Jurnal Pembangunan Sosial Jilid 21 (September) 2018: 105-122

Love Scam Di Selangor: Satu Penerokaan Terhadap *Modus Operandi* Jenayah Siber Ke Atas Wanita Profesional

(Love Scam in Selangor: An Exploratory Research on Modus Operandi in Cyber Crime towards Professional Women)

Khadijah Alavi dan Mohammad Syahrul Azha Sooed
Pusat Pengajian Psikologi dan Pembangunan Manusia, FSSK,
Universiti Kebangsaan Malaysia
E-mel: *khadijah@ukm.edu.my*

Al-Azmi Bakar
Institut Sosial Malaysia
Kementerian Pembangunan Wanita, Keluarga dan Masyarakat

Abstrak

Komplot Cinta (Love Scam) merupakan jenayah siber/komersil mensasarkan wanita terutamanya wanita profesional yang mengakibatkan kerugian berjuta ringgit kepada Malaysia. Kajian ini bertujuan meneroka faktor keterlibatan mangsa dan modus operandi yang digunakan oleh scammer. Kajian kualitatif dijalankan secara temu bual mendalam dalam kalangan 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 di temu bual dengan bantuan anggota polis dari IPPD yang mengendalikan kes jenayah komersil ini. Hasil kajian mendapati bahawa faktor yang dikenal pasti ialah layanan baik daripada pelaku, sosialisasi, capaian internet yang mudah dan tekanan dalam diri mangsa. Modus operandi yang sering digunakan pelaku untuk memerangkap mangsa adalah melalui penipuan profil, janji manis palsu, penghantaran bungkusan dan menyamar sebagai wakil agensi percukaian.

Kata kunci: *Jenayah Siber, Modus Operandi, Wanita Profesional, Pekerja Sosial*

Abstract

Love Scam is a cyber or commercial crime targeting women, especially professional women's who have lost millions of ringgit in Malaysia. This study explores the factor of victim involvement and modus operandi used by the

scammer. The interviews were conducted at the District Police Headquarters (IPPD) in Selangor. A total of five love scam victims were interviewed, with the assistance of police officers dealing with commercial crime cases. The findings show that prominent factors identified are the perpetrators sweet talk, socializing, easy internet access and self pressure among victims. The modus operandi often used by the perpetrators to trap victims is through fraud profile picture in social media, fake sweet promises, and packaged delivery and posing as representatives of tax agencies.

Keywords: *Cyber crime, modus operandi, profesional women and social workers.*

Pengenalan

Jenayah melalui laman siber meningkat dengan mendadak dan amat membimbangkan terutama dalam kalangan wanita professional. Malaysia juga tidak terlepas daripada salah satu destinasi atau pangkalan sindiket jenayah siber. Sindiket penipuan percintaan melalui laman siber terutama membabitkan warga negara Afrika merugikan jutaan ringgit Malaysia. Statistik oleh 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; sebanyak RM80.3 juta (tahun 2013); RM816 juta (tahun 2014); dan RM1.09 bilion (tahun 2015). Laporan akhbar Utusan *Online* pada 12 Mac 2016 dengan tajuk *Love Scam* Terus 'Mengganas' di mana 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 dengan 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.

Love Scam boleh 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 telah menjadi satu fenomena atau trend bagi golongan profesional termasuk di Malaysia. Manakala terdapat banyak laman sesawang menyediakan perkhidmatan untuk mencari jodoh di dalam talian (*online*) merupakan pemangkin kepada pelaku *Love Scam*.

Love Scammer merupakan individu yang terlibat dalam sindiket cinta palsu dengan cuba meluahkan perasaan cinta kepada mangsa walau pun hubungan mereka baru bermula. Penggunaan laman sosial yang sah merupakan platform untuk menjalinkan hubungan percintaan dengan menggunakan profil palsu seperti gambar muka cantik dan menggoda. *Scammer* juga mempamerkan gambar studio yang berkualiti tinggi untuk mendapatkan senario yang terbaik sehingga mampu memukau dan meluluhkah hati seseorang melalui laman sosial (Rege, 2009). *Scammer* akan menjerat mangsa untuk berkomunikasi melalui telefon dan laman sosial sehingga perbualan mereka semakin rapat dan sangat kerap. Setelah mendapat *rapport* (keakraban), *scammer* akan cuba memasang perangkap dengan meminta hadiah kecil daripada mangsa seperti telefon. Sekiranya mangsa menurut kehendak *scammer*, kebarangkalian untuk meminta jumlah yang besar akan meningkat dari semasa ke semasa (Buchmanan & Monica, 2014). Jabatan Pengguna, New Zealand melaporkan *Love Scam* berfungsi dengan begitu sistematik di mana bermula dengan (i) mesej dihantar dalam talian kepada mangsa yang berpotensi; (ii) pelaku akan memperoleh maklumat peribadi mangsa dan kadang-kadang pelaku terus meluahkan perasaan cinta dan menggoda mangsa; (iii) strategi seterusnya, pelaku akan menghubungi mangsa melalui perbualan telefon, e-mel atau sms (mesej pesanan ringkas) di mana pelaku meninggalkan laman media sosial yang boleh mengaktifkan perjalanan penipuan percintaan mereka tanpa mempunyai rekod pertemuan; (iv) pelaku akan terus menerus berkomunikasi antara satu sama lain dengan mangsa berpotensi melalui e-mel atau sms dan berselang-seli dengan perbualan telefon; (v) pelaku akan menghantar gambar dirinya kepada mangsa melalui e-mel dan tidak pernah menunjukkan wajah sebenar beliau melalui kamera semasa perbualan secara dalam talian; (vi) hubungan semakin akrab di mana pelaku dan mangsa akan membuat perancangan untuk hidup bersama; (vii) selepas beberapa lama, pelaku akan meminta bantuan mangsa supaya menghantar wang bagi tambang perjalanan pelaku menemui mangsa dan membeli barang keperluan hidup untuk persediaan hidup bersama; (viii) pelaku akan mengarahkan untuk memindahkan wang secara dalam talian kepada nombor akaun yang dinyatakan; (x) setelah transaksi wang berjaya diperoleh, pelaku akan berhenti berkomunikasi dan terus menghilangkan diri untuk selama-lamanya. Mangsa yang telah bekerja keras berpuluh-puluh tahun untuk mengumpul wang tetapi *Love Scammer* boleh mengambilnya dalam beberapa minit sahaja.

Menurut Sundramoorthy (2014), penjenayah *Love Scam* daripada Afrika adalah golongan yang licik menggunakan kemahiran infrastruktur ICT di Malaysia. Tambah beliau, mereka bukan penjenayah bodoh, mereka telah mengkaji infrastruktur ICT dengan terperinci, malah cukup faham mengenai sistem perbankan, perundangan dan hak asasi manusia di Malaysia yang digunakan sebagai kelebihan dalam proses memohon untuk mendapatkan pas

pelajar. Walau bagaimanapun ramai warga Afrika yang ditangkap sukar didakwa ekoran kekurangan bukti disebabkan mangsa tidak mengenali langsung suspek. Pihak imigresen membatalkan visa pelajar serta mendokumentasikan sebagai "*con wanted*" supaya tidak bolos ke Malaysia lagi. Modus operandi *love scam* yang sering digunakan oleh sindiket untuk menipu mangsa seperti menggunakan identiti palsu, laman sosial untuk menjerat mangsa, memperdayakan mangsa dengan janji palsu, meminta mangsa memasukkan sejumlah wang dalam akaun bank mereka, transaksi akaun bank rakyat tempatan, menghilangkan diri selepas transaksi wang dilakukan dan tempoh menjalinkan cinta sekurang-kurangnya 3 bulan (Sinar Harian, 8 April 2013).

Jaringan laman sesawang merupakan alat yang penting dalam jenayah cinta siber yang tidak mengira bangsa, agama dan budaya mangsa. Bahkan perhubungan ini boleh berlaku tanpa mengira sempadan geografi, politik dan masa (Yong Siow Wei, 2007). Bahkan lebih membimbangkan lagi ialah penggunaan telefon pintar dan internet yang cukup canggih boleh menembusi dinding rumah bagi menjalin hubungan cinta melalui laman siber tanpa sempadan ini. Pelbagai jenis laman sosial yang tersedia dalam internet seperti *facebook, twitter, myspace, yahoo, messenger, tagged* dan sebagainya adalah medium yang digunakan oleh pelaku. Carian kata kunci *love scam* melalui google telah mengumpulkan lebih banyak maklumat berbanding enjin perayau yang lain. Google dengan teknologi "PageRank" memperoleh sebanyak dua puluh (20) kata kunci seperti '*internet dating scam'* (penipuan cinta siber); '*online dating fraud'* (penipuan cinta dalam talian) dan '*romance 419 scams'* (penipuan percintaan 419) dan empat tema yang bersilang yang ditemui ialah '*online dating, scams, frauds, the organization of cyber criminals*' (Rege, 2009).

Faktor utama golongan wanita profesional di Malaysia yang terlibat dalam penipuan cinta siber adalah kerana ketagihan dalam melayari laman sosial. Kajian Shazli et al (2011) melibatkan 47 wanita Melayu berpendidikan tinggi mendapati bahawa 68% daripada mereka kerap mengamalkan aktiviti bersembang dalam talian. Dapatan kajian juga mendapati bahawa responden mempunyai masalah kebosanan (38.8 %); ketagihan internet (36.2%); kesunyian (34.0%) dan kemurungan (17.0). Menurut Lawson dan Leck (2006) kesunyian dan kemurungan merupakan pemangkin seseorang terlibat dalam percintaan laman siber. Semakin tinggi kesunyian dan kemurungan, maka semakin kerap melibatkan diri dalam perhubungan laman siber. Penggunaan media dalam kalangan wanita profesional juga disebabkan mereka berasa sunyi, malu, tekanan dan sebagainya menyebabkan mereka lebih kerap menggunakan internet untuk mendapatkan hiburan dan sebagai cara pintas untuk melepaskan diri daripada kesunyian dan kemurungan.

Artikel ini bertujuan memahami faktor penglibatan mangsa dan *modus operandi* 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 amat penting dalam memberi gambaran sebenar penipuan cinta siber yang diceritakan oleh pengalaman peribadi mangsa yang perlu dikongsi bersama masyarakat setempat berkaitan faktor terlibat dengan *love scammer*, *modus operandi* pelaku dan langkah-langkah menangani isu jenayah cinta siber terutama dalam kalangan wanita dan remaja perempuan.

Metod Kajian

Reka bentuk kajian menggunakan pendekatan penerokaan (*exploratory*) kes 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 *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 sindiket jenayah cinta siber. Daripada aspek protokol kajian yang dikemukakan ialah bagaimanakah faktor golongan wanita profesional tertarik menjalinkan hubungan cinta siber dan memahami *modus operandi* yang digunakan dalam sindiket mengumpan wanita profesional terbabit dalam sindiket *Love Scam*. Analisis tematik telah digunakan untuk menginterpretasikan data bagi menjawab objektif kajian.

Dapatan Kajian dan Perbincangan

Profil Responden dan Informan

Bagi melengkapkan kajian ini, pengkaji menggunakan 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 satu dan dua yang dikemukakan dalam kajian ini. Kajian ini juga turut melibatkan tiga informan yang mempunyai latar belakang pendidikan

kerja sosial bagi menjawab objektif tiga kajian ini. Profil responden adalah seperti Jadual 1 manakala profil informan diperincikan di Jadual 2.

Jadual 1

Profil Responden Mangsa *Love Scam*

Responden	Umur	Kerjaya	Tahap Pendidikan	Tempoh Perkenalan	Jumlah Kerugian RM (ribu)
A	36	Guru	Ijazah	2 bulan	50
B	34	Pegawai Tadbir	Diploma	1½ bulan	35
C	33	Doktor	Ijazah	2 bulan	50
D	35	Ahli Perniagaan	Diploma	1 bulan	80
E	37	Pensyarah	Phd	2 bulan	70

Jadual 1 di atas memaparkan maklumat latar belakang responden yang dipilih bagi menjalankan kajian ini. Responden ini diperoleh daripada pegawai polis yang bertugas di JSJK Ibu Pejabat Polis Daerah X. Purata umur responden yang terjebak dalam jenayah komersil ini adalah di antara 34 hingga 37 tahun. Status perkahwinan keseluruhan responden yang dipilih adalah belum mendirikan rumah tangga. Manakala 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 daripada memiliki diploma hingga ke 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 mengikut responden 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.

Jadual 2

Profil Informan

Informan	Umur	Jantina	Status Pendidikan	Pekerjaan
1	30	Lelaki	Diploma	Sarjan
2	37	Perempuan	Phd	Pensyarah
3	30	Perempuan	Pelajar PhD	Pelajar
4	35	Lelaki	Pelajar PhD	Pegawai Kerajaan

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 satu dan dua 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). Responden 2 merupakan seorang pensyarah dalam bidang kerja sosial di UA, manakala responden 3 dan responden 4 merupakan pelajar sepenuh masa di UA yang merupakan pegawai di Jabatan Kebajikan Masyarakat (JKM).

Permulaan Modus Operandi

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 operandinya 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 daripada 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 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 ianya

dilihat sebagai satu cara yang paling berkesan untuk mendapatkan mangsa seperti yang terjadi kepada responden C. Hal ini disebabkan oleh, mengikut statistik, rakyat Malaysia menghabiskan masa selama tiga hingga lima jam sehari secara purata di alam siber dengan 58% 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 daripada British. 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-negara lain seperti Amerika. Hal ini kerana, media Malaysia lebih banyak memfokuskan kepada isu-isu berkaitan Amerika sama ada di dalam perfileman, politik, ekonomi dan sebagainya. Perkara ini secara tidak langsung membuatkan sindiket ini lebih berhati-hati dalam penyamaran identiti berkaitan kewarganegaraan.

Tempoh 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 baru.

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 *material* 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 *parcel* yang dijanjikan cuma alat untuk memanipulasikan mangsa.

Kesinambungan Modus Operandi

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, kebanyakkan 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 Dollar 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 *parcel* ke Malaysia. Kebiasaannya, hadiah yang dijanjikan oleh sindiket melibatkan barang-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.

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.

Penyamaran sebagai agensi percukaian

a) Pihak National Curier

> *…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 Curier* ini adalah untuk menghubungi mangsa dan menyatakan bahawa mangsa mendapat kiriman *parcel* 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

parcel yang dikirimkan dari luar negara terpaksa dikenakan pelbagai cukai seperti cukai pengangkutan, dan duti-duti penghantaran.

b) Pihak Kastam

> *…lepas tu sindiket akan drag (*mengheret*) mangsa pada 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 *parcel* kerana didapati kiriman *parcel* 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 *parcel* 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 *parcel*, tetapi pada hakukatnya 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.

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.* Jadual 3 menunjukkan jumlah pembayaran transaksi yang dilakukan oleh setiap responden kepada *scammer.*

Jadual 3

Profil Transaksi Mengikut Responden dan Peringkat

Responden	Jumlah Kerugian	Kadar Transaksi (peringkat) ('000 RM)					
		1	2	3	4	5	6
A	50 ribu	17	10	23	-	-	-
B	35 ribu	8	7	4	5	11	-
C	50 ribu	20	15	18	-	-	-
D	80 ribu	25	15	10	7	15	8
E	70 ribu	15	8	25	13	19	-

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.

Mengikut jadual 3, 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 *parcel* daripada luar negara dan perkara ini disebabkan oleh pihak peguam merupakan individu yang lebih arif terhadap undang-undang di dalam sesebuah negara dan ianya 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 dan Cadangan

Isu penglibatan wanita profesional menjadi mangsa *love scam* perlu diberi perhatian serius oleh pihak berkuasa dan kerajaan bagi membendung kesan negatif kepada individu, keluarga dan negara. Salah satu faktor dominan yang dikenal pasti ialah penggunaan bahasa dan layanan manis penuh kasih sayang yang diberikan oleh *love scammer* merupakan wanita terperangkap dalam jenayah cinta siber. Layanan manis seperti komunikasi yang berkesan, janji kemewahan selepas hidup bersama, ambil berat tentang mangsa sehingga mangsa terpukau dengan *love scammer* sehingga bertindak menjalin cinta di laman siber. Faktor seterusnya ialah capaian internet yang mudah, gaya hidup dan tekanan perasaan yang menyebabkan wanita mudah terjebak dalam cinta laman siber. Golongan wanita pada peringkat umur 30 hingga 35 tahun yang pada amnya telah pun stabil dalam kerjaya tetapi belum mempunyai pasangan hidup. Golongan ini menggunakan media sosial sebagai medium untuk berkongsi perasaan, masalah keluarga, tekanan kerja dan sebagainya sehingga ada individu yang mengambil kesempatan dalam kesempitan mangsa.

Sebaliknya bagi pihak *love scammer* pula, mereka merancang dengan licik untuk memanipulasi individu bagi mengaut keuntungan yang luar biasa. *Modus operandi* yang digunakan hampir sama kepada kesemua wanita yang ingin dijerat. Tempoh yang diambil tidak melebihi tiga bulan tetapi pendapatan yang diperoleh adalah puluhan ribu ringgit Malaysia. Sekiranya dalam tempoh tersebut *love scammer* ini tidak dapat menjerat mangsa, pihak sindiket ini akan mencari mangsa baru untuk dimanipulasi dan begitulah seterusnya sehingga berjaya. *Scammer* juga menghantar hadiah atau barangan melalui *parcel* sebagai penghargaan menjalinkan hubungan dengan *scammer*. Kemuncak *modus operandi* ialah pihak sindiket akan menyamar sebagai agensi percukaian dan menuntut bayaran terhadap *parcel* tersebut atas nama *scammer*. Pihak sindiket akan membuat pelbagai alasan mengenai *parcel* dan menuntut bayaran sehingga mangsa sedar bahawa mereka tertipu.

Justeru, penglibatan pihak polis dan pekerja sosial dapat membendung isu *love scam* daripada terus berleluasa. Peranan pekerja sosial dalam

menyediakan perkhidmatan intervensi krisis, kolaborasi dengan pihak berkuasa dalam membantu memberi pendedahan dan pendidikan psikososial terutama amalan inklusif dalam kalangan wanita agar wanita terutamanya kalangan profesional tidak mudah terpedaya. Kumpulan sokongan dalam komuniti perlu digerakkan bagi kempen kesedaran, pergiatkan tangkapan dan memantau laman web yang dikenal pasti terjebak dalam jenayah cinta siber. Intervensi psikososial bertujuan untuk memperbaiki hubungan mangsa dengan persekitaran hidup mereka setelah mengalami sesuatu krisis atau trauma. Peranan pekerja sosial sangat signifikan bagi membantu mangsa mencapai tahap kesejahteraan hidup.

Langkah-langkah menangani isu jenayah cinta siber ialah (a) menghantar wang kepada individu yang dikenali sahaja dan berhati-hati pertemuan dalam talian; (b) berhati-hati kepada sesiapa sahaja yang meminta bantuan dalam talian-tinggalkan laman sosial tersebut tanpa meninggalkan nombor telefon atau alamat e-mel; (c) jangan sesekali berikan maklumat perbankan anda kepada individu atau penjualan dalam talian yang tidak dikenali; (d) penipuan secara dalam talian menggunakan pelbagai cara untuk mendapatkan sesuatu barangan atau kewangan melalui kad kredit, kad pengenalan dan alamat peribadi di mana mangsa perlu melaporkan kepada pihak berkuasa untuk tindakan segera; dan (e) jangan berasa malu atau ingin menyembunyikan isu jenayah siber kerana pelaku sentiasa mencari mangsa seterusnya.

RUJUKAN

Hamburger, Y. A & Ben-Artzi, E. (2003). *Loneliness internet use. computers in human behavior* 19: 71-80.

Lawson, H. M. & Leck, K. (2006). *Dynamics of internet dating social science computer review*. (24): 662-676.

Jabatan Pengguna New Zealand. (2006). *www.westernunion.co.nz/.../romance-scam-awareness*

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

New Straits Times, (18 Feb 2013). Cyber security malaysia. online love scams are growing. heed the advice of cybersecurity malaysia. http://www.cybersecurity.my/en/knowledge_bank/news/2013

Rege, Aunshul. (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.

Sundramoorthy P. Buta cinta punca wanita diperbodohkan. Utusan Online (8 November 2011). 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. ISSN 1511-1893.

Sinar Harian, 8 April 2013.

The Straits Times, 27 Mac 2016.

Utusan Malaysia, 5 Mei 2014.

Utusan Malaysia, 6 Mei 2014.

Utusan Malaysia, 12 Mac 2016.

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