobudaya, literasi digital serta pelaksanaan dasar keselamatan siber. Proses adaptasi melibatkan pemilihan domain konseptual daripada instrumen dan kerangka terdahulu, diikuti pengubahsuaian kandungan serta bahasa item agar sesuai dengan pengalaman mangsa penipuan siber dalam masyarakat majmuk Malaysia. Pendekatan ini digunakan kerana instrumen terdahulu tidak dibangunkan secara khusus untuk mengukur hubungan antara orientasi sosiobudaya, amalan keselamatan digital dan penilaian terhadap pelaksanaan dasar keselamatan siber dalam konteks penipuan siber di Malaysia.

Bagi konstruk orientasi sosiobudaya, pembentukan item dipandu oleh Multigroup Ethnic Identity Measure yang menekankan rasa kepunyaan, penglibatan dan penzahiran identiti etnik (Phinney, 1992) serta CVSCALE yang mengukur nilai budaya pada peringkat individu (Yoo et al., 2011). Kedua-dua sumber ini digunakan sebagai asas konseptual untuk membentuk item berkaitan pengamalan nilai budaya, penggunaan nilai budaya dalam menilai maklumat, kepercayaan terhadap maklumat komuniti, pengaruh budaya terhadap komunikasi dalam talian dan penzahiran identiti etnik dalam ruang digital. Oleh sebab item-item tersebut telah diubah suai secara substantif untuk konteks penilaian maklumat dan komunikasi digital, instrumen ini dianggap sebagai instrumen adaptasi dan kontekstualisasi, bukannya penggunaan semula secara langsung skala asal.

Item literasi digital pula diadaptasi berdasarkan konseptualisasi literasi digital yang merangkumi dimensi teknikal, kognitif dan sosial-emosi (Ng, 2012), keupayaan menggunakan teknologi secara berkesan dalam persekitaran digital (Tang & Chaw, 2016) serta domain kompetensi maklumat, komunikasi, keselamatan dan penyelesaian masalah dalam kerangka DigComp 2.2 (Vuorikari et al., 2022). Berdasarkan sumber tersebut, item literasi digital memberikan tumpuan kepada amalan menyemak mesej atau pautan, melindungi maklumat peribadi, mengesahkan laman sesawang rasmi, menggunakan saluran pelaporan rasmi dan mengaktifkan ciri keselamatan digital.

Konstruk persepsi terhadap pelaksanaan dasar keselamatan siber dibentuk berdasarkan literatur mengenai kempen kesedaran, latihan keselamatan maklumat dan kapasiti institusi dalam pengurusan keselamatan siber. Bada et al. (2019) menegaskan bahawa kempen kesedaran perlu melampaui penyampaian maklumat dengan membantu pengguna menterjemahkan pengetahuan kepada tingkah laku perlindungan. Alshaikh et al. (2018) pula menunjukkan bahawa latihan dan kesedaran keselamatan maklumat perlu dinilai berdasarkan pelaksanaan, penerimaan dan keupayaannya mempengaruhi amalan pengguna. Domain institusi turut dipandu oleh National Cyber Security Index yang menekankan kapasiti dasar, pencegahan ancaman, pengurusan insiden dan tindak balas terhadap jenayah siber (e-Governance Academy, n.d.). Sumber-sumber ini digunakan sebagai panduan domain dan bukannya sebagai satu skala persepsi dasar yang diterima pakai secara langsung. Item akhir menilai kejelasan maklumat rasmi, kebolehgunaan garis panduan, manfaat kempen, pengetahuan tentang saluran bantuan rasmi dan keyakinan terhadap keberkesanan tindakan pihak berkuasa.

Kesahan kandungan dan kesahan muka instrumen dinilai sebelum pengumpulan data sebenar. Kesahan kandungan melibatkan semakan pakar terhadap kerelevanan item, kejelasan bahasa, kesepadanan antara item dengan definisi konstruk dan kesesuaian item dengan objektif serta konteks kajian. Penilaian tersebut penting untuk memastikan setiap item mewakili domain konstruk yang hendak diukur dan tidak menyimpang daripada skop konseptual yang ditetapkan (DeVellis, 2017; Lynn, 1986; Rubio et al., 2003). Kesahan muka pula memberi tumpuan kepada kebolehfahaman item, kesesuaian istilah, kejelasan arahan dan sensitiviti bahasa kepada responden daripada pelbagai latar etnik, pendidikan dan pengalaman digital. Struktur ayat dan istilah tertentu diperhalus berdasarkan maklum balas pakar serta respons awal individu yang mempunyai ciri hampir sama dengan populasi sasaran.

Kajian rintis kemudiannya dijalankan terhadap 60 orang responden yang mempunyai ciri hampir sama dengan populasi kajian, iaitu warganegara Malaysia berumur 18 tahun dan ke atas yang pernah menjadi mangsa penipuan siber. Saiz tersebut memadai untuk penilaian awal kefahaman item, prosedur pengumpulan data dan konsistensi dalaman instrumen pada peringkat kajian rintis (Johanson & Brooks, 2010). Kebolehpercayaan awal dinilai menggunakan pekali alfa Cronbach dengan nilai sekurang-kurangnya 0.70 dianggap memadai bagi penyelidikan sosial (Nunnally & Bernstein, 1994; Tavakol & Dennick, 2011). Hasil kajian rintis menunjukkan nilai alfa Cronbach sebanyak 0.823 bagi orientasi sosiobudaya, 0.845 bagi literasi digital dan 0.861 bagi persepsi terhadap pelaksanaan dasar keselamatan siber. Kesemua nilai tersebut melebihi nilai ambang 0.70 dan menunjukkan bahawa item bagi setiap konstruk mempunyai konsistensi dalaman awal yang baik. Berdasarkan hasil semakan dan kajian rintis, beberapa penambahbaikan kecil dilakukan terhadap susunan ayat, penggunaan istilah dan kejelasan arahan sebelum instrumen digunakan dalam kajian sebenar.

Pengukuran Konstruk

Kajian ini menggunakan tiga konstruk reflektif, iaitu orientasi sosiobudaya, literasi digital dan persepsi terhadap pelaksanaan dasar keselamatan siber. Setiap konstruk diukur menggunakan lima indikator reflektif. Semua item dinilai menggunakan skala Likert lima mata daripada 1 iaitu sangat tidak setuju, hingga 5 iaitu sangat setuju (Likert, 1932). Skor yang lebih tinggi menunjukkan tahap persetujuan yang lebih tinggi terhadap pernyataan yang dikemukakan.

Orientasi Sosiobudaya

Orientasi sosiobudaya merujuk kepada sejauh mana nilai budaya, identiti sosial dan hubungan komuniti mempengaruhi cara individu berinteraksi serta menilai maklumat dalam persekitaran digital. Konstruk ini merupakan pengoperasian pada peringkat individu yang diadaptasi daripada dimensi identiti etnik dan nilai budaya yang dikemukakan oleh Phinney (1992) serta Yoo et al. (2011). Lima item digunakan untuk menilai pengamalan nilai budaya dalam interaksi sosial, penggunaan nilai budaya ketika menentukan kesahihan maklumat, kecenderungan mempercayai dan berkongsi maklumat daripada komuniti etnik, pengaruh budaya terhadap komunikasi dalam talian serta penzahiran identiti etnik melalui bahasa, simbol atau kandungan digital. Skor yang lebih tinggi menunjukkan bahawa pertimbangan dan amalan komunikasi digital individu lebih kuat dipengaruhi oleh orientasi sosiobudayanya. Konstruk ini tidak mengukur kategori etnik responden dan tidak mengandaikan bahawa semua individu daripada sesuatu kumpulan etnik mempunyai nilai atau tingkah laku yang seragam. Sebaliknya, konstruk tersebut menilai variasi orientasi sosiobudaya pada peringkat individu. Pendekatan ini mengurangkan risiko menghasilkan generalisasi atau stereotaip terhadap mana-mana kumpulan etnik.

Literasi Digital

Literasi digital merujuk kepada keupayaan individu menggunakan teknologi secara kritikal, selamat dan bertanggungjawab ketika menerima maklumat, berkomunikasi atau menjalankan urusan dalam talian. Pengukuran konstruk ini dipandu oleh dimensi teknikal, kognitif dan sosial-emosi literasi digital (Ng, 2012), keupayaan menggunakan teknologi dalam persekitaran pembelajaran digital (Tang & Chaw, 2016) serta domain literasi maklumat, komunikasi, keselamatan dan penyelesaian masalah dalam DigComp 2.2 (Vuorikari et al., 2022). Lima item digunakan untuk menilai amalan menyemak mesej atau pautan sebelum memberikan respons, melindungi maklumat peribadi, mengesahkan alamat laman sesawang rasmi sebelum menjalankan urusan, melaporkan mesej atau panggilan mencurigakan melalui saluran rasmi dan menggunakan ciri keselamatan seperti kata laluan kukuh atau pengesahan dua faktor. Skor yang lebih tinggi menunjukkan keupayaan verifikasi dan amalan perlindungan digital yang lebih baik. Dalam kajian ini, literasi digital tidak dihadkan kepada kemahiran mengendalikan peranti atau aplikasi. Konstruk tersebut turut merangkumi pertimbangan kritikal terhadap kesahihan maklumat, pengenpastian risiko, perlindungan data peribadi dan tindakan menggunakan mekanisme keselamatan atau pelaporan yang sesuai.

Persepsi terhadap Pelaksanaan Dasar Keselamatan Siber

Persepsi terhadap pelaksanaan dasar keselamatan siber merujuk kepada penilaian individu terhadap kejelasan, kebolehgunaan, kebolehcapaian dan keberkesanan maklumat, garis panduan, kempen, saluran bantuan serta tindakan penguatkuasaan yang dilaksanakan oleh kerajaan atau agensi berkaitan. Pembentukan konstruk ini dipandu oleh literatur mengenai keberkesanan kempen kesedaran dan perubahan tingkah laku keselamatan (Bada et al., 2019), amalan latihan serta kesedaran keselamatan maklumat dalam organisasi (Alshaikh et al., 2018) dan domain kapasiti institusi dalam National Cyber Security Index (e-Governance Academy, n.d.). Lima item digunakan untuk menilai sama ada maklumat rasmi keselamatan siber daripada kerajaan atau agensi mudah difahami, garis panduan pihak berkuasa mudah diikuti, kempen keselamatan siber membantu mengenal pasti dan mengelakkan penipuan, responden mengetahui cara menghubungi pihak berkuasa atau saluran bantuan rasmi dan tindakan

penguatkuasaan, amaran atau kempen pihak berkuasa dipercayai berkesan dalam membantu mengurangkan penipuan siber. Skor yang lebih tinggi menunjukkan persepsi yang lebih positif terhadap kejelasan, kebolegunaan dan keberkesanan pelaksanaan dasar keselamatan siber. Konstruk ini tidak mengukur kewujudan formal dokumen dasar semata-mata. Sebaliknya, konstruk tersebut menilai bagaimana pelaksanaan mekanisme keselamatan siber diterima dan dialami oleh pengguna pada peringkat individu.

Prosedur Pengumpulan Data

Data dikumpulkan menggunakan soal selidik berstruktur dalam talian daripada warganegara Malaysia berumur 18 tahun dan ke atas yang pernah menjadi mangsa penipuan siber serta telah membuat laporan polis berkaitan kejadian tersebut. Responden dikenal pasti melalui kerjasama rasmi dengan Jabatan Siasatan Jenayah Komersial, Polis Diraja Malaysia berdasarkan saluran pelaporan kes penipuan siber. Sebelum pengedaran soal selidik, bakal responden dihubungi melalui saluran yang dibenarkan dan diberikan penerangan mengenai tujuan kajian, bentuk penglibatan, penggunaan data, kerahsiaan maklumat serta hak mereka sebagai peserta kajian. Hanya individu yang memenuhi kriteria penyertaan dan bersetuju secara sukarela diberikan pautan soal selidik melalui aplikasi WhatsApp. Penggunaan soal selidik dalam talian membolehkan responden menjawab pada masa yang sesuai di samping memudahkan pengurusan data secara sistematik. Penerangan yang jelas, susunan soal selidik yang teratur dan jaminan kerahsiaan turut digunakan untuk mengurangkan kekeliruan serta meningkatkan kualiti respons (Dillman et al., 2014). Saringan kelayakan dilakukan pada bahagian awal soal selidik dengan mengesahkan status kewarganegaraan, umur, pengalaman sebagai mangsa penipuan siber dan kewujudan laporan polis. Pengumpulan data diteruskan sehingga memperoleh 500 respons yang lengkap dan boleh dianalisis. Respons kemudiannya diperiksa dari segi kelengkapan, konsistensi jawapan, pematuhan terhadap kriteria penyertaan dan kewujudan pola respons yang tidak munasabah. Hanya respons yang lengkap, sah dan memenuhi semua kriteria kajian dikekalkan dalam analisis akhir.

Penganalisisan Data

Data dianalisis menggunakan IBM SPSS Statistics dan SmartPLS 4. IBM SPSS Statistics digunakan untuk penyaringan awal data dan analisis deskriptif yang merangkumi kekerapan, peratusan, min dan sisihan piawai. SmartPLS 4 pula digunakan untuk menjalankan pemodelan persamaan berstruktur berasaskan varians atau partial least squares structural equation modelling bagi menilai model pengukuran, model struktur serta hubungan langsung dan tidak langsung antara konstruk (Hair et al., 2022; Ringle et al., 2024).

Oleh sebab semua konstruk dimodelkan secara reflektif, penilaian model pengukuran melibatkan kebolehpercayaan indikator, kebolehpercayaan dalaman, kesahan konvergen dan kesahan diskriminan. Kebolehpercayaan indikator dinilai melalui nilai outer loading, manakala kebolehpercayaan dalaman dinilai menggunakan alfa Cronbach, rho_A dan kebolehpercayaan komposit. Kesahan konvergen ditentukan melalui nilai varians purata diekstrak atau average variance extracted dan kesahan diskriminan dinilai menggunakan kriteria Fornell-Larcker serta nisbah heterotrait-monotrait (Fornell & Larcker, 1981; Henseler et al., 2015). Secara umum, nilai outer loading sekurang-kurangnya 0.708, nilai alfa Cronbach, rho_A dan kebolehpercayaan komposit antara 0.70 hingga 0.95 serta nilai varians purata diekstrak sekurang-kurangnya 0.50 digunakan sebagai kriteria penilaian. Kesahan diskriminan dinilai menggunakan kriteria Fornell-Larcker dan nisbah heterotrait-monotrait (HTMT), dengan

ambang HTMT di bawah 0.90. Sela keyakinan bootstrap turut diperiksa untuk menilai sama ada nilai 1.00 termasuk dalam julat anggaran. Walau bagaimanapun, pengecualian nilai 1.00 daripada sela keyakinan tidak dengan sendirinya menunjukkan bahawa ambang HTMT 0.90 telah dipenuhi. Keputusan kedua-dua penilaian ini ditafsir secara berasingan bagi mengenal pasti kemungkinan pertindihan empirikal antara konstruk (Hair et al., 2022; Henseler et al., 2015).

Penilaian model struktur merangkumi pemeriksaan kolineariti melalui faktor inflasi varians, penilaian pekali laluan, aras signifikan statistik, pekali penentuan dan saiz kesan. Nilai faktor inflasi varians di bawah 5.00 digunakan bagi menunjukkan bahawa isu kolineariti tidak berada pada tahap kritikal. Pekali penentuan digunakan untuk menilai keupayaan konstruk peramal menjelaskan varians konstruk endogen, manakala nilai f^2 digunakan untuk menentukan sumbangan relatif setiap konstruk eksogen terhadap konstruk endogen (Hair et al., 2022; Sarstedt et al., 2021). Signifikan hubungan langsung dan tidak langsung dinilai menggunakan prosedur bootstrapping dengan 5,000 subsampel. Hubungan dianggap signifikan apabila nilai p kurang daripada 0.05 dan sela keyakinan 95 peratus tidak merangkumi nilai sifar. Bagi analisis pengantaraan, penilaian memberi tumpuan kepada magnitud, arah dan signifikan kesan tidak langsung tanpa bergantung pada andaian taburan normal kesan pengantaraan (Hair et al., 2022).

Memandangkan semua konstruk diukur menggunakan soal selidik sendiri daripada responden yang sama dalam satu tempoh pengumpulan data, beberapa langkah prosedural dilaksanakan bagi mengurangkan risiko bias kaedah sepunya. Langkah tersebut merangkumi jaminan kerahsiaan, penggunaan bahasa item yang jelas dan tidak terlalu teknikal, pengelakan pernyataan yang terlalu mengarah serta pengasingan item mengikut bahagian konstruk yang berbeza. Langkah-langkah ini bertujuan mengurangkan kebimbangan penilaian, kecenderungan memberikan jawapan yang dianggap dikehendaki penyelidik dan pengaruh konteks item terhadap respons peserta (Podsakoff et al., 2003).

Dapatan Kajian

Statistik Deskriptif dan Penilaian Model Pengukuran

Jadual 2 membentangkan statistik deskriptif, kebolehpercayaan dalaman dan kesahan konvergen bagi ketiga-tiga konstruk kajian. Orientasi sosiobudaya mencatatkan skor min tertinggi, iaitu 3.835 dengan sisihan piawai 0.842. Nilai ini berada di atas titik tengah skala dan menunjukkan bahawa unsur budaya, identiti serta hubungan komuniti mempunyai pengaruh yang relatif jelas terhadap interaksi dan penilaian maklumat digital responden. Literasi digital mencatatkan skor min 2.708 dengan sisihan piawai 1.223, manakala persepsi terhadap pelaksanaan dasar keselamatan siber mencatatkan skor min 2.793 dengan sisihan piawai 1.211. Kedua-dua nilai tersebut berada sedikit di bawah titik tengah skala lima mata. Dapatan ini menunjukkan bahawa tahap amalan literasi digital dan penilaian positif terhadap pelaksanaan dasar keselamatan siber masih belum tinggi dalam kalangan responden, walaupun semua responden mempunyai pengalaman sebagai mangsa penipuan siber dan telah membuat laporan polis.

Jadual 2: Statistik Deskriptif, Kebolehpercayaan dan Kesahan Konvergen

Konstruk	Min	SP	Julat muatan	α	rho_A	CR	AVE
Orientasi sosiobudaya	3.835	0.842	0.836–0.892	0.919	0.924	0.939	0.754
Literasi digital	2.708	1.223	0.785–0.950	0.951	0.958	0.963	0.839
Persepsi terhadap pelaksanaan dasar keselamatan siber	2.793	1.211	0.909–0.942	0.960	0.961	0.969	0.863

Nota. N = 500; SP = sisihan piawai; α = alfa Cronbach; CR = kebolehpercayaan komposit; AVE = varians purata diekstrak.

Kesemua indikator mempunyai nilai muatan melebihi 0.708, manakala nilai AVE antara 0.754 hingga 0.863 melebihi nilai minimum 0.50. Dapatan ini menunjukkan bahawa ketiga-tiga konstruk memenuhi kriteria kebolehpercayaan indikator dan kesahan konvergen. Nilai alfa Cronbach, rho_A dan CR juga melebihi nilai minimum 0.70. Walau bagaimanapun, beberapa pekali kebolehpercayaan bagi literasi digital dan persepsi terhadap pelaksanaan dasar keselamatan siber melebihi 0.95. Nilai yang sangat tinggi tersebut menunjukkan konsistensi dalaman yang kukuh, tetapi turut menimbulkan kemungkinan pertindihan atau keserupaan kandungan antara indikator. Oleh itu, kesahan diskriminan diperiksa bagi menentukan sejauh mana setiap konstruk dapat dibezakan secara empirikal.

Kesahan Diskriminan

Jadual 3 menunjukkan bahawa kriteria Fornell-Larcker dipenuhi kerana punca kuasa dua AVE bagi setiap konstruk melebihi korelasinya dengan konstruk lain. Orientasi sosiobudaya juga memenuhi kriteria HTMT apabila hubungannya dengan literasi digital dan persepsi terhadap pelaksanaan dasar keselamatan siber masing-masing mencatatkan nilai 0.470 dan 0.422. Sebaliknya, nilai HTMT antara literasi digital dengan persepsi terhadap pelaksanaan dasar keselamatan siber ialah 0.952 dan melebihi nilai ambang 0.90 yang dicadangkan oleh Henseler et al. (2015). Analisis tambahan menggunakan bootstrapping menunjukkan bahawa sela keyakinan 95% bagi hubungan tersebut berada antara 0.922 hingga 0.975 dan tidak merangkumi nilai 1.00.

Jadual 3: Kesahan Diskriminan Konstruk Kajian

Konstruk	1	2	3
1. Orientasi sosiobudaya	0.868	0.470	0.422
2. Literasi digital	–0.442	0.916	0.952
3. Persepsi terhadap pelaksanaan dasar keselamatan siber	–0.400	0.911	0.929

Nota. Nilai pada pepenjuru dan bercetak tebal ialah punca kuasa dua AVE. Nilai di bawah pepenjuru ialah korelasi antara konstruk, manakala nilai di atas pepenjuru ialah HTMT.

Kriteria Fornell–Larcker dipenuhi bagi ketiga-tiga konstruk. Walau bagaimanapun, kesahan diskriminan antara literasi digital dengan persepsi terhadap pelaksanaan dasar belum mendapat sokongan yang memadai berdasarkan ambang HTMT 0.90. Nilai HTMT bagi pasangan tersebut ialah 0.952, dengan sela keyakinan bootstrap 95% antara 0.922 hingga 0.975. Walaupun sela ini tidak merangkumi 1.00, keseluruhan sela berada di atas 0.90. Oleh itu, keputusan tersebut tidak menghapuskan kebimbangan tentang pembezaan empirikal kedua-dua konstruk. Kedua-duanya dikekalkan dalam model yang dilaporkan berdasarkan perbezaan

konseptual, tetapi pekali laluan, saiz kesan, varians yang diterangkan dan kesan tidak langsung perlu ditafsir dengan mengambil kira kemungkinan pertindihan pengukuran.

Model Struktur dan Pengujian Hipotesis

Model struktur menerangkan 19.6% varians dalam literasi digital dan 82.9% varians dalam persepsi terhadap pelaksanaan dasar keselamatan siber. Nilai R^2 bagi literasi digital menunjukkan keupayaan penjelasan yang relatif rendah, manakala nilai R^2 bagi persepsi terhadap pelaksanaan dasar menunjukkan keupayaan penjelasan yang tinggi. Pemeriksaan kolineariti menunjukkan nilai VIF sebanyak 1.000 bagi orientasi sosiobudaya sebagai peramal literasi digital. Nilai VIF bagi orientasi sosiobudaya dan literasi digital sebagai peramal persepsi terhadap pelaksanaan dasar masing-masing ialah 1.243. Kesemua nilai tersebut berada di bawah nilai ambang 5.00 dan menunjukkan bahawa kolineariti antara konstruk peramal tidak menjadi masalah dalam model struktur yang berfokuskan pelaksanaan dasar. Keputusan hubungan langsung dan kesan tidak langsung berdasarkan prosedur bootstrapping dengan 5,000 subsampel ditunjukkan dalam Jadual 4.

Jadual 4: Keputusan Pengujian Hubungan Langsung dan Kesan Tidak Langsung

Hipotesis	Hubungan	β	SE	t	p	Selang keyakinan 95%	f^2	Keputusan
H1	Orientasi sosiobudaya → Literasi digital	-0.442	0.044	10.012	<.001	[-0.529, -0.355]	0.243	Disokong
H2	Literasi digital → Persepsi terhadap pelaksanaan dasar	0.912	0.016	57.808	<.001	[0.880, 0.941]	3.919	Disokong
H3	Orientasi sosiobudaya → Persepsi terhadap pelaksanaan dasar	0.003	0.026	0.136	.892	[-0.047, 0.053]	0.000	Tidak disokong
H4	Orientasi sosiobudaya → Literasi digital → Persepsi terhadap pelaksanaan dasar	-0.404	0.040	9.970	<.001	[-0.483, -0.322]	—	Disokong

Nota. β = pekali laluan atau kesan tidak langsung piawai; SE = ralat piawai. Hubungan dianggap signifikan apabila $p < .05$ dan selang keyakinan 95% tidak merangkumi sifar.

Hubungan Orientasi Sosiobudaya dengan Literasi Digital

H1 disokong apabila orientasi sosiobudaya menunjukkan hubungan negatif yang signifikan dengan literasi digital ($\beta = -0.442$, SE = 0.044, $t = 10.012$, $p < .001$, 95% CI $[-0.529, -0.355]$). Nilai f^2 sebanyak 0.243 menunjukkan saiz kesan sederhana. Dalam sampel kajian ini, peningkatan orientasi sosiobudaya berkait dengan penurunan skor literasi digital.

Hubungan Literasi Digital dengan Persepsi terhadap Pelaksanaan Dasar

H2 disokong dalam model yang dianggarkan. Literasi digital mempunyai hubungan positif yang signifikan dengan persepsi terhadap pelaksanaan dasar keselamatan siber ($\beta = 0.912$, SE = 0.016, $t = 57.808$, $p < .001$, selang keyakinan 95% $[0.880, 0.941]$). Nilai f^2 ialah 3.919. Walaupun pekali laluan dan saiz kesan adalah tinggi, kedua-duanya perlu ditafsir bersama nilai HTMT 0.952 yang menunjukkan masalah pembezaan empirikal antara konstruk. Oleh itu, magnitud hubungan ini tidak wajar dianggap sebagai bukti muktamad sumbangan substantif literasi digital tanpa mengambil kira kemungkinan pertindihan pengukuran.

Hubungan Orientasi Sosiobudaya dengan Persepsi terhadap Pelaksanaan Dasar

H3 tidak disokong. Orientasi sosiobudaya tidak mempunyai hubungan langsung yang signifikan dengan persepsi terhadap pelaksanaan dasar keselamatan siber ($\beta = 0.003$, SE = 0.026, $t = 0.136$, $p = .892$, 95% CI $[-0.047, 0.053]$). Nilai f^2 sebanyak 0.000 turut menunjukkan bahawa orientasi sosiobudaya tidak memberikan sumbangan langsung yang bermakna kepada persepsi terhadap pelaksanaan dasar apabila literasi digital dimasukkan secara serentak sebagai peramal.

Peranan Pengantara Literasi Digital

Kesan tidak langsung orientasi sosiobudaya terhadap persepsi pelaksanaan dasar melalui literasi digital adalah signifikan ($\beta = -0.404$, SE = 0.040, $t = 9.970$, $p < .001$, selang keyakinan 95% $[-0.483, -0.322]$). Oleh itu, H4 disokong secara statistik dalam model yang dianggarkan. Kesan tidak langsung yang signifikan bersama hubungan langsung yang tidak signifikan adalah konsisten dengan corak pengantaraan tidak langsung sahaja. Arah negatif mencerminkan gabungan hubungan negatif orientasi sosiobudaya dengan literasi digital dan hubungan positif literasi digital dengan persepsi pelaksanaan dasar. Walau bagaimanapun, reka bentuk keratan rentas tidak mengesahkan urutan sebab-akibat, manakala pertindihan antara pengantara dengan pemboleh ubah hasil mengehadkan keteguhan tafsiran pengantaraan.

Perbincangan

Literasi Digital dan Penilaian terhadap Pelaksanaan Dasar

Dapatan paling menonjol dalam kajian ini ialah hubungan positif yang signifikan antara literasi digital dengan persepsi terhadap pelaksanaan dasar keselamatan siber. Responden yang melaporkan keupayaan lebih baik dalam menyemak mesej dan pautan, melindungi maklumat peribadi, mengesahkan laman sesawang, menggunakan ciri keselamatan dan mengakses

saluran rasmi turut memberikan penilaian yang lebih positif terhadap maklumat, garis panduan, kempen dan mekanisme perlindungan kerajaan. Nilai R^2 sebanyak 0.829 menunjukkan bahawa literasi digital bersama-sama orientasi sosiobudaya menerangkan sebahagian besar varians dalam persepsi terhadap pelaksanaan dasar. Dapatan ini menunjukkan bahawa kewujudan dasar, kempen atau saluran pelaporan sahaja belum mencukupi untuk menjamin manfaat kepada masyarakat. Rakyat perlu mempunyai keupayaan untuk mengenal pasti sumber rasmi, memahami arahan, menilai kesahihan komunikasi dan menterjemahkan maklumat yang diterima kepada tindakan perlindungan. Dalam pengertian ini, literasi digital berfungsi sebagai keupayaan penghubung antara sumber perlindungan yang disediakan oleh kerajaan dengan keupayaan rakyat untuk menggunakannya secara bermakna.

Tafsiran tersebut selaras dengan kajian terdahulu yang menghubungkan literasi digital dengan pengurangan risiko pemangsaan, peningkatan kesedaran keselamatan dan pengukuhan tingkah laku perlindungan (Elrayah & Jamil, 2023; Graham & Triplett, 2017; Li et al., 2024; Thani et al., 2026). Kajian ini memperluas perbincangan tersebut dengan menunjukkan bahawa literasi digital bukan sahaja berkait dengan perlindungan individu daripada penipuan, tetapi juga dengan cara rakyat menilai kebolegunaan mekanisme keselamatan siber yang dilaksanakan oleh institusi kerajaan. Individu yang mampu mengenal pasti saluran rasmi dan mengikuti prosedur yang ditetapkan lebih berkemungkinan melihat dasar sebagai jelas, dekat dan boleh digunakan. Sebaliknya, individu yang menghadapi kesukaran mengesahkan sumber, memahami amaran atau menggunakan saluran bantuan mungkin menilai mekanisme yang sama sebagai jauh, mengelirukan atau kurang berkesan. Hal ini menunjukkan bahawa persepsi terhadap pelaksanaan dasar tidak hanya dibentuk oleh ciri objektif sesuatu dasar, tetapi turut bergantung pada keupayaan pengguna berinteraksi dengan mekanisme tersebut.

Walaupun bagaimanapun, nilai R^2 yang tinggi tidak boleh ditafsir sebagai bukti bahawa literasi digital menentukan keberkesanan objektif dasar kerajaan. Konstruk yang diukur dalam kajian ini ialah persepsi responden terhadap pelaksanaan dasar dan bukannya prestasi institusi yang dinilai melalui audit, tempoh respons, kadar penyelesaian kes atau hasil penguatkuasaan. Namun demikian, persepsi rakyat tetap penting kerana ia boleh mempengaruhi kesediaan untuk mendapatkan bantuan, mematuhi nasihat, membuat laporan dan menggunakan mekanisme perlindungan yang disediakan. Kekuatan hubungan tersebut juga perlu ditafsir bersama dapatan kesahan diskriminan. Nilai HTMT sebanyak 0.952 antara literasi digital dengan persepsi terhadap pelaksanaan dasar melebihi nilai ambang 0.90. Walaupun sela keyakinan bootstrap antara 0.922 hingga 0.975 tidak merangkumi nilai 1.00, dapatan ini menunjukkan bahawa kedua-dua konstruk mempunyai pertindihan empirikal yang tinggi. Oleh itu, hubungan yang signifikan tersebut lebih wajar ditafsir sebagai perkaitan antara dua pengalaman yang saling berdekatan, iaitu keupayaan menggunakan perlindungan digital dan penilaian terhadap mekanisme perlindungan institusi, bukannya bukti bahawa kedua-dua konstruk telah dibezakan secara sempurna.

Daripada Jurang Akses kepada Jurang Penggunaan Perlindungan

Dapatan kajian turut menyokong perkembangan konsep jurang digital daripada persoalan akses kepada perbezaan dalam kemahiran, bentuk penggunaan dan hasil yang diperoleh daripada teknologi. Pemilikan telefon pintar, penggunaan media sosial, aplikasi pemesejan atau perbankan dalam talian tidak semestinya menunjukkan bahawa seseorang mampu menggunakan teknologi secara kritikal dan selamat. Jurang yang lebih penting dalam konteks keselamatan siber melibatkan keupayaan mengesahkan maklumat, melindungi privasi,

mengenal pasti sumber institusi yang sah, memahami amaran awam, mengikuti prosedur pelaporan dan membuat keputusan ketika berada dalam tekanan. Jurang ini boleh ditafsir sebagai jurang penggunaan perlindungan, iaitu perbezaan dalam keupayaan rakyat menterjemahkan maklumat, kempen, ciri keselamatan dan saluran bantuan yang tersedia kepada tindakan perlindungan sebenar. Konsep tersebut membezakan antara kewujudan sumber keselamatan siber dengan kebolehan masyarakat menggunakan sumber berkenaan pada waktu yang kritikal. Seseorang mungkin mempunyai akses kepada maklumat dan mengetahui bahawa saluran bantuan wujud, tetapi masih gagal menggunakannya apabila berhadapan dengan komunikasi yang mendesak, penyamaran autoriti atau tekanan emosi.

Skor min literasi digital dan persepsi terhadap pelaksanaan dasar yang berada pada tahap sederhana memberikan makna penting kerana semua responden pernah menjadi mangsa penipuan siber dan telah membuat laporan polis. Pengalaman menjadi mangsa serta interaksi dengan institusi tidak semestinya menghasilkan keupayaan digital yang tinggi atau persepsi yang sangat positif terhadap mekanisme perlindungan. Dapatan ini mencadangkan bahawa proses pelaporan tidak seharusnya berakhir sebagai urusan pentadbiran atau perekodan kes semata-mata. Interaksi selepas laporan dibuat boleh digunakan sebagai titik intervensi untuk memberikan pendidikan bersasar, panduan tindakan, senarai saluran rasmi dan sokongan susulan kepada mangsa. Sebagai contoh, mangsa boleh dibekalkan dengan panduan ringkas tentang pengesahan identiti, perlindungan akaun, tindakan selepas kebocoran maklumat dan prosedur respons terhadap percubaan penipuan berikutnya. Pendekatan tersebut dapat mengubah proses pelaporan daripada mekanisme reaktif kepada peluang pembelajaran dan pemulihan keupayaan digital.

Orientasi Sosiobudaya Beroperasi Melalui Literasi Digital

Ketiadaan hubungan langsung yang signifikan antara orientasi sosiobudaya dengan persepsi terhadap pelaksanaan dasar memberikan implikasi teoritikal yang penting. Dapatan ini menunjukkan bahawa orientasi sosiobudaya tidak secara langsung menentukan cara responden menilai maklumat, kempen dan mekanisme keselamatan siber kerajaan apabila literasi digital dimasukkan dalam model. Sebaliknya, kesan tidak langsung melalui literasi digital adalah signifikan dengan pekali -0.404 dan sela keyakinan yang tidak merangkumi sifar. Corak hubungan langsung yang tidak signifikan tetapi kesan tidak langsung yang signifikan menunjukkan pengantaraan tidak langsung sahaja. Dengan kata lain, hubungan antara orientasi sosiobudaya dengan persepsi terhadap pelaksanaan dasar berlaku melalui tahap literasi digital individu dan bukannya melalui laluan langsung. Orientasi sosiobudaya mungkin membentuk persekitaran pembelajaran, sumber kepercayaan, bahasa komunikasi dan kebiasaan mendapatkan maklumat. Faktor-faktor tersebut seterusnya berkaitan dengan keupayaan membuat semakan dan menggunakan perlindungan digital yang akhirnya mempengaruhi penilaian terhadap mekanisme kerajaan. Tafsiran ini mengelakkan pandangan deterministik yang menganggap budaya atau identiti etnik sebagai kelemahan semula jadi. Dapatan tidak menunjukkan bahawa sesuatu budaya menyebabkan individu menilai dasar secara negatif. Sebaliknya, ia menunjukkan bahawa konteks sosiobudaya berhubung dengan proses pembentukan keupayaan digital. Oleh itu, perhatian perlu diberikan kepada cara keluarga, komuniti, bahasa dan jaringan sosial menyokong atau menghalang perkembangan budaya verifikasi.

Dapatan ini selaras dengan Teori Pembelajaran Sosial yang menjelaskan bahawa amalan menyemak sumber, melindungi data, menggunakan saluran rasmi dan membuat laporan dipelajari melalui pemerhatian, pengalaman, pengulangan dan pengukuhan sosial (Bandura, 1986). Keluarga dan komuniti boleh menjadi sumber perlindungan apabila mereka membudayakan semakan bersama, perkongsian amaran yang tepat dan rujukan kepada saluran rasmi. Sebaliknya, komuniti juga boleh meningkatkan risiko apabila maklumat diterima dan disebarkan berdasarkan kepercayaan interpersonal tanpa proses pengesahan. Teori Pembinaan Realiti Sosial turut membantu menjelaskan dapatan kajian. Rakyat mengenali institusi dan autoriti melalui bahasa, simbol, gelaran, logo, nombor telefon dan bentuk komunikasi yang digunakan dalam kehidupan harian (Berger & Luckmann, 1966). Penipu mengeksploitasi unsur yang sama untuk menghasilkan gambaran institusi palsu yang kelihatan sah. Oleh itu, pengenalan terhadap simbol institusi semata-mata tidak mencukupi sebagai perlindungan kerana simbol tersebut juga boleh ditiru. Komunikasi dasar keselamatan siber perlu membina dua keupayaan secara serentak. Pertama, masyarakat perlu mengetahui identiti, fungsi dan saluran rasmi institusi. Kedua, masyarakat perlu mengamalkan pengesahan sebelum mempercayai komunikasi yang menggunakan identiti institusi tersebut. Pendekatan ini penting kerana kepercayaan terhadap kerajaan tanpa amalan pengesahan boleh dieksploitasi melalui penyamaran autoriti. Matlamat komunikasi keselamatan siber dengan itu bukan sekadar meningkatkan kepercayaan, tetapi membina kepercayaan termaklum yang sentiasa disertai proses semakan.

Implikasi terhadap Kerajaan dan Dasar Keselamatan Siber

Hubungan antara literasi digital dengan persepsi terhadap pelaksanaan dasar memberikan asas untuk meneliti bagaimana keupayaan pengguna dapat disepadukan dalam tadbir urus keselamatan siber. Implikasi kajian tertumpu pada tiga aspek, iaitu komunikasi dan latihan, pengalaman pelaporan serta penilaian kebolegunaan mekanisme perlindungan. Cadangan ini perlu dinilai melalui penyelidikan lanjut kerana kajian mengukur persepsi responden dan tidak menguji keberkesanan intervensi secara langsung.

Komunikasi dan Latihan Berasaskan Tindakan

Komunikasi keselamatan siber perlu membantu pengguna memahami tindakan yang boleh dilakukan ketika berhadapan dengan ancaman. Kandungan kempen wajar menjelaskan cara mengesahkan identiti pengirim, menyemak mesej atau pautan, melindungi maklumat peribadi dan mengenal pasti saluran bantuan rasmi. Panduan berasaskan senario boleh digunakan untuk menerangkan urutan tindakan apabila pengguna menerima panggilan penyamaran, arahan pemindahan wang atau permintaan maklumat sulit. Kad tindakan, video simulasi dan panduan langkah demi langkah merupakan antara bentuk penyampaian yang boleh dibangunkan dan diuji mengikut keperluan pengguna. Latihan literasi digital pula wajar disepadukan dalam program pendidikan, tempat kerja, komuniti dan sokongan selepas pelaporan. Latihan boleh merangkumi pengesahan sumber, penggunaan kata laluan yang kukuh, pengesahan dua faktor serta tindakan terhadap komunikasi mencurigakan. Pelaksanaan secara berulang, disertai latihan membuat keputusan dan maklum balas, menyediakan ruang untuk menilai sama ada pengetahuan keselamatan dapat diterjemahkan kepada amalan perlindungan. Hubungan yang diperhatikan dalam kajian ini menyokong perhatian terhadap keupayaan tersebut, tetapi tidak membuktikan bahawa sesuatu bentuk latihan akan meningkatkan keberkesanan dasar. Komunikasi dan latihan juga perlu peka terhadap kepelbagaian bahasa, umur, pendidikan serta pengalaman digital. Kerjasama dengan sekolah, persatuan penduduk, institusi agama dan

organisasi masyarakat boleh dipertimbangkan bagi menyampaikan panduan dalam bahasa serta contoh yang mudah difahami. Penyesuaian ini hendaklah mengekalkan ketepatan maklumat dan keseragaman tindakan yang disarankan. Setiap bahan perlu menyatakan sumber rasmi, tarikh dan saluran pengesahan supaya perkongsian melalui komuniti turut menggalakkan amalan menyemak maklumat. Pendekatan peka bahasa bertujuan memperluas kefahaman dan kebolehcapaian, tanpa menganggap mana-mana kumpulan etnik mempunyai kelemahan digital yang seragam.

Pengalaman Pelaporan yang Terselaras dan Menyokong Mangsa

Pengalaman pelaporan merupakan ruang penting untuk memperbaiki hubungan antara pengguna dengan mekanisme perlindungan institusi. Semua responden kajian telah membuat laporan polis, namun pengalaman tersebut tidak dengan sendirinya menunjukkan bahawa mereka mempunyai keupayaan digital yang tinggi atau menilai pelaksanaan dasar secara positif. Oleh itu, proses pelaporan wajar diteliti dari sudut kejelasan arahan, kemudahan mendapatkan bantuan dan kesinambungan tindakan antara institusi. Pengguna perlu dapat membezakan fungsi saluran semakan, pemberitahuan kepada institusi kewangan, laporan penguatkuasaan dan penyerahan bukti sokongan. Penyelarasan pelaporan boleh merangkumi arahan yang konsisten, penerangan tentang maklumat yang diperlukan serta penjelasan mengenai pihak yang mengendalikan tindakan susulan. Selepas laporan dibuat, mangsa wajar dimaklumkan tentang langkah seterusnya, jangkaan tempoh respons dan cara mendapatkan perkembangan kes. Bantuan melalui petugas juga perlu dipertimbangkan bagi pengguna yang memerlukan penjelasan tambahan, termasuk warga emas, individu berkeperluan khas dan mereka yang kurang yakin menggunakan saluran digital. Layanan terhadap mangsa perlu mengambil kira kemungkinan tekanan emosi, rasa malu dan kebimbangan untuk berkongsi pengalaman. Prosedur yang mudah difahami serta komunikasi yang menghormati mangsa wajar menjadi sebahagian daripada reka bentuk perkhidmatan. Interaksi selepas pelaporan juga boleh dimanfaatkan untuk memberikan panduan perlindungan akaun, pengesahan identiti dan pengurusan maklumat peribadi. Manfaat sokongan tersebut terhadap keyakinan pengguna dan risiko pemangsa berulang perlu dinilai, bukannya dianggap telah dibuktikan oleh dapatan kajian ini.

Penilaian Kebolehgunaan Mekanisme Perlindungan

Penilaian pelaksanaan dasar perlu merangkumi sejauh mana mekanisme perlindungan dapat dikenal pasti, difahami dan digunakan oleh kumpulan sasaran. Jumlah kempen, amaran atau saluran yang disediakan boleh menerangkan keluasan aktiviti pentadbiran, tetapi perlu dilengkapi dengan maklumat tentang pengalaman pengguna. Antara aspek yang boleh dinilai ialah keupayaan mengenal pasti saluran rasmi, memahami arahan, melengkapkan laporan dan mengetahui tindakan susulan yang diperlukan. Penilaian kebolehgunaan boleh dilaksanakan melalui tugas berasaskan senario, pemerhatian penggunaan perkhidmatan dan maklum balas mangsa. Penunjuk seperti kadar penyempurnaan laporan, masa yang diperlukan, kesilapan semasa mengisi maklumat dan keperluan mendapatkan bantuan dapat digunakan untuk mengenal pasti bahagian proses yang menyukarkan pengguna. Pada peringkat institusi, penilaian boleh merangkumi tempoh respons, kesinambungan rujukan antara agensi, kejelasan maklum balas dan pengalaman layanan. Perbandingan mengikut bahasa, umur, pendidikan dan pengalaman digital pula boleh membantu mengenal pasti keperluan penambahbaikan yang khusus. Dalam kajian ini, persepsi terhadap pelaksanaan dasar ialah penilaian sendiri responden dan tidak mewakili ukuran langsung prestasi institusi. Oleh itu, dapatan persepsi

wajar dilengkapi dengan rekod perkhidmatan dan ukuran tingkah laku sebelum kesimpulan dibuat tentang keberkesanan perlindungan. Gabungan maklumat tersebut dapat membantu membezakan kesukaran yang berpunca daripada keupayaan pengguna dengan masalah reka bentuk atau pelaksanaan perkhidmatan.

Sumbangan Teoritikal

Sumbangan kajian ini terletak pada pengujian literasi digital sebagai pengantara statistik antara orientasi sosiobudaya dengan persepsi terhadap pelaksanaan dasar dalam kalangan mangsa yang telah membuat laporan polis. Dapatan menyediakan asas untuk meneliti hubungan antara konteks sosial, keupayaan digital dan pengalaman berinteraksi dengan mekanisme perlindungan institusi. Istilah jurang penggunaan perlindungan digunakan sebagai cadangan tafsiran bagi menghubungkan perbincangan jurang digital dengan penggunaan mekanisme keselamatan siber; istilah ini bukan konstruk baharu yang telah disahkan dalam kajian. Kesimpulan teori perlu dibatasi oleh reka bentuk keratan rentas dan pertindihan empirikal antara literasi digital dengan persepsi pelaksanaan dasar. Gabungan Teori Pembelajaran Sosial dengan Teori Pembinaan Realiti Sosial memberikan penjelasan yang lebih menyeluruh tentang hubungan tersebut. Teori Pembelajaran Sosial menerangkan bagaimana amalan menyemak, melindungi maklumat dan menggunakan saluran rasmi dipelajari melalui pemerhatian, pengalaman dan pengukuhan sosial (Bandura, 1986). Teori Pembinaan Realiti Sosial pula menerangkan bagaimana rakyat mengenali kesahihan, autoriti dan identiti institusi melalui bahasa, simbol serta interaksi sosial (Berger & Luckmann, 1966). Gabungan kedua-dua teori menunjukkan bahawa komunikasi keselamatan siber mempunyai dimensi tingkah laku dan simbolik. Rakyat perlu mempelajari tindakan perlindungan yang betul dan pada masa yang sama mampu menilai sama ada simbol, bahasa dan identiti institusi yang digunakan dalam sesuatu komunikasi benar-benar sah. Tadbir urus keselamatan siber dengan itu perlu membina kemahiran praktikal sambil memastikan komunikasi rasmi mudah dikenal pasti, konsisten dan dipercayai.

Limitasi dan Cadangan Kajian Masa Hadapan

Kajian ini mempunyai beberapa limitasi yang perlu diambil kira. Pertama, penggunaan reka bentuk keratan rentas tidak membolehkan hubungan sebab-akibat ditentukan secara muktamad. Literasi digital diukur selepas responden mengalami penipuan siber dan membuat laporan polis. Oleh itu, tidak dapat dipastikan sama ada tahap literasi digital mempengaruhi pengalaman serta persepsi mereka atau telah berubah akibat pengalaman menjadi mangsa dan proses pelaporan. Kedua, pensampelan bertujuan hanya melibatkan mangsa yang telah membuat laporan polis. Dapatan kajian tidak mewakili semua pengguna Internet, mangsa yang tidak membuat laporan atau individu yang menerima percubaan penipuan tetapi tidak mengalami kerugian. Mangsa yang membuat laporan juga mungkin berbeza daripada mangsa yang tidak melapor dari segi tahap kesedaran, keyakinan terhadap institusi dan kesediaan mendapatkan bantuan. Ketiga, semua konstruk diukur menggunakan laporan sendiri. Oleh itu, jawapan mungkin dipengaruhi oleh ingatan, persepsi, kecenderungan sosial dan penilaian sendiri responden. Persepsi terhadap pelaksanaan dasar juga tidak mewakili prestasi objektif institusi seperti kepantasan tindak balas, kadar penyelesaian kes atau keberkesanan penguatkuasaan. Keempat, HTMT antara literasi digital dengan persepsi terhadap pelaksanaan dasar ialah 0.952, dengan sela keyakinan bootstrap 95% [0.922, 0.975]. Nilai dan keseluruhan sela tersebut melebihi ambang 0.90. Oleh itu, kesahan diskriminan bagi pasangan konstruk ini belum dapat dipastikan dengan memadai, walaupun kriteria Fornell–Larcker dipenuhi.

Pertindihan kandungan item mungkin menyumbang kepada pekali laluan, saiz kesan dan kesan tidak langsung yang tinggi. Dapatan memerlukan pengesahan melalui pemurnian ukuran dan analisis yang menilai keteguhan keputusan terhadap spesifikasi pengukuran alternatif. Kelima, langkah prosedural seperti jaminan kerahsiaan, penggunaan bahasa yang jelas dan pengasingan konstruk telah digunakan untuk mengurangkan bias kaedah sepunya. Namun, kajian tidak menggunakan sumber data bebas, penanda kaedah atau ukuran objektif yang dapat menilai bias tersebut secara lebih langsung.

Kajian masa hadapan perlu memperhalus indikator literasi digital dan pelaksanaan dasar supaya keupayaan individu dapat dibezakan dengan lebih jelas daripada ciri institusi. Model pengukuran alternatif boleh dibandingkan, termasuk model faktor peringkat lebih tinggi atau pemisahan antara pengetahuan saluran, penggunaan saluran dan penilaian terhadap prestasi saluran. Penyelidikan seterusnya juga perlu menggabungkan data persepsi dengan indikator objektif seperti rekod penggunaan perkhidmatan, tempoh tindak balas, bilangan rujukan antara agensi dan kadar penyelesaian laporan. Perbandingan antara mangsa yang membuat laporan dengan mangsa yang tidak melapor juga dapat menjelaskan peranan kepercayaan institusi, literasi digital dan halangan penggunaan saluran rasmi. Reka bentuk longitudinal boleh digunakan untuk menilai perubahan literasi digital sebelum dan selepas pengalaman penipuan atau penyertaan dalam program latihan. Analisis kumpulan pula boleh meneliti perbezaan mengikut umur, pendidikan, lokasi, pengalaman digital dan jenis penipuan. Penggunaan data berbilang sumber, indikator tingkah laku dan ukuran prestasi institusi dapat mengurangkan pergantungan kepada laporan sendiri serta memberikan penilaian yang lebih kukuh terhadap pelaksanaan dasar keselamatan siber.

Kesimpulan

Dalam sampel 500 mangsa penipuan siber yang telah membuat laporan polis, literasi digital mempunyai hubungan positif dengan persepsi terhadap pelaksanaan dasar keselamatan siber. Kesan tidak langsung orientasi sosiobudaya melalui literasi digital adalah signifikan, manakala hubungan langsung orientasi sosiobudaya dengan persepsi tersebut tidak signifikan. Corak ini menyokong penelitian lanjut terhadap peranan keupayaan digital dalam menghubungkan konteks sosiobudaya dengan penilaian rakyat terhadap mekanisme perlindungan institusi. Namun, hubungan ini tidak membuktikan sebab-akibat atau keberkesanan objektif dasar. Nilai HTMT yang tinggi turut mengehadkan keteguhan tafsiran hubungan dan pengantaraan yang dilaporkan. Dari sudut pelaksanaan, dapatan memberikan alasan untuk menilai komunikasi berasaskan tindakan, saluran pelaporan mesra pengguna dan latihan literasi digital berasaskan senario. Keberkesanan cadangan tersebut perlu diuji melalui pengalaman pengguna, ukuran tingkah laku dan petunjuk prestasi institusi. Pendekatan ini membolehkan usaha memperbaiki perlindungan awam mengambil kira keupayaan pengguna tanpa menyalahkan mangsa atau menganggap identiti budaya sebagai punca kelemahan digital.

Penghargaan:	Penulis merakamkan penghargaan kepada Jabatan Siasatan Jenayah Komersial, Polis Diraja Malaysia atas kerjasama yang diberikan dalam pelaksanaan kajian. Penghargaan turut diberikan kepada semua responden yang berkongsi pengalaman mereka bagi tujuan akademik.
Penyataan Pembiayaan:	Kajian ini tidak menerima sebarang pembiayaan luar.
Pernyataan Konflik Kepentingan:	Penulis mengisytiharkan bahawa tiada konflik kepentingan berkaitan penerbitan artikel ini. Semua penulis telah menyumbang kepada kajian dan meluluskan versi akhir manuskrip untuk penyerahan kepada International Journal of Law, Government and Communication (IJLGC).
Pernyataan Etika:	Kajian ini telah dijalankan selaras dengan piawaian etika penyelidikan. Semua prosedur yang melibatkan responden manusia telah disemak dan diluluskan oleh Jawatankuasa Etika Penyelidikan Universiti Kebangsaan Malaysia dengan nombor kelulusan JEP-2025-589. Kebenaran kerja lapangan diperoleh melalui rujukan UKM.IKE.600-4/6 (P153634). Persetujuan bermaklumat diperoleh daripada semua responden sebelum pengumpulan data. Penyertaan adalah secara sukarela, manakala kerahsiaan dan ketanpanamaan responden dipelihara. Data digunakan semata-mata bagi tujuan akademik.
Pernyataan Sumbangan Penulis:	Adi Sofuan bin Md Yusof bertanggungjawab terhadap pengkonsepan, penyiasatan, pengumpulan data, analisis formal dan penyediaan draf asal. Mohd Sobhi bin Ishak menyumbang kepada pengkonsepan, metodologi, penyeliaan utama, pengesahan, pentafsiran dapatan, semakan kritikal dan penyuntingan manuskrip. Zafari Zulkifli menyumbang melalui penyeliaan bersama, kepakaran dalam kriminologi dan siasatan jenayah komersial, pengesahan konteks institusi, pentafsiran implikasi dasar serta semakan kritikal manuskrip. Semua penulis telah membaca dan meluluskan versi akhir manuskrip sebelum penyerahan.
Pengisytiharan Penggunaan Kecerdasan Buatan (AI)	Penulis mengisytiharkan bahawa kecerdasan buatan (AI) generatif atau teknologi berbantuan AI telah digunakan semasa penyediaan manuskrip ini. Alat/perisian AI berikut telah digunakan: ChatGPT. Alat/perisian tersebut digunakan untuk penyuntingan bahasa, penambahbaikan tatabahasa dan terjemahan. Semua kandungan yang dihasilkan atau dibantu oleh AI telah disemak dan disahkan oleh penulis. Penulis bertanggungjawab sepenuhnya terhadap ketepatan, keaslian, integriti dan kandungan akhir manuskrip ini.

Rujukan

- Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). COVID-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic. *IEEE Access*, 9, 121916–121929. <https://doi.org/10.1109/ACCESS.2021.3109091>
- Alcántara-Pilar, J. M., del Barrio-García, S., & Porcu, L. (2013). A cross-cultural analysis of the effect of language on perceived risk online. *Computers in Human Behavior*, 29(3), 596–603. <https://doi.org/10.1016/j.chb.2012.10.021>
- Alcántara-Pilar, J. M., del Barrio-García, S., & Rodríguez-López, M. E. (2018). Does language matter? A cross-national comparison of the moderating effect of language on website information-processing. *Journal of Business Research*, 88, 66–78. <https://doi.org/10.1016/j.jbusres.2018.03.011>
- Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018). An exploratory study of current information security training and awareness practices in organizations. In *Proceedings of the 51st Hawaii International Conference on System Sciences* (pp. 5085–5094). <https://doi.org/10.24251/HICSS.2018.635>
- Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv*. <https://doi.org/10.48550/arXiv.1901.02672>
- Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Prentice-Hall.
- Berger, P. L., & Luckmann, T. (1966). *The social construction of reality: A treatise in the sociology of knowledge*. Anchor Books.
- Chishty, S. K., Al Qahtani, S., Sayari, S., Alam, S., & Alvi, A. M. (2025). Cybersecurity strategies and service quality in mobile payments: The moderating role of fintech literacy in building customer trust. *International Journal of Safety and Security Engineering*, 15(8), 1681–1689. <https://doi.org/10.18280/ijss.150813>
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE.
- de Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology*, 41(8), 1796–1808. <https://doi.org/10.1080/0144929X.2021.1905066>
- Department of Statistics Malaysia. (2025). *ICT use and access by individuals and households survey report, 2024*. <https://www.dosm.gov.my/portal-main/release-content/ict-use-and-access-by-individuals-and-households-survey-report-2024>
- DeVellis, R. F. (2017). *Scale development: Theory and applications* (4th ed.). SAGE.
- Dupont, B. (2019). Enhancing the effectiveness of cybercrime prevention through policy monitoring. *Journal of Crime and Justice*, 42(5), 500–515. <https://doi.org/10.1080/0735648X.2019.1691855>
- Economic Planning Unit. (2021). *Malaysia digital economy blueprint*. Prime Minister's Department. <https://www.ekonomi.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf>
- e-Governance Academy. (n.d.). *National Cyber Security Index* [Live database].
- Elrayah, M., & Jamil, S. (2023). Impact of digital literacy and online privacy concerns on cybersecurity behaviour: The moderating role of cybersecurity awareness. *International Journal of Cyber Criminology*, 17(2), 166–187. <https://doi.org/10.5281/zenodo.4766711>

- Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1–4. <https://doi.org/10.11648/j.ajtas.20160501.11>
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39–50. <https://doi.org/10.1177/002224378101800104>
- Graham, R., & Triplett, R. (2017). Capable guardians in the digital environment: The role of digital literacy in reducing phishing victimization. *Deviant Behavior*, 38(12), 1371–1382. <https://doi.org/10.1080/01639625.2016.1254980>
- Guermat, A. M. E., & Boubekri, A. E. (2026). Bridging digital divides: The correlation between critical digital literacy and intercultural communicative competence. In *Addressing digital divides in international higher education*. IGI Global. <https://doi.org/10.4018/979-8-3373-6911-2.ch012>
- Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). SAGE.
- Hanoch, Y., & Wood, S. (2021). The scams among us: Who falls prey and why. *Current Directions in Psychological Science*, 30(3), 260–266. <https://doi.org/10.1177/0963721421995489>
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115–135. <https://doi.org/10.1007/s11747-014-0403-8>
- Johanson, G. A., & Brooks, G. P. (2010). Initial scale development: Sample size for pilot studies. *Educational and Psychological Measurement*, 70(3), 394–400. <https://doi.org/10.1177/0013164409355692>
- Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *Information Systems Journal*, 28(1), 227–261. <https://doi.org/10.1111/isj.12131>
- Krishna, B., Krishnan, S., & Sebastian, M. P. (2025). Understanding the process of building institutional trust among digital payment users through national cybersecurity commitment trustworthiness cues: A critical realist perspective. *Information Technology & People*, 38(2), 714–756. <https://doi.org/10.1108/ITP-05-2023-0434>
- Li, P., Li, Q., & Du, S. (2024). Does digital literacy help residents avoid becoming victims of frauds? Empirical evidence based on a survey of residents in six provinces of east China. *International Review of Economics & Finance*, 91, 364–377. <https://doi.org/10.1016/j.iref.2024.01.056>
- Likert, R. (1932). A technique for the measurement of attitudes. *Archives of Psychology*, 22(140), 1–55.
- Lynn, M. R. (1986). Determination and quantification of content validity. *Nursing Research*, 35(6), 382–385.
- Ng, W. (2012). Can we teach digital natives digital literacy? *Computers & Education*, 59(3), 1065–1078. <https://doi.org/10.1016/j.compedu.2012.04.016>
- Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.
- OECD. (2020). *The OECD digital government policy framework: Six dimensions of a digital government* (OECD Public Governance Policy Papers No. 02). OECD Publishing. <https://doi.org/10.1787/f64fed2a-en>
- Phinney, J. S. (1992). The Multigroup Ethnic Identity Measure: A new scale for use with diverse groups. *Journal of Adolescent Research*, 7(2), 156–176. <https://doi.org/10.1177/074355489272003>

- Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879–903. <https://doi.org/10.1037/0021-9010.88.5.879>
- Ringle, C. M., Wende, S., & Becker, J.-M. (2024). *SmartPLS 4*. SmartPLS. <https://www.smartpls.com>
- Rubio, D. M., Berg-Weger, M., Tebb, S. S., Lee, E. S., & Rauch, S. (2003). Objectifying content validity: Conducting a content validity study in social work research. *Social Work Research*, 27(2), 94–104. <https://doi.org/10.1093/swr/27.2.94>
- Sarstedt, M., Ringle, C. M., & Hair, J. F. (2021). Partial least squares structural equation modeling. In C. Homburg, M. Klarmann, & A. Vomberg (Eds.), *Handbook of market research* (pp. 587–632). Springer. https://doi.org/10.1007/978-3-319-57413-4_15
- Satar, M., Seedhouse, P., Kharrufa, A., Ganassin, S., Dooly, M., Peña, J. B., Öztekin, E., Akcan, S., & Haznedar, B. (2025). Migrants' digital skills development: Engaging with and creating digital cultural activities on the ENACT web app. *ReCALL*, 37(2), 191–214. <https://doi.org/10.1017/S0958344024000351>
- Tang, C. M., & Chaw, L. Y. (2016). Digital literacy: A prerequisite for effective learning in a blended learning environment? *Electronic Journal of e-Learning*, 14(1), 54–65.
- Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, 2, 53–55. <https://doi.org/10.5116/ijme.4dfb.8dfd>
- Thani, S. M. S. A., Raut, J., & Tomašević, V. (2026). The role of digital literacy in shaping cybersecurity awareness across young generations in the United Arab Emirates. *Applied Sciences*, 16(10), 5027. <https://doi.org/10.3390/app16105027>
- United Nations Department of Economic and Social Affairs. (2024). *UN e-government survey 2024: Accelerating digital transformation for sustainable development*. United Nations. <https://desapublications.un.org/publications/un-e-government-survey-2024>
- van Deursen, A. J. A. M., & van Dijk, J. A. G. M. (2014). The digital divide shifts to differences in usage. *New Media & Society*, 16(3), 507–526. <https://doi.org/10.1177/1461444813487959>
- Vedung, E. (1997). *Public policy and program evaluation*. Routledge. <https://doi.org/10.4324/9781315127767>
- Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The digital competence framework for citizens—With new examples of knowledge, skills and attitudes*. Publications Office of the European Union. <https://doi.org/10.2760/115376>
- Wu, D., Fan, S., Yao, S., & Xu, S. (2023). An exploration of ethnic minorities' needs for multilingual information access of public digital cultural services. *Journal of Documentation*, 79(1), 1–20. <https://doi.org/10.1108/JD-12-2021-0238>
- Yoo, B., Donthu, N., & Lenartowicz, T. (2011). Measuring Hofstede's five dimensions of cultural values at the individual level: Development and validation of CVSCALE. *Journal of International Consumer Marketing*, 23(3–4), 193–210. <https://doi.org/10.1080/08961530.2011.578059>