

TAHAP KEYAKINAN MELINDUNGI DIRI REMAJA TERHADAP JENAYAH SCAM: ANALISIS INDEKS

Fidlizan Muhammad^{*1} Nik Nur Ainsyah Mohd Radzuan², Siti Zulaikha Zainudin³, Ahmad Zakirullah
Mohamed Shaarani⁴ & Salwa Amirah Awang⁵

^{1,2,3,4} Fakulti Pengurusan dan Ekonomi, Universiti Pendidikan Sultan Idris,
Tanjong Malim, Perak

²Politeknik Sultan Azlan Shah, Behrang Stesen, Perak.

ABSTRAK

Jenayah *scam* di Malaysia mencatatkan peningkatan membimbangkan dalam bilangan kes dan nilai kerugian. Pihak berkuasa telah melaksanakan pelbagai kempen dan strategi untuk mengatasi isu dan mendidik masyarakat menangani jenayah ini. Persoalannya, sejauh mana masyarakat khususnya golongan muda peduli mengenai bahaya jenayah *scam* ini. Keterdedahan dengan teknologi dan sasaran sebagai mangsa baru penjenayah telah mendorong pengkaji untuk memilih golongan belia berumur 18 hingga 25 tahun sebagai responden kajian. Penyelidikan ini menggunakan pendekatan kuantitatif melalui instrumen soal selidik yang diadaptasi bagi mendapatkan data kajian. Data kajian ini dianalisis menggunakan kaedah deskriptif iaitu kekerapan dan peratus, manakala analisis indeks pula diaplikasikan bagi mengukur tahap pengetahuan jenis *scam* mengikut jantina, umur dan secara keseluruhan. Hasil kajian mendapati pemancangan data dan pemangsaan berlaku melalui tiga medium media sosial iaitu Telegram, Facebook dan Instagram. Malah, dua elemen utama digunakan oleh pejenayah bagi menjayakan modus operandi *scam* iaitu menawarkan hadiah lumayan dan kesegeraan membuat tindakan. Sebaliknya, *scam cash on delivery* (COD) dan pelaburan merupakan dua jenis *scam* yang kurang diyakini oleh responden mengikut kategori jantina, umur dan secara keseluruhannya. Implikasinya, kajian ini mencadangkan agar golongan muda perlu diberi pendedahan mengenai jenayah *scam* secara berterusan. Justeru, pendidikan berkaitan teknologi selamat khususnya merupakan elemen yang perlu diberi fokus bagi memastikan pengguna mengetahui kaedah untuk melindungi diri dan keselamatan data daripada penjenayah dalam talian.

Kata Kunci: *scam*; golongan muda; pendidikan; pengetahuan; keselamatan; indeks keyakinan

ABSTRACT

Scam-related crime in Malaysia has shown an alarming increase in both the number of cases and the amount of financial loss. Authorities have implemented various campaigns and strategies to address the issue and to educate the public on how to deal with such crimes. The question remains: to what extent does the public, particularly the youth, care about the dangers of scam crimes? The exposure to technology and the increasing trend of youth being targeted as new victims have led researchers to select young individuals aged 18 to 25 as the study's respondents. This research employed a quantitative approach using a questionnaire instrument adapted to collect the study data. The data were analyzed using descriptive methods, namely frequencies and percentages, while an index analysis was applied to measure the level of knowledge about different types of scams by gender, age, and overall. The findings revealed that data phishing and victimization occur through three main social media platforms: Telegram, Facebook, and Instagram. Furthermore, two key elements are commonly used by scammers in executing their modus operandi—offering attractive rewards and creating a sense of urgency to act. In contrast, scams involving cash on delivery (COD) and investment were the least believed types of scams among respondents across gender, age, and overall categories. The implication of this study is that young people should be continuously exposed to information about scam-related crimes. Therefore, education focused specifically on safe technology practices is essential to ensure users are equipped with knowledge on how to protect themselves and their data from online criminals.

Keywords: scam, young generation, education, knowledge, security; confidence index

1. PENGENALAN

Scam merupakan jenayah yang dilakukan pemangsa menggunakan pelbagai taktik memanipulasi psikologi mangsa untuk percaya dengan informasi yang disebarkan (Hidajat et al., 2020). Antara taktik sering digunakan pemangsa adalah membina hubungan akrab sebelum menjerat mangsa dengan pelbagai tipu daya (Couch et al., 2012), menawarkan habuan atau kadar pinjaman istimewa (Chariri et al., 2018), menghantar pautan (*link*) melalui email, SMS untuk mencuri maklumat peribadi atau kewangan, penyamaran sebagai figura berautoriti (Wilson et al., 2023) seperti polis, pegawai kastam atau cukai, dan pelbagai taktik lain.

Kajian oleh Global Anti-Scam Alliance (GASA) dan *Scam Adviser* pada tahun 2023 mendedahkan bahawa 25.5 peratus penduduk dunia terjerumus sebagai mangsa *scam* membabitkan kerugian keseluruhan USD1.026 trilion dengan tiga faktor dominan telah dikenalpasti iaitu tertarik dengan tawaran, tidak mengetahui kewujudan jenayah *scam*, dan kurang pengetahuan mengenai taktik *scam* (GASA, 2023). Penganalisis jenayah di Malaysia, Kamal Affandi mengkategorikan jenayah *scam* kepada enam jenis atau 6P iaitu percintaan, produk, pangkat palsu, perkhidmatan, pekerjaan dan pelaburan (Mukhriz, 2022). Menurut beliau lagi, taktik *scam* melalui pautan (*link*) merupakan faktor penyumbang utama jenayah ini. Pemangsa mencerooboh ke dalam sistem teknologi (telefon bimbit dan aplikasi) mangsa, mencuri dengar dan merakam butiran dan perbualan mangsa sebagai bahan ugutan. Keadaan ini menyebabkan mangsa enggan melaporkan kepada pihak berkuasa atas faktor keselamatan dan status diri.

Di Malaysia, keparahan jenayah ini dikategorikan pada tahap '*scamdemic*' (Hasimi, 2023) di mana bilangan kes dan nilai kerugian dilaporkan semakin serius. Antara tahun 2018 hingga 2023, nilai kerugian terkumpul berjumlah RM2.3 bilion (Mohd Fadhli, 2023) dengan tahun 2023 mencatatkan nilai kerugian berjumlah RM1.3 bilion, iaitu meningkat sebanyak RM500 juta berbanding tahun 2022, dan bilangan kes pula meningkat sebanyak 37 peratus (Nurqalby, 2023). Menurut pihak berkuasa, angka-angka ini diunjur lebih tinggi disebabkan terdapat sebilangan mangsa yang tidak melaporkan kes atas sebab tertentu (Nurqalby, 2023; Marzuki, 2023). Kajian Ipsos (2023) di Malaysia menyokong dakwaan ini dengan mendapati terdapat 12 peratus mangsa tidak melaporkan kes *scam* kepada pihak berkuasa.

Pemerhatian dalam laporan akhbar yang dikumpulkan oleh Persatuan Bank-Bank Dalam Malaysia (ABM) melalui laman sesawang berkaitan kes-kes *scam* pada bulan Januari 2024 menunjukkan terdapat lima (5) kes yang berlaku. Kes-kes berkenaan dapat diringkaskan dalam Jadual 1.

Jadual 1: Kes-kes *Scam* Bulan Januari 2024

Tarikh Akhbar	Nilai Kerugian	Punca
3 Januari	RM1.08 juta	Menyamar pegawai polis
11 Januari	RM1 Juta	Menyamar pegawai polis
11 Januari	RM 540 ribu	Menyamar pegawai polis
22 Januari	RM 49 ribu	Menyamar Pegawai BNM
31 Januari	RM 260 ribu	Menyamar Pegawai NSRC

Sumber: <https://www.abm.org.my/safe-online-banking/scam-alerts-listing/>

Berdasarkan Jadual 1, nilai kerugian tertinggi dicatatkan adalah RM1.08 juta, dan kerugian terkecil pula adalah RM49 ribu. Dalam kesemua kes dilaporkan, teknik pemangsa menyamar sebagai figura berautoriti merupakan modus berkesan memanipulasi mangsa untuk mengikuti arahan yang diberikan. Senario ini menunjukkan wujud lompong dalam pengetahuan dan kesedaran masyarakat berkaitan taktik pemangsa dalam jenayah *scam*.

Rentetan itu, kecanggihan teknologi semata, tidak menjamin individu untuk merasa selamat daripada jenayah *scam*. Muniandy et al. (2016) mendapati, kepelbagaian jenis teknologi dan aplikasi menyebabkan masyarakat mengambil mudah dalam menjaga keselamatan data seperti

kata laluan, nombor pin, akaun bank dan sebagainya. Gavet et al. (2017) menyokong senario ini dan mendapati sikap terlalu yakin dengan keselamatan IT menyebabkan pemangsa mampu memanipulasi modus operandi berdasarkan tahap literasi teknologi mangsa. Amalan digital seperti berkongsi cerita, gambar, perbincangan, mencari bahan berita dan sebagainya oleh pengguna internet dan media sosial tanpa kawalan memudahkan pemangsa untuk mengenalpasti kelebihan dan kekurangan mangsa (Cross & Layt, 2022; Azianura et al., 2019). Pada tahun 2022, pautan (*link*) yang dihantar pemangsa melalui email, SMS dan media sosial merupakan strategi yang dominan memerangkap mangsa. Ironinya, unsur hadiah telah mempengaruhi sebahagian mangsa untuk menekan atau mengklik pautan berkaitan walaupun mengetahui ia adalah *scam* (Halevi et al. 2013).

Bagi mengatasi isu ini, penerapan pengetahuan secara berterusan mengenai *scam* adalah signifikan untuk semua peringkat. Golongan muda melibatkan remaja dan belia khususnya perlu dididik bagi memastikan elemen emosi, sosial dan ekonomi generasi ini selamat daripada jenayah *scam*. Keterdedahan golongan muda dengan teknologi memberikan satu soalan tentang kepedulian mereka terhadap isu ini. Isu kepedulian jenayah *scam* ini adalah mustahak memandangkan pihak berkuasa seperti Polis Diraja Malaysia (PDRM), Bank Negara Malaysia (BNM) dan institusi kewangan dan perbankan, Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) telah menyebarkan informasi jenayah *scam* ini melalui media cetak dan media elektronik. Medium penyampaian maklumat ini adalah sejajar dengan teknologi digunakan oleh golongan muda. Walaupun statistik mangsa *scam* menunjukkan penglibatan golongan muda amat sedikit, namun ia tidak boleh dipandang mudah. Raja Noraina (2022) melaporkan bahawa terdapat tanda-tanda yang dikenal pasti oleh pihak berkuasa mengenai sasaran pemangsa terhadap golongan muda sebagai mangsa atau rekrut baru kumpulan. Selain itu, kecenderungan orang muda untuk hidup mewah mendorong golongan ini mencuba pelbagai kaedah yang dapat memenuhi kehendak mereka. Keadaan ini menyebabkan sebahagian orang muda dikenal pasti melabur dalam skim tertentu dan terdedah sebagai mangsa jenayah (Jamaliah, 2024).

Sehubungan itu, kajian ini cuba untuk mengenal pasti tahap keyakinan berhadapan dengan pelbagai jenis *scam* yang berlaku kini dalam kalangan orang muda. Bagi membincangkan perkara ini, makalah ini disusun seperti berikut. Bahagian berikutnya iaitu kedua menerangkan mengenai kajian lepas, disusuli metodologi dan hasil analisis pada bahagian ketiga dan keempat. Bahagian akhir pula adalah kesimpulan kajian.

2. KAJIAN LEPAS

Penelitian penyelidikan lepas berkaitan jenayah *scam* dapat dibahagikan kepada dua bahagian. Bahagian pertama ialah penyelidikan empirikal yang meneliti faktor-faktor penyebab signifikan kepada berlakunya sesuatu jenayah *scam*, manakala bahagian kedua pula adalah penyelidikan berbentuk profil. Ia melibatkan analisis deskriptif yang mencirikan profil mangsa, strategi pemangsa dan sebagainya.

Antara kajian yang meneliti jenayah *scam* dalam bahagian pertama secara spesifik di Malaysia adalah Khadijah et al. (2020), Zulkufli dan Azmi (2019), Azianura et al. (2019), Khadijah et al. (2018) dan Nor Azlina et al. (2018) berkaitan *scam* cinta, Mohd Irwan et al. (2022) dan Masnita et al. (2021) mengenai *scam* akaun bank, Kasim et al. (2023), Azman (2017) dan Hazlina et al. (2021) pula mengenai *scam* pelaburan, *scam* pembelian atas talian oleh Nor Hasaliza et al. (2023) dan *scam* umrah oleh Nurul Ain dan Faezi, (2019). Penyelidikan bahagian kedua pula dilaksanakan pihak industri atau organisasi tertentu seperti Global Anti-Scam Alliance (GASA) dan Scam Adviser (<https://www.gasa.org/resources>), IPSOS (<https://www.ipsos.com/en-my>), dan ScamWatch (<https://www.scamwatch.gov.au/>).

Secara empirikal, dikenal pasti beberapa faktor penting menyumbang kepada jenayah *scam*. Pertama, teknik penyamaran yang disesuaikan dengan bentuk *scam* yang dilakukan oleh

pemangsa. Dalam *scam* cinta, Couch et al. (2012) dan Azianura et al. (2019) mendapati pemangsa menyamar dalam tiga tahap iaitu memikat, menjalin hubungan dan memanipulasi mangsa. Dalam ketiga-tiga tahap ini, mangsa tidak menyedari pemangsa mengumpulkan maklumat peribadi yang dimanipulasi sebagai bahan pujukan atau ugutan bagi mendapatkan wang. Zulkufli dan Azmi (2019) dan Khadijah et al. (2018) mendapati profil mangsa *scam* cinta merupakan individu yang kesunyian dan gemar bersosial (*extraversion*). Empat kriteria mangsa *scam* cinta dirumuskan oleh Whitty (2015) iaitu mencari sensasi, kepercayaan romantis, ciri peribadi dan kesunyian. Penyamaran pemangsa sebagai individu yang berautoriti dari agensi kerajaan atau korporat tertentu seperti pegawai polis, pegawai cukai, pegawai bank dan lain-lain juga banyak memerangkap mangsa *scam*. Identiti palsu ini digunakan pemangsa bagi menunjukkan kredibiliti yang mampu menakutkan dan menakutkan mangsa untuk bertindak selari dan segera dengan arahan mereka (Wilson et al., 2023).

Faktor kedua pula ialah sikap masyarakat yang mudah percaya dan terlalu yakin dengan kemampuan diri sendiri. Dalam *scam* umrah, pengiklanan oleh individu atau agensi dengan tawaran harga murah, penginapan selesa, jarak dekat, bimbingan mutawif popular dan sebagainya telah melalaikan mangsa membuat siasatan lanjut kesahihan pakej berkaitan (Nor Azaruddin Husni, 2022; NurulAin & Faezi, 2019). Tawaran atau hadiah merupakan strategi pemangsa untuk meningkatkan sikap yakin pengguna dalam kebanyakan jenayah *scam* (Halevi et al., 2013). Selain itu, kekerapan email, SMS dan panggilan telefon yang diterima mangsa menyebabkan mangsa berasa takut dan seterusnya menurut arahan yang diberikan (Atkins & Huang, 2013). Muniandy et al. (2016) dan Gavet et al. (2017) pula mendapati sikap terlalu yakin dengan diri sendiri merupakan antara punca menyebabkan sebahagian pengguna siber tidak menitikberatkan aspek keselamatan data. Antaranya ialah penggunaan maklumat peribadi sebagai kata laluan, menekan atau mengklik pautan (*link*) diterima, muat turun aplikasi atau malware yang tidak digunakan dan sebagainya.

Faktor ketiga pula berkaitan literasi atau pengetahuan masyarakat mengenai jenayah *scam* melibatkan taktik dan kaedah perlindungan diri. Dalam menangani isu ini, literasi mengenai keselamatan data peribadi ketika menggunakan teknologi dan siber adalah penting. Aktiviti mencari pasangan, berkongsi gambar atau cerita, melaksanakan urusan ~~atas~~ dalam talian, mencari bahan berita atau maklumat dan sebagainya memerlukan pengguna mengetahui ciri-ciri laman sesawang atau platform yang asli (Ernawati et al., 2023; Khadijah et al., 2020, Zahari et al., 2019; Naksawat et al., 2016; Foozy et al., 2014). Aspek keselamatan dan perlindungan data perlu diketahui pengguna dengan baik bagi memastikan aktiviti dilakukan adalah selamat (Wilson et al., 2023; Puram et al., 2011). Gaya bahasa, perkataan dan imej yang diiklankan menyerupai jenayah *scam* wajar diketahui oleh pengguna sebagai perisai awal melindungi diri daripada terjerumus sebagai mangsa isu ini (Naksawat et al., 2016). Memandangkan literasi atau pendidikan pengetahuan *scam* ini signifikan bagi melindungi masyarakat, beberapa elemen perlu diberi fokus telah dicadangkan oleh beberapa pengkaji lepas. Antaranya ialah kaedah penggunaan teknologi dan siber dengan selamat (Wei et al., 2021; Teitcher et al., 2015), kaedah penyimpanan dan perkongsian data (Robb & Wendel, 2023; Baruh & Popescu, 2017), dan kaedah menyelesaikan dan menangani masalah *scam* (Devahish, 2022).

Melalui penyelidikan lepas oleh pihak industri pula, beberapa dapatan penting mengenai profil jenayah *scam* yang berlaku di Malaysia telah dilaksanakan. Antaranya ialah kajian oleh Global Anti-Scam Alliance (GASA) dan *Scam Adviser* pada tahun 2023 melibatkan 50 ribu responden di 43 buah negara. Secara umum, kajian ini mendapati 25.5 peratus penduduk dunia terjebak sebagai mangsa *scam* membabitkan kerugian keseluruhan USD1.026 trilion (GASA, 2023). Di Malaysia, hasil dapatan profil responden menunjukkan 43 peratus responden menyatakan boleh mengenali modus operandi *scam*, 79 peratus pernah mengalami kejadian *scam*, dengan 36 peratus daripadanya mengalami kehilangan wang dengan nilai kerugian antara USD1000 ke

USD1500. Ironinya, hanya 45 peratus mangsa tampil dan melaporkan kejadian jenayah *scam* kepada pihak berkuasa.

Kajian Ipsos (2023) melibatkan 1000 responden mendapati 24 peratus responden pernah mengalami kejadian *scam*, dengan 51 peratus pernah mengalaminya dalam tempoh tiga (3) bulan lepas (September-November 2023), dan 14 peratus dalam tempoh sebulan (November 2023) terkini. Lima platform utama digunakan pemangsa ialah panggilan telefon (56%), whatsapp (54%), Facebook (31%), Telegram (30%) dan SMS (29%). Dari segi jenis *scam* pula, 40 peratus menjadi mangsa *scam* panggilan telefon, *scam* dalam talian (27%), *scam* pelaburan (24%), *scam* kerja (20%), *scam* parcel (18%) dan *scam* cinta (6%). Secara purata, 48 peratus mangsa melaporkan kejadian *scam* kepada pihak berkuasa sama ada bank, peguam, persatuan pengguna dan agensi lain, manakala 12 peratus mangsa tidak melaporkannya. Aspek pencegahan pula, 90 peratus responden mengetahui mengenai keselamatan siber, namun tindakan mengemas kini perisian keselamatan teknologi (perisian dan antivirus) terkini hanya dilakukan oleh 29 peratus pengguna. Dari segi literasi, 76 peratus mengetahui jenayah *scam*, namun hanya 32 peratus menyatakan kesediaan bertanya dengan pakar ketika berhadapan dengan isu *scam*. Manakala, 46 peratus responden menyatakan maklumat personal dan sensitif dilindungi dengan baik.

Scamwatch (2023) pula merupakan pangkalan data yang diselenggara di bawah *Australian Competition and Consumer Commission* (ACCC). Menariknya, data jenayah *scam* dilaporkan dalam bentuk bulanan dan tahunan dari tahun 2020 sehingga kini. Antara maklumat yang boleh diperolehi ialah data mengikut kategori *scam*, jumlah kerugian, kumpulan mangsa mengikut umur, mangsa mengikut gender, kategori laporan *scam* tertinggi, nilai kerugian dan lain-lain. Namun demikian, tiada data khusus bagi Malaysia diperolehi melalui pangkalan data ini. Data jenayah di Malaysia umumnya dilaporkan secara rasmi dalam Statistik Jenayah secara tahunan oleh pihak Jabatan Perangkaan Malaysia. Berdasarkan laporan, nisbah kes tipu berbanding kes-kes lain (pecah amanah, siber, dan lain-lain) dalam jenayah komersil adalah antara 89 ke 92 peratus (DOSM, 2022, 2023). Data mengenai jenayah *scam* pula banyak diperolehi melalui laporan akhbar. Contohnya, bilangan *scammer* yang ditangkap antara 2019 hingga Mei 2023 adalah 43,959 orang (Zareen Humairah, 2023), kes *scam* cinta adalah tertinggi antara tahun 2018 sehingga Jun 2023 iaitu 7548 kes, nilai kerugian RM 382 juta, 82.8 peratus mangsa adalah wanita (Farik, 2023) dan penjawat awam bekerja sebagai guru adalah mangsa paling tinggi di Johor (Bernama, 2023).

Berdasarkan penelitian kajian lepas ini, didapati informasi berkaitan profil pengetahuan atau keyakinan *scam* masih belum diteroka sepenuhnya. Pelbagai kempen dan kaedah telah dilaksanakan oleh pihak berkuasa bagi mengatasi isu dan memberi kefahaman kepada masyarakat mengenai jenayah *scam* dan tip melindungi diri. Oleh yang demikian, relevan untuk meneroka keberkesanan usaha yang dilaksanakan ini sampai kepada masyarakat bagi tujuan menambahbaik kaedah penyampaian pada masa hadapan.

3. METODOLOGI

Kajian ini dilaksanakan menggunakan pendekatan kuantitatif melalui instrumen soal selidik bagi mengumpulkan data responden. Soal selidik kajian ini dibahagikan kepada dua bahagian iaitu profil responden mengenai jantina dan umur pada Bahagian A, dan pengetahuan dan pengalaman berkaitan jenayah *scam* pada Bahagian B. Jenis-jenis *scam* ini diambil berdasarkan e-book jenayah komersil terkini yang diterbitkan oleh pihak Jabatan Siasatan Jenayah Komersil (JSJK) Polis Diraja Malaysia (PDRM) yang boleh dimuat turun melalui laman sesawang Jaringan Pendidikan Kewangan (The Financial Education Network, FEN) iaitu <https://www.fenetwork.my/trend-terkini-jenayah-komersil/>. Maklumat jenayah *scam* juga boleh diperolehi melalui laman sesawang Persatuan Bank-bank Dalam Malaysia (ABM) iaitu <https://www.abm.org.my/safe-online-banking/jangankenascam/>, Persatuan Institusi Perbankan Islam Malaysia (AIBIM) iaitu <https://aibim.com/national-scam-awareness-campaign>,

dan Bank Negara Malaysia (BNM) iaitu <https://www.bnm.gov.my/consumer-info/scam-notice>, dan Suruhanjaya Sekuriti Malaysia (SC) iaitu <https://www.sc.com.my/investor-empowerment/scam>.

Dalam kajian ini, tujuh (7) jenis *scam* diajukan kepada responden iaitu *scam* macau iaitu pemangsa menyamar sebagai figura berautoriti seperti pegawai polis, kastam atau imigresen untuk menipu mangsa, *scam* KWSP iaitu pemangsa menyamar sebagai pegawai KWSP, *scam* LHDN iaitu pemangsa menyamar sebagai pegawai cukai, *scam* cinta iaitu pemangsa menyamar sebagai kekasih, *scam* kerja iaitu pemangsa menyamar sebagai majikan atau orang tengah, *scam* *cash on delivery* (COD) atau parcel iaitu pemangsa menyamar sebagai penghantar barang, dan *scam* pelaburan iaitu pemangsa menyamar sebagai agen institusi kewangan, pelaburan dan sebagainya. Manakala, tiga (3) soalan berkaitan pengalaman responden berhadapan dengan isu *scam* iaitu platform yang digunakan pemangsa bagi mencari mangsa (GASA, 2023; Ipsos, 2023), strategi digunakan pemangsa bagi menipu mangsa (Wilson et al. 2023; Naksawat et al., 2016; Foozy et al., 2014) dan tahap keyakinan responden melindungi diri (GASA, 2023).

Pengukuran keyakinan belia melindungi diri daripada jenayah *scam* ini dilakukan dengan mengadaptasi indeks TIPP. Indeks ini dibangunkan oleh *Techonometrica Institute of Policy and Politics (TIPP)* bagi menilai sentimen atau keyakinan pengguna terhadap ekonomi dan dasar negara. Adaptasi kaedah ini turut digunakan dalam kajian berkaitan keyakinan zakat oleh Iman dan Sanep (2011). Kaedah pengiraan indeks mempunyai dua formula berpandukan kepada skala likert yang digunakan. Oleh kerana skala likert digunakan dalam instrumen kajian ini adalah tiga skala, maka kaedah pengiraan yang digunakan sebagaimana persamaan (1)

$$K_i = 50 + 0.5 (P^+ - P^-) \quad (1)$$

di mana, K ialah indeks, P⁺ bagi skala sangat yakin, dan P⁻ pula bagi skala tidak yakin. Melalui formula ini, jumlah K_i ditentukan dengan nilai 0 hingga 100. Sekiranya jumlah K_i adalah 0, ia menunjukkan responden amat tidak yakin untuk melindungi diri dengan jenayah *scam*, dan sebaliknya jika jumlahnya adalah 100 yang menunjukkan responden sangat yakin untuk melindungi diri. Klasifikasi skor indeks keyakinan adalah seperti berikut iaitu tahap keyakinan sederhana atau nilai ambang dengan nilai 50 (=50); tahap keyakinan yang baik mempunyai nilai melebihi 50 (>50) dan tahap keyakinan yang kurang baik mempunyai nilai kurang daripada 50 (<50). (TIPP staff, 2023; Iman & Sanep, 2011). Analisis keputusan indeks dilaporkan dalam dua bentuk iaitu indeks keseluruhan dan indeks mengikut jantina dan umur.

Set soal selidik diedarkan secara bersemuka dalam tempoh empat (4) bulan bermula September hingga Disember 2023. Sebanyak 450 borang soal selidik diedarkan dan 404 borang (90%) diterima dalam keadaan maklumat lengkap. Populasi kajian ini terdiri daripada golongan belia berumur 18 hingga 25 tahun yang aktif menggunakan media sosial dan menetap di kawasan bandar dan luar bandar melibatkan beberapa negeri iaitu Wilayah Persekutuan Kuala Lumpur dan Putrajaya, Selangor, Negeri Sembilan, Perak, Pulau Pinang, Johor, Kelantan, Terengganu dan Pahang. Kajian menggunakan kaedah persampelan bertujuan untuk mendapatkan responden yang berpengetahuan atau pernah terdedah kepada jenayah *scam*.

Instrumen soal selidik yang digunakan dalam kajian ini telah melalui proses penilaian kesahan kandungan oleh dua orang pakar, iaitu seorang dalam bidang undang-undang dan jenayah siber dan seorang orang dalam bidang pendidikan pengguna. Ujian kebolehpercayaan telah dijalankan melalui kajian rintis melibatkan 40 responden belia yang tidak termasuk dalam sampel utama. Hasil ujian menunjukkan nilai Cronbach's Alpha adalah 0.827 yang menandakan tahap kebolehpercayaan yang tinggi. Data yang diperolehi telah dianalisis menggunakan perisian IBM SPSS Statistics versi 29 bagi mendapatkan analisis profil responden, manakala pengiraan indeks dilakukan menggunakan Microsoft Excel.

4. HASIL KAJIAN

Hasil analisis deskriptif latar belakang responden ditunjukkan dalam Jadual 2.

Jadual 2. Profil Responden (n=404)

Maklumat	Keterangan	Kekerapan	Peratus (%)
Jantina	Lelaki	125	30.9
	Perempuan	279	69.1
Umur	18-21	220	54.5
	22-25	184	45.5

Sumber: Data Kajian

Berdasarkan Jadual 2, 69 peratus responden kajian adalah belia golongan wanita, dan 31 peratus pula adalah belia lelaki. Golongan belia berumur 18 hingga 21 tahun mewakili 54.5 peratus sampel kajian, manakala 45.5 peratus adalah belia berumur 22 hingga 25 tahun. Dari segi pengalaman berhadapan dengan jenayah *scam*, hasil analisis ditunjukkan dalam Jadual 3 hingga Jadual 5.

Jadual 3. Platform Jenayah *Scam*

Maklumat	Keterangan	Kekerapan	Peratus (%)
Pernah menerima informasi pelaburan <i>scam</i> daripada...	Telegram	350	86.6
	Facebook@Meta	204	50.5
	Instagram	183	45.3
	Tiktok	102	25.2
	Twitter@X	73	18.1
Jawapan (YA)	Iklan Youtube	163	40.3
	SMS	274	67.8

Sumber: Data Kajian

Analisis mengenai platform jenayah *scam* dalam Jadual 3 menunjukkan beberapa hasil yang penting. Dari aspek kekerapan, Telegram menjadi medium yang paling tinggi penyebaran informasi cubaan jenayah *scam* dalam kalangan responden iaitu 350 orang atau 86.6 peratus. Taktik menggunakan SMS pula menunjukkan kekerapan kedua tertinggi iaitu 274 orang (67.8%), diikuti Facebook@Meta dan Instagram pada turutan ketiga dan keempat. Seramai 163 responden (40.3%) turut mengakui menerima informasi cubaan *scam* melalui iklan Youtube, manakala platform Twitter @X menunjukkan kekerapan yang paling sedikit. Hasil analisis ini menunjukkan, pemangsa menggunakan pelbagai platform bagi mendapatkan mangsa. Rentetan kebergantungan dan keterdedahan golongan belia dengan variasi media sosial pada masa kini, maka pendedahan mengenai pengetahuan keselamatan berkaitan penggunaan teknologi bagi melindungi mereka dari terperangkap sebagai anggota atau mangsa jenayah *scam* adalah penting. Hasil analisis ini menyokong kajian Ipsos (2023) yang turut mendapati media sosial digunakan secara meluas oleh pemangsa bagi memerangkap mangsa. Bezanya, Ipsos (2023) mendapati platform Telegram sebagai turutan keempat, Facebook (ke-3), dan panggilan telefon sebagai platform utama. Hal ini tidak janggal disebabkan golongan belia didapati lebih cenderung menggunakan teks iaitu perkataan atau imej yang ringkas dalam komunikasi (Forgays et al., 2014)

Strategi yang digunakan oleh pemangsa bagi memerangkap mangsa merupakan pengetahuan yang signifikan untuk diketahui dan didedahkan secara berterusan kepada masyarakat. Ia merupakan perisai atau benteng awal bagi melindungi diri daripada terperdaya dan terjerumus dalam jenayah ini. Pendekatan yang digunakan pemangsa dalam platform media sosial ditunjukkan dalam Jadual 4.

Jadual 4. Strategi Jenayah *Scam*

Maklumat	Keterangan	Kekerapan	Peratus (%)
	Tawaran kelihatan terlalu bagus	266	65.8

Strategi Pemangsa ... Jawapan (YA)	Dakwa "Semua orang lain sudah membelinya".	260	64.4
	peluang pelaburan 'bebas risiko'	236	58.4
	Permintaan bayaran pendahuluan	218	54.0
	digesa untuk melabur sekarang atau anda akan terlepas peluang	210	52.0
	Penjual berusaha untuk mendapatkan maklumat peribadi	205	50.7
	dijanjikan pulangan besar dalam tempoh singkat	194	48.0
	Penjual agresif dengan memberikan maklumat berlebih-lebihan	172	42.6
	Bayaran dipindah ke akaun peribadi atau luar negara	147	36.4
	Mendakwa sebagai agen pelaburan berlesen	129	31.9
	dakwa sensasi dan maklumat 'orang dalam'	114	28.2

Sumber: Data Kajian

Berdasarkan Jadual 4, enam (6) strategi dominan yang mencatatkan peratus kekerapan melebihi 50 peratus, empat (4) strategi pada tahap 30 hingga 49 peratus, dan satu (1) strategi pada tahap di bawah 30 peratus. Tawaran yang terlalu bagus atau "*too good to be true*" mendominasi strategi pemangsa dengan kekerapan paling tinggi iaitu 266 responden (65.8%), diikuti strategi "Semua orang lain sudah membelinya" dan peluang pelaburan 'bebas risiko' pada kekerapan kedua dan ketiga tertinggi. Ravenelle et al. (2022) mendapati memberi tawaran yang bagus merupakan taktik popular pemangsa dalam *scam* pekerjaan ketika musim pandemik Covid19 yang lalu. Dapatan ini ditemui dalam analisis temubual dengan remaja berusia 19 tahun yang belajar dan bekerja sebagai pekerja gig yang menceritakan kejanggalan dalam tawaran kerja oleh pemangsa iaitu tiada pengalaman diperlukan, anda akan dilatih dan dibayar \$3000 sebulan. Dalam *scam* Ponzi, menawarkan pulangan yang banyak merupakan bentuk strategi pemasaran yang berkesan untuk menjadikan mangsa sebagai agen atau wakil untuk menarik mangsa lain dalam perangkap ini. Keadaan ini diteliti telah membentuk piramid dalam *scam* Ponzi yang memerangkap bilangan mangsa yang ramai dengan nilai kerugian yang tinggi (Benson, 2009; Buckhoff & Kramer, 2011)

Memandangkan pemangsa menggunakan pelbagai strategi dalam memerangkap mangsa, maka usaha meningkatkan literasi dan kesedaran masyarakat agar dapat mengenali taktik penipuan yang sering digunakan perlu digiatkan. Dalam kalangan remaja dan belia, usaha ini dapat dilaksanakan menerusi pedagogi yang sesuai dengan keperluan semasa (Hazlina et al., 2021). Jadual 5 menunjukkan gambaran keseluruhan tahap pengetahuan responden mengenai jenayah *scam*.

Jadual 5. Tahap Pengetahuan Jenayah *Scam*

Maklumat	Keterangan	Kekerapan	Peratus (%)
Tahap Pengetahuan Mengenai <i>Scam</i>	0-24	8	2.0
	25-49	14	3.5
	50-74	162	40.1
	75-100	220	54.5

Sumber: Data Kajian

Berdasarkan Jadual 5, 95 peratus responden mempunyai tahap pengetahuan *scam* yang memuaskan dengan 220 orang pada tahap amat baik (75-100) dan 162 orang pula pada tahap baik. Sebilangan kecil responden iaitu enam (6) peratus berada pada tahap kurang memuaskan di bawah 50 peratus iaitu 3.5 peratus pada tahap sederhana (25-49) dan dua peratus pada tahap lemah (0-24). Hasil ini menunjukkan bahawa, belia secara umumnya mengetahui mengenai

jenayah *scam* yang berlaku. Namun, usaha mendidik mengenai jenayah *scam* dan melindungi diri masih perlu diteruskan kerana terdapat sebahagian kecil responden yang mempunyai tahap pengetahuan minimal dan berpotensi terdedah sebagai mangsa jenayah *scam* pada masa hadapan.

Hasil analisis berikutnya menerangkan indeks keyakinan untuk melindungi diri daripada setiap jenayah *scam* berdasarkan pengetahuan yang diketahui oleh belia. Hasil ini ditunjukkan dalam Jadual 6.

Jadual 6. Indeks Keyakinan Keseluruhan Mengikut Jenis *Scam*

Jenis <i>Scam</i>	Indeks		Tidak	
	Keseluruhan	Menjawab	Menjawab	Jumlah
Macau	74.4	399	5	404
KWSP	71.1	401	3	404
LHDN	67.5	400	4	404
Cinta	65.3	398	6	404
Kerja	65.0	397	7	404
Pelaburan@Ponzi	58.4	399	5	404
COD@Parcel	53.1	399	5	404

Sumber: Data Kajian

Berdasarkan Jadual 6, didapati responden mempunyai tahap keyakinan baik untuk melindungi diri daripada kesemua bentuk jenayah *scam* dengan nilai indeks melebihi 50 (TIPP staff, 2023; Iman & Sanep, 2011). Perincian mengikut item pula mendapati dua jenis *scam* menunjukkan indeks keyakinan melebihi 70 iaitu *scam* Macau dan KWSP, tiga (3) pada indeks melebihi 60 iaitu *scam* LHDN, Cinta dan Kerja, manakala dua (2) pada indeks melebihi 50 iaitu *scam* Pelaburan dan *scam* barangan melibatkan COD dan parcel. Petunjuk indeks keyakinan yang tinggi pada *scam* Macau merupakan satu indikator yang baik terhadap usaha yang telah dilaksanakan oleh pihak berkuasa dalam membentaras jenayah *scam*. Petunjuk positif ini adalah signifikan kerana *scam* Macau merupakan jenayah *scam* yang melibatkan ramai mangsa, nilai kerugian tertinggi, modus operandi yang kerap memperdaya mangsa dan sentiasa menjadi tajuk akhbar utama (Nurul Anessa et al., 2023). *Scam* Macau yang dilaksana menggunakan panggilan telefon atau SMS melibatkan talian tempatan dan antarabangsa dengan pemangsa menyamar diri sebagai figura berautoriti merupakan taktik sering memerangkap mangsa untuk melakukan tindakan yang diarahkan pemangsa (Wilson et al., 2023). Analisis tambahan bagi indeks keyakinan dilakukan berdasarkan jantina dan umur responden, dan hasilnya ditunjukkan dalam Jadual 7 dan Jadual 8.

Jadual 7. Indeks Keyakinan Jenayah *Scam* Mengikut Jantina

Indeks Mengikut Jantina	Lelaki	Perempuan
Macau	65.6	78.3
KWSP	62.6	74.8
LHDN	61.8	70.0
Cinta	63.9	65.9
Kerja	57.4	68.4
COD@parcel	47.5	55.6
Pelaburan@Ponzi	47.5	63.2
Purata	58.04	68.03

Sumber: Data Kajian

Berdasarkan Jadual 7, secara keseluruhan atau purata didapati indeks keyakinan melindungi diri daripada jenayah *scam* bagi belia lelaki dan wanita adalah baik iaitu melebihi nilai 50. Namun, secara perbandingan pula menunjukkan indeks keyakinan mengikut jenis *scam* bagi belia wanita adalah lebih baik berbanding belia lelaki. Perbezaan ini terjadi kerana kesemua jenis *scam* bagi belia wanita menunjukkan indeks keyakinan melebihi nilai 50, manakala dua jenis *scam* iaitu COD@parcel dan pelaburan bagi belia lelaki menunjukkan nilai indeks di bawah 50 atau tidak memuaskan. Terdapat kajian yang meneliti sikap lelaki dan wanita terhadap jenayah *scam* dan mendapati wanita lebih terbuka untuk mengetahui dan melaporkan jenayah *scam* berbanding

golongan lelaki yang mengambil sikap mudah, bertindak sendirian dan berkeyakinan menyelesaikan sendiri. Keadaan ini menyebabkan ramai golongan lelaki terlibat sebagai mangsa berbanding dengan wanita (Hanoch & Wood, 2021; Whitty, 2020; Weijer et al., 2019).

Berdasarkan Jadual 8, indeks keyakinan jenayah *scam* mengikut umur belia menunjukkan nilai purata indeks yang baik iaitu melebihi nilai 50.

Jadual 8. Indeks Keyakinan Jenayah *Scam* Mengikut Umur

Indeks Mengikut Umur	Indeks (18-21 tahun)	Indeks (22-25 tahun)
Macau	80.3	67.4
KWSP	73.5	68.1
LHDN	74.8	58.8
Cinta	67.4	62.8
Kerja	72.0	56.4
COD@Parcel	55.7	50.0
Pelaburan	67.0	48.1
Purata	70.1	58.8

Sumber: Data Kajian

Secara perbandingan mengikut kategori umur, indeks keyakinan belia berumur antara 18 hingga 21 tahun lebih tinggi berbanding belia berumur 22 hingga 25 tahun. Walaupun sampel kajian ini dalam golongan belia, namun terdapat beberapa kajian lepas yang mendapati faktor usia mempunyai pengaruh positif terhadap jenayah penipuan (Sarno et al., 2020). Van Wyk dan Benson (1997) dan Titus et al. (1995) pula menjelaskan bahawa pengalaman kemandirian kehidupan mendorong individu untuk meneroka pelbagai peluang bagi meningkatkan kualiti kehidupan. Keadaan ini menyebabkan golongan yang semakin meningkat usianya untuk mencuba dan terdedah kepada risiko terjerumus sebagai mangsa.

5. KESIMPULAN

Pelbagai jenis jenayah *scam* wujud masa kini seiring dengan perkembangan teknologi dan perubahan gaya hidup manusia. Namun begitu, modus operandi pemangsa ini tidak berjaya untuk direalisasi sekiranya masyarakat mempunyai pengetahuan berkaitan taktik dan kaedah melindungi diri daripada terjebak dengan jenayah *scam*. Walaupun pelbagai usaha dan kempen telah dilaksana oleh pihak berkuasa, sejauh mana tindakan ini membuahkan hasil perlu diteliti bagi menambahbaik dan mencari ikhtiar baru untuk menangani isu ini. Hasil kajian ini menunjukkan golongan belia mempunyai tahap pengetahuan yang baik berkaitan jenayah *scam* yang berlaku kini. Selain itu, tahap keyakinan untuk melindungi diri daripada jenayah *scam* berdasarkan pengetahuan semasa yang diukur menggunakan indeks keyakinan menunjukkan hasil yang baik. Oleh yang demikian, dapatan ini membuktikan bahawa usaha yang digerakkan oleh pihak berkuasa memberi pengetahuan berkaitan jenayah *scam* turut mendapat perhatian dalam kalangan belia. Walau bagaimanapun, usaha ini perlu diteruskan dengan efektif disebabkan terdapat sebilangan kecil golongan belia yang menunjukkan tahap pengetahuan dan indeks keyakinan yang sederhana sekiranya berhadapan dengan jenayah *scam*.

Penghargaan

Penyelidikan ini mendapat peruntukan di bawah Geran Penyelidikan Fundamental Universiti (GPFU: 2021-0217-106-010) yang disediakan oleh Universiti Pendidikan Sultan Idris. Pihak penulis mengucapkan terima kasih kepada Pusat Pengurusan Penyelidikan dan Inovasi (RMIC, UPSI) atas bantuan dan sokongan yang diberikan

RUJUKAN

- Atkins, B. & Huang, W. (2013). A Study of Social Engineering in Online Frauds. *Open Journal of Social Sciences*, 1, 23-32. doi: 10.4236/jss.2013.13004
- Azianura Hani Shaari, Mohammad Rahim Kamaluddin, Wan Fariza Paizi@Fauzi & Masnizah Mohd. (2019). Online-Dating Romance Scam in Malaysia: An Analysis of Online Conversations between Scammers and Victims. *GEMA Online® Journal of Language Studies*, 19(1), 97-115
- Azman, Mohd Noor. (2017). Sharī'ah Issues in Gold Trading and Gold Related Scam Schemes. *Al-Shajarah Journal of Islamic Thought and Civilization the International Islamic University Malaysia (IIUM) Special Issue (Islamic Banking and Finance)*, 61-84.
- Baruh, L., & Popescu, M. (2017). Big data analytics and the limits of privacy self-management, *New Media & Society*, 19(4), 579-596
- Benson, S. (2009). Recognizing the red flags of a Ponzi scheme. *The CPA Journal*, 79, 19-25
- Bernama (2023). Guru paling ramai dalam kalangan penjawat awam jadi mangsa scammer di Johor – Polis. *AstroAwani*. <https://www.astroawani.com/berita-malaysia/guru-paling-ramai-dalam-kalangan-penjawat-awam-jadi-mangsa-scammer-di-johor-polis-440063?>
- Buckhoff, T.A. & Kramer, B.K.P. (2011). Conducting effective Ponzi scheme investigations. *Journal of Forensic and Investigative Accounting*, 3, 1-24.
- Chariri, A., Sektiyani, W., Nurlina, N. & Wulandari, R.W. (2018). Individual characteristics, financial literacy and ability in detecting investment scams. *Jurnal Akuntansi Dan Auditing*, 15(1), 91-114.
- Couch, D., Liamputtong, P., & Pitts, M. (2012). What are the real and perceived risks and dangers of online dating? Perspectives from online daters. *Health, Risk & Society*, 14(7-8), 697-714.
- Cross, C., & Layt, R. (2022). "I Suspect That the Pictures Are Stolen": Romance Fraud, Identity Crime, and Responding to Suspicions of Inauthentic Identities. *Social Science Computer Review*, 40(4), 955-973
- Devashish, D. 2022. The use of technology to counter frauds and scams for the benefit of society: a detailed study. *MPRA Paper* No. 115323. Available at <https://mpra.ub.uni-muenchen.de/115323/>
- DOSM (2022). Statistik Jenayah, Malaysia, 2022. <https://www.dosm.gov.my/portal-main/release-content/crime-statistics-malaysia-2022>.
- DOSM (2023). Statistik Jenayah, Malaysia, 2023. <https://www.dosm.gov.my/portal-main/release-content/crime-statistics-malaysia-2023>.
- Ernawati Abdul Wahab, Muhammad Adnan Pitchan & Ali Salman. 2023. Pengetahuan, Sikap dan Amalan Masyarakat di Kuala Lumpur Terhadap Kempen Pencegahan Jenayah Penipuan Dalam Talian. *Jurnal Komunikasi: Malaysian Journal of Communication*, 39(1), 240-258.
- Farik Zolkefli (2023). Over 7,000 love scam reported since 2018, mostly female victims. *TheStar*. <https://www.thestar.com.my/news/nation/2023/07/12/over-7000-love-scams-reported-since-2018-mostly-female-victims>.
- Foozy, C.F.M., Ahmad, R., Faizal, M.A. (2014). A framework for SMS spam and phishing detection in Malay language: A case study. *International Review on Computers and Software*, 9(7), 1248-1255.
- Forgays, D. K., Hyman, I., & Schreiber, J. (2014). Texting everywhere for everything: Gender and age differences in cell phone etiquette and use. *Computers in Human Behavior*, 31, 314-321. <https://doi.org/10.1016/j.chb.2013.10.053>.
- GASA (2023). The Global State of Scams Report (2023). <https://www.gasa.org/resources>. Retrieved on, 2 January 2024.
- Gavett, B. E. G., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *PLoS One*, 12(2), e0171620
- Halevi, T., Lewis, J. & Memon, M. (2013). Phishing, personality traits and facebook. *Cornel University, arXiv*. Available at: <https://arxiv.org/abs/1301.7643>. Accessed 11 January 2024.

- 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>
- Hasimi Muhamad (2023). Lubuk scam; Jenayah penipuan tahap 'Scamdemic', hampir 40% pernah berdepan cubaan. *Astro Awani*. <https://www.astroawani.com/berita-malaysia/lubuk-scam-jenayah-penipuan-tahap-scamdemic-hampir-40-pernah-berdepan-cubaan-446551?>
- Hazlina Mohd Padil, Eley Suzana Kasim, Salwa Muda, Norhidayah Ismail & Norlaila Md Zin. (2022). Financial literacy and awareness of investment scams among university students Accounting. *Journal of Financial Crime*, 29(1), 355-367
- Hidajat, T., Primiana, I., Rahman, S. & Febrian, E. (2020). Why are people trapped in Ponzi and pyramid schemes?. *Journal of Financial Crime*, 28(1), 187-203.
- Iman Salleh & Sanep Ahmad (2011). Indeks Keyakinan Terhadap Lembaga Zakat Selangor (LZS): Kajian Kes Kakitangan Universiti Kebangsaan Malaysia. Prosiding PERKEM VI, 5 – 7 Jun 2011, Jilid 1, 115 – 123
- Ipsos (2023). *Scam in Malaysia*- Press Release. Ipsos. <https://www.ipsos.com/en-my/press-release-scam-malaysia>. Accessed on, 10 January 2024.
- Jamaliah Abdulllah (2024). Anak muda kejar kemewahan punca ramai jadi mangsa scammer. *Utusan Malaysia*. <https://www.utusan.com.my/nasional/2024/01/anak-muda-kejar-kemewahan-punca-ramai-jadi-mangsa-scammer/> 24 Januari.
- Kasim, E.S., Awalludin, N.R., Zainal, N., Ismail, A. & Ahmad Shukri, N.H. (2023). The effect of financial literacy, financial behaviour and financial stress on awareness of investment scams among retirees. *Journal of Financial Crime* (in print)
- Khadijah Alavi, Maizatul Haizan Mahbob, & Mohammad Syahrul Azha Soood. (2020). Strategi Komunikasi Penjenayah Cinta Siber Terhadap Wanita Profesional. *Jurnal Komunikasi: Malaysian Journal of Communication*, 36(3), 296-311.
- Khadijah Alavi, Mohammad Syahrul Azha Soood & Al-Azmi Bakar. (2018). Love Scam di Selangor: Satu Penerokaan Terhadap Modus Operandi Jenayah Siber Ke Atas Wanita Profesional. *Jurnal Pembangunan Sosial*, 21 (September), 105-122.
- Marzuki Yusoff. (2023). Kenapa dibiari scammer terus berleluasa?. *SinarHarian*. <https://www.sinarharian.com.my/article/270495/suara-sinar/analisis-sinar/kenapa-dibiari-scammer-terus-berleluasa>. 28 July
- Masnita Misirana, Shi Er Tan, Pheng Hong Augustus Saw, Nur Azuin Mohd Subri, Nur Syazana Ahmad Darus, Zahayu Md Yusof & Nazihah Ahmad. 2021. Early Detection method for money fraudulent activities on e-commerce platform via sentiment analysis. *Journal of Entrepreneurship and Business*, 9(2): 121-142.
- Mohd Fadhli Mohd Sulaiman. 2023. Dewan Rakyat: RM23 bilion kerugian akibat jenayah scam. *Utusan Malaysia*. <https://www.utusan.com.my/nasional/2023/10/dewan-rakyat-rm23-bilion-kerugian-akibat-jenayah-scam/>. 18 October
- Mohd Irwan Abdul Rani, Salwa Zolkafil, & Sharifah Nazatul Faiza Syed Mustapha Nazri. (2022). Money Mule Risk Assessment: An Introductory Guidance for Financial Crime Compliance Officers. *Asian Journal of Research in Business and Management*, 4(1), 208-217
- Mukhriz Mat Husin. (2022). Jenayah 'scammer' ada enam kategori. *SinarHarian*. <https://www.sinarharian.com.my/article/224536/khas/rasuah-busters/jenayah-scammer-ada-enam-kategori>
- Muniandy, L., Muniandy, B., & Samsudin, Z. (2016). Cyber security behaviour among higher education students in Malaysia. *Journal of Information Assurance & Cyber Security*, 1-13.
- Naksawat, C., Songyut Akkakoson & Chek Kim Loi. (2016). Persuasion Strategies: Use of Negative Forces in Scam. *GEMA Online® Journal of Language Studies*, 16(1), 1-17.
- Nor Azaruddin Husni Nuruddin. 2022. Kempen Anti-Scam dan system kepercayaan individu. IKIM, <https://www.ikim.gov.my/index.php/2022/09/12/kempen-anti-scam-dan-sistem-kepercayaan-individu/>. Retrieved on 20 November 2023
- Nor Azlina Zainal Abidin, Mohammad Rahim Kamaluddin, Azianura Hani Shaari, Norazura Din, & Saravanan Ramasamy. 2018. Pengetahuan dan Amalan Perlindungan Pengguna Facebook

- Wanita Terhadap Penipuan Cinta di Malaysia. *Jurnal Komunikasi Malaysian Journal of Communication*, 34(4), 113-133.
- Nor Hasaliza Asikin Nawi, Shazleen Mohamed, Mohamad Razali Ramdzan@Raaban. 2023. Understanding the Social Commerce *Scam* and Consumers Self Disclosure. *International Journal of Business and Technology Management*, 5(2), 251-262
- Nurqalby Mohd Reda. 2023. Jangan leka jenayah penipuan kewangan masih berleluasa. *Bernama.com*. <https://www.bernama.com/bm/rencana/news.php?id=2258033>. 29 December
- Nurul Anessa Rosley, Hasnizam Hashim & Norman Zakiyy Chow Jen-T'Chiang (2023). The Issues of Macau *Scam* in Malaysia: An Analysis from Perspective Maqasid Syariah. Proceedings of the 9th International Conference on Quran as Foundation of Civilization (SWAT 2023) FPQS, Universiti Sains Islam Malaysia, 4-5 October 2023
- NurulAin, M., & Faezi, K. (2019). Penipuan Pakej Umrah: Penyelesaian Daripada Perspektif Perniagaan Islam. *Global Journal Al-Thaqafah*, Special Issue (November), 145-157
- Puram, P.K., Kaparathi, M., & Rayaprolu, A.K.H. (2011). Online *scams*: taking the fun out of the internet. *Indian Journal of Computer Science and Engineering*, 2(4), 559-565.
- Raja Noraina Raja Rahim. 2022. Pelajar, belia dijangka jadi sasaran baharu 'scammer'. *BHonline*. <https://www.bharian.com.my/berita/nasional/2022/09/1004869/pelajar-belia-dijangka-jadi-sasaran-baharu-scammer>. 26 September.
- Ravenelle, A. J., Janko, E., & Kowalski, K. C. (2022). Good jobs, *scam* jobs: Detecting, normalizing, and internalizing online job *scams* during the COVID-19 pandemic. *New Media & Society*, 24(7), 1591-1610.
- Robb, C.A., & Wendel, S. (2023). Who can you trust? Assessing vulnerability to digital imposter *scams*. *Journal of Consumer Policy*, 46, 27-51
- Sarno, D. M., Lewis, J. E., Bohil, C. J., & Neider, M. B. (2020). Which Phish Is on the Hook? Phishing Vulnerability for Older Versus Younger Adults. *Human Factors*, 62(5), 704-717.
- Teitcher, J.E., Bockting W.O., Bauermeister, J.A., Hoefer, C.J., Miner, M.H., & Klitzman, R.L. 2015. Detecting, preventing, and responding to "fraudsters" in internet research: ethics and tradeoffs', *Journal of Law, Medicine & Ethics*, 43(1): 116-33, doi: 10.1111/jlme.12200
- TIPP Staff (2023). TIPP Indexes Methodology. TippiInsights. <https://tippinsights.com/tipp-indexes-methodology/>. Accessed on; 11 January 2024.
- Titus, R. M., Heinzelmann, F., & Boyle, J. M. (1995). Victimization of Persons by Fraud. *Crime & Delinquency*, 41(1), 54-72
- Van Wyk, J., & Benson, M. L. (1997). Fraud victimization: Risky business or just bad luck? *American Journal of Criminal Justice*, 21(2), 163-179
- Wei, L., Peng, M., & Wu, W. 2021. Financial literacy and fraud detection Evidence from China. *International Review of Economics Finance*, 76 (November), 478-494
- Weijer, S.V.D., Leukfeldt, R. & Sophie, V. D.Z. (2019). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal*, 43(1), 17-34
- Whitty, M.T. (2020). Is There a *Scam* for Everyone? Psychologically Profiling Cyberscam Victims. *European Journal on Criminal Policy and Research*, 26, 399-409. <https://doi.org/10.1007/s10610-020-09458-z>
- Wilson, S., Hassan, N.A., Khor, K.K., Sinnappan, S., Abu Bakar, A.R. & Tan, S.A. (2023). A holistic qualitative exploration on the perception of *scams*, *scam* techniques and effectiveness of anti-*scam* campaigns in Malaysia. *Journal of Financial Crime*, (in print). <https://doi.org/10.1108/JFC-06-2023-0151>
- Zahari, A. I., Bilu, R. & Said, J. (2019). The Role of Familiarity, Trust and Awareness Towards Online Fraud, *Journal of Research and Opinion*, 6(9), 2470-2480, <https://doi.org/10.15520/jro.v6i9.23>
- Zareen Humairah Sejalan (2023). 43959 *scammer* ditahan. *Utusan Malaysia*. <https://www.utusan.com.my/berita/2023/06/43949-scammer-ditahan/>
- Zulkufli Ismail & Azmi Aziz. (2019). Jenayah siber cinta terhadap wanita profesional. *e-Bangi: Journal of Social Sciences and Humanities*, 16(401), 1-10.