Jurnal Komunikasi:
Malaysian Journal of Communication
Jilid 36(3) 2020: 296-311

Strategi Komunikasi Penjenayah Cinta Siber Terhadap Wanita Profesional

KHADIJAH ALAVI
MAIZATUL HAIZAN MAHBOB
MOHAMMAD SYAHRUL AZHA SOOED
Universiti Kebangsaan Malaysia

ABSTRAK

Ancaman jenayah Penipuan Pencintaan (*Love Scam*) merupakan jenayah siber atau komersil yang mensasarkan wanita terutamanya wanita profesional hingga mengakibatkan kerugian berjuta ringgit kepada mangsa dan negara. Kajian ini meneroka faktor keterlibatan mangsa dan strategi komunikasi yang digunakan oleh *scammer* dalam proses penipuan. Kajian dijalankan secara temu bual mendalam ke atas pihak polis dan pekerja sosial dalam menangani isu *Love Scam.* Kajian ini dijalankan di sebuah Ibu Pejabat Polis Daerah (IPPD) di Selangor. Seramai lima responden iaitu mangsa *Love Scam* telah ditemuduga dengan bantuan anggota polis dari IPPD yang mengendalikan kes jenayah komersil ini. Data dianalisis menggunakan kaedah tematik. Hasil kajian mendapati mangsa terjebak dengan *Love Scam* dalam laman sosial disebabkan beberapa faktor iaitu layanan baik daripada pelaku, sosialisasi, capaian internet yang mudah dan tekanan dalam diri mangsa. Strategi komunikasi yang sering digunakan pelaku untuk memerangkap mangsa adalah melalui penipuan profil, janji manis palsu, penghantaran bungkusan dan menyamar sebagai wakil agensi percukaian. Perkhidmatan sedia ada pihak polis hanya mengambil laporan bertulis daripada mangsa yang sedang trauma. Kebarangkalian penggunaan sihir dan pukau dalam talian menyukarkan mangsa untuk melindungi diri daripada ditipu. Dicadangkan kajian masa depan meneroka hubungan pukau, hipnosis, sihir yang diaplikasikan melalui ancaman kejuruteraan sosial (social engineering attack). Kajian ini mencadangkan bahawa pihak polis perlu bekerjasama dengan pekerja sosial dalam menyediakan perkhidmatan intervensi krisis, konsultasi membantu trauma mangsa dan menyediakan perkhidmatan psikososial bagi memberi kesedaran dan advokasi dalam menangani isu *Love Scam.*

Kata kunci: *Jenayah siber, penipuan cinta, strategi komunikasi, wanita, profesional.*

Communication Strategy of Cyber Love Crime towards Professional Women

ABSTRACT

The love crime threat is a cyber or commercial crime targeted at professional women, resulting in millions of ringgit of losses to victims and the country. This study explores the factors of victim involvement and the communication strategy by scammers in the process of fraud. The study was conducted through in-depth interviews with police officers and social workers in addressing the Love Scam issue. The location of the study is at a District Police Headquarters (IPPD) in Selangor. Five respondents were interviewed with the assistance of IPPD police in handling this commercial crime case. Data were analysed using a thematic method. The findings of this study show that the victim was stuck with Love Scam on social media due to several factors such as sweet love treatment from the perpetrator, socialization, easy internet access and stress on the victims. The communication strategies often used by the perpetrators to trap victims are through profile fraud, sweet lies, parcel deliveries and disguises as tax agency

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2020-3603-18

representatives. The existing services provided by the police are only taking written reports from victims who are traumatized. The probability of using black magic and online reverting makes it difficult for victims to protect themselves from disruption. Future research should explore the relationships of online reverting, hypnosis, black magic applied through social engineering attacks. The police should work with social workers in providing crisis intervention services, consultation to assist traumatized victims and providing psychosocial interventions to provide awareness and advocacy in addressing the Love Scam or other commercial crimes issue.

Keywords: *Cybercrime, love scam, communication strategy, women, professional.*

PENGENALAN

Laporan jenayah siber kerap dipaparkan di dalam dada akhbar dan pelbagai kempen penerangan tentang tidak berkongsi maklumat peribadi melalui media elektronik dan cetak. Namun, kes jenayah laman siber terus meningkat dengan mendadak terutama dalam kalangan wanita profesional. Sindiket penipuan percintaan melalui laman siber terutama membabitkan warga negara Afrika telah mengakibatkan kerugian jutaan ringgit Malaysia. Statistik Jabatan Siasatan Jenayah Komersial (JSJK) Polis DiRaja Malaysia (PDRM) Bukit Aman melaporkan bahawa, peningkatan kerugian yang mendadak kepada mangsa penipuan *Love Scam* iaitu sebanyak RM40.9 juta pada tahun 2012; meningkat kepada RM80.3 juta (tahun 2013); RM816 juta (tahun 2014); dan RM1.09 bilion (tahun 2015) menunjukkan suatu angka yang sangat membimbangkan. Laporan akhbar Utusan Online pada 12 Mac 2016 dengan tajuk *Love Scam* Terus 'Mengganas' melibatkan seramai 407 mangsa dengan kerugian sebanyak RM19.2 juta dalam tempoh 70 hari. Penipuan cinta laman siber dilaporkan paling banyak terjadi di Selangor (122 wanita) diikuti Kuala Lumpur (54 wanita) dengan jumlah kerugian sebanyak RM4.9 juta. Dalam pada itu, laporan The Straits Times Singapura pada 27 Mac 2016 memetik hasil kajian yang dibiayai oleh Telenor Group (syarikat telekomunikasi multinasional Norway) menyatakan bahawa dalam kalangan negara Asia, Malaysia adalah negara paling teruk terjejas akibat penipuan internet, diikuti Thailand dan Singapura. Laporan Bernama Online pada 29 Oktober 2019 melaporkan kerugian berjumlah RM410.6 juta akibat *scam* sepanjang tahun 2018 hingga 2019 membabitkan 8,489 kes yang melibatkan kegiatan jenayah *scammer* (*Macau Scammer, Lover Scammer*, penipuan cinta, pakej penipuan dan pinjaman yang tidak wujud) yang menyebabkan rakyat Malaysia kehilangan antara RM200,000.00 hingga RM1 juta berupa wang tunai dan barangan berharga (Khalid, 2019).

SOROTAN LITERATUR

Love Scam bermula akibat mangsa mempamerkan profil di laman sosial seperti gambar profil, status pendidikan, status pekerjaan, status kemewahan dan kegembiraan diri mangsa bagi menjalinkan hubungan cinta siber. Kecanggihan teknologi dan kelajuan jaringan internet telah mendorong perhubungan cinta siber yang menjadi satu fenomena atau trend bagi golongan profesional termasuk di Malaysia. Kemunculan banyak laman sesawang yang menyediakan perkhidmatan untuk mencari jodoh dalam talian (*online*) merupakan pemangkin kepada pelaku *Love Scammer*. Azianura Hani et al. (2019) memperincikan perbahasan secara linguistik perhubungan antara mangsa dengan pelaku *scammer* jenayah cinta siber yang menggunapakai pujukan untuk mengaburi mangsa. Manakala Zulkifli dan Azmi (2019) membahaskan tentang skandal penipuan jenayah cinta siber dengan memfokuskan kepada kajian tempatan dan kes

jenayah siber di Australia, United Kingdom, Amerika Syarikat dan kepakaran warga Afrika yang tertumpu kepada mangsa yang mempunyai masalah kemurungan, tekanan psikologi dan mangsa yang pemalu (Whitty & Buchanan, 2016; Kopp et al., 2016).

Menurut Norazlina et al. (2018), penipuan cinta dalam talian atau *love scam* merupakan satu bentuk jenayah komersil iaitu penjenayah menjalinkan hubungan cinta palsu dengan wanita demi menipu dan mengaut keuntungan daripada mangsa dalam bentuk wang atau seksual. Penggunaan *Facebook* merupakan medium paling ketara wanita terjebak dalam kes penipuan cinta siber. Dapatan kajian Norazlina et al (2018) terhadap 460 responden mendapati 76 peratus pengguna *Facebook* adalah wanita. Penggunaan *Facebook* dan *Instagram* (68%) merupakan media sosial yang paling popular terutama dalam kalangan pengguna internet di Malaysia (Noor Afiza, 2017). *Facebook* memiliki fungsi yang memungkinkan penggunanya berinteraksi dengan pelbagai cara seperti *chatting, tag foto, blog, game* dan kemaskini status. Dengan memanfaatkan cara ini pengguna dapat mengekspresi dan meluahkan keadaan yang sedang terjadi pada dirinya dan ini merupakan cara pengguna menyalurkan segala emosi, perasaan dan kesenangan yang dirasakan (Ali & Siti, 2017; Lee, Normah & Ali, 2014). Namun begitu, persoalan keselamatan dan kesedaran penggunaan internet masih di tahap paling rendah. Penggunaan internet dan strategi komunikasi yang selamat perlu didedahkan kepada masyarakat bagi mencapai kesedaran tentang literasi dan keselamatan alam siber. Muhammad Adnan et al. (2019) berpendapat bahawa amalan keselamatan siber pengguna internet yang menggunakan perkhidmatan dalam talian melalui *Facebook* dan *Instagram* amat rendah di Malaysia. Penggunaan media sosial sebagai sumber pencarian maklumat, pembelian barangan sehingga kepada pencarian teman hidup membawa kepada ancaman kewangan, emosi, kognitif, sosial dan fizikal seseorang mangsa *love scam.*

Strategi komunikasi *love scam* yang sering digunakan oleh sindiket untuk menipu mangsa ialah menggunakan identiti palsu, menggunakan laman sosial untuk menjerat mangsa, memperdayakan mangsa dengan janji palsu, meminta mangsa memasukkan sejumlah wang dalam akaun bank mereka, menggunakan transaksi akaun bank rakyat tempatan, menghilangkan diri selepas transaksi wang dilakukan dan menjalinkan cinta sekurang-kurangnya tiga bulan (Sinar Harian, 8 April 2013). Strategi komunikasi menjadi kerangka dalam perbincangan ini kerana jenayah *love scam* menggunakan komunikasi yang cukup terancang. Komunikasi terancang adalah penting bagi menjayakan sesuatu tujuan komunikasi khususnya dalam mempengaruhi sikap dan tingkah laku mangsa. Strategi komunikasi merupakan elemen yang terkandung di bawah komunikasi strategik, yang digunakan oleh organisasi atau kumpulan untuk mendapatkan hasil optimum daripada aktiviti berorganisasi. Ia juga boleh dianggap sebagai satu bentuk komunikasi yang berkesan kerana matlamatnya adalah untuk mencapai tujuan komunikasi sepenuhnya. Antara ciri strategi komunikasi ialah komunikator dengan jelas atau secara tersurat memilih apa yang perlu dibincangkan dan apa yang harus diabaikan (pemilihan mesej yang berhati-hati). Strategi juga melibatkan penetapan matlamat komunikator (penetapan matlamat secara khusus) dan jangkaan tindak balas orang lain (penilaian terhadap mesej). Strategi pada dasarnya berfungsi sebagai asas untuk tindakan, iaitu menyediakan asas untuk penstrukturan, pelaksanaan dan penilaian amalan komunikasi (pemilihan struktur komunikasi). Pemilihan medium komunikasi seperti e-mel, *WhatsApp*, telefon dan *Facebook* sebagai kaedah menyampaikan hasrat memperdayakan mangsa juga merupakan strategi komunikasi (pemilihan

medium komunikasi) (Clampitt, 2005). Justeru penggunaan media sosial yang dikemaskini dan konsisten merentasi saluran komunikasi memerlukan koordinasi yang sistematik bagi memastikan strategi komunikasi dapat dipantau dan mengelakkan diri daripada terjebak dalam penipuan laman siber masa kini (Zeti Azreen, 2019).

Dengan mengambil kira ciri-ciri strategi komunikasi di atas, maka artikel ini akan membincangkan bagaimana *love scammer* menjalankan modus operandinya memperdayakan mangsa yang baharu sahaja dikenali. Kebanyakan wanita yang terbabit dalam *love scam* terdiri daripada wanita profesional yang berpendidikan tinggi, masih bujang dan berpendapatan tinggi. Kemahiran komunikasi strategik yang dimiliki oleh pelaku (love scammer) membolehkan sesiapa sahaja menjadi mangsa mereka dan meninggalkan jejak yang sukar untuk dikesan. Artikel ini bertujuan memahami faktor penglibatan mangsa dan strategi komunikasi *scammer* dalam memancing mangsa *love scam*. Kajian ini tepat pada masanya untuk meningkatkan pendidikan psikososial dalam kalangan wanita dan remaja perempuan yang menggunakan laman media sosial dalam mengecapi impian percintaan dengan orang yang tidak dikenali, belum sahih latar belakang individu yang ingin dicintai dan sanggup mengeluarkan pelaburan yang besar untuk berhubung dengan *love scammer*. Pendedahan isu penipuan cinta siber adalah penting untuk memberi gambaran sebenar penipuan cinta siber yang diceritakan mangsa tentang pengalaman peribadi mereka untuk dikongsi bersama dengan masyarakat. Pengalaman tersebut melibatkan faktor yang berkait dengan *love scammer*, strategi komunikasi pelaku dan langkah-langkah menangani isu jenayah cinta siber terutama dalam kalangan wanita dan remaja perempuan. Strategi keturutan dalam menjayakan modus operandi jenayah *love scam* terbahagi kepada tiga tahap iaitu mood positif, timbal balik dan pemberian sebab. Mood positif menggerakkan perasaan menyenangkan dalam hubungan antara mangsa dan pelaku. Kedua, mood timbal balik, merupakan strategi saling membalas hadiah dan penceritaan luahan memikat hati mangsa. Ketiga, pemberian barangan yang dikirim, isu tahanan imigresen, urusan visa dan hajat untuk melawat mangsa di Malaysia. Semua bentuk pemberian ini mengharapkan ihsan kewangan mangsa atau pelbagai alasan lain dengan menggunakan strategi komunikasi licik (Rozmi, 2011). Justeru, kajian ini meneroka faktor keterlibatan mangsa dan strategi komunikasi yang digunakan oleh *scammer* dalam proses penipuan *Love Scam*.

METODOLOGI

Kajian ini menggunakan pendekatan kualitatif di mana gambaran holistik dan temu bual mendalam digunakan sebagai teknik pengumpulan data. Pemetaan lokasi kajian dipilih ialah daerah X di Selangor di mana Ibu Pejabat Polis Diraja Malaysia melaporkan bahawa Selangor merupakan negeri teratas dalam kegiatan penipuan cinta siber. Pemilihan responden menggunakan teknik bebola salji (*snowball*) di mana pengkaji telah menemu bual lima responden yang menjadi mangsa cinta siber dalam daerah X. Pengkaji juga menemu bual pegawai polis daerah X yang mengendalikan kes mangsa siber dan pegawai kebajikan masyarakat daerah X bagi mendapatkan maklumat mengenai modus operandi dan strategi komunikasi sindiket jenayah cinta siber. Daripada aspek protokol kajian yang dikemukakan, artikel ini menganalisis faktor yang menyebabkan golongan wanita profesional tertarik menjalinkan hubungan cinta siber dan sejauh mana mereka memahami strategi komunikasi yang digunakan oleh sindiket *Love Scam* dalam mengumpan wanita profesional terbabit. Analisis tematik telah digunakan untuk menginterpretasi data bagi menjawab objektif kajian.

HASIL KAJIAN DAN PERBINCANGAN

Profil Responden dan Informan

Kajian ini melibatkan lima orang responden yang menjadi mangsa *Love Scam* yang diperoleh melalui informan utama iaitu pegawai polis. Kesemua responden ini dirujuk berdasarkan kes bagi menjawab persoalan pertama dan kedua yang dikemukakan dalam kajian ini. Kajian ini juga turut melibatkan tiga informan yang mempunyai latar belakang pendidikan kerja sosial bagi menjawab persoalan ketiga kajian ini. Maklumat latar belakang responden (mangsa *love scam)* pula diperoleh daripada pegawai polis yang bertugas di JSJK Ibu Pejabat Polis Daerah X. Purata umur mangsa yang terjebak dalam jenayah komersial ini adalah di antara 34 hingga 37 tahun. Status perkahwinan keseluruhan responden yang dipilih adalah bujang (belum mendirikan rumah tangga). Manakala dari aspek kerjaya pula, kesemua responden mempunyai kerjaya di peringkat profesional iaitu responden A bekerja sebagai seorang guru, responden B sebagai seorang pegawai tadbir, responden C bekerja sebagai doktor, responden D sebagai ahli perniagaan dan responden E sebagai pensyarah. Dari segi taraf pendidikan pula, kesemua responden mempunyai latar pendidikan yang berbeza iaitu memiliki diploma hingga ijazah doktor falsafah.

Tempoh perkenalan yang dicatatkan bagi *scammer* memperdayakan mangsa mengikut responden A, C dan E adalah dua bulan. Responden B pula mengambil masa satu bulan setengah manakala tempoh yang paling singkat pula melibatkan responden D iaitu sebulan. Dari segi jumlah kerugian pula, responden A dan responden C mencatatkan jumlah kerugian sebanyak RM50 ribu, responden D mengalami kerugian sebanyak RM80 ribu dan responden E sebanyak RM70 ribu. Responden B mencatatkan kerugian yang paling rendah iaitu sebanyak RM35 ribu.

Kajian ini telah mengambil seorang pegawai polis sebagai informan 1 (utama) iaitu Sarjan Y yang bertugas di JSJK di IPD Daerah X. Melalui informan 1 ini, pengkaji memperolehi lima responden yang telah menjadi mangsa *Love Scam* sebagai fokus utama bagi menjawab persoalan pertama dan kedua yang dikemukakan dalam kajian ini. Selain itu, pengkaji juga turut mendapatkan informan yang mempunyai latar belakang pendidikan kerja sosial bagi menjawab persoalan ketiga dalam kajian ini. Informan yang dipilih terdiri daripada dua orang perempuan dan dua orang lelaki yang berumur dalam lingkungan 30 hingga 37 tahun. Kesemua informan yang dipilih mempunyai status pendidikan tinggi iaitu informan 1 memiliki diploma, informan 2 memiliki kelulusan PhD dan informan 3 serta informan 4 masing-masing merupakan pelajar PhD dalam jurusan kerja sosial di universiti awam (UA). Informan 2 merupakan seorang pensyarah dalam bidang kerja sosial di UA, manakala informan 3 dan informan 4 merupakan pelajar sepenuh masa di UA yang merupakan pegawai di Jabatan Kebajikan Masyarakat (JKM). Menurut Khalid (2019), wanita profesional sering menjadi mangsa disebabkan oleh jadual kerja sibuk seperti doktor, pensyarah, jururawat dan sebagainya yang menjadikan media sosial sebagai penghubung dunia luar. Golongan ini mudah menjadi sasaran apabila sering berkongsi kehidupan harian dan kurang kesedaran tentang keselamatan penggunaan media sosial serta teknik penipuan dalam alam maya.

Permulaan Strategi Komunikasi

i. Profil Pemangsa dan Cara Perkenalan

Pemalsuan identiti atau profil berlaku apabila seseorang itu menggunakan maklumat individu lain tanpa kebenaran untuk kegunaan peribadi. Mengikut seksyen 233 Akta Komunikasi dan Multimedia, adalah menjadi satu kesalahan apabila seseorang individu mendaftar perkhidmatan komunikasi dan multimedia dengan niat untuk melakukan penipuan atau khianat dan boleh dikenakan denda maksimum RM300 ribu atau tiga tahun penjara atau kedua-duanya sekali (petikan daripada Cyber Security Malaysia (MyCERT) 2013).

> …dari semua responden yang saya kendalikan, modus operandi semuanya hampir sama. *Basically* (pada asasnya), pemangsa akan attack (menyerang) mangsa ni dengan profil gambar kat laman sosial biasanya memang tarik minat mana-mana perempuan. Dengan status kerjaya yang bagus macam pemilik syarikat-syarikat besar, bisnessman (ahli perniagaan), lepas tu perkara wajib mesti mereka akan mengaku ada saudara mara dari Malaysia, nak balik Malaysia mulakan hidup baru, yang penting mesti mereka pandai cakap Melayu sikit-sikit. Mangsa kebanyakannya Melayulah, lepas tu Cina dan *last* (akhir) sekali baru India. (Responden B)

Taktik yang sering digunakan oleh sindiket ini adalah pemalsuan profil di akaun laman sosial, misalnya penggunaan gambar palsu yang berupaya menarik perhatian pengguna laman sosial yang lain. Kebiasaannya, sindiket ini menggunakan profil gambar lelaki British dalam penyamaran untuk berkenalan. Selain itu, sindiket ini juga memalsukan latar belakang mereka seperti maklumat pekerjaan, latar belakang dan sejarah diri serta keluarga. Malahan, demi meyakinkan mangsa, sindiket ini juga akan cuba bertutur dalam bahasa Malaysia untuk menunjukkan perkaitan diri mereka dengan Malaysia. Tambahan pula, bahasa Malaysia merupakan bahasa yang ditutur oleh semua penduduk di Malaysia terutama golongan berbangsa Melayu. Oleh sebab itu, tidak hairanlah, kebanyakan mangsa *Love Scam* ini terdiri daripada mereka yang berbangsa Melayu.

> …majoriti mangsa ni kenal kat laman sosial, biasanya di *Facebook*. Setakat responden yang saya kendalikan, tiada lagi responden-responden mangsa berkenalan menerusi laman *Twitter, Instagram* atau laman-laman sosial yang lain. Mungkin sebab *Facebook* ni lebih efektif untuk pemangsa perangkap mangsa. Macam mangsa ni, walaupun doktor, even busy (walau pun sibuk) dengan kerja pun masa tuk *Facebook* tu macam dah satu benda yang wajib. Sebab bagi mangsa, *Facebook* tu satu medium untuk cari kawan dan lepaskan stress. (Responden C)

Facebook merupakan medium laman sosial yang paling popular berbanding dengan laman sosial lain seperti *Twitter, Instagram, Yahoo Messenger* dan sebagainya. Sindiket ini menggunakan platform *Facebook* sebagai salah satu kaedah untuk memperdayakan mangsa. Mengikut informan, kebanyakan mangsa berkenalan dengan sindiket melalui akaun *Facebook* kerana ia dilihat sebagai satu cara yang paling berkesan untuk mendapatkan mangsa seperti yang

terjadi kepada responden C. Hal ini disebabkan mengikut statistik, rakyat Malaysia menghabiskan masa selama tiga hingga lima jam sehari secara purata di alam siber dengan 58-peratus daripada mereka melayari laman sosial menggunakan telefon pintar (Utusan, 2014).

> …kebanyakan sindiket ni pula biasanya akan mengaku asal daripada British. Kenapa tak pilih macam Amerika? Sebab mereka ni pandai, mereka tahu, orang Malaysia ni lebih tahu pasal Amerika berbanding UK. Orang Malaysia, tau pasal Amerika sebab media kita banyak dedah pasal Amerika macam movie, berita. Sebab tu, dia orang ni pilih British untuk menyamar sebab orang kita tak berapa nak tau pasal British. Misalnya responden ni, laki ni dia perangkap mangsa yang ada bisnes, *then* dia cakap dia nak balik ke Malaysia then (selepas itu) dia nak bukak bisnes kat Malaysia. (Responden D)

Majoriti mangsa ditipu tentang kewarganegaraan *scammer* dengan mengaku dirinya berasal dari Britain. Mengikut informan, kebanyakan *scammer* akan menggunakan kewarganegaraan British di awal perkenalan disebabkan oleh rakyat Malaysia tidak terlalu didedahkan dengan kerakyatan British jika dibandingkan dengan negara lain seperti Amerika Syarikat. Hal ini kerana, media Malaysia lebih banyak memfokuskan kepada isu berkaitan Amerika Syarikat sama ada di dalam filem, politik, ekonomi dan sebagainya. Perkara ini secara tidak langsung membuatkan sindiket ini lebih berhati-hati dalam penyamaran identiti berkaitan kewarganegaraan. Menurut Ahmad Safwan et al. (2015), mangsa penipuan jenayah cinta siber disebabkan oleh faktor individu yang mana mangsa sendiri melayari laman web media sosial seperti *Facebook*, *Twoo, Instagram, Linked-In, Viber* yang dapat dikategori sebagai *False Victims*.

Perkongsian maklumat peribadi seperti profil media sosial, nombor telefon peribadi dan pejabat, nombor akaun bukti transaksi dan alamat kediaman serta latar belakang diri memudahkan penjenayah menggunakan data-data tersebut untuk merancang sindiket yang berasaskan modus operandi pengiriman barang. Daripada aspek cara berkenalan dan taktik pendedahan identiti diri adalah berasal daripada kurang literasi tentang penggunaan ICT dan panggilan telefon daripada penjenayah (Zulkufli Ismail & Azmi Aziz, 2019). Kesedaran tentang kerahsiaan identiti, asal, pekerjaan dan kewujudan profil yang mampu menimbulkan kecekapan kesangsian terhadap penipuan cinta siber perlu diwar-warkan secara komprehensif kepada rakyat Malaysia. Menurut Coluccia et al. (2020), epidemologi pula menunjukkan bahawa 88.6 peratus mangsa jenayah cinta siber mendapati mereka mempunyai kesedaran tentang penipuan dalam laman maya, 63 peratus adalah pengguna *Facebook* dan 29 peratus tidak pasti keterlibatan dengan jenayah cinta siber tersebut.

Secara keseluruhan, responden menyatakan bahawa mereka menjadi mangsa cinta siber sekali (6.17%) atau lebih daripada sekali (2.81%). Majoriti penjenayah cinta siber berasal daripada negara Afrika dan Asia. Penjenayah juga akan menggunakan serangan psikologi kepada mangsa dengan perasaan terkejut, marah, menyalahkan diri sendiri dan mereka-reka pelbagai masalah peribadi yang baru untuk terus menerus memanipulasi mangsa untuk melabur dalam perancangan masa depan.

ii. Tempoh Strategi Perkenalan

Tempoh perkenalan dalam cinta siber ini diambil kira bermula daripada awal perkenalan di laman sosial sehingga mangsa sedar dirinya telah ditipu dan mangsa mengalami kerugian. Kebiasaannya, semakin lama tempoh perkenalan akan menyebabkan mangsa mengalami kerugian yang lebih tinggi.

> …diorang (sindiket) biasanya tak ambil masa lama dengan mana-mana mangsa. Biasanya sebulan atau dua bulan paling lambat. Bila mangsa yang cuba diperangkap tak berjaya, biasanya pemangsa akan terus *move on* ke mangsa seterusnya. Diorang biasanya tak buat kajian tentang *background* mangsa, mereka main sapu je, asalkan si mangsa layan.
>
> …contoh kalau mangsa tu main tarik tali pun, tapi macam melayan dia akan tetap kekal dengan perempuan tu, sebab diorang nie akan letakkan limit masa sampai tiga bulan, kalau tak dapat apa-apa, baru diorang (sindiket) akan blah. Ikut pengalaman saya, paling lama tempoh untuk mangsa ikut cakap penipu selalunya lebih kurang dua bulan dan jarang lebih dari dua bulan. (Responden A)
>
> …mengikut pengalaman saya, paling cepat masa yang diorang (sindiket) ambil sebulan tuk perangkap mangsa. Nak-nak bila perempuan tu pula dah macam terdesak nak kenal laki tu dan mudah sangat termakan dengan janji manis laki tu. (Responden D)

Pada keseluruhannya, perkenalan di antara responden dan *scammer* tidak lebih daripada dua bulan. Sepanjang tempoh perkenalan di antara *scammer* dan responden, *scammer* akan cuba sedaya upaya untuk memanipulasi keadaan sehingga *scammer* berjaya mengaut keuntungan daripada responden. Menurut informan 1, sindiket ini mempunyai limitasi masa dalam proses memperdaya mangsa di mana sekiranya individu yang disasarkan tidak memberi keuntungan kepada sindiket, sindiket akan meninggalkannya dan mula mencari sasaran baharu.

Tempoh masa yang sering digunakan oleh sindiket untuk membuat permintaan yang pertama selalunya setelah sebulan tempoh perkenalan di laman siber dan telah berjaya mendapat kepercayaan daripada individu yang disasarkan. *Scammer* akan mengaburi mata mangsa dengan menjanjikan pelbagai helah seperti kata-kata manis dan juga barangan mewah sehingga *scammer* berjaya memanipulasikan individu yang disasarkan. Tempoh perhubungan akan berakhir apabila mangsa itu sendiri sedar bahawa dirinya telah dimanipulasikan oleh *scammer* sehingga dirinya mengalami kerugian. Kerugian yang dimaksudkan adalah mangsa telah mengeluarkan sejumlah wang pembayaran untuk mendapatkan bungkusan (*parcel*) yang dijanjikan. Malangnya bungkusan yang dijanjikan cuma alat untuk memanipulasikan mangsa sahaja.

Kesinambungan Strategi Komunikasi

i. Menabur Kemewahan

Taktik seterusnya yang sering digunakan oleh sindiket adalah dengan mengaburi mata mangsa dengan kemewahan. Kemewahan palsu yang sering dijanjikan oleh *scammer* akan membuatkan mangsa tidak sedar yang dirinya ditipu sehingga mangsa mengalami kerugian beribu-ribu ringgit.

> …sindiket ni selalunya melibatkan ramai individu, setiap orang tu ada bahagian masing-masing. Modus operandi yang biasa sangat diguna, macam nak bagi hadiah masa birthday pastu diorang ni jugak cakap nak hantar hadiah sebagai tanda terima kasih sebab sudi berkenalan dengan dia. Macam-macam lagi alasan yang selalu sindiket ni guna supaya mangsa percaya yang laki tu akan hantar bungkusan untuk mereka. *Totally* responden yang saya *handle*, kebanyakan mangsa ditipu dengan alasan-alasan yang macam ni, semuanya mudah kabur dengan barang-barang yang berharga ni. (Responden A)
>
> …contoh lain ada yang ambil tugasan sweet talker, mereka akan main peranan untuk goda mana-mana gadis sampai dapat. Tabur janji manis. Contoh janji nak jumpa kat Malaysia, bagi barang berharga, duit, barang kemas dan macam-macam lagi. Macam responden yang ahli perniagaan tu, mangsa cakap laki tu nak hantar duit 100 ribu USD untuk bantu mangsa punya bisness dan sebagai modal untuk kehidupan mereka bersama di Malaysia nanti. (Responden D)

Menurut informan 1, sindiket ini bergerak secara berkumpulan dan setiap ahli akan memainkan peranan masing-masing yang bertujuan untuk memperdaya mangsa. Sindiket akan menggunakan alasan pemberian hadiah seperti hadiah ulang tahun kelahiran, dan hadiah sebagai tanda sudi berkenalan dengannya. Perkara ini sebenarnya bertujuan untuk mendapatkan kepercayaan dan keyakinan mangsa bahawa *scammer* akan menghantar barangan ke Malaysia. Kebiasaannya, hadiah yang dijanjikan oleh sindiket melibatkan barang yang berjenama, barang bernilai seperti emas dan sejumlah wang yang besar. Kemewahan yang dijanjikan kepada mangsa telah membuatkan mangsa gelap mata dengan taktik sindiket ini sehingga menyebabkan mangsa mengalami kerugian.

ii. Helah dalam Penyamaran

Helah boleh didefinisikan sebagai muslihat, tipu daya dan alasan yang direka bertujuan untuk menipu seseorang (Kamus Dewan). Manakala penyamaran pula disifatkan sebagai pemalsuan identiti bagi tujuan memanipulasikan seseorang atau persekitaran demi mendapatkan faedah daripada perbuatan tersebut. Hasil kajian ini mendapati bahawa sindiket ini akan cuba menyamar sehingga individu yang disasarkan percaya dan menuruti segala permintaan *scammer.*

> …*love scam* ada dua jenis, satu *love scam* kenal kat *Facebook*, elok bercinta bagai nak rak lepas tu buat macam-macam alasan, mak dia sakit, bisnes down. Nak datang Malaysia jumpa. *So,* dia guna alasan ni minta perempuan masukkan duit. Satu jenis lagi, sindiket ni akan guna *parcel* untuk kaut keuntungan. Keuntungan yang diorang dapat ni, hasil daripada mereka cuba *drag* mangsa dengan kononnya kenakan cukai terhadap *parcel* tu. (Informan 1)

Informan 1 menjelaskan bahawa terdapat dua kategori dalam *love scam* iaitu, penggunaan alasan untuk memanipulasi mangsa dan mendapatkan keuntungan. Manakala, kategori seterusnya ialah penipuan melalui penggunaan *parcel* sebagai alasan untuk

memanipulasi mangsa dalam mendapatkan keuntungan. Sindiket akan cuba mencipta pelbagai alasan untuk menjerat mangsa sehingga mangsa sedar bahawa dirinya telah ditipu.

iii. Strategi Penyamaran sebagai agensi percukaian

a) Pihak National Courier

> …*love scam* berkaitan dengan parcel ni macam ni, dia akan guna helah *parcel* sebagai medium dia minta duit. Contohnya, parcel dihantar, sindiket ni akan menyamar sebagai *National Curier*, diorang yang menyamar akan call si mangsa untuk minta duit kononnya cukai berkaitan dengan *parcel*, duti, kos *transportation* luar negara. (Informan 1)

Scammer akan menyamar sebagai wakil daripada pihak *National Curier* sebagai langkah pertama dalam agenda penipuan mereka. Tugas penyamaran sebagai wakil *National Courier* ini adalah untuk menghubungi mangsa dan menyatakan bahawa mangsa mendapat kiriman barangan yang mengandungi barang-barang berharga, dan sejumlah wang seperti yang dijanjikan oleh *scammer* kepada mangsa. Hal ini bertujuan untuk mempengaruhi mangsa untuk mengeluarkan bayaran seperti yang diminta dengan menyatakan bahawa barangan yang dikirimkan dari luar negara terpaksa dikenakan pelbagai cukai seperti cukai pengangkutan, dan duti penghantaran.

b) Pihak Kastam

> …lepas tu sindiket akan *drag* (mengheret) mangsa pada kastam, sindiket akan menyamar sebagai kastam dan bagitahu mangsa yang dalam *parcel* tu ada barang berharga. Barang-barang yang kastam akan kenakan cukai. *So* dia mintak mangsa bayar kat dia, mereka akan ugut untuk tangkap mangsa kalau tak bayar caj yang dikenakan. (Informan 1)

Menurut informan 1, selepas individu yang menjadi mangsa ini terperangkap dengan penyamaran *scammer* yang pertama, *scammer* ini akan mencipta pelbagai alasan untuk menarik mangsa kepada penipuan yang lebih jauh iaitu dengan bertindak melakukan penyamaran sebagai individu yang bekerja dengan pihak kastam yang merupakan agensi yang bertanggungjawab mengutip cukai. Mengikut informan, penglibatan pihak kastam dalam *modus operandi* sindiket ini adalah bertujuan mendapatkan bayaran kali kedua. Alasan yang sering digunakan adalah terdapat barangan di dalam *parcel* yang dikenakan cukai oleh pihak kastam Malaysia. Sekiranya mangsa enggan menuruti permintaan *scammer*, mangsa diugut akan ditangkap oleh pihak kastam kerana bertindak mengelak daripada pembayaran cukai yang telah ditetapkan.

c) Pihak Bank Negara

> …sindiket ni tak henti kat sini je, mereka kononnya akan bawa responden ni pada pihak Bank Negara dengan alasan Bank Negara tak nak keluarkan *release letter* sebab didapati dalam *parcel* ni mengandungi *amount USD* yang tinggi. *So*, mangsa perlu bayar pada Bank Negara *certain amount* untuk mangsa dapatkan *parcel* tu. Macam mana pun dia akan hentam mangsa ni kaw-kaw punya. Kalau ikut logik memang kita takkan bayar apa-apa sebab tu bukan dari kita, tapi kalau dah ugut sampai nak naik turun mahkamah, siapa yang sanggup nak tanggung? (Informan 1)

Apabila sindiket ini mendapati bahawa mangsa meletakkan kepercayaan yang tinggi terhadap penyamaran mereka, sindiket ini akan bertindak membawa penyamaran mereka kepada pihak Bank Negara. Mangsa terpaksa mengeluarkan sejumlah wang untuk mendapatkan kiriman barangan kerana didapati kiriman barangan tersebut mengandungi jumlah wang yang besar dan pihak Bank Negara terpaksa mengenakan cukai. Mengikut informan 1, apabila mangsa percaya bahawa kiriman bungkusan tersebut mempunyai sejumlah wang yang tinggi, mangsa akan bertindak mengikuti permintaan *scammer* disebabkan teruja mendengar jumlah kiriman wang tersebut. Namun sekiranya mangsa menolak dan enggan menerima barangan tersebut, mangsa akan diugut untuk dikenakan tindakan undang-undang seperti Akta Bank Negara. Sekiranya mangsa memberitahu bahawa dirinya tidak mempunyai sejumlah wang yang diminta, *scammer* akan menjelaskan bahawa mangsa boleh membayar separuh daripada jumlah diminta dan separuh lagi dibayar apabila telah menerima barangan, tetapi pada hakikatnya ia satu penipuan semata-mata.

> …saya bagi satu contoh responden ni, mangsa dijanjikan dengan *parcel* yang mengandungi 100 ribu USD. Mangsa percaya sebab sindiket ni ada hantar gambar *parcel* yang siap dengan tarikh semasa, tambah pula bila pihak *National Curier*, kastam, Bank Negara call dia, mangsa ni ikut permintaan daripada penyamar sehingga mangsa sendiri sedar dia sebenarnya kena tipu. (Responden D)

Menurut informan 1, faktor yang menyebabkan responden D percaya kepada setiap permintaan daripada pihak yang menghubungi responden yang menyamar sebagai wakil daripada agensi pengutip cukai adalah disebabkan oleh mangsa terlebih dahulu menerima kiriman gambar *parcel.* Kiriman gambar tersebut diambil daripada pusat *national courier* yang menunjukkan tarikh semasa parcel itu dikirim. Walau bagaimanapun, gambar yang dikirim adalah palsu dan telah diubahsuai oleh *scammer*. Hal ini terjadi disebabkan oleh mangsa percaya sepenuhnya terhadap kekasih siber tanpa membuat kajian terlebih dahulu sehingga mangsa tertipu.

IV. Jumlah Transaksi

Jumlah pembayaran mangsa kepada *scammer* tidak berlaku hanya sekali tetapi beberapa peringkat pembayaran. Pembayaran wang transaksi secara berperingkat disebabkan responden disogok dengan pelbagai alasan dan tipu helah daripada *scammer.* Informan 1 menjelaskan bahawa mangsa *Love Scam* tidak hanya akan dikenakan caj transaksi sekali sahaja, tetapi caj yang dikenakan akan berlarutan sehingga mangsa sedar dirinya diperdaya. Merujuk kepada responden A dan C, masing-masing mengalami kerugian sebanyak RM50 ribu. Responden A membuat transaksi sebanyak tiga kali masing-masing sebanyak RM17 ribu, RM10 ribu dan RM23 ribu. Manakala kadar transaksi responden C pula melibatkan jumlah bayaran RM20 ribu, RM15 ribu dan RM18 ribu. Responden B melibatkan kerugian sebanyak RM35 ribu menerusi lima kali transaksi dengan kadar bayarannya RM8 ribu, RM7 ribu, RM4 ribu, RM5 ribu dan transaksi terakhir RM11 ribu. Responden D mencatatkan peringkat pembayaran yang paling banyak (enam kali) dengan kadar transaksi RM25 ribu, RM15 ribu, RM10 ribu, RM7 ribu, RM15 ribu dan RM8 ribu.

Pola pembayaran yang dikenakan oleh sindiket menunjukkan peringkat pertama bayaran yang dikenakan adalah tinggi berbanding pada peringkat kedua dan berikutnya di mana setiap peringkat pembayaran adalah mengikut kemampuan mangsa. Pada setiap peringkat transaksi, sindiket akan memberikan alasan pembayaran cukai yang melibatkan pelbagai agensi sehingga mangsa itu sendiri sedar bahawa dirinya telah diperdaya atau ditipu.

Menurut informan 1 lagi, transaksi pembayaran yang dibuat oleh responden menggunakan akaun peribadi dan bukannya akaun milik syarikat atau agensi yang berkaitan. Sekiranya mangsa mempersoalkan mengenai status akaun transaksi, *scammer* memberikan alasan bahawa pemilik akaun peribadi tersebut adalah peguam kepada syarikat yang menguruskan barangan daripada luar negara dan perkara ini disebabkan oleh pihak peguam merupakan individu yang lebih arif terhadap undang-undang di dalam sesebuah negara dan ia memudahkan urusan kedua-dua belah pihak. Ini menunjukkan bahawa *scammer* akan bertindak dengan pelbagai alasan dalam memperdayakan mangsa bagi terus membuat transaksi pembayaran. Kes jenayah cinta siber boleh berlaku kepada siapa sahaja tanpa mengira latar belakang demografi. Sifat berhati-hati sebelum mengambil tindakan mampu mengelakkan individu mengalami kerugian dan ia perlu ditekankan kepada setiap pengguna laman sosial yang menjadikannya sebagai medium perhubungan dalam memenuhi keghairahan bercinta.

RUMUSAN

Golongan wanita profesional yang berumur antara 30 hingga 50 tahun banyak terlibat dalam menjalinkan hubungan cinta di laman siber. Terdapat beberapa faktor yang mendorong mereka menjadi mangsa jenayah komersil. Antara salah satu faktor yang dominan dalam penglibatan golongan wanita profesional ialah faktor layanan manis dan santunan emosi yang diberikan oleh pasangan di laman siber. Layanan melalui komunikasi dengan baik, membuat janji dengan kemewahan, ambil kisah dan sebagainya telah menyebabkan responden bertindak untuk menjalinkan cinta di laman siber. Faktor sosialisasi, faktor capaian internet dan faktor tekanan dilihat sebagai penyumbang kepada penglibatan golongan wanita terjebak dalam menjalinkan hubungan cinta di laman siber. Faktor sosialisasi merujuk kepada gaya hidup responden yang tidak mempunyai pasangan, kesunyian fokus kepada kerjaya, tiada masa untuk bersosial dan

keterujaan dengan kehadiran warga asing untuk berkenalan membuatkan responden tidak berfikir panjang untuk menjalinkan cinta di laman siber.

Daripada aspek strategi komunikasi, *love scammer* merancang dengan terperinci profil mangsa dan cara perkenalan melalui penipuan identiti pelaku "lelaki kacak dan segak", latar belakang keluarga dan pekerjaan yang berupa jutawan muda. Tempoh berkenalan sangat singkat antara dua bulan, jika perkenalan berlanjutan kerugian yang akan dialami juga akan meningkat. Akhirnya, mangsa akan sedar daripada lamunan cinta apabila kehilangan harta dan mengalami kerugian kewangan. Bagi mengaburi mangsa, beberapa kaedah penyamaran dilakukan oleh *scammer* seperti agensi percukaian, pihak penghantar barangan courier, pihak kastam, pegawai Bank Negara dan pegawai Polis Bukit Aman. Jumlah transaksi boleh mencapai dari RM10,000 sehinggalah RM4.8 juta ringgit yang hilang dalam sekelip mata.

Kempen kesedaran jenayah siber dan meningkatkan hubungan rakan strategik oleh Kementerian Komunikasi dan Multi Media (KKMM) yang menjurus kepada kumpulan sasaran seperti pesara, wanita bekerjaya, dan pelajar semua peringkat pengajian perlu ditingkatkan. KKMM perlu menjalin kerjasama dengan rakan strategik antaranya Polis DiRaja Malaysia (PDRM), agensi dan jabatan di bawah KKMM seperti Jabatan Penyiaran, Jabatan Penerangan, Suruhanjaya Komunikasi dan Multimedia Malaysia, FINAS, dan BERNAMA. Bank Negara Malaysia juga terlibat sebagai rakan strategik di samping badan bukan kerajaan (NGO) dan kumpulan pemimpin masyarakat (KKMM 2019). Manakala Coluccia et al. (2020) pula mencadangkan jalinan hubungan rakan strategik seperti institusi undang-undang dan perkhidmatan kesihatan mental juga perlu diambil kira sebagai strategi pembangunan protokol penyelidikan. Pusat penjagaan kesihatan mental perlu menggunakan alat saringan pemantau risiko jenayah cinta siber bagi membantu mangsa yang mengalami gangguan psikologi dan memerlukan bantuan klinikal.

Penyelidikan masa depan dapat meneroka penggunaan hipnosis, trik psikologi, sihir dan pukau dalam talian yang juga dikenali sebagai ancaman kejuruteraan sosial (social engineering attack) yang memberi implikasi besar kepada keselamatan siber. Masyarakat dunia telah memahami penggunaan amalan sihir dan penggunaan cara halus untuk tipu daya dan menggoda manusia. Dalam masyarakat nusantara pun telah lama mengenali amalan sihir "minyak dagu", sihir kasih sayang yang bertujuan untuk menipu dan menggoda wanita. Terdapat kebarangkalian semua jenis sihir telah melalui proses *reengineering* sesuai dengan kehendak zaman milenium. Jika zaman dahulu tukang sihir menggunakan kemenyan, keris, darah, telur, jarum, rambut, patung dan gambar untuk menyempurnakan hasrat mereka, dalam alaf baru alat yang digunakan hampir sama iaitu gambar dan penggunaan komunikasi memujuk secara aplikasi media sosial boleh dicapai dengan mudah dan cepat seiring dengan gaya hidup masyarakat moden yang gemar berkongsi gambar, lokasi dan kekayaan material yang dimiliki. Berpandukan pendekatan antropologi dalam memahami peranan penjenayah siber yang menggunakan sihir, pukau, trik psikologi atau hipnosis wajar dikaji bagi membantu pihak polis, pekerja sosial dan kaunselor dalam menangani isu jenayah cinta siber dan lain-lain jenayah komersil dalam talian yang semakin bermaharajalela dan licik untuk didakwa.

BIODATA

Khadijah Alavi merupakan Pensyarah Kanan di Pusat Kajian Psikologi dan Kesejahteraan Sosial, Fakulti Sains Sosial dan Kemanusiaan, Universiti Kebangsaan Malaysia (UKM), Bangi, Selangor, Malaysia. Bidang pengkhususan beliau ialah kerja sosial gerontologi dan pembangunan komuniti. E-mel: khadijah@ukm.edu.my

Maizatul Haizan Mahbob merupakan Pensyarah Kanan di Pusat Kajian Media dan Komunikasi, Fakulti Sains Sosial dan Kemanusiaan, Universiti Kebangsaan Malaysia (UKM), Bangi, Selangor, Malaysia. Bidang pengkhususan beliau ialah Komunikasi keorganisasian dan komunikasi pembangunan. E-mel: maiz@ukm.edu.my

Mohammad Syahrul Azha Sooed merupakan Graduan Prasiswazah Program Kerja Sosial, Pusat Kajian Psikologi dan Kesejahteraan Manusia, UKM, Bangi, Selangor. E-mel: syahrul_azha92@yahoo.com

RUJUKAN

Ahmad Safwan Hamsi, Farrah Diana Saiful Bahry, Siti Noraini Mohd. Tobi, & Maslin Masrom. (2015). Cybercrime over internet love scams in Malaysia: A discussion on the theoretical perspective, connecting factors and key to the problem. *Journal of Management Research*, 7(2).

Ali Salman, & Siti Minanda Pulungan. (2017). Pendedahan diri, motivasi dan kepuasan penggunaan Facebook dalam menjalin persahabatan. *Jurnal Komunikasi: Malaysian Journal of Communication,* 33(1), 438-459.

Azianura Hani Shaari, Mohammad Rahim Kamaluddin, Wan Fariza Paizi@Fauzi, & Manizah 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.

Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A., & Gualtieri, G. (2020). Online romance scams: Relational dynamics and psychological characteristics of the victims and scammers. A scoping review. *Clinical Practice and Epidemiology in Mental Health,* 16, 24-35. http://dx.doi.org/10.2174/1745017902016010024

Hamburger, Y. A., & Ben-Artzi, E. (2003). Loneliness internet use*. Computers in Human Behavior,* 19, 71-80.

Hadnagy, C. (2011). *Social engineering: The art of human hacking*. Canada: Wiley Publishing.

Lawson, H. M., & Leck, K. (2006). Dynamics of internet dating*. Social Science Computer Review*, 24, 662-676.

Lee Hui Er, Normah Mustaffa, & Ali Salman. (2014). Faktor-faktor yang mempengaruhi remaja Lembah Klang untuk terus membaca dan membeli melalui pengiklanan Facebook. *Jurnal Komunikasi: Malaysian Journal of Communication,* 30(1), 220-241.

Jabatan Pengguna New Zealand. (2006, June 15). Diperoleh dari www.westernunion.co.nz/.../romance-scam-awareness

Kamus Dewan. (2013). Kuala Lumpur: Penerbit Dewan Bahasa dan Pustaka, Malaysia

Khalid K. (2019). Penipuan cinta di media sosial makin menjadi di Malaysia. Diperoleh pada Februari 7, 2020, dari https://socialmediamalaysia.my/blog/2019/08/12/media-sosial

Koop, C., Sillitoe, J., Gondal, I., & Layton, R. (2016). The online romance scam: A complex two - layer scam. *Journal of Psychological and Educational Research*, 24(2), 144-161.

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. https://www.doi.org/10.17576/JKMJC-2019-3503-13

Norazlina 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. https://www.doi.org/10.17576/JKMJC-2018-3404-07

New Straits Times. (2013, Feb 18). *Cyber security Malaysia. Online love scams are growing. Heed the advice of Cybersecurity Malaysia*. Diperoleh pada Jun 20, 2016, dari http://www.cybersecurity.my/en/knowledge_bank/news/2013

Rege, A. (2009). What's love got to do with It? Exploring online dating scams and identity fraud. *International Journal of Cyber Criminology*, 3(2), 494-512.

Rozmi Ismail. (2011). *Psikologi sosial.* Bangi: Penerbit UKM. Bangi, Selangor.

Sundramoorthy P. (2011, November 8). Buta cinta punca wanita diperbodohkan. *Utusan Online*. Diperoleh dari http://ww1.utusan.com.my/utusan/info.asp?y=2011&dt=1108&pub=Utusan_Malaysia&sec=Jenayah&pg=je_02.htm

Shazli Ezzat Ghazali, Roosfa Hashim, Ponnusamy Subramaniam, Normah Che Din, & Mahadir Ahmad. (2011). Faktor-faktor mempengaruhi amalan bersembang dalam kalangan wanita Melayu dewasa awal: Satu kajian awal. *MALIM: SEA Journal of General Study*, 12, 121-127.

Sinar Harian. (2013, April 8).

KKMM. (2019). Teks ucapan Dato' Dr Mohd Ali Mohamad Nor. Taklimat kesedaran pencegahan jenayah siber dan antipemerdagangan orang. Diperoleh dari https://www.kkmm.gov.my/pdf/ucapan/2019/190307-JENAYAHSIBER.pdf

The Straits Times. (2016, Mac 27).

Utusan Malaysia. (2014, Mei 5).

Utusan Malaysia. (2014, Mei 6).

Utusan Malaysia. (2016, Mac 12).

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims–both financial and non-financial. *Criminology and Criminal Justice,* 16(2), 176-194.

Yong, S. W. (2007). *Persepsi orang awam terhadap cinta siber* (Latihan Ilmiah Sarjana Muda, Fakulti Sains Sosial dan Kemanusiaan, Universiti Kebangsaan Malaysia).

Zeti Azreen Ahmad. (2019). Embracing social media: The change and disruption to public relations practices in Malaysia. *Jurnal Komunikasi: Malaysian Journal of Communication,* 35(1), 319-337. https://www.doi.org/10.17576/JKMJC-2019-3501-21

Zulkufli Ismail, & Azmi Aziz. (2019). Jenayah cinta siber di Malaysia: Suatu penelitian terhadap pengalaman mangsa. e-*Bangi Journal of Social Sciences and Humanities*, 16(4), 1-10.