e-Bangi Faculty of Social Sciences and Humanities Universiti Kebangsaan Malaysia
Journal of Social Sciences and Humanities

eISSN: 1823-884x

Volume 22, Issue 3, DOI: https://doi.org/10.17576/ebangi.2025.2203.49

Artikel

Pengaruh Pengetahuan Terhadap Persepsi Risiko *Mule Account* Dalam Kalangan Pengguna Bank Digital

(The Influence of Knowledge on Mule Account Risk Perceptions among Digital Bank Users)

Norazmee Mohamed & Nur Hafizah Yusoff*

Center for Research in Development, Social and Environment,,Faculty of Social Sciences and Humanities, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor Malaysia

*Pengarang Koresponden: nur_hafizah@ukm.edu.my

Diserah: 01 Jun 2025
Diterima: 20 Ogos 2025

Abstrak: Kajian ini bertujuan untuk meneliti tahap pengetahuan pemegang akaun terhadap risiko penglibatan dalam aktiviti *mule account* serta persepsi mereka terhadap kemungkinan menjadi mangsa jenayah kewangan siber *Mule account* merujuk kepada individu yang membenarkan akaun bank mereka digunakan bagi tujuan pemindahan wang secara tidak sah sama ada secara sedar ataupun tidak, dan sering kali dikaitkan dengan penipuan dalam talian dan jenayah siber. Kajian ini menggunakan reka bentuk tinjauan secara kuantitatif dengan persampelan bertujuan, melibatkan pengumpulan data melalui borang soal selidik berstruktur dan analisis deskriptif. Dapatan kajian menunjukkan walaupun majoriti responden mempunyai pengetahuan umum yang tinggi tentang konsep asas mule account seperti definisi, risiko undang-undang dan bentuk tawaran mencurigakan, tahap pengetahuan terhadap aspek praktikal seperti saluran pelaporan rasmi, aplikasi keselamatan, dan nombor h*otline* bank masih sederhana rendah. Kekurangan ini menyumbang kepada kelemahan kesedaran risiko dan tindakan pencegahan, termasuk persepsi bahawa kemungkinan menjadi mangsa adalah rendah. Implikasi kajian menegaskan bahawa peningkatan literasi kewangan praktikal dan pendedahan terhadap saluran perlindungan rasmi adalah penting bagi membentuk kesedaran dan mencegah eksploitasi akaun bank oleh rangkaian jenayah siber. Justeru, institusi kewangan dan pihak berkuasa perlu memperkukuh pendidikan pengguna dengan menekankan aspek pencegahan dan kemudahan akses maklumat keselamatan bagi mengekang pertumbuhan *mule account* di Malaysia.

Kata Kunci: Jenayah kewangan siber; pengetahuan; akaun keldait; penipuan online; persepsi terhadap risiko

Abstract: This study aims to examine account holders' level of knowledge regarding the risks of involvement in mule account activities, as well as their perception of the likelihood of becoming victims of financial cybercrime. A mule account refers to an individual who allows their bank account to be used for unauthorised money transfers, either knowingly or unknowingly. It is often linked to online fraud and cybercriminal networks. This study employed a quantitative survey design involving a purposively selected group of respondents. The data were collected using a structured questionnaire and analysed using descriptive statistics. The findings revealed that most respondents had a high level of general knowledge about mule accounts, including their definition, legal risks, and common forms of fraudulent offers. However, practical knowledge regarding official reporting channels, security applications, and bank hotline numbers was found to be moderately low. This gap in practical knowledge contributed

to a lower awareness of personal risk and inadequate preventive actions among account holders. The study also found that individuals unaware of how to protect their accounts proactively were more likely to underestimate their risk of becoming victims. The findings highlight the importance of improving practical financial literacy and increasing public exposure to official protection channels to strengthen user awareness and prevent account exploitation by cybercriminals. The study recommends that financial institutions and relevant authorities enhance consumer education efforts by focusing on actionable preventive measures and improving access to official security information to curb the rise of mule accounts in Malaysia.

Keywords: Cyber financial crime; knowledge; mule account; online fraud; risk perception

Pengenalan

Jenayah siber (*cybercrime*) merujuk kepada aktiviti jenayah yang dilakukan dengan menggunakan teknologi maklumat atau sistem komputer sebagai alat, sasaran, atau lokasi. Menurut Brenner (2010) dalam bukunya *Cybercrime, Criminal Threats from Cyberspace*, jenayah siber didefinisikan sebagai aktiviti jenayah yang menggunakan teknologi komputer untuk memanipulasi data, sistem, atau rangkaian bagi mendapatkan keuntungan atau menyebabkan kerugian kepada pihak lain. Sabillon et al. (2016) pula menyatakan bahawa jenayah siber secara umumnya merujuk kepada suatu perbuatan yang dilakukan secara sengaja atau tidak, oleh individu atau kumpulan yang mewakili mana-mana organisasi bagi mendapatkan maklumat secara tidak sah atau merosakkan peranti komputer, telefon pintar dan rangkaian internet. Selain itu, Holt et al. (2020) mendefinisikan jenayah siber sebagai "sebarang tindakan jenayah yang melibatkan penggunaan komputer, rangkaian atau peranti lain sebagai alat utama untuk melakukan atau memudahkan perbuatan jenayah. Mereka turut (2020) mengelaskan jenayah siber kepada beberapa jenis seperti penggodaman komputer dan perisian berbahaya, cetak rompak digital dan pencurian hak intelek, jenayah ekonomi dan penipuan dalam talian, pornografi dan jenayah seksual dalam talian, buli siber dan mengintai siber, serta keganasan siber dan ekstremisme.

Mule account merupakan bahagian penting dalam rangkaian jenayah dan sangat penting/signifikan bagi ahli utama dalam sesuatu organisasi jenayah kerana digunakan untuk mangaburkan jejak yang boleh membawa pihak berkuasa kepada dalang sebenar rangkaian tersebut, (Leukfeldt & Jurjen Jansen 2015)). Sebagai contoh, pengirim wang mendaftar akaun bank atau perniagaan atas nama mereka, namun akaun tersebut sebenarnya dieksploitasi oleh rangkaian jenayah Beberapa kajian turut mengakui peranan penting *mule account* dalam pengalihan wang yang dicuri oleh penjenayah siber yang terlibat dalam jenayah kewangan siberseperti serangan kad kredit (carding) atau phishing (Choo, 2008; Moore & Clayton, 2009; McCombie, 2011; Aston et al,. 2009; Soudijn & Zegers, 2012; Leukfeldt, 2014; Leukfeldt et al., 2016b, 2016c).

Menurut Nik Adzeriman et al. (2023), *mule account* ditaksirkan juga sebagai individu yang menerima wang daripada pihak ketiga ke dalam akaun bank mereka, lalu memindahkannya kepada individu lain dalam bentuk tunai atau bentuk lain selepas memperoleh komisen. Walaupun mereka tidak terlibat secara langsung dalam jenayah yang menghasilkan wang tersebut seperti jenayah siber, penipuan pembayaran dan dalam talian, dadah, pemerdagangan manusia dan sebagainya. Mereka tetap dianggap sebagai rakan subahat. Selain itu, menurut Vedamanikam dan Chethiyar (2020) menjelaskan bahawa *mule account* ialah individu yang bukan sebahagian daripada rangkaian jenayah, tetapi diupah dan dimasukkan ke dalam rangkaian tersebut untuk mengaburkan jejak aliran wang. Mereka memutuskan jejak aliran wang sementara penjenayah mendapat manfaat daripada dana yang dibersihkan. *Mule account* menerima wang daripada pihak ketiga ke dalam akaun bank mereka dan kemudian mengeluarkan wang tunai atau memindahkan dana ke akaun lain serta menerima komisen bagi pemindahan tersebut.

Selain itu, Ilyas et el.(2022) pula menambah bahawa m*ule account* juga merujuk kepada sebagai akaun bank yang digunakan oleh orang lain, sama ada tanpa pengetahuan pemilik akaun atau dengan kerelaaan mereka, untuk memperoleh ganjaran melalui transaksi kewangan haram atau tidak sah. tanpa pengetahuan atau secara sukarela oleh pemilik akaun untuk memperoleh ganjaran atau melalui cara penipuan bagi transaksi kewangan

yang haram atau tidak sah. Artikel *Financial Times* melaporkan bahawa organisasi jenayah semakin menjadikan igolongan muda/remaja sebagai *mule account* untuk mencuci wang hasil aktiviti haram dengan membuat iklan pekerjaan palsu di laman web pekerjaan dan platform media sosial (Uddin,2021). Digelar sebagai "Generasi Covid", mangsa lazimnya berumur antara 21 hingga 30 tahun dan sedang mencari pekerjaan semasa pandemik. Penjenayah menggunakan media sosial untuk mengiklankan "peluang pekerjaan" dengan memaparkan gambar wang yang banyak atau gaya hidup mewah. Individu kemudian dipujuk untuk menjadi "ejen pemindahan wang" atau "pemproses tempatan" dengan jani menjana pendapatan cepat.

Keadaan/fenomena ini sangat membimbangkan kerana peningkatan penggunaan *mule account* jelas kelihatan berdasarkan statistik daripada Jabatan Siasatan Jenayah Komersil, Bukit Aman. Bagi tempoh tiga jumlah *mule account* yang dikenal pasti ialah 33,267 akaun pada tahun 2022, meningkat kepada 46,048 akaun pada tahun 2023, dan seterusnya 50,295 akaun sehingga tahun 2024.Peningkatan ini secara tidak langsung memberi kesan kepada jumlah kes di bawah pengendalian Jabatan Siasatan Jenayah Komersil (JSJK). Petikan daripada *Facebook* Polis Di Raja Malaysia bertarikh 15 November 2024, bertajuk (Jabatan Siasatan Jenayah Komersil (JSJK) sentiasa perhebat usaha perangi pelbagai jenayah Komersil oleh Ketua Polis Negara mengatakan bahawa bahawa bagi tahun 2024, sebanyak 29,010 kes jenayah komersil dilaporkan dari Januari hingga September, berbanding 30,422 kes dalam tempoh sama pada tahun 2023. Ini menunjukkan penurunan sebanyak 4.6 peratus atau 1,412 kes. Namun begitu, jumlah kerugian yang direkodkan dalam tempoh sama pada tahun 2024 meningkat kepada RM1.98 bilion, iaitu peningkatan 22.6 peratus berbanding tahun sebelumnya.

Sehubungan itu, objektif penulisan ini adalah untuk menganalisis tahap pengetahuan responden dan bagaimana pengetahuan tersebut mempengaruhi persepsi mereka berkaitan risiko menjadi mangsa jenayah *mule account.*

Sorotan Literatur

1. Senario Pengubahan Wang Haram Melalui *Mule Account*

Menurut Europol (2023), terdapat peningkatan ketara dalam kes *mule account* dalam beberapa tahun kebelakangan ini, di mana ribuan individu terlibat secara tidak sengaja dalam operasi ini, sering kali akibat terpedaya dengan tawaran pekerjaan yang kelihatan sah dan menarik. Kesedaran masyarakat dilihat sebagai elemen utama dalam mencegah penglibatan dalam aktiviti *mule account*. Kajian oleh Jones et al. (2022) menunjukkan bahawa kurangnya kesedaran mengenai risiko dan akibat undang-undang yang terlibat boleh meningkatkan kemungkinan seseorang menjadi mangsa penipuan ini. Walaupun agensi penguatkuasaan undang-undang dan institusi kewangan telah melaksanakan pelbagai program kesedaran untuk mendidik orang awam, masih wujud persoalan mengenai keberkesanan program-program tersebut dalam mengubah tingkah laku. Sebagai contoh, Smith dan Hernandez (2021) menegaskan bahawa walaupun program kesedaran semakin banyak diperkenalkan, masih ramai individu yang tidak menyedari implikasi undang-undang dan isu etika yang berkait rapat dengan peranan sebagai *money mule*. Kekurangan kesedaran ini menekankan keperluan untuk memahami pelbagai faktor yang mempengaruhi keputusan individu untuk terlibat dalam aktiviti ini.

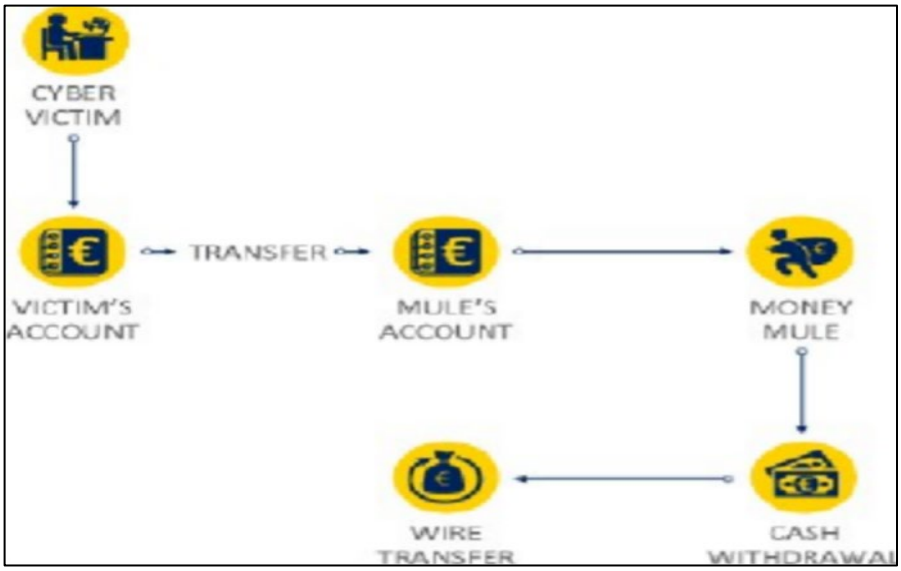
Di samping itu, aktiviti *mule account* semakin menjadi isu yang meruncing di Malaysia, khususnya dalam kalangan golongan muda. Kajian-kajian terkini menunjukkan bahawa pelajar universiti kini menjadi sasaran utama dalam perekrutan aktiviti ini. Menurut Hashim dan Abdul Rahman (2020), keputusan pelajar untuk menerima tawaran pekerjaan berkaitan *mule account* sering kali berpunca daripada kurangnya pemahaman mengenai implikasi undang-undang serta persepsi bahawa memperoleh wang secara mudah dan pantas adalah sah dan selamat. Penemuan ini selaras dengan kajian Jones et al. (2019) dan Lee dan Smith (2018), yang turut mendapati tahap kesedaran yang rendah serta pemahaman yang lemah mengenai penipuan kewangan dalam kalangan golongan muda menjadikan mereka mudah terdedah kepada eksploitasi. Tambahan pula, Brown (2017) melaporkan bahawa remaja yang mempunyai tahap literasi kewangan yang rendah lebih mudah terpedaya dengan tawaran pekerjaan palsu atau imbuhan lumayan tanpa menyedari implikasi undang-undang yang serius apabila menjadi *money mule*.

Selain itu, tren semasa menunjukkan peningkatan penyertaan golongan muda, khususnya mereka yang dilahirkan antara tahun 2000 hingga 2010. Sekitar 15% daripada semua *mule account* yang dikenal pasti berasal daripada kumpulan umur ini, dengan kira-kira 95% daripadanya adalah lelaki (Tietoevry, 2024). Kajian-kajian sebelumnya secara konsisten menunjukkan perbezaan jantina dalam perekrutan *mule account*, dengan lelaki lebih kerap menjadi sasaran kerana kecenderungan mereka mengambil risiko serta pengaruh daripada kumpulan sebaya (Smith & Hernandez, 2021). Statistik dan penemuan ini menyoroti jurang kesedaran yang kritikal dalam kalangan belia, yang memerlukan intervensi pendidikan yang lebih tertumpu bagi meningkatkan pemahaman mereka tentang risiko serta implikasi undang-undang melibatkan diri dalam skim *mule account*. Tanpa intervensi tersebut, individu-individu ini berisiko untuk terus dieksploitasi, sekaligus memperburuk lagi landskap jenayah kewangan di Malaysia.

2. Modus Operandi *Mule Account*

Menurut Vedamanikam dan Chethiyar (2020), *keldai wang* bukanlah sebahagian daripada rangkaian jenayah secara langsung, tetapi mereka dimasukkan secara khusus ke dalam rangkaian tersebut untuk mengaburkan jejak wang yang terlibat dalam aktiviti haram serta mengelirukan pihak berkuasa. Kebanyakan *keldai wang* terdiri daripada golongan muda yang tidak mempunyai pengetahuan mencukupi tentang tingkah laku jenayah dan menyangka bahawa ia merupakan pekerjaan yang sah. Golongan penganggur, pelajar, dan mereka yang berada dalam keadaan kewangan terdesak sering menjadi sasaran mudah bagi penjenayah. Individu yang berumur antara 15 hingga 44 tahun dikenal pasti aktif terlibat dalam kegiatan ini, dengan kumpulan umur 24 hingga 34 tahun mencatatkan kadar penyertaan tertinggi.

Aliran proses *keldai wang* ditunjukkan dalam Rajah 1, di mana mereka menerima dana daripada aktiviti haram ke dalam akaun bank peribadi. Dana tersebut kemudiannya dipindahkan kepada individu lain atau akaun lain yang dikawal oleh penjenayah. Selain beroperasi sendiri, terdapat juga *keldai wang* yang membuka akaun bank atau perniagaan atas nama mereka, yang kemudiannya digunakan sepenuhnya oleh rangkaian penjenayah untuk tujuan pencucian wang haram. Oleh itu, *keldai wang* dianggap sebagai rakan subahat dalam aktiviti jenayah kerana mereka membantu secara langsung dalam proses pengubahan wang haram.



Rajah 1. Aliran proses keldai wang
Sumber: Europol (2019)

Terdapat empat kaedah utama yang digunakan oleh rangkaian jenayah untuk merekrut *keldai wang*, iaitu melalui pertemuan bersemuka, enjin carian kerja dalam talian, rangkaian sosial, serta laman web temu janji dalam talian. Penjenayah akan memaparkan iklan kekosongan jawatan palsu seperti pengurus akaun, pengurus

pelanggan, pembeli misteri, ejen pemprosesan pembayaran, ejen pemindahan wang, dan pelbagai lagi dengan kriteria kerja yang menarik, tawaran gaji lumayan, serta fleksibiliti bekerja. Iklan ini dipaparkan di platform seperti *Facebook, WhatsApp*, laman sosial pencarian kerja seperti *LinkedIn,* forum kerja dalam talian, sesi sembang, iklan akhbar, *e-mel,* serta enjin carian kerja. Tawaran kerja sebegini biasanya mendapat sambutan segera kerana faktor fleksibiliti, insentif kewangan, dan ganjaran yang ditawarkan, sehingga membuatkan individu percaya bahawa mereka benar-benar diambil bekerja untuk jawatan tersebut (Arevalo, 2015; Vedamanikam & Chethiyar, 2020).

Kes *mule account* yang direkrut melalui hubungan dalam talian atau penipuan cinta juga dilaporkan semakin meningkat, sejajar dengan modus operandi penjenayah yang kini lebih aktif merekrut melalui laman temu janji dalam talian dan rangkaian sosial. Penjenayah biasanya membina hubungan, meraih kepercayaan mangsa, dan meyakinkan mereka untuk melakukan pemindahan dana atau membuka akaun bank atas alasan menghantar atau menerima wang. Maklumat yang diberikan kepada mangsa adalah terhad, dengan penekanan diberikan kepada hubungan peribadi bagi menyembunyikan tujuan jenayah yang sebenar. Selain penipuan cinta, penjenayah turut menggunakan media sosial untuk merekrut rakan jenayah baharu melalui iklan dalam talian yang menjanjikan kekayaan segera, penipuan loteri, penipuan pekerjaan, serta penipuan harta pusaka (Arevalo, 2015; Vedamanikam & Chethiyar, 2020).

Metodologi Kajian

1. Reka Bentuk Kajian

Kajian ini menggunakan reka bentuk kuantitatif kerana ia membolehkan data dikumpulkan secara objektif dan dianalisis menggunakan kaedah statistik. Menurut Sabitha (2006), reka bentuk kajian ialah tindakan sistematik yang menggariskan prosedur penyelidikan, manakala Mohd Najib (1999) mentakrifkannya sebagai kaedah terancang untuk memperoleh maklumat bagi menjawab persoalan serta mencapai objektif kajian. Pendekatan kuantitatif dipilih kerana sesuai untuk menilai tahap pengetahuan dan kesedaran pemegang akaun bank mengenai risiko mule account melalui pengumpulan data berbentuk angka yang boleh diukur dan dibandingkan secara saintifik.

2. Kaedah Persampelan

Populasi kajian ini terdiri daripada dua kumpulan utama. Kumpulan pertama ialah pemegang akaun CIMB Bank dan Maybank di cawangan Bangi, Selangor yang berumur 18 tahun ke atas serta memiliki akaun simpanan. Kumpulan kedua pula terdiri daripada pegawai bank yang terlibat secara langsung dalam pengurusan akaun di kedua-dua bank tersebut. Pemilihan populasi ini dibuat berdasarkan pertimbangan bahawa CIMB Bank dan Maybank mempunyai jumlah pemegang akaun yang tinggi serta rekod yang jelas berkaitan masalah *mule account*. Selain itu, kedua-dua bank ini mempunyai bilangan cawangan yang banyak, sekali gus membolehkan kajian ini memberikan gambaran yang lebih luas mengenai isu yang dikaji.

Kajian ini menggunakan pendekatan kuantitatif bagi mengumpul data yang objektif dan boleh dianalisis secara statistik. Instrumen utama yang digunakan ialah soal selidik, yang diedarkan kepada pemegang akaun bank. Populasi keseluruhan bagi kajian ini berjumlah 102,367 orang pemegang akaun di CIMB Bank dan Maybank cawangan Bangi dalam tempoh tiga tahun terkini. Saiz sampel ditentukan dengan merujuk kepada jadual Krejcie dan Morgan (1970), yang mencadangkan seramai 390 responden sebagai saiz sampel yang sesuai.

Bagi memastikan keterwakilan yang seimbang, penyelidik menggunakan kaedah persampelan rawak berstrata, di mana 50% responden dipilih daripada Maybank dan 50% lagi daripada CIMB Bank. Kaedah ini dipilih kerana ia dapat mengurangkan bias pemilihan serta menjamin pengedaran sampel yang lebih representatif antara kedua-dua bank. Soal selidik yang diedarkan bertujuan mendapatkan data berkaitan tahap pengetahuan dan kesedaran responden mengenai risiko *mule account*.

3. Kaedah Pengumpulan Data

Pengumpulan data dalam kajian ini dijalankan menggunakan borang soal selidik berstruktur sebagai instrumen utama. Soal selidik ini diedarkan kepada pemegang akaun CIMB Bank dan Maybank di cawangan Bangi, Selangor yang dipilih sebagai responden kajian. Kaedah soal selidik dipilih kerana ia dapat mengumpul maklumat dalam jumlah yang besar dengan kos dan masa yang lebih efisien, di samping membolehkan data dianalisis secara kuantitatif. Proses pengumpulan data dilaksanakan dalam tempoh tertentu dengan kerjasama pihak pengurusan bank. Responden diberikan penjelasan ringkas mengenai tujuan kajian, manakala aspek kerahsiaan, anonimit**i**, dan persetujuan termaklum (*informed consent*) diberi penekanan bagi mematuhi etika penyelidikan. Semua soal selidik dikumpul semula setelah diisi bagi memastikan kadar pulangan yang memuaskan dan kesahan data yang diperoleh.

3. Kaedah Memproses dan Menganalisis Data

Setelah data diperoleh melalui borang soal selidik, aplikasi *Statistical Package for Social Science* (SPSS) telah digunakan untuk menganalisis maklumat yang didapati dari responden. Data dipersembahkan secara analisis deskriptif melalui analisis frekuensi, peratusan dan min. Analisis deskriptif telah dilakukan untuk setiap jawapan kepada objektif kajian yang diberikan oleh responden. Analisis kesahan kebolehpercayaan instrumen telah dilakukan pada bahagian B, C dan D. Analisis frekuensi dan min juga telah digunakan dalam kajian ini.

Hasil Kajian dan Perbincangan

1. Profil Sosiodemografi

Seramai 390 orang responden telah menjawab soal selidik yang diedarkan secara dalam talian. Daripada jumlah tersebut, 62.3% adalah lelaki, manakala bakinya adalah wanita. Dari segi bangsa, majoriti responden terdiri daripada kaum Melayu, iaitu sebanyak 89.0% daripada keseluruhan responden. Taburan ini mencerminkan realiti demografi kawasan kajian iaitu Bangi, yang terletak dalam daerah Hulu Langat, Selangor. Menurut Jabatan Perangkaan Malaysia (DOSM, 2020), etnik Bumiputera merupakan kumpulan penduduk terbesar di daerah Hulu Langat (58.3%), diikuti kaum Cina (25.3%) dan India (14.9%). Struktur penduduk di peringkat nasional turut menunjukkan dominasi etnik Melayu/Bumiputera, iaitu sekitar 69.4% daripada populasi warganegara Malaysia (DOSM, 2020). Oleh itu, peratusan responden Melayu yang tinggi dalam kajian ini adalah sejajar dengan demografi tempatan dan kebangsaan, sekali gus menjadikan dapatan ini representatif dari segi komposisi etnik.

Tahap pendidikan merupakan indikator penting dalam menentukan literasi kewangan serta keupayaan individu memahami dan menilai risiko kewangan, termasuk risiko penyalahgunaan akaun bank seperti *mule account*. Berdasarkan dapatan kajian, majoriti responden mempunyai tahap pendidikan tinggi. Sebanyak 32.6% merupakan pemegang Ijazah Sarjana Muda, diikuti oleh 28.2% Diploma, 15.9% Ijazah Sarjana, dan 1.3% Ijazah Kedoktoran (PhD). Selebihnya berpendidikan sekolah menengah (17.4%), sijil kemahiran (4.1%), dan sekolah rendah (0.5%). Taburan ini menunjukkan bahawa sebahagian besar responden mempunyai latar belakang akademik yang tinggi, yang berkait rapat dengan tahap celik kewangan lebih baik. Seperti ditegaskan oleh Lusardi dan Mitchell (2014), tahap pendidikan yang lebih tinggi secara signifikan meningkatkan literasi kewangan serta kebolehan individu membuat keputusan kewangan yang rasional.

Dari segi pekerjaan, responden datang daripada pelbagai latar belakang, sekali gus memberikan gambaran menyeluruh terhadap kumpulan pemegang akaun bank. Sebanyak 45.4% bekerja dalam sektor kerajaan, menjadikan mereka kumpulan terbesar dalam kajian ini. Responden dari sektor swasta mewakili 18.5%, pelajar (15.6%), pesara (12.6%), bekerja sendiri (5.1%), tidak bekerja (2.6%), manakala sektor badan bukan kerajaan (NGO) hanya 0.3%. Dapatan ini menunjukkan bahawa penjawat awam merupakan kumpulan pekerjaan paling ramai dalam kalangan responden, yang boleh dijelaskan berdasarkan faktor lokasi kajian, struktur demografi tempatan, serta kemudahan capaian terhadap kumpulan ini.

Jenis akaun bank yang dimiliki responden juga merupakan elemen penting dalam menilai keterlibatan mereka dalam sistem perbankan serta risiko terhadap jenayah kewangan seperti *mule account*. Hasil analisis

menunjukkan bahawa jenis akaun paling dominan ialah akaun simpanan sahaja (71.8%), diikuti oleh gabungan akaun simpanan dan semasa (16.4%), serta akaun semasa sahaja (6.4%). Baki responden memiliki pelbagai gabungan lain termasuk akaun pelaburan dan akaun khas. Kepelbagaian jenis akaun ini mencerminkan tahap keterlibatan responden dalam urusan kewangan, namun dominasi akaun simpanan menunjukkan kebanyakan responden menggunakan akaun bank untuk transaksi asas dan penyimpanan wang.

Majoriti responden (lebih dua pertiga) hanya mempunyai akaun simpanan, iaitu jenis akaun paling asas dan lazim digunakan untuk menyimpan wang dan menjalankan transaksi harian. Akaun simpanan mudah diakses melalui kad ATM, perbankan internet, dan aplikasi mudah alih, yang menjadikannya berisiko tinggi untuk disalahgunakan sindiket penipuan sekiranya pemegang akaun tidak berhati-hati menguruskan keselamatan maklumat mereka. Sebanyak 16.4% pula memiliki gabungan akaun simpanan dan semasa, yang menunjukkan penglibatan mereka dalam urusan kewangan lebih aktif seperti perniagaan kecil atau transaksi rasmi. Akaun semasa lazimnya digunakan oleh individu atau syarikat untuk urus niaga yang lebih kerap dan kompleks, justeru pemilik akaun ini lebih berhati-hati dalam pengurusan kewangan. Hanya sebilangan kecil responden mempunyai gabungan tiga jenis akaun atau akaun "lain-lain" seperti akaun pelaburan, akaun perniagaan kecil, akaun Tabung Haji, Amanah Saham, atau e-wallet yang dikaitkan dengan sistem bank utama.

2. Pengetahuan Berkaitan *Mule Account*

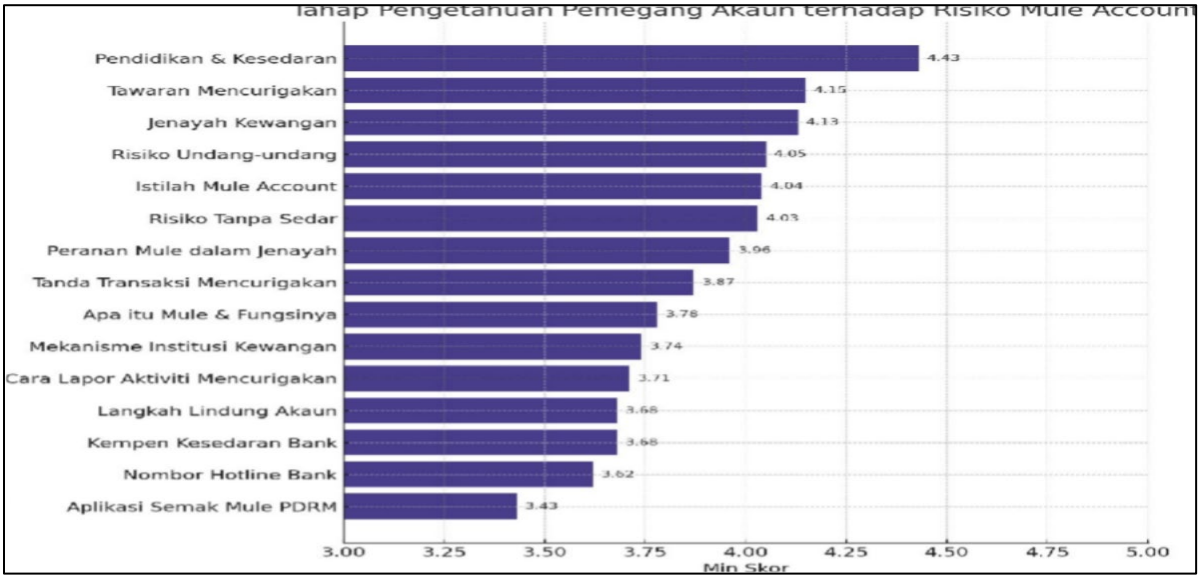
Sebanyak 15 item berkaitan aspek pengetahuan telah diajukan kepada responden dan dianalisis menggunakan kaedah statistik deskriptif melalui SPSS. Hasil dapatan menunjukkan kesemua item mencatatkan skor min melebihi 3.40, menandakan bahawa secara umumnya tahap pengetahuan responden berada pada kategori tinggi, manakala satu item mencatatkan tahap sangat tinggi. Dapatan ini memperlihatkan bahawa responden mempunyai asas yang baik dalam mengenal pasti risiko berkaitan *mule account* serta memahami implikasi undang-undang dan peranan institusi kewangan dalam mencegah jenayah ini. Tahap pengetahuan yang tinggi dalam kalangan pemegang akaun amat penting kerana mereka merupakan barisan hadapan yang paling mudah menjadi sasaran sindiket penipuan kewangan.

Kajian ini meneliti tahap pengetahuan pemegang akaun bank terhadap risiko penglibatan dalam aktiviti *mule account*. Berdasarkan analisis soal selidik kuantitatif, min skor bagi 15 item yang dikaji dipaparkan dalam bentuk carta bar (Rajah 2). Secara keseluruhan, skor min bagi semua item berada dalam julat sederhana tinggi iaitu antara 3.43 hingga 4.43 (skala Likert 1 hingga 5). Item dengan skor min tertinggi ialah "Pendidikan & Kesedaran" (min = 4.43), menunjukkan majoriti responden menyedari bahawa pendedahan maklumat dan pendidikan merupakan elemen penting dalam mencegah penglibatan sebagai *money mule*. Item ini diikuti oleh "Tawaran Mencurigakan" (min = 4.15) dan "Jenayah Kewangan" (min = 4.13), yang mencerminkan tahap kesedaran yang tinggi terhadap kewujudan tawaran pekerjaan berisiko serta kefahaman asas bahawa aktiviti *mule account* berkait rapat dengan jenayah kewangan.

Selain itu, beberapa item turut mencatatkan skor min melebihi 4.00, iaitu "Risiko Undang-undang" (4.05), "Istilah Mule Account" (4.04), dan "Risiko Tanpa Sedar" (4.03). Dapatan ini menunjukkan responden memahami risiko dari sudut implikasi undang-undang serta kesedaran bahawa mereka boleh terlibat dalam aktiviti ini tanpa niat atau secara tidak sedar. Walau bagaimanapun, terdapat item yang mencatatkan skor min sederhana rendah, iaitu "Langkah Lindung Akaun" (3.68), "Kempen Kesedaran Bank" (3.68), "Nombor Hotline Bank" (3.62), dan yang paling rendah ialah "Aplikasi Semak Mule PDRM" (3.43). Penemuan ini menunjukkan wujudnya kelemahan pengetahuan dalam kalangan responden terhadap mekanisme pelaporan rasmi serta saluran perlindungan diri yang disediakan oleh pihak berkuasa dan institusi kewangan.

Dapatan kajian juga menunjukkan bahawa walaupun sebahagian besar responden mengetahui kewujudan hotline bank, tahap pengetahuan mereka terhadap nombor khusus setiap institusi kewangan masih rendah. Kekurangan ini berpunca daripada kaedah penyampaian maklumat oleh pihak bank yang tidak seragam serta sukar diakses melalui medium utama seperti laman sesawang atau aplikasi mudah alih. Keadaan ini berpotensi menyebabkan kelewatan proses pelaporan apabila berlaku aktiviti mencurigakan. Kelewatan tersebut secara langsung boleh melambatkan tindakan pencegahan atau sekatan transaksi, sekali gus meningkatkan risiko

kerugian kewangan. Dalam kes jenayah seperti *mule account*, tindakan pantas amat kritikal kerana dana yang dipindahkan biasanya segera dialihkan ke akaun lain, menjadikan proses pengesanan dan pemulangan dana lebih rumit.



Rajah 2. Tahap pengetahuan pemegang akaun terhadap risiko *mule account*
Sumber: Kajian lapangan (2025)

Sebagai langkah intervensi nasional, kerajaan telah menubuhkan Pusat Respons Scam Kebangsaan (NSRC) di bawah Pusat Jenayah Kewangan Nasional (NFCC). NSRC telah memperkenalkan talian hotline 997, iaitu saluran tunggal nasional untuk orang awam melaporkan penipuan kewangan dalam talian, khususnya yang melibatkan aplikasi perbankan dan e-dompet. Tujuan utama talian ini adalah untuk: (i) mempercepatkan proses pelaporan, (ii) membolehkan tindakan segera menyekat transaksi mencurigakan, dan (iii) memastikan koordinasi pantas antara bank serta agensi penguatkuasaan. Walau bagaimanapun, keberkesanan talian ini masih bergantung pada tahap kesedaran pengguna, iaitu sama ada mereka mengetahui kewujudan talian 997 serta memahami bila dan bagaimana ia perlu digunakan. Oleh itu, dapatan kajian ini menekankan keperluan memperluas pendedahan awam kepada inisiatif sebegini, agar pengguna bukan sahaja sedar tentang kewujudan talian hotline, tetapi juga mampu bertindak segera dan tepat apabila diperlukan.

Tingginya skor min bagi item seperti "Pendidikan & Kesedaran" dan "Tawaran Mencurigakan" menunjukkan bahawa pendedahan awam mengenai risiko pekerjaan palsu dan aktiviti jenayah berkaitan *mule account* telah mencapai tahap keberkesanan tertentu. Dapatan ini selaras dengan kajian Hashim dan Abdul Rahman (2020) yang mendapati bahawa golongan muda mempunyai kesedaran am tentang kewujudan risiko pekerjaan tidak sah, namun masih lemah dari segi keupayaan melindungi diri secara efektif. Peningkatan kesedaran ini juga mungkin berpunca daripada usaha pelbagai agensi seperti Bank Negara Malaysia (BNM), Polis Diraja Malaysia (PDRM), serta bank-bank komersial yang giat melaksanakan kempen media sosial, ceramah, dan infografik mengenai isu *money mule*. Namun demikian, keberkesanan mesej masih tidak menyeluruh memandangkan item berkaitan kempen bank hanya mencatatkan skor min sederhana.

Selain itu, skor min yang tinggi bagi item "Risiko Undang-undang" (4.05) menunjukkan bahawa responden menyedari akibat serius menjadi *mule*, termasuk kemungkinan penahanan, denda, dan rekod jenayah. Dapatan ini konsisten dengan kajian Jones et al. (2019) yang menekankan bahawa walaupun individu muda menyedari risiko undang-undang, mereka masih sanggup mengambil risiko sekiranya ganjaran kewangan dilihat tinggi.

Sebaliknya, kelemahan ketara dapat dilihat dalam aspek penggunaan alat sokongan rasmi, seperti Aplikasi Semak Mule PDRM (3.43) dan Hotline Bank (3.62). Tahap pengetahuan yang rendah dalam aspek ini menunjukkan bahawa walaupun responden peka terhadap bahaya *mule account*, mereka tidak mengetahui cara menyemak atau melaporkan aktiviti mencurigakan. Keadaan ini memperlihatkan kekurangan dalam literasi teknologi keselamatan kewangan, terutamanya dalam kalangan responden muda atau pelajar yang mungkin belum pernah berurusan secara langsung dengan agensi penguatkuasaan. Penemuan ini menyokong laporan Europol (2023) yang menegaskan bahawa kurangnya kesedaran terhadap saluran pelaporan rasmi sering menyebabkan individu menjadi mangsa secara tidak sedar.

3. Pengetahuan dan Persepsi Risiko Sebagai Mangsa *Mule Account*

Dapatan kajian menunjukkan bahawa pemegang akaun mempunyai pengetahuan umum yang tinggi mengenai konsep dan risiko *mule account*, namun pengetahuan praktikal mereka tentang saluran bantuan dan perlindungan masih rendah. Perbezaan ini memberikan impak besar terhadap persepsi individu terhadap risiko menjadi mangsa, sekali gus mempengaruhi tingkah laku pencegahan. Menurut Teori Perlakuan Terancang (Ajzen, 1991), pengetahuan seseorang membentuk kepercayaan mereka terhadap risiko dan hasil sesuatu tindakan, yang kemudiannya membentuk persepsi serta niat untuk bertindak. Dalam konteks ini, individu yang mempunyai pengetahuan tinggi tentang bentuk penipuan *mule account*, risiko undang-undang, serta cara mengendalikan akaun bank dengan selamat cenderung untuk memiliki persepsi risiko yang lebih tinggi dan lebih berhati-hati. Sebaliknya, kekurangan pengetahuan praktikal seperti tidak mengetahui cara menggunakan aplikasi PDRM untuk menyemak akaun atau tidak mengetahui nombor hotline bank untuk melaporkan aktiviti mencurigakan\ menyebabkan individu merasakan risiko mereka rendah, kerana ancaman tersebut tidak dilihat wujud secara dekat dan nyata.

Dalam kajian ini, min skor bagi item "Aplikasi Semak Mule PDRM" adalah 3.43, iaitu yang terendah daripada 15 item pengetahuan. Hal ini menunjukkan bahawa sebahagian besar responden tidak mengetahui kewujudan aplikasi ini, apatah lagi cara menggunakannya. Implikasinya, mereka mungkin tidak pernah menyemak sama ada akaun telah digunakan oleh pihak ketiga, dan seterusnya tidak menganggap diri berisiko menjadi mangsa. Begitu juga, skor min bagi item "Nombor Hotline Bank" hanya 3.62, menunjukkan tahap pengetahuan terhadap saluran bantuan rasmi adalah terhad. Kekurangan ini menjejaskan tindakan proaktif seperti membuat semakan akaun, menghubungi institusi kewangan, atau melaporkan tawaran kerja mencurigakan, kerana persepsi mereka ialah bahawa risiko hanya berlaku kepada orang lain.

Kajian terdahulu menyokong dapatan ini. Smith dan Hernandez (2021) menegaskan bahawa walaupun terdapat kempen kesedaran, ramai individu tidak menyedari implikasi undang-undang serta realiti sebenar *mule account*, menyebabkan persepsi risiko mereka rendah. Sindrom "personal invincibility" atau rasa kebal terhadap risiko sering berlaku apabila individu tidak memiliki pengalaman atau maklumat langsung mengenai jenayah berasaskan akaun. Dalam konteks Malaysia, kajian oleh Hashim dan Abdul Rahman (2020) mendapati bahawa pelajar universiti yang kurang pendedahan kepada pendidikan kewangan dan saluran sokongan rasmi cenderung melihat tawaran kerja sebagai peluang untuk cepat kaya, bukan sebagai ancaman undang-undang. Oleh itu, persepsi mereka terhadap risiko adalah kabur dan tidak realistik, walaupun pengetahuan asas tentang *mule account* dimiliki.

Persepsi bahawa risiko menjadi mangsa adalah rendah membuka ruang luas kepada eksploitasi oleh sindiket jenayah siber. Dalam banyak kes, individu hanya menyedari bahawa mereka telah menjadi mangsa setelah pihak berkuasa mengenakan tindakan. Hal ini disokong oleh Europol (2023) yang melaporkan bahawa ribuan individu menjadi mangsa *mule account* setiap tahun tanpa sedar, kerana mereka tidak menganggap pemindahan wang tersebut sebagai jenayah. Kajian ini juga mendapati bahawa walaupun responden memiliki pengetahuan tinggi tentang "Tawaran Mencurigakan" (min = 4.15), pengetahuan mereka mengenai cara melapor atau melindungi diri masih rendah. Dapatan ini menonjolkan wujudnya jurang antara pengetahuan kognitif (konsep/teori) dan pengetahuan praktikal (tindakan). Jurang ini sangat penting kerana ia menentukan sejauh mana seseorang mengambil serius risiko menjadi mangsa serta bertindak dengan langkah pencegahan yang sewajarnya.

Kesimpulan

Kajian ini meneliti tahap pengetahuan pemegang akaun terhadap risiko penglibatan dalam aktiviti *mule account* serta hubungannya dengan persepsi individu terhadap kemungkinan menjadi mangsa jenayah kewangan tersebut. Dapatan menunjukkan bahawa walaupun responden memiliki pengetahuan umum yang baik mengenai definisi *mule account*, risiko undang-undang dan bentuk tawaran mencurigakan, tahap pengetahuan terhadap aspek praktikal seperti penggunaan aplikasi semakan dan saluran pelaporan rasmi masih berada pada tahap sederhana rendah. Kelemahan ini menunjukkan/menggambarkan wujudnya jurang pengetahuan yang berpotensi mempengaruhi persepsi individu terhadap risiko khususnya tanggapan bahawa mereka tidak mudah menjadi mangsa kerana tidak menyedari kewujudan ancaman yang dekat. Persepsi risiko yang rendah ini berpotensi menyumbang kepada tingkah laku tidak berwaspada seperti berkongsi maklumat akaun, menerima tawaran pekerjaan tanpa semakan, dan kegagalan mengambil langkah perlindungan asas.

Tahap kesedaran tentang risiko juga didapati berkait rapat dengan tahap pengetahuan. Individu yang tidak menyedari wujudnya alat dan saluran keselamatan cenderung untuk menganggap risiko sebagai rendah atau tidak relevan kepada diri mereka, sekali gus berpotensi menjadi mangsa jenayah kewangan tanpa disedari. Persepsi bahawa risiko hanya menimpa orang lain merupakan antara faktor utama yang menyebabkan pemilik akaun mudah dieksploitasi oleh sindiket jenayah. Secara keseluruhannya, kajian ini merumuskan bahawa walaupun tahap kesedaran umum adalah memuaskan, masyarakat masih kurang bersedia secara praktikal untuk berdepan dengan ancaman *mule account*. Oleh itu, usaha pendidikan awam perlu ditingkatkan, terutamanya/khususnya dalam aspek penerapan tindakan pencegahan yang spesifik dan mudah diakses agar pemegang akaun dapat melindungi diri daripada menjadi mangsa jenayah siber yang semakin berleluasa. Tambah cadangan kajian akan datang.

Penghargaan: Terima kasih kepada semua responden kajian yang sudi terlibat sebagai subjek kajian dalam penyelidikan ini.

Konflik Kepentingan: Penyelidik mengisytiharkan tiada konflik kepentingan bagi penyelidikan ini.

Etika Kajian: Penyelidikan ini telah menerima kebenaran dan memenuhi syarat etika penyelidikan.

Rujukan

Aston, M., McCombie, S., Bossi, E., & Choo, K.-K. R. (2009). Malware for sale: An analysis of the advanced underground marketplace. *Trends & Issues in Crime and Criminal Justice*, (377), 1–6.

Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger.

Brown, T. (2017). Financial literacy and youth vulnerability to cybercrime scams. *Journal of Youth Studies*, *20*(4), 489–504. https://doi.org/10.1080/13676261.2016.1241862

Choo, K.-K. R. (2008). Money laundering and terrorism financing risks of prepaid cards in Australia. *Journal of Money Laundering Control*, *11*(3), 246–266. https://doi.org/10.1108/13685200810889485

Chua, Y. P. (2011). *Kaedah dan statistik penyelidikan: Kaedah penyelidikan buku 1* (2nd ed.)McGraw-Hill Education.

Europol. (2023, Julai 23). *Internet Organised Crime Threat Assessment (IOCTA) 2023*. Europol. https://www.europol.europa.eu/publications-documents/internet-organised-crime-threat- assessment-iocta-2023

Hashim, N., & Abdul Rahman, S. (2020). Employment vulnerability among Malaysian university students: A study on illegal job recruitment. *Malaysian Journal of Youth Studies*, *14*(2), 33–47.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2020). *Cybercrime and digital forensics: An introduction* (2nd ed.). Routledge.

Jones, A., Patel, R., & Wong, S. (2022). Awareness and prevention of money mule schemes: A behavioural analysis. *Journal of Financial Crime*, *29*(3), 712–728. https://doi.org/10.1108/JFC-10-2021-0210

Jones, L., Patel, R., & Wong, S. (2019). Money mules and youth: Understanding the appeal of quick cash. *Journal*

of Financial Crime, *26*(1), 211–225. https://doi.org/10.1108/JFC-03- 2018-0034

Lee, H., & Smith, J. (2018). Awareness of online fraud among young adults: A Malaysian perspective. *Asian Journal of Criminology*, *13*(3), 189–206. https://doi.org/10.1007/s11417-017-9256-1

Leukfeldt, E. R. (2014). Cybercrime and social ties: Phishing in Amsterdam. *Trends in Organized Crime*, *17*(4), 231–249. https://doi.org/10.1007/s12117-014-9228-3

Leukfeldt, E. R., & Jansen, J. (2015). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology*, *56*(3), 1–18. https://doi.org/10.1093/bjc/azv049

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016b). A typology of cybercriminal networks: From low-tech fraudsters to high-tech hackers. *Crime, Law and Social Change*, *67*(1), 21– 37.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016c). Criminal networks in a digitised world: The good, the bad and the vulnerable. *Trends in Organized Crime*, *19*(1), 1–15.

Malhotra, N. K., Hall, J., Shaw, M., & Oppenheim, P. (1996). *Marketing research: An applied orientation*. Prentice-Hall.

McCombie, S. (2011). Cybercrime: The trust factor. In K.-K. R. Choo & R. Slay (Eds.), *Future directions in cyber crime research* (pp. 85–100). Australian Institute of Criminology.

Mohd Najib, A. G. (1999). *Penyelidikan pendidikan*. Dewan Bahasa dan Pustaka.

Moore, T., & Clayton, R. (2009). *The consequence of non-cooperation in the fight against phishing*. eCrime Researchers Summit 2009. IEEE. https://doi.org/10.1109/ECRIME.2009.5342259

Sabillon, R., Cavaller, V., Cano, J., & Serra, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security*, *4*(2), 41–55.

Sabitha, M. (2006). *Kaedah penyelidikan sains sosial*. Pearson Malaysia.

Smith, L., & Hernandez, M. (2021). Evaluating the effectiveness of anti-money mule awareness campaigns. *Crime Prevention and Community Safety*, *23*(2), 145–161. https://doi.org/10.1057/s41300-021-00112-x

Smith, L., & Hernandez, M. (2021). *Financial cybercrime and the role of awareness: Understanding vulnerabilities to money mule schemes*. *Journal of Financial Crime, 28*(4), 1230–1245. https://doi.org/10.1108/JFC-03-2021-0058

Soudijn, M. R. J., & Zegers, B. (2012). Cybercrime and virtual currencies: Different sides of the same coin? *Journal of Financial Crime*, *19*(1), 25–36. https://doi.org/10.1108/13590791211194707

Vedamanikam, V., & Chethiyar, S. D. (2020). Money mule: A threat to financial security. *Journal of Money Laundering Control*, *23*(4), 789–802. https://doi.org/10.1108/JMLC-12-2019- 0090