Akademika 94(2), 2024: 179-196
https://doi.org/10.17576/akad-2024-9402-10

Pengaruh Pengetahuan Tip Pencegahan Terhadap Keyakinan Remaja di Pantai Timur bagi Melindungi Diri daripada Jenayah *Scam*

The Influence of Safety Tips Knowledge on the Confidence of East Coast Youths for Self-Protection from Scam Crimes

FIDLIZAN MUHAMMAD, SALWA AMIRAH AWANG, AHMAD ZAKIRULLAH MOHAMED SHAARANI, MOHD YAHYA MOHD HUSSIN & NURHANIE MAHJOM

ABSTRAK

Scammer mempelbagaikan modus operandi bagi melaksanakan jenayah penipuan. Rentetan itu, pengetahuan mengenai tip pencegahan merupakan langkah awal mengenalpasti dan menangani sesuatu kejadian penipuan daripada berlaku. Pihak berkuasa telah menyebarluaskan beberapa tip pencegahan yang disampaikan melalui pelbagai saluran bagi melindungi masyarakat terjerumus sebagai mangsa jenayah scam. Walaupun statistik kes melibatkan golongan remaja adalah kecil, namun pengetahuan mengenai pencegahan relevan untuk membantu mereka menanganinya pada masa depan. Sehubungan itu, kajian ini menganalisis pengaruh pengetahuan beberapa tip pencegahan berkaitan jenayah scam dalam meningkatkan keyakinan golongan remaja untuk melindungi diri dari jenayah ini. Data kajian diperoleh melalui instrumen soal selidik yang diedarkan dalam kalangan remaja di Pantai Timur, Semenanjung Malaysia. Seramai 261 responden telah dipilih dalam kajian ini. Data yang diperoleh telah dianalisis menggunakan kaedah regresi logistik dengan enam pembolehubah tidak bersandar. Hasil analisis mendapati lima pembolehubah signifikan dan dua tip pencegahan menunjukkan pengaruh positif yang tinggi iaitu berwaspada dalam mengemaskini maklumat dan urusan transaksi online. Menamatkan panggilan palsu, tidak menyertai skim cepat kaya dan tidak mendedahkan maklumat kewangan merupakan tiga pembolehubah lain yang turut menunjukkan pengaruh positif yang signfikan. Dapatan ini membuktikan, tip pencegahan jenayah scam diketahui oleh remaja dan efektif membantu sebagai petunjuk mengenalpasti taktik scam dan mencegahnya daripada terjebak sebagai mangsa. Sehubungan itu, tip pencegahan perlu disebarluaskan secara berterusan bagi mencapai objektif mengatasi jenayah scam. Hal ini mampu dilaksana dengan berkesan melalui penglibatan bersama daripada institusi sosial seperti keluarga, rakan, jiran, guru, dan masyarakat.

Kata kunci: Jenayah; Pengetahuan; Penipuan; Remaja; Regresi Logistik

ABSTRACT

Scammers diversify the modus operandi to commit fraud crimes. Therefore, knowledge of prevention tips is the first step in identifying and addressing an incident of fraud. The authorities have spread a number of prevention tips delivered through various channels to protect the community as victims of scam crime. Although the statistics of cases involving adolescents are small, knowledge of prevention is relevant to help them deal with it in the future. In this regard, this study analyses the influence of some of the prevention tips related to scam crime in increasing the confidence of youths to protect themselves from these crimes. The data of this study was obtained through questionnaire instruments distributed among adolescents in the East Coast, Peninsular Malaysia. A total of 261 respondents were selected in this study. The data obtained were analysed using the logistics regression method with six non-dependent variables. The results of the analysis found that five significant variables and two prevention tips showed a high positive influence namely vigilance in updating information and online transactions. Ending fake calls, not participating in get-rich-quick schemes and not disclosing financial information are three other variables that also indicated a positive influence. This finding proves that scam crime prevention tips are known to teenagers and effectively help to identify scam tactics and prevent them from getting caught as victims. In this regard, prevention tips should be distributed continuously to achieve the objective of tackling scam crime. This can be implemented effectively through joint involvement from social institutions such as family, friends, neighbours, teachers, and the community.

Keywords: Crime; Knowledge; Scam; Youths; Logistics Regression

PENGENALAN

Jenayah penipuan dalam talian (scam) merupakan fenomena yang semakin meningkat dalam era digital ini. Dengan pesatnya kemajuan teknologi dan penyebaran luas internet, penjenayah semakin kreatif dan cekap menggunakan kaedah penipuan untuk meraih keuntungan secara tidak sah. Jenayah penipuan melibatkan penggunaan strategi tertentu untuk memperdaya individu atau organisasi dengan tujuan mendapatkan maklumat peribadi, kewangan, yang menyebabkan mangsa mengalami kerugian kewangan. Penipuan atas talian merupakan bentuk jenayah licik yang dilakukan dengan modus operandi yang sistematik. Situasi jenayah penipuan ini sedikit berbeza dengan jenayah lain seperti mencuri, merompak atau menyamun kerana jenayah penipuan dalam talian berlaku dengan penglibatan mangsa tanpa sedar atau mangsa dimanipulasi oleh penjenayah (HSBC UK, n.d.). Terdapat pelbagai kategori jenayah penipuan dalam talian yang berlaku dalam kalangan masyarakat Malaysia. Antaranya adalah penipuan cinta, Macau *scam*, penipuan kerja separuh masa (part time), penipuan pinjaman atas talian, dan penipuan bungkusan (parcel) (MKN,2023). Umumnya, tindakan jenayah scam bermula dengan strategi mengumpan mangsa melalui pelbagai tawaran berbentuk keuntungan atau ugutan yang mengakibatkan mangsa percaya dan menuruti arahan diberikan. Misalnya, taktik penyamaran penjenayah sebagai anggota pihak berkuasa yang mendakwa mangsa mempunyai kes jenayah, telah menyebabkan mangsa menuruti semua arahan dengan memindahkan dan memberikan maklumat akaun kewangan kepada penjenayah (Nor Azura, 2023). Modic dan Lea (2013) mendapati, penyamaran sebagai figura berautoriti mempengaruhi psikologi dan tahap kepercayaan mangsa.

Keterdedahan masyarakat dengan penggunaan teknologi seperti gajet dan pelbagai media sosial tanpa tahap pengetahuan yang baik mengenai kaedah melindungi keselamatan data dan diri daripada jenayah siber, telah dikenalpasti menyumbang kepada peningkatan masalah ini (Nurqalby, 2023). Penjenayah dikenali "scammer" menggunakan kaedah panggilan telefon dan khidmat pesanan ringkas (SMS) bagi memerangkap mangsa dengan kadar 82.7 peratus (Farah Marshita, 2023). Email, SMS dan media sosial telah dikenalpasti sebagai medium utama digunakan penjenayah bagi memerangkap mangsa. Petrosyan (2023) mendapati hampir 57 peratus mangsa *scam* pada tahun 2022 dijerat melalui pautan (link) yang dihantar melalui medium-medium berkaitan. Ironinya, mangsa mengetahui pautan tersebut mempunyai unsur *scam*, namun tindakan menekan pautan menimbulkan persoalan. Dalam hal ini, didapati unsur hadiah mempengaruhi pengguna untuk menekan pautan tersebut (Halevi et al. 2013). Konsep berani mencuba ini didapati berpunca daripada sikap diri sendiri yang merasakan mempunyai kecekapan kendiri yang tinggi untuk mengesan informasi *scam* dan mengelak daripada terperangkap ketika penggunaan internet (Ribeiro et al. 2024).

Bagi mengatasi isu ini, pihak Suruhanjaya Komunikasi Multimedia Malaysia (SKMM) telah menyekat 410,590,277 SMS tidak diminta (unsolicited SMS) untuk 9 bulan pertama (Januari-September) 2023, dan 19 juta pautan SMS (hyperlink SMS) untuk tempoh masa 5 bulan (Mei-September) 2023. Dalam tempoh sama, pihak SKMM turut menamatkan hampir 80 ribu talian telefon mudah alih dan tetap yang menghantar SMS, dan menyekat 553,173,467 panggilan meragukan kepada pihak pengguna. (KKD, 2023). Selain itu, sejumlah 1,247 laman sesawang disyaki digunakan oleh *scammer* bagi pemancingan maklumat (phishing) telah turut disekat (Mohd Fadhli, 2023; SKMM,n.d.).

Jenayah *scam* telah memberikan nilai kerugian yang besar kepada mangsa dan negara dunia. Sejak tahun 2018 hingga Oktober 2023, sejumlah RM23 bilion kerugian dicatatkan (Mohd Fadhli, 2023). Antara Januari hingga November 2023, dibandingkan dengan tempoh sama

sebelumnya, kes jenayah penipuan kewangan didapati meningkat sebanyak 37 peratus (Nurqalby, 2023). Jumlah kerugian pula dianggarkan berjumlah RM1.3 bilion (2023) berbanding tahun sebelumnya iaitu RM771.1 juta (Farah Mashita, 2023). Namun, angka dan nilai kerugian ini dilaporkan lebih tinggi disebabkan terdapat mangsa yang enggan melaporkan jenayah yang berlaku kepada pihak berkuasa (Nurqalby, 2023; Marzuki, 2023). Penganalisis jenayah, Kamal Affandi mendapati kegiatan 'scammer' di Malaysia dapat dikategorikan kepada enam jenis atau diringkaskan sebagai 6P, iaitu percintaan, produk, pangkat palsu, perkhidmatan, pekerjaan dan pelaburan (Mukhriz, 2022). Menurut beliau lagi, penipuan perkhidmatan merupakan teknik *scammer* yang menyebabkan banyak maklumat mangsa diperoleh. Lebih parah, penjenayah turut boleh mencuri dengar dan merekodkan butiran perbualan mangsa sebagai bahan ugutan. Hal ini berlaku melibatkan langganan perkhidmatan dalam talian yang memerlukan mangsa menekan atau mengklik pautan (link) yang telah diubahsuai oleh penjenayah.

Bagi mengekang jenayah ini, sebuah agensi bertanggungjawab khusus telah ditubuhkan oleh beberapa agensi pelaksana seperti Bank Negara Malaysia (BNM), Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) dan Polis DiRaja Malaysia (PDRM) dengan dikenali Pusat Respons Scam Kebangsaan (National Scam Response Center, NSRC) pada Oktober 2022. Sejak ditubuhkan, pusat ini menerima secara purata 30 kes jenayah *scam* setiap hari (Suzalina, 2023). Pelbagai kempen kesedaran dan tip pencegahan dilaksana oleh agensi-agensi berkaitan bagi membendung masalah ini. Moto #JanganKenaScam telah dilaksana oleh pemain industri kewangan iaitu Persatuan Bank-Bank Dalam Malaysia (The Association of Banks in Malaysia, ABM) dan Persatuan Institusi Perbankan dan Kewangan Islam Malaysia (Association of Islamic Banking and Finacial Institutions Malaysia, AIBIM) dengan sokongan Bank Negara Malaysia (BNM) bagi mendidik pengguna berkaitan penggunaan kewangan dan perlindungan data yang efektif (ABM, n.d.; AIBIM, n.d.). Prosedur keselamatan transaksi atas talian yang lebih ketat juga telah diperkenalkan oleh pihak BNM bagi menghalang urusan kewangan yang diragui dan dilaksana tanpa pengetahuan pemilik akaun (Nik Shamsiah, 2022).

Menyokong usaha ini, pihak PDRM turut melaksanakan langkah sama. Laman sesawang atau pangkalan data khusus dengan moto #SemakMule disediakan sebagai kemudahan untuk menyemak nombor telefon dan akaun perbankan yang disyaki digunakan oleh penjenayah dalam iklan, produk dan maklumat yang diterima oleh pengguna. Sebuah buku panduan atas talian juga telah diterbitkan berjudul "Trend Terkini Jenayah Komersil" yang menerangkan pelbagai jenis *scam*, taktik dan tip pencegahan kepada pengguna (PDRM, 2022).

Remaja merupakan kumpulan berisiko dengan jenayah ini pada masa depan. Walaupun Kementerian Pembangunan Wanita dan Pembangunan Masyarakat (KPWKM, 2021) mendapati golongan remaja merupakan golongan yang paling sedikit terbabit dalam jenayah *scam* antara tahun 2019 hingga 2021 iaitu 1.5 peratus, namun literasi secukupnya relevan kepada kumpulan ini. Ini disebabkan, penjenayah telah mengekploitasi perubahan teknologi dengan mewujudkan modus operandi bertujuan menarik kumpulan remaja sebagai mangsa dan anggota sindiket terutama membabitkan urusan pinjaman wang, keldai akaun dan sebagainya (Raja Noraina, 2022). Oleh yang demikian, kajian ini cuba menganalisis tahap pengetahuan remaja berkaitan tip pencegahan yang dihebahkan oleh pihak berkuasa terhadap keyakinan mereka untuk melindungi diri daripada terjerumus dalam jenayah *scam*. Kajian ini dilaksana dalam kalangan remaja di Pantai Timur, Semenanjung Malaysia melibatkan negeri Kelantan dan Terengganu.

Pemilihan kawasan Pantai Timur didorong oleh peningkatan ketara jenayah *scam* yang dilaporkan oleh pihak PDRM, Negeri Kelantan. Di samping itu, penjenayah turut memanipulasi derma masjid sebagai taktik *scam* yang dipadankan dengan profil majoriti masyarakat Muslim

(Adam, 2022). Menarik dalam kes scam di Kelantan ialah terdapat kes dilaporkan melibatkan mangsa dari golongan politik berprofil tinggi yang mengalami kerugian hampir RM85 ribu (Nor Fazlina, 2022). Situasi sama turut dilaporkan oleh pihak berkuasa di Terengganu yang melibatkan peningkatan kes *scam* (Bernama, 2022) dan mangsa dalam pelbagai kategori seperti guru, pesara (Faizul, 2023), dan kakitangan pengajian tinggi (Tengku Danish Bahri, 2023). Profil majoriti masyarakat Islam di Terengganu sebagaimana Kelantan turut mendorong penjenayah memanipulasi modus operandi *scam* berkonsepkan Islam (Bernama, 2019) telah memotivasikan kajian ini difokuskan dalam kalangan remaja Pantai Timur, Semenanjung Malaysia. Di samping itu, pengkaji turut mendapati kajian empirikal mengenai jenayah *scam* melibatkan dua buah negeri berkenaan masih terhad. Kajian-kajian lepas yang diteliti didapati banyak dijalankan di Selangor seperti Khadijah et al. (2018); Zulkufli dan Azmi (2019), Khadijah et al. (2020) dan Nor Hasaliza et. al., (2023). Sehubungan itu, dapatan kajian ini diharapkan dapat memberikan satu bukti empirikal baharu berkaitan isu jenayah *scam* dalam kalangan masyarakat di Pantai Timur, Semenanjung Malaysia.

SOROTAN LITERATUR

Jenayah *scam* semakin meningkat pada peringkat global. 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 (GASA, 2023). Beberapa dapatan utama daripada kajian survei GASA melibatkan hampir 50 ribu responden membabitkan 43 negara termasuk Malaysia. Tiga faktor dikenalpasti penyebab individu menjadi mangsa *scam* iaitu tertarik dengan tawaran, tidak mengetahui kewujudan jenayah *scam*, dan kurang pengetahuan mengenai taktik *scam.* Menariknya, faktor-faktor dikenalpasti ini turut berlaku di negara maju seperti Taiwan (30%), Perancis (27%) dan Korea Selatan (26%). Jenayah *scam* turut didapati berlaku melalui tiga modus operandi utama iaitu pembelian, pelaburan dan memancing maklumat (phishing). Dapatan khusus mengenai Malaysia pula menunjukkan 43 peratus responden menyatakan boleh mengecam atau mengenali modus operandi yang cenderung dianggap sebagai *scam*, 79 peratus pernah mengalami kejadian *scam*, di mana 36 peratus daripadanya mengalami kehilangan wang. Nilai kerugian individu secara purata adalah antara USD1000 ke USD1500, nilai kerugian kepada KDNK ialah 2.5 ke 3 peratus, dan hanya 45 peratus mangsa melaporkan kejadian jenayah kepada pihak berkuasa.

Terdapat beberapa jenis jenayah *scam* yang telah dikaji di Malaysia. Antaranya ialah *scam* cinta oleh Khadijah et al., (2020), Zulkufli dan Azmi (2019), Azianura et al. (2019), Khadijah et al. (2018) dan Nor Azlina et. al., (2018). *Scam* akaun bank dilakukan oleh Mohd Irwan et al. (2022) dan Masnita et al., (2021), manakala *scam* pelaburan pula diteliti oleh Kasim et al. (2023), Azman (2017) dan Hazlina et. al., (2021). Kajian *scam* lain pula ialah *scam* belian atas talian oleh Nor Hasaliza et. al., (2023) dan *scam* umrah oleh NurulAin dan Faezi, (2019). Dapatan kajian-kajian ini didapati relevan dengan kajian GASA (2023). Penjenayah memanipulasi mangsa dengan panggilan mesra dan manja bagi memikat dan memperdayakan mangsa. Untuk beberapa tempoh waktu, hubungan erat dibina dan terdapat sebahagian mangsa menyerahkan segalanya kerana begitu mempercayai janji-janji penjenayah. Tanpa mereka sedari, wang diambil oleh penjenayah dengan memberikan pelbagai alasan, akhirnya mangsa ditinggalkan begitu sahaja (Couch et al., 2012).

Penipuan cinta yang dikaji oleh Azianura et al. (2019) mengenalpasti wujud tiga peringkat dilaksana oleh penjenayah. Tahap satu dan dua adalah sama sebagaimana yang Couch et al. (2012) iaitu memikat dan membina hubungan. Berbezanya, peringkat ketiga dilakukan dengan memanipulasi maklumat mangsa yang diperoleh pada peringkat satu dan dua. Pada ketika ini, penjenayah menukar watak dirinya kepada figura berautoriti dan menggunakan maklumat berkaitan menggunakan taktik ugutan, amaran dan peringatan kepada mangsa yang enggan menuruti sesuatu yang diminta.

Kajian Wilson et al. (2023) turut mendapati terdapat pelbagai figura berautoriti yang digunakan oleh penjenayah untuk memperdaya mangsa. Antara figura yang digunakan oleh *scammer* adalah penyamaran sebagai pegawai kerajaan seperti polis, pegawai cukai, atau pegawai bank. Mereka akan menggunakan identiti palsu untuk memenangi kepercayaan mangsa, termasuklah menggunakan elemen ugutan ketakutan atau taktik menakut-nakutkan untuk memaksa mangsa bertindak dengan segera tanpa berfikir panjang. Di samping itu, penjenayah akan berkomunikasi dengan mangsa menggunakan gaya bahasa yang sah dan formal untuk mengekalkan kesan kredibiliti. Penjenayah juga cuba meyakinkan mangsa agar tidak berkongsi perbualan atau butiran transaksi dengan orang lain, dengan harapan mengurangkan peluang pendedahan penipuan. Teknik lain termasuklah memberikan rasa keperluan segera atau kecemasan kepada mangsa. Tujuannya adalah untuk memaksa mereka membuat keputusan tanpa memeriksa kesahihan atau berfikir panjang. Penipu juga sering menghantar pautan muat turun untuk pembayaran, yang sebenarnya boleh membawa kepada penyebaran perisian berbahaya atau pencurian maklumat peribadi.

Mudah percaya ini turut berlaku dalam jenayah *scam* yang lain. Keterujaan menunaikan umrah dengan pelbagai tawaran harga yang murah, jarak dekat dan keselesaan tempat penginapan, penyertaan selebriti dan sebagainya telah melalaikan mangsa untuk menyemak kesahihan informasi penting mengenai syarikat dengan pihak berwajib (Nor Azaruddin Husni, 2022; NurulAin & Faezi, 2019). Keperluan pengguna melakukan semakan secara berulang dengan pemilik atau pengirim email atau SMS ini amat penting. Ini kerana, sukar membezakan email sah dan palsu, khususnya melibatkan alamat pengirim daripada bank atau agensi kerajaan. Pengguna umumnya memberikan respon yang segera melibatkan agensi-agensi ini yang akhirnya mendedahkan mereka kepada taktik pemancingan data ketika membuka email atau mengklik pautan (Wilson et al., 2023).

Boateng dan Amanor (2014) turut mendapati pengguna berhadapan isu dalam memastikan kesahihan SMS yang diterima daripada agensi bank dan pihak penguatkuasaan undang-undang. Mesej yang meminta mangsa untuk memberikan butiran peribadi, nombor akaun bank, atau maklumat kewangan lain, berserta tempoh masa terhad menyebabkan mangsa bertindak dengan segera dan tidak berfikir panjang. Berhadapan situasi sebegini, Boateng dan Amanor (2014) mencadangkan untuk sentiasa berwaspada terhadap SMS yang mencurigakan. Mangsa perlu memastikan bahawa mereka tidak memberikan maklumat peribadi atau sensitif melalui SMS tanpa mengesahkan kesahihan sumber terlebih dahulu. Atkins dan Huang (2013) menerangkan bahawa masyarakat turut dapat mengenalpasti email berbentuk *scam*. Kebiasaannya, email yang dikirimkan kepada mangsa dibahagikan kepada tiga tahap iaitu waspada, amaran dan perhatian. Kekerapan menerima email sama akan membuatkan mangsa berasa takut dan selanjutnya mengambil tindakan membalas email dengan segera. Kesedaran terhadap taktik dan kewaspadaan semasa berurusan dengan SMS dan email adalah penting untuk mengelakkan mangsa terperangkap dengan jenayah *scam*. Frauenstein dan Flowerday (2020) mendapati elemen kecerewetan atau kewaspadaan dalam media sosial dengan memilih bahan-bahan tertentu sahaja signifikan

melindungi individu daripada *scam* melibatkan pancingan data.

Selain itu, tahap literasi rendah mengenai keselamatan siber juga memberi peluang kepada penjenayah untuk mencuri maklumat penting berkaitan diri pengguna (Muhammad Adnan et al., 2019). Ernawati et al. (2023) dan Lee et al. (2022) mendapati pengguna tidak sedar bahawa beberapa maklumat penting boleh terdedah kepada penjenayah melalui pelbagai aktiviti yang dilakukan dalam banyak aplikasi media sosial. Antara aktiviti berkenaan seperti mencari pasangan, berkongsi cerita, transaksi atas talian, mencari bahan berita dan sebagainya (Khadijah et al., 2020). Melalui aktiviti yang dilakukan ini, penjenayah melaksanakan modus operandi mengikut sasaran mangsa. Terdapat sebahagian mangsa diperangkap menggunakan kaedah gaya percakapan, imej dan harga produk sahaja (Naksawat et al., 2016; Foozy et.al, 2014), dan sebahagian lain pula diperangkap menggunakan pemalsuan laman sesawang (Zahari et al. 2019).

Kegagalan bagi mengenalpasti dan membezakan ciri-ciri platform atau laman sesawang asli dan palsu merupakan antara faktor yang menyebabkan maklumat kewangan sulit seperti nombor akaun, nombor cukai, identifikasi akses perbankan atas talian dan sebagainya dicuri oleh penjenayah (Hamsi et al., 2015; Zahari et al., 2019). Oleh yang demikian, pengetahuan berkaitan siber dan melindungi keselamatan data perlu dititikberatkan ketika melakukan aktiviti berkenaan (Dunham, 26 Ogos, 2022; Puram et al., 2011; Wilson et al. 2023). Ge et al. (2021) mendapati profil atau personaliti seseorang individu memainkan peranan penting bagi melindungi diri daripada diperangkap sebagai mangsa *scam*. Tahap kesedaran yang rendah, keterbukaan yang rendah dan neurotikisme yang tinggi, pengalaman internet dan pengetahuan mengenai komputer dan web yang rendah merupakan elemen yang merisikokan individu untuk mudah terpengaruh dengan informasi yang berunsurkan jenayah *scam*.

Kajian oleh Muniandy et al. (2016) dalam kalangan pelajar pengajian tinggi yang menfokuskan pada tingkah laku siber pelajar dalam aspek perisian yang merbahaya dikenali *malware* (Malicious Software), penggunaan kata laluan, dan kejuruteraan sosial mendapati bahawa majoriti pelajar menggunakan maklumat peribadi mereka sebagai kata laluan. Selain itu, majoriti pelajar juga tidak memeriksa kebenaran atau identiti individu yang menyatakan diri sebagai pihak berkuasa tertentu semasa menerima panggilan atau informasi. Gavet et al. (2017) merungkai punca ini sama ada berlaku kepada golongan muda sahaja atau turut diamalkan dalam kalangan berusia. Menariknya, penemuan kajian ini signifikan dalam golongan muda, dan sebaliknya kepada golongan berusia. Menjustifikasikan situasi ini, pengkaji mendapati golongan muda merasa begitu yakin dengan keselamatan IT yang digunakan dan tidak mengambil langkah-langkah perlindungan kendiri. Hal ini didapati berbeza dengan golongan berusia yang lebih berwaspada dalam penggunaan teknologi rentetan daripada pengalaman sendiri atau orang lain yang terjerat dengan jenayah.

Berhadapan dengan situasi jenayah, peranan keluarga dan orang terdekat adalah amat penting. Perkongsian merupakan tip pencegahan yang dapat membantu individu mendapatkan pandangan dan kepastian tentang sesuatu informasi yang meragukan. Kajian NorAzlina et al. (2018) mendapati bahawa amalan perlindungan penipuan cinta dengan memberitahu keluarga atau rakan terdekat tentang individu yang mencurigakan di laman sosial menunjukkan nilai min kedua terendah daripada 23 item. Hal ini selari dengan kajian GASA (2023) yang menunjukkan terdapat mangsa *scam* yang enggan untuk membuat laporan kepada pihak berkuasa atas pelbagai faktor seperti emosi, kedudukan dan keupayaan pihak berkuasa menyelesaikan kes dengan berjaya.

Berdasarkan kajian-kajian lepas berkaitan jenayah penipuan dalam talian, pengetahuan mengenai tip pencegahan adalah relevan untuk membantu masyarakat berhadapan secara selamat dengan jenayah *scam*. Sehubungan itu, fokus kajian ini adalah kalangan remaja bertujuan

mengetahui tahap kepedulian atau ambil berat mereka mengenai isu *scam* dan tip pencegahan yang telah disebarluas dalam pelbagai media massa kini. Buku panduan yang merupakan tips pencegahan yang disediakan oleh pihak berkuasa di Malaysia didapati mengandungi banyak elemen penting yang diperlukan bagi melindungi diri masyarakat daripada jenayah *scam* iaitu teknologi selamat (Wei et al., 2021; Teitcher et al., 2015), keselamatan data (Robb &Wendel,2023; Baruh & Popescu, 2017), kemahiran mengenali *scam* (Azianura et al., 2019; Aung & Mon, 2020) dan menangani isu (Devashish, 2022). Sehubungan itu, tip pencegahan yang dikeluarkan oleh pihak berkuasa ini relevan untuk memberi kefahaman mengenai taktik, jenis *scam* terkini dan kaedah mengatasi yang boleh dipraktikkan oleh masyarakat awam (Ernawati et al., 2023, Wilson et al. 2023).

Tip pencegahan yang sama turut dikemuka dalam hasil kajian Wilson et al. (2023) dan Nur Farhana et al. (2021). Antaranya ialah masyarakat perlu membaca bagi mengetahui berita terkini jenayah *scam*, berbincang dengan keluarga dan rakan-rakan, memeriksa kredibiliti laman web atau URL atau pautan, menghubungi agensi kerajaan rasmi untuk penjelasan, memadamkan semua maklumat pada sampul bungkusan apabila pembelian sudah lengkap dan diterima, tidak memberi perhatian kepada panggilan yang mencurigakan, dan tidak membuka atau mengklik pautan yang mencurigakan. Tindakan-tindakan ini membantu individu untuk lebih berwaspada terhadap potensi penipuan dan menjaga keselamatan pengguna dalam penggunaan teknologi serta transaksi dalam talian. Aplikasi berterusan amalan atau tip pencegahan ini, dijangka mampu mengurangkan risiko seseorang terjebak sebagai mangsa kepada jenayah *scam* dan memastikan pengalaman dalam talian yang lebih selamat dan terlindung.

METODOLOGI

Kajian ini dilaksana dalam kalangan remaja di Pantai Timur, Semenanjung Malaysia melibatkan dua buah negeri iaitu Kelantan dan Terengganu. Responden yang dipilih merupakan remaja yang berasal dan menetap di kedua-dua negeri berkaitan dan berusia antara 17 hingga 20 tahun. Perolehan data kajian diperoleh melalui instrumen soal selidik yang diedarkan antara bulan September hingga Disember, 2023. Pengedaran borang soal selidik dilakukan secara bersemuka melibatkan kawasan Kota Bharu, Pasir Mas, Tanah Merah dan Machang di Negeri Kelantan, dan Besut/Setiu, Kuala Nerus, Kuala Terengganu dan Kemaman di Terengganu.

Sebanyak 300 borang soal selidik diedarkan dalam tempoh masa kajian, dan sejumlah 261 borang iaitu 87 peratus yang diterima telah diisi dengan lengkap. Kecukupan jumlah sampel kajian diukur melalui model Demidenko (2007) menggunakan aplikasi Gpower. Maklumat daripada ujian rintis berkaitan jantina, pendedahan formal responden berkaitan jenayah *scam*, min dan sisihan piawai pembolehubah bersandar digunakan bagi menghitung saiz sampel minimum (Yenipinar et al. 2019). Hasil analisis kuasa untuk ujian-z bagi regresi logistik satu hala menunjukkan bahawa saiz sampel minimum untuk mencapai kuasa statistik sekurang-kurangnya 0.90 dan 0.95 dengan ralat kesilapan 0.05 adalah 149 dan 162 data. Sehubungan itu, sampel kajian sebenar berjumlah 261 yang digunakan dalam bahagian analisis kajian memenuhi kriteria saiz sampel dan sesuai untuk analisis lanjut.Instrumen soal selidik kajian pula dibentuk berdasarkan buku panduan dan bahan-bahan hebahan atau kempen yang dilaksana oleh pihak berkuasa di Malaysia seperti PDRM dan institusi kewangan di bawah BNM.

Data yang diperoleh dianalisis menggunakan kaedah regresi logit atau logistik. Regresi ini menggunakan pembolehubah bersandar berbentuk dwikotomi iaitu 1 dan 0. Dalam kajian ini, tujuh

pembolehubah digunakan melibatkan satu pembolehubah bersandar iaitu keyakinan melindungi diri dari jenayah *scam*, dan enam pembolehubah tidak bersandar mencakupi enam tip pencegahan penting. Tip pencegahan yang dipilih daripada buku panduan (PDRM, 2022) adalah sesuai berdasarkan beberapan dapatan kajian lepas, antaranya ialah GASA (2023), Wilson et al. (2023), Muhammad Adnan et al., 2019, Ernawati et al. (2023), Zahari et al. (2019), NorAzlina et al. (2018) dan Hamsi et al., (2015)

Model regresi logit kajian ditunjukkan dalam persamaan (1) di bawah.

$$L = \ln(P_i/(1 - P_i) = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \beta_5 X_5 + \beta_6 X_6 + \varepsilon \quad (1)$$

Di mana;

L adalah log bagi nibsah 'odds' keyakinan remaja untuk melindungi diri daripada di"*scam*"; 1(Ya), 0 (Tidak),

β_i Nilai koefisien pembolehubah,

X1 adalah tindakan responden ketika diminta mengemaskini maklumat; 1(menyemak kesahihan), 0 (mengemaskini tanpa semakan),

X2 adalah tindakan responden ketika menerima panggilan telefon meragukan daripada pihak berkuasa seperti polis, kastam dan sebagainya, 1(menamatkan perbualan tanpa memberikan maklumat dipohon), 0 (memberikan maklumat dan mengikut arahan),

X3 adalah tindakan responden ketika ditawarkan skim pelaburan dengan modal rendah dan keuntungan tinggi; 1(tidak menyertai skim), 0 (menyertai skim),

X4 adalah tindakan responden ketika diminta memberikan maklumat kewangan (akaun bank) melalui panggilan telefon; 1(abaikan), 0 (berikan),

X5 adalah tindakan responden ketika diminta memasukkan maklumat tidak berkaitan barangan dalam talian; 1(abaikan), 0 (isi maklumat),

X6 adalah tindakan responden dalam berkongsi maklumat; 1(kongsi dengan ibu bapa sahaja), 0 (kongsi dengan sesiapa sahaja).

Kesemua data pembolehubah tidak bersandar dalam kajian ini juga berbentuk dwikotomi iaitu tindakan betul atau salah yang dilakukan oleh responden apabila berhadapan dengan taktik *scam*. Tindakan yang tepat bagi setiap pembolehubah ditanda dengan 1, dan 0 bagi tindakan tidak tepat. Analisis logit dimulakan dengan analisis taburan kekerapan bagi pembolehubah bersandar bagi mengetahui nisbah antara jawapan Ya dan Tidak, dan menganalisis kadar peluang. Kadar peluang ini dihitung dengan membahagikan nisbah Ya dan Tidak (Antônio Alves et al. 2020). Langkah berikutnya ialah analisis klasifikasi regresi logit yang bertujuan mengukur keupayaan meramal model dengan betul berdasarkan pemerhatian sebenar. Nilai ambang yang diletakkan ialah 0.5. (Sanep et al. 2007). Model yang mempunyai nilai meramal lebih tinggi daripada nilai ambang, dianggap sebagai model yang baik dan mampu menerangkan model kajian dengan baik. Melalui hasil analisis regresi logistik, beberapa perkara diteliti iaitu mengenalpasti pembolehubah signifikan, tanda arah (+ / -) pada koefisien β, dan nilai Exp.(β). Pengujian tahap signifikan parameter adalah berdasarkan ujian Wald. Hasil ujian Wald yang signifikan menunjukkan pembolehubah X_i merupakan pembolehubah penerang terhadap pembolehubah bersandar dalam model. Sebaliknya berlaku, jika didapati ujian Wald adalah tidak signfikan (Sanep et al., 2007). Bagi pembolehubah yang signifikan, nilai perubahan atau pengaruh terhadap pembolehubah

kajian yang diteliti pada Exp.(β) dihitung menggunakan formula, (exp (β-1) x 100) (Antônio Alves et al. 2020; Sanep et al. 2007).

Bagi menguji ketepatan atau kesesuaian model, ujian diagnostik dikenali Ujian Hosmer dan Lemeshow dengan hipotesis nol adalah model sesuai (fit). Ujian Nagelkerke pula bertujuan mengetahui kadar peratus sumbangan pembolehubah penerang untuk menerangkan pembolehubah bersandar (Antônio Alves et al. 2020, Sanep et al. 2007).

ANALISIS DAN PERBINCANGAN

Maklumat ringkas mengenai analisis profil responden ditunjukkan dalam Jadual 1 di bawah.

JADUAL 1. Profil Responden (n=261)

Profil Responden	**n**	**%**
Jantina		
Lelaki	71	27.2
Perempuan	190	72.8
Negeri		
Kelantan	158	60.5
Terengganu	103	39.5
Mengikuti Bengkel berkaitan Scam?		
Ya	61	23.8
Tidak	199	76.2
Pernah menerima email/SMS scam?		
Ya	215	82.4
Tidak	46	17.6
Pernah menerima panggilan scammer?		
Ya	218	83.5
Tidak	43	16.5

Sumber: Data Analisis SPSS

Berdasarkan Jadual 1, didapati majoriti responden dalam kajian ini adalah golongan remaja wanita (72.8%) berbanding lelaki (27.2%). Berdasarkan negeri, 60 peratus responden merupakan remaja yang berasal dan menetap di Kelantan, dan 40 peratus pula adalah di negeri Terengganu. Hasil analisis turut mendapati, majoriti responden menyatakan tidak pernah mengikuti bengkel atau seminar yang membincangkan mengenai jenayah *scam* iaitu 199 orang (76.2%). Sebahagian kecil iaitu 23.8 peratus responden sahaja menyatakan pernah mengikuti bengkel berkaitan jenayah *scam*. Dari aspek pengalaman berhadapan modus operandi penjenayah, 82 peratus responden menyatakan pernah menerima email atau SMS yang disyaki adalah *scam*, dan 17.6 peratus pula menyatakan sebaliknya.

Modus operandi menggunakan panggilan telefon juga pernah dilalui oleh responden dengan 84 peratus responden menyatakan pernah menerima panggilan telefon daripada *scammer*, dan 16.5 peratus pula sebaliknya. Angka dapatan ini adalah menyokong dan selari dengan beberapa beberapa laporan akhbar berkaitan jenayah *scam* di Malaysia yang menunjukkan email, SMS dan panggilan telefon sebagai medium penjenayah melakukan jenayah (Farah Marshita, 2023; Mohd Fadhli, 2023). Di samping itu, nilai peratus yang tinggi ini turut membuktikan bahawa penjenayah mensasarkan mangsa baru dalam kalangan remaja sebagaimana dilaporkan oleh Raja

Noraina (2022). Rumusan pertama daripada analisis profil ini menunjukkan bahawa golongan remaja tidak terkecuali daripada sasaran penjenayah. Memandangkan majoriti responden kajian mempunyai pengalaman berhadapan dengan taktik *scam*, maka analisis menggunakan pembolehubah berkaitan dengan tip pencegahan jenayah ini didapati relevan dan mampu memberikan bukti empirikal yang sesuai.

Hasil analisis regresi logit ditunjukkan dalam tiga jadual iaitu Jadual 2, Jadual 3 dan Jadual 4. Jadual 2 menunjukkan taburan kekerapan bagi pembolehubah bersandar iaitu keyakinan remaja untuk melindungi diri daripada jenayah *scam*.

JADUAL 2. Taburan Kekerapan Pembolehubah Bersandar

Keyakinan Diri Melindungi Jenayah *Scam*	**N**	**%**
Ya	240	92.0
Tidak	21	8.0
Jumlah	261	100

Sumber: Data Analisis SPSS

Berdasarkan Jadual 2, 92 peratus atau 240 responden menyatakan yakin melindungi diri daripada jenayah *scam*, manakala lapan (8) peratus, iaitu 21 responden pula sebaliknya. Bagi mengukur kadar peluang iaitu berjaya melindungi diri daripada jenayah *scam*, kedua-dua angka ini dapat ditulis semula dalam angka kebarangkalian iaitu 0.92 dan 0.08. Secara alternatif, kadar peluang untuk responden berjaya mengelakkan diri daripada jenayah *scam* boleh dikira semula dengan membahagikan antara dua nilai kebarangkalian (ya/tidak) iaitu 0.92/0.08, dan jawapannya ialah 11.5. Dapatan ini menerangkan responden yang mempunyai pengetahuan mengenai tip pencegahan mempunyai tahap keyakinan sebanyak 11.5 kali ganda lebih peluang positif untuk berjaya mengelak dan melindungi diri daripada terjerumus dalam jenayah *scam*.

Jadual 3 pula menunjukkan keupayaan model yang dianggar untuk meramal dengan betul data-data dari pemerhatian sebenar.

JADUAL 3. Klasifikasi Regresi Logit

		Diramalkan	
Pemerhatian		Tidak Yakin	Yakin
Melindungi Diri Jenayah	Tidak Yakin	7	14
Scam	Yakin	2	238

Sumber: Data Analisis SPSS
Nota: yakin melindungi diri = 99.2%; tidak yakin melindungi diri = 33.3%;
dan keseluruhan = 93.9%

Jadual 3 yang ditunjukkan menerangkan hasil analisis regresi logit untuk meramalkan apakah seseorang yakin atau tidak yakin melindungi diri dari jenayah *scam*. Dalam analisis ini, terdapat dua klasifikasi utama: iaitu “Tidak Yakin” dan “Yakin”. Dalam kategori “Tidak Yakin”, terdapat 21 (14+7) responden yang menyatakan tidak yakin melindungi diri dari jenayah *scam*, di mana sebanyak tujuh (7) pemerhatian diramalkan sebagai "Tidak Yakin" oleh model dan memang benar-benar tidak yakin melindungi diri. Data ini menunjukkan kategori "Tidak Yakin Melindungi Diri" adalah sebanyak 33.3 peratus. Hasil ini menunjukkan bahawa model logit meramalkan individu yang sebenarnya tidak yakin melindungi diri sebanyak 33.3 peratus.

Dalam kategori “Yakin” melindungi diri pula, terdapat 240 responden menyatakan yakin, di mana 238 orang adalah betul-betul yakin, manakala dua (2) orang yang seharusnya yakin, namun berpandangan sebaliknya. Jumlah 238 pemerhatian yang diramalkan sebagai "Yakin" oleh model dan benar-benar yakin melindungi diri ini mewakili kelompok "Yakin Melindungi Diri"

mencapai 99.2 peratus. Kadar ini menandakan bahawa model logit ini efisien dalam meramalkan individu yang sebenarnya yakin melindungi diri berbanding kelompok "tidak yakin melindungi diri". Kadar peramalan benar model ini pula dapat dihitung berdasarkan responden yang berada dalam kategori "yakin" dan "tidak yakin" sepenuhnya iaitu 245 orang. Dalam bentuk peratus, kelompok ini mewakili 93.9 peratus daripada keseluruhan responden. Oleh yang demikian, model yang digunakan dalam kajian ini didapati sesuai kerana berupaya meramal dengan betul sebanyak 93.9 peratus daripada pemerhatian sebenar yang melepasi nilai ambang ditetapkan iaitu 0.5.

Keputusan analisis regresi logit bagi model (1) kajian ditunjukkan dalam Jadual 4 di bawah.

JADUAL 4. Keputusan Analisis Regresi

Pembolehubah	β	S.E	Wald	Sig	Exp (β)	(exp (β-1) X 100
Konstan	-5.000	2.029	6.075	0.014	0.007	-99.3
X1	3.054	1.341	5.188	0.023	21.205	2020.5
X2	1.688	0.815	4.290	0.038	5.409	440.9
X3	0.826	0.465	3.158	0.076	2.283	128.3
X4	1.339	0.729	3.374	0.066	3.816	281.6
X5	-1.835	1.139	2.596	0.107	0.160	-84.0
X6	-1.835	1.139	2.596	0.000	14.298	1329.8
Hosmer dan Lemeshow = Chi-Square(1.079); sig. (0.782)						
Pseudo $R^{2;}$ Nagelkerke = 0.320						

Sumber: Data Analisis SPSS

Berdasarkan Jadual 4, dapat diperhatikan bahawa lima pembolehubah penerang adalah signifikan, dengan empat menunjukkan tanda arah positif dan satu menunjukkan tanda arah negatif. Keempat-empat tip pencegahan yang menunjukkan tanda arah positif, dengan nilai pengaruh positif tertinggi, bermula dengan tip untuk berhati-hati dalam mengemaskini maklumat dengan membuat semakan kesahihan (X1), diikuti oleh tip pencegahan menamatkan panggilan telefon meragukan (X2), tip tidak berkongsi maklumat kewangan (X4), dan tip tidak menyertai skim pelaburan meragukan (X3)

Penerangan bagi setiap pembolehubah berkaitan dapat dijelaskan seperti berikut. Pertama, untuk pembolehubah X1 yang berkaitan dengan menyemak kesahihan ketika mengemaskini maklumat, nilai log nisbah odds adalah 3.054 dan berhubungan positif pada nilai exp koefisien 21.205. Ini bermakna bahawa terdapat kebarangkalian jika pembolehubah X1 meningkat sebanyak 1 unit, maka keyakinan untuk melindungi diri daripada jenayah *scam* meningkat sebanyak 2021 peratus. Dalam konteks ini, kesedaran responden terhadap pentingnya menyemak kesahihan maklumat memainkan peranan besar dalam meningkatkan keupayaan mereka untuk mengelakkan terjerumus dalam jenayah *scam*. Kedua, untuk pembolehubah X2 yang berkaitan dengan tindakan untuk menamatkan panggilan telefon meragukan, nilai log nisbah odds adalah 1.688, berhubungan positif pada nilai exp koefisien 5.409. Ini menunjukkan kebarangkalian bahawa jika responden tahu bahawa mengambil tindakan untuk menamatkan panggilan telefon meragukan meningkat sebanyak 1 unit, maka keyakinan untuk mengelakkan diri terjeremus dalam jenayah ini meningkat sebanyak 441 peratus. Kesedaran dan tindakan responden untuk tidak terlibat dalam panggilan telefon meragukan menjadi faktor penting dalam mengurangkan risiko terlibat dalam jenayah *scam*.

Ketiga, bagi pembolehubah yang berkaitan dengan tidak berkongsi maklumat kewangan (X4), nilai log nisbah odds adalah 1.339, dan berhubungan positif dengan nilai exp koefisien 3.816. Artinya, peningkatan 1 unit dalam pengetahuan responden berkaitan tip pencegahan mengenai keperluan menjaga keselamatan maklumat kewangan, maka keyakinan untuk melindungi diri

daripada terperangkap sebagai mangsa *scam* meningkat sebanyak 282 peratus. Ini selaras dengan saranan dari dapatan kajian Ali dan Mohd Zaharon (2024) yang menekankan perlunya pendidikan kepada pengguna mengenai kaedah mengelakkan pancingan data serta manipulasi kejuruteraan sosial yang dapat mengakibatkan kebocoran data-data sulit pengguna.

Pengetahuan mengenai tip pencegahan untuk tidak terlibat atau menyertai dalam mana-mana skim pelaburan yang meragukan (X3) menunjukkan nilai log nisbah odds sebanyak 0.826, dengan nilai exp koefisien 2.283. Sehubungan itu, peningkatan sebanyak 1 unit untuk menghindari pelaburan dalam skim yang meragukan, maka keyakinan untuk menghindari diri dari terjebak dalam taktik jenayah ini meningkat sebanyak 128 peratus. Hasil ini menyokong penemuan sebelumnya oleh Kasim et al. (2023) dan Hazlina et al. (2021). Kedua-dua kajian ini menunjukkan bahawa perilaku dan sikap yang berwaspada terhadap *scam* mempunyai pengaruh yang signifikan dalam mengurangi risiko untuk terlibat dalam jenayah *scam* pelaburan. Kepentingan perilaku yang bijak dalam urusan kewangan tidak terbatas sekadar bertujuan menghindari daripada jenayah *scam* semata-mata, sebaliknya ia bermanfaat sebagai sebahagian proses persiapan awal untuk merencanakan kehidupan masa depan dengan sistematik (Zaimah et al. 2023). Eley et al. (2020) menemukan bahwa langkah-langkah pencegahan terhadap skim pelaburan atau Ponzi ini memerlukan kombinasi tiga elemen, iaitu pendidikan, peraturan, dan penguatkuasaan undang-undang. Elemen pendidikan diakui sebagai pendasar terbaik untuk melindungi diri. Namun, ia harus ditunjangi oleh peraturan khusus yang mampu mengawasi dan membenteras pihak yang terbabit dalam jenayah ini. Dalam konteks ini, pihak berkuasa seperti Bank Negara Malaysia (BNM) telah secara berkala menyenarai dan mengemaskini skim-skim pelaburan yang meragukan di laman sesawang BNM, misalnya https://www.bnm.gov.my/consumer-info/scam-notices dan https://www.bnm.gov.my/financial-fraud-alerts.

Responden yang berkongsi maklumat peribadi tanpa sekatan diwakili oleh pembolehubah X6 menunjukkan nilai log nisbah odds yang negatif, iaitu -1.835, dengan nilai exp koefisien 14.298. Dengan peningkatan sebanyak 1 unit dalam perkongsian maklumat tanpa kawalan, potensi untuk menjadi mangsa *scam* meningkat sebanyak 1430 peratus. Keadaan ini menjelaskan bahawa individu yang berkongsi maklumat tanpa kawalan sukar untuk menganggap diri mereka dilindungi sepenuhnya daripada menjadi sasaran penjenayah sebagai mangsa *scam* pada masa depan. Dapatan ini menyokong hasil analisis Lee et al. (2022) yang menggalakkan remaja dan pengguna siber untuk mengambil sikap berjaga-jaga ketika berkongsi maklumat dalam talian untuk mengurangkan risiko, terutamanya dalam jenayah yang melibatkan pancingan data (phishing). Halevi et al. (2013) juga menekankan hal yang serupa dengan menemui bahawa individu yang terbuka dan gemar menyebarkan banyak informasi diri di media sosial serta tidak menjaga privasi dengan ketat, cenderung untuk mudah terperangkap dalam jenayah *scam*.

Ujian kesesuaian atau diagnostik model menggunakan Ujian Hosmer dan Lemeshow untuk model (1) menunjukkan nilai Chi Square sebanyak 1.079 dengan nilai signifikan 0.782. Oleh itu, hipotesis nol bagi model ini tidak dapat ditolak. Hasil ini menunjukkan bahawa model dan hasil analisis yang diperoleh adalah sesuai dengan data yang dicerap. Secara keseluruhan, enam pembolehubah penerang yang dimasukkan dalam model (1) mampu menjelaskan sekitar 32 peratus variasi dalam model kajian berdasarkan ujian Nagelkerke.

KESIMPULAN

Pengetahuan memainkan peranan yang sangat penting dalam kehidupan seharian masyarakat. Dalam konteks ini, pengetahuan tentang tip pencegahan *scam* menjadi salah satu elemen yang sangat kritikal untuk memastikan individu mampu menghadapi kehidupan dengan selamat. Dengan peningkatan kejadian jenayah *scam*, memahami dan mengamalkan tip-tip pencegahan menjadi kunci untuk membantu masyarakat menangani ancaman ini terutamanya kumpulan remaja atau belia, yang hidup di era yang dikelilingi oleh teknologi, dan menghadapi cabaran yang kompleks. Walaupun statistik semasa menunjukkan bahawa nisbah kejadian jenayah ini dalam kalangan remaja masih rendah, hasil kajian ini menyoroti bahawa kumpulan ini juga berisiko terhadap penipuan atas talian pada masa akan datang. Penerimaan informasi scam melalui email dan panggilan telefon oleh majoriti responden menunjukkan kumpulan ini rentan dengan jenayah ini. Bagi mengatasi masalah ini, pendedahan berterusan terhadap kaedah penjagaan dan pencegahan jenayah scam menjadi penting. Ini disebabkan jenayah scam merupakan bentuk kejahatan yang mampu memanipulasi mangsa mengikut perkembangan situasi dan teknologi terkini. Pengetahuan tentang tip pencegahan untuk melindungi keselamatan data, maklumat peribadi, perkongsian data, pelaburan yang meragukan, dan lain-lain, menjadi relevan dalam konteks ini.

Kumpulan remaja sebagai generasi penerus masa hadapan perlu disiapsiagakan dengan baik untuk menghadapi ancaman jenayah *scam* dengan yakin dan selamat. Pendekatan ini memerlukan usaha dilaksana secara formal dan tidak formal dalam pelbagai sistem penyampaian. Untuk memastikan matlamat ini berkesan, peranan institusi keluarga dan pendidikan adalah amat relevan. Tujuan utamanya adalah memastikan remaja memiliki pengetahuan yang mencukupi mengenai taktik dan kaedah untuk mencegah diri daripada menjadi mangsa jenayah scam. Kejayaan usaha ini juga bergantung kepada komitmen bersama-sama dari setiap lapisan masyarakat melibatkan keluarga, rakan kenalan, jiran dan masyarakat. Oleh itu, mencegah jenayah scam bukanlah tanggungjawab tunggal pihak berkuasa, akan tetapi merupakan usaha bersama yang melibatkan partisipasi aktif dari seluruh masyarakat. Sebagai contoh, pendidikan berkaitan integriti dan penekanan terhadap rasuah yang semakin ditekankan dalam sektor pendidikan tinggi di Malaysia dapat dijadikan model bagi menjayakan usaha pendidikan pencegahan jenayah penipuan dan *scammer* secara lebih meluas.

PENGHARGAAN

Penyelidikan ini mendapat peruntukan di bawah Geran Penyelidikan Fundamental Universiti (GPUBP: 2022-0I47-107-01) 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

ABM. n.d. Safe Online Banking Scam Alerts. https://www.abm.org.my/safe-online-banking/scam-alerts-listing/. Retrieved on: 10 Oktober 2023.

Adam Darwish. 2022. Statistik jenayah komersial di Kelantan meningkat, kes Macau Scam paling tinggi. *AstroAwani*. https://www.astroawani.com/berita-malaysia/statistik-jenayah-komersial-di-kelantan-meningkat-kes-macau-scam-paling-tinggi-394943. 3 December.

AIBIM. n.d. *National Scam Awareness Campaign*. https://aibim.com/national-scam-awareness-campaign. Retrieved on: 10 Oktober 2023.

Ali, M. M., & Mohd Zaharon, N. F. 2024. Phishing—A Cyber Fraud: The Types, Implications and Governance. *International Journal of Educational Reform* 33(1): 101-121.

Antônio Alves, T.F., Dalson Britto, F. F., Enivaldo Carvalho, d. R., & Willber da, S. N. 2020. Read this paper if you want to learn logistic regression. *Revista De Sociologia e Política,* 28(74): 1-19. https://doi.org/10.1590/1678-987320287406en

Aung, N.N., & Mon, H.H. 2020. Budgeting habit behavior of undergraduate students in Yangon University of Economics. *Journal of the Myanmar Academy of Arts and Science* 18(8): 39-50.

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.

Bernama. 2022. Terengganu rekod 662 kes jenayah komersial. *AstroAwani.* https://www.astroawani.com/berita-malaysia/terengganu-rekod-662-kes-jenayah-komersial-373104. 27 July.

Bernama. 2019. Taktik baharu 'love scam' gunakan Islam di Terengganu. *AstroAwani.* https://www.astroawani.com/berita-malaysia/taktik-baharu-love-scam-gunakan-islam-di-terengganu-197639?. 3 February.

Boateng, E. O. Y., & Amanor, P. M. 2014. Phishing, SMiShing & Vishing: An assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences* 5(4): 297-307

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.

Demidenko, E. (2007) Sample Size Determination for Logistic Regression Revisited. *Statistics in Medicine* 26 : 3385-3397.

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/

Dunham, D. 2022. Why men are more likely to fall for scams. The Consumer Lawyer. https://theconsumerlawyer.blog/2022/08/26/why-men-are-more-likely-to-fall-for-online-scams/. 26 August.

Eley Suzana Kasim, Norlaila Md Zin, Hazlina Mohd Padiland Normah Omar. 2020. Ponzi Schemes and its Prevention: Insights from Malaysia. *Management & Accounting Review* 19(3):89-118.

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.

Faizul Azlan Razak. 2023. Adik beradik rugi RM658,00 angkara 'Phone Scam'. *MyMetro*. https://www.hmetro.com.my/mutakhir/2023/04/953613/adik-beradik-rugi-rm658000-angkara-phone-scam. 5 April.

Farah Marshitah Abdul Patah. 2023. Penipuan melalui panggilan telefon pilihan utama 'scammer'. *BHOnline*. https://www.bharian.com.my/berita/kes/2023/12/1187143/penipuan-melalui-panggilan-telefon-pilihan-utama-scammer. 9 December.

Frauenstein, E.D. & Flowerday, S. 2020. Susceptibility to phishing on social network sites: A personality information processing model. *Comput Security* Jul;94:101862

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.

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

Ge, Y., Lu, L., Cui, X., Chen, Z., & Qu, W. 2021. How personal characteristics impact phishing susceptibility: The mediating role of mail processing. *Applied Ergonomics* 97: 103526

Hamsi, A. S., Tobi, S. N., & Masrom, M. 2015. Cybercrime over Internet Love Scams in Malaysia: A Discussion on the Theoretical Perspectives, Connecting Factors and Keys to the Problem", *Journal of Management Research* 7(2): 169-181.

Halevi, T., Lewis, J. & Memon, M. 2013. Phishing, personality traits and facebook. Cornel University, arXiv. Available at: https//arvix.org/abs/1301.7643. Accessed 11 January 2024.

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.

HSBC UK (n.d.). What's the difference between fraud and a scam? https://www.hsbc.co.uk/help/security-centre/fraud-guide/difference-between-fraud-and-scams/. Retrieved on 11 October 2023.

Kasim, E.S., Awalludin, N.R., Zainal, N., Ismail, A. and 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 Sooed. 2020. Strategi Komunikasi Penjenayah Cinta Siber Terhadap Wanita Profesional. *Jurnal Komunikasi: Malaysian Journal of Communication* 36(3): 296-311.

Khadijah Alavi, Mohammad Syahrul Azha Sooed & 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.

KKD. online. Kes Jenayah Dalam Talian Bagi Tempoh Jan-Sept Meningkat 23 Peratus – Teo**.** https://www.kkd.gov.my/awam/berita/25030-kes-jenayah-dalam-talian-bagi-tempoh-jan-sept-meningkat-23-peratus-teo. Retrieved on 10 December 2023.

KPWKM. 2021. Statistik Panggilan Palsu dan Macau Scam. Facebook. https://www.facebook.com/kpwkm/posts/sejumlah-5527-kes-penipuan-macau-scam-melibatkan-kerugian-berjumlah-lebih-rm328-/10157762902386790/. Retrieved on 15 November 2023. Retrieved on 11 November 2023.

Lee, Y.Y., Gan, C.L. & Liew, T.W. 2022. Phishing victimization among Malaysian young adults: cyber routine activities theory and attitude in information sharing online. *The Journal of Adult Protection* 24(3/4):179-194

Marzuki Yusoff. 2023. Kenapa dibiar scammer terus berleluasa?. *SinarHarian*. https://www.sinarharian.com.my/article/270495/suara-sinar/analisis-sinar/kenapa-dibiar-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.

MKN. 2023. Jenis Penipuan Atas Talian! https://www.mkn.gov.my/web/ms/2023/03/28/jenis-penipuan-atas-talian/. Retrieved on: 11 October 2023.

Modic, D. & Lea, Stephen E. G. 2012. How Neurotic are Scam Victims, Really? The Big Five and Internet Scams (September 10, 2012). Available at SSRN: https://ssrn.com/abstract=2448130 or http://dx.doi.org/10.2139/ssrn.2448130.

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 Zolkaflil, & 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.

Muhammad Adnan Pitchan, Siti Zobidah Omar, & Akmar Hayati Ahmad Ghazali. 2019. Amalan keselamatan siber pengguna internet terhadap buli siber, pornografi, e-mel phishing dan pembelian dalam talian. *Jurnal Komunikasi: Malaysian Journal of Communication* 35(3): 212-227.

Muniandy, L., Muniandy, B., & Samsudin, Z. 2016. Cyber security behaviour among higher education students in Malaysia. *Journal of Information Assurance & Cyber Security* 1-13.

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

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.

Nik Shamsiah, M.Y. 2022. Governor's Speech at the Launching of Financial Crime Exhibition. *BNM*. https://www.bnm.gov.my/-/financial-crime-exhibition-speech-en. 26 September.

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 Azura Md Amin. 2023. Wanita rugi RM1.08j diperdaya 'pegawai polis'. *Sinar Harian*. https://www.sinarharian.com.my/article/642027/berita/semasa/wanita-rugi-lebih-rm108-juta-diperdaya-pegawai-polis. 31 December.

Nor Fazlina Abdul Rahman. 2022. ADUN Kelantan rugi RM84,529 kena scam. *BHOnline*. https://www.bharian.com.my/berita/kes/2022/04/944800/adun-kelantan-rugi-rm84529-kena-scam. 11 April.

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

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.

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.

NurulAin, M., & Faezi, K. 2019. Penipuan Pakej Umrah: Penyelesaian Daripada Perspektif Perniagaan Islam. *Global Journal Al-Thaqafah* Special Issue (November): 145–157.

PDRM (2022). Trend Terkini Jenayah Komersil. (PDRM). https://heyzine.com/flip-book/cb606d5783.html. Retreived on 1 September.

Petrosyan, A. 2023. Scam encounter rate in selected countries 2022, by vector. *Statista.* https://www.statista.com/statistics/1389388/scam-rate-in-selected-countries-by-vector/. Accessed 10 January 2024.

Puram, P.K., Kaparthi, 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.

Ribeiro, L., Guedes, I.S. & Cardoso, C.S. 2024. Which factors predict susceptibility to phising? *Computers & Security* 136:103558.

Robb, C.A., & Wendel, S. 2023. Who can you trust? Assessing vulnerability to digital imposter scams. *Journal of Consumer Policy 46*: 27-51.

Sanep Ahmad, Hairunnizam Wahid & Adnan Mohamad. 2007. Pengswastaan Institusi Zakat dan Kesannya Terhadap Pembayaran secara formal di Malaysia. *International Journal of Management (IJMS)* 13(2): 175-196.

SKMM. n.d. Apa itu phising? SKMM. https://www.mcmc.gov.my/ms/faqs/phishing-attack/1-what-is-phishing. Retrieved on 16 October 2023.

Suzalina Halid. 2023. Purata 30 kes penipuan angkara scammer dilaporkan setiap hari sepanjang tahun. *BHOnline*. https://www.bharian.com.my/berita/kes/2023/12/1187845/purata-30-kes-penipuan-angkara-scammer-dilaporkan-setiap-hari-sepanjang. 11 December.

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

Tengku Danish Bahri. 2023. Kakitangan IPT rugi RM500,000 ditipu 'Love Scam'. *Kosmo.* https://www.kosmo.com.my/2023/03/28/kakitangan-ipt-rugi-rm500000-ditipu-love-scam/. 28 Mac

Wei, L., Peng, M., & Wu, W. 2021. Financial literacy and fraud detection Evidence from China. *International Review of Economics Finance* 76 (November): 478-494.

Wilson, S., Hassan, N.A., Khor, K.K., Sinnappan, S., Abu Bakar, A.R. and 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.

Yenipinar, A., Koç, S., Çanga, D. & Kaya, F. 2019. Determining Sample Size In Logistic Regression With G-Power. *Black Sea Journal Ofengineering And Science* 2(1): 16-22

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.

Zulkufli Ismail & Azmi Aziz. 2019. Jenayah siber cinta terhadap wanita professional. *e-Bangi: Journal of Social Sciences and Humanities* 16(401): 1-10.

Zaimah, R., Nurulhuda Muhamad Yusof, Sarmila, M. S. & Abd Hair Awang. 2023. Hubungan Pengetahuan dan Tingkah Laku Kewangan dengan Perancangan Kewangan Persaraan dalam Kalangan Generasi Milenial**.** *Akademika* 93(1): 373-387.

Fidlizan Muhammad (Penulis koresponden)
Fakulti Pengurusan dan Ekonomi,
Universiti Pendidikan Sultan Idris
35900 Tanjong Malim, Perak, Malaysia
Email: fidlizan@fpe.upsi.edu.my

Salwa Amirah Awang
Jabatan Pengajian Am
Politeknik Sultan Azlan Shah,
35950 Behrang Stesen, Perak, Malaysia
Email: salwa@psas.edu.my

Ahmad Zakirullah Mohamed Shaarani
Fakulti Pengurusan dan Ekonomi,
Universiti Pendidikan Sultan Idris
35900 Tanjong Malim, Perak, Malaysia
Email: zakirullah@fpe.upsi.edu.my

Mohd Yahya Mohd Hussin
Fakulti Pengurusan dan Ekonomi,
Universiti Pendidikan Sultan Idris
35900 Tanjong Malim, Perak, Malaysia
Email: yahya@fpe.upsi.edu.my

Nurhanie Mahjom
Fakulti Pengurusan dan Ekonomi,
Universiti Pendidikan Sultan Idris
35900 Tanjong Malim, Perak, Malaysia
Email: nurhanie@fpe.upsi.edu.my