Malaysian Journal of Social Sciences and Humanities (MJSSH) (e-ISSN : 2504-8562)
2023, Volume 8, Issue 7, e002392
DOI: https://doi.org/10.47405/mjssh.v8i7.2392

Pandangan Dunia Pengguna Perniagaan Dalam Talian Tentang Jenayah Siber

(The World View of Online Business Users on Cybercrime)

Muhamad Yusri Abdul Karim[1*], Novel Lyndon[2]

[1]Fakulti Sains Sosial dan Kemanusiaan, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia.
Email: yusrikarim29@gmail.com
[2]Fakulti Sains Sosial dan Kemanusiaan, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia.
Email: novel@ukm.edu.my

CORRESPONDING AUTHOR (*):
Muhamad Yusri Abdul Karim (yusrikarim29@gmail.com)

KATA KUNCI:
Jenayah Siber
Pengguna dalam talian
Internet

KEYWORDS:
Cybercrime
Online users
Internet

CITATION:
Muhamad Yusri Abdul Karim & Novel Lyndon. (2023). Pandangan Dunia Pengguna Perniagaan Dalam Talian Tentang Jenayah Siber. *Malaysian Journal of Social Sciences and Humanities (MJSSH), 8*(7), e002392. https://doi.org/10.47405/mjssh.v8i7.2392

ABSTRAK

Pengguna perniagaan dalam talian sering kali menjadi mangsa jenayah siber walaupun pelbagai usaha telah dilakukan oleh pihak kerajaan melalui penguatkuasaan dan program pencegahan. Secara konseptualnya, jenayah siber merupakan suatu bentuk perlakuan jenayah yang menggunakan sebarang jenis peranti elektronik melalui sambungan perkhidmatan internet yang mampu menjangkaui batasan dari sesebuah negara ke negara yang lain dalam tempoh masa yang singkat dan tidak mempunyai sempadan. Justeru itu kajian ini dilakukan adalah untuk meneliti pandangan dunia pengguna dalam talian tentang jenayah siber dan faktor-faktor yang menyebabkan mereka berpandangan demikian. Di samping itu, kajian ini turut mengenal pasti faktor-faktor yang menyebabkan pengguna memilih pembelian dalam talian berbanding dengan pembelian secara konvensional. Kajian ini menggunakan pendekatan kualitatif melalui paradigma penyelidikan abduktif. Sejumlah 16 orang informan telah dipilih menggunakan teknik persampelan bola salji yang terdiri daripada lima orang lelaki dan sebelas orang wanita yang ditemu bual secara mendalam. Hasil kajian mendapati terdapat lima pemahaman mereka tentang jenayah siber. Lima perkara tersebut ialah jenayah siber ialah aktiviti peras ugut siber, pelanggaran data peribadi pengguna, aktiviti kecurian identiti pengguna, gangguan psikologikal, mental, buli siber dan kepura-puraan mendapatkan data berdasarkan organisasi yang terkenal. Kesimpulannya, hubungan sosial dan teknologi saling bergantung antara satu sama lain dan hampir kesemua masyarakat di dunia ini telah beralih daripada pembelian secara konvensional kepada teknologi pintar. Implikasi kajian ialah jangkaan sosial dan struktur kuasa yang mengelilingi perbuatan jenayah perlu dikawal bukan sahaja oleh pihak berkuasa tetapi juga oleh struktur sosial masyarakat.

© 2023 by the authors. Published by Secholian Publication. This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

ABSTRACT

Despite implementing enforcement and prevention programmes by the government, online business users remain susceptible to cybercrime. Cybercrime is a type of criminal activity that employs electronic devices and internet connectivity to transcend national boundaries and operate rapidly without geographical limitations. Consequently, the present study was undertaken to investigate the perspective of internet users regarding cybercrime and the determinants that contribute to shaping their viewpoint. Furthermore, this investigation also delineates the determinants that prompt customers to opt for online transactions in contrast to traditional ones. The present investigation employs a qualitative methodology within the framework of an abductive research paradigm. The study employed the snowball sampling technique to select 16 informants, comprising five male and 11 female participants, who underwent in-depth interviews. The findings of the research indicate that there exist five distinct conceptualisations of cybercrime. The five categories of cybercrime include cyber extortion, unauthorised access to personal data, identity theft, psychological harm, cyberbullying, and impersonation of reputable organisations to obtain sensitive information. In summary, a reciprocal relationship exists between social interactions and technological advancements, and a vast majority of global societies have transitioned from traditional modes of commerce to intelligent technological systems. The study suggests that effective management of social norms and power dynamics about criminal behaviour necessitates the intervention of law enforcement agencies and the active involvement of the broader societal framework.

Sumbangan/Keaslian: Kajian ini akan menjadi penyumbang kepada kajian literatur sedia ada mengenai pemahaman pengguna mengenai jenayah siber. Kajian ini juga akan menjadi rujukan kepada pengguna dalam talian mengenai jenayah siber dan seterusnya memberi pemahaman kepada pengguna mengenai apa itu jenayah siber.

1. Pengenalan

Globalisasi hari ini telah menyebabkan kehidupan masyarakat pada masa kini telah berubah yang menyebabkan masyarakat pada hari ini bergantung dan terikat kepada teknologi pengkomputeran dalam mengurus dan mengatur urusan seharian (Zaini & Shawaluddin, 2009). Hal ini ditambah lagi dengan perkembangan yang berlaku dalam bidang teknologi maklumat serta pertumbuhan internet yang menyebabkan wujudnya pelbagai aplikasi yang semakin membangun. Perkara ini secara tidak langsung telah menyebabkan ia penggunaan internet menjadi rutin penting dalam gaya hidup masyarakat pada hari ini. Menurut World Stats (2021) statistik pertumbuhan penggunaan internet di Malaysia sehingga Jun 2021 mencecah angka seramai 27.43 juta orang bersamaan dengan 85.72% daripada 32 juta orang penduduk Malaysia menggunakan internet. Menjelang tahun 2025, angka ini dijangka akan diunjurkan meningkat menjadi 97.5%. peningkatan penggunaan internet ini bukan sahaja berlaku di dalam Malaysia Malah ia melibatkan seluruh dunia.

© 2023 by the authors. Published by Secholian Publication. This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

Namun begitu, pertumbuhan penggunaan internet ini juga mendatangkan bahaya dan keburukan yang tidak dapat dielakkan. Hal ini demikian kerana, terdapat banyak pihak yang tidak bertanggungjawab telah menyalahgunakan kemajuan teknologi demi memenuhi kehendak serta keuntungan diri mereka. Kemudahan internet ataupun siber ini boleh menyebabkan pengguna terdedah kepada penyalahgunaan oleh pihak yang tidak bertanggungjawab. Antara penyalahgunaan yang dilakukan oleh pihak yang tidak bertanggungjawab ialah merupakan satu bentuk jenayah dan jenayah tersebut boleh diklasifikasikan sebagai jenayah siber. Jenayah siber ini merupakan perkara yang sangat serius dan tidak boleh dianggap sebagai perkara yang remeh. Jenayah siber merupakan jenayah yang menjadi penyumbang utama kepada kes-kes jenayah di negara-negara maju seperti negara-negara Eropah, Amerika dan Jepun (Boateng et al., 2011; Natsui, 2003). Jenayah siber merupakan jenayah yang unik kerana ia berlaku di atas talian dan tidak mempunyai bukti fizikal yang memudahkan pihak berkuasa menangkap penjenayah. Kebiasaannya, jenayah siber melibatkan jenayah rompakan atau pemindahan wang ke akaun penjenayah dengan amaun yang banyak tanpa disedari oleh mangsa. Menurut Anita dan Nazura (2004), jenayah siber berlaku terhadap seseorang individu atau sekumpulan orang yang mampu melangkaui batasan dari sebuah negara ke negara yang lain dalam sekelip mata dengan tempoh yang singkat dan tidak terhad kepada sesuatu batasan. Menurutnya lagi, jenayah siber merupakan jenayah yang menggunakan peranti elektronik yang disambungkan dengan internet yang membolehkan jenayah itu berlaku.

Justeru itu, bagi menangani masalah jenayah siber ini, pengetahuan mengenai perkara tersebut merupakan perkara yang sangat penting. Dalam pembentukan model *Knowledge, Attitude dan Practices (KAP),* elemen pengetahuan merupakan komponen yang sangat penting. Hal ini demikian kerana, seseorang itu tidak mampu bertindak terhadap sesuatu maklumat yang diperoleh tanpa ilmu pengetahuan yang mencukupi (Ramsey & Rickson, 2010). Hal ini jelas menunjukkan bahawa pengetahuan terhadap sesuatu perkara itu akan menyebabkan seseorang lebih berhati-hati atas setiap tingkah laku mereka. Menurut kajian yang dilakukan oleh Pitchan et al. (2017), ramai rakyat di negara ini telah menjadi mangsa kepada kes jenayah siber ini adalah disebabkan oleh kurangnya kefahaman serta kesedaran mengenai keselamatan penggunaan Internet. Hal ini demikian kerana masih ramai dalam kalangan pengguna Internet menganggap keselamatan dalam internet sebagai satu perkara yang remeh dan mengabaikan prinsip-prinsip keselamatan dalam Internet. Perkara ini boleh dilihat melalui peningkatan statistik dalam kes jenayah siber di Malaysia di mana pada tahun 2018 merekodkan kes sebanyak 8313 meningkat kepada 13,703 kes pada tahun 2019 dan seterusnya 17,227 kes pada tahun 2020. Bagi tahun 2021 kes meningkat kepada 20,701 dan pada tahun 2022 dari Januari hingga Julai mencatatkan kes sebanyak 12,092 (Bernama, 2022). Jumlah Kes yang dilaporkan ini amat membimbangkan dan memberi impak yang negatif kepada pengguna digital. Peningkatan kes ini berlaku adalah disebabkan oleh penggunaan Internet telah menjadi rutin harian dan risiko terdedah kepada ancaman siber juga amat tinggi. Justeru itu, kajian ini dilakukan bagi mengetahui kefahaman pengguna mengenai jenayah siber.

Oleh yang demikian, pertumbuhan internet yang berlaku di dalam negara kita bahkan secara global menyebabkan kegiatan jenayah siber ini juga turut berkembang dengan pesat. Kedua-dua elemen ini mempunyai kaitan yang sangat rapat dan ia akan menyebabkan masalah ini akan berlarutan jika tidak dibendung. Oleh hal yang demikian, kajian ini mengambil peluang untuk meneliti pemahaman pengguna dalam talian tentang jenayah siber dan mengapakah mereka berpandangan demikian.

© 2023 by the authors. Published by Secholian Publication. This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

2. Jenis Jenayah Siber Secara Global

2.1. Peras ugut siber

Peras ugut siber merupakan jenayah kategori luas yang berkaitan dengan internet dan komputer. Peras ugut siber ini melibatkan penjenayah yang memaksa orang ramai dan perniagaan menyerahkan wang atau data sensitif dengan cara ancaman dan juga paksaan (Sulkowski & Shea, 2007). Terdapat beberapa teknik yang biasa dilakukan oleh pemeras ugut siber dalam menjalankan modus operandi mereka iaitu dengan menceroboh perisian dan rangkaian komputer dan melumpuhkan sehingga anda membayar yuran ataupun denda yang dikenakan. Sebagai contoh, satu taktik yang biasa dilakukan ialah perisian tebusan yang melibatkan penggodam memperdaya salah seorang pekerja syarikat supaya mengklik pada pautan fail atau fail dalam mesej e-mel. Hal ini telah menyebabkan pengguna tidak dapat mengakses aplikasi dan fail pengguna. Oleh yang demikian, pengguna harus membayar kepada penggodam sebagai kunci untuk membaik pulih sistem yang telah tergendala supaya dapat diakses semula. Hal ini jelas menunjukkan peras ugut siber merupakan satu aktiviti yang telah dirancang di mana ia membuatkan perisian pengguna mengalami masalah dan memaksa pengguna membayar penggodam untuk memastikan pengguna dapat mengakses perisian dan juga fail yang telah digodam (Sulkowski & Shea, 2007).

2.2. Pelanggaran data peribadi pengguna

Pelanggaran data merupakan satu aktiviti di mana maklumat dicuri atau diambil daripada sistem tanpa pengetahuan atau kebenaran pemilik sistem. Kebiasaannya ia pelanggaran data ini melibatkan syarikat kecil atau organisasi besar. Antara data yang dicuri mungkin melibatkan maklumat sensitif atau sulit seperti data pelanggan, nombor kad kredit, hal keselamatan negara atau rahsia perdagangan atau. Kesan yang ditimbulkan oleh pelanggaran data boleh datang dalam bentuk kerosakan pada reputasi syarikat sasaran disebabkan oleh 'pengkhianatan amanah'. Mangsa dan pelanggan mereka juga mungkin mengalami kerugian kewangan sekiranya rekod berkaitan menjadi sebahagian daripada maklumat yang dicuri. Berdasarkan bilangan insiden pelanggaran data yang direkodkan antara Januari 2005 dan April 2015, maklumat pengenalan peribadi (PII) ialah jenis rekod yang paling banyak dicuri manakala data kewangan berada di tempat kedua. Kaedah pelanggaran lain yang sering diperhatikan termasuk kebocoran orang dalam yang mempunyai akses istimewa untuk mencuri data, penipuan kad pembayaran, kehilangan atau kecurian seperti komputer riba dan fail, pendedahan yang tidak disengajakan melalui kesilapan atau kecuaian, dan pelanggaran data yang tidak diketahui puncanya atau tidak didedahkan (Maurya et al., 2022).

2.3. Kecurian identiti pengguna

Jenayah kecurian identiti merupakan satu jenayah mendapatkan maklumat peribadi atau kewangan orang lain untuk menggunakan identiti mereka untuk melakukan penipuan, seperti membuat transaksi atau pembelian yang tidak dibenarkan. Kecurian identiti dilakukan dalam pelbagai cara dan mangsanya biasanya mengalami kerosakan pada kredit, kewangan dan reputasi mereka. Kecurian identiti berlaku apabila seseorang mencuri maklumat peribadi seperti nombor akaun bank dan maklumat kad kredit. Kecurian identiti boleh dilakukan dalam pelbagai cara dan antaranya ialah mengakses pangkalan data korporat untuk mencuri senarai maklumat pelanggan, menyelongkar tong sampah untuk mencari penyata bank akaun dan kad kredit serta menggodam

© 2023 by the authors. Published by Secholian Publication. This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

komputer atau rangkaian komputer untuk mengakses rekod awam. Terdapat beberapa jenis kecurian identiti antaranya ialah kecurian identiti kewangan, kecurian identiti perubatan, kecurian identiti sintetik dan kecurian identiti keselamatan sosial. Kesemua jenis kecurian identiti ini boleh digunakan oleh penjenayah dalam mendapatkan apa saja faedah melalui kecurian yang dilakukan. Menurut Hussain (2022), sukar untuk mengetahui sama ada kita pernah menjadi mangsa kecurian identiti. Hal ini berlaku kerana kita jarang menyemak penyata kewangan dan beberapa petunjuk jelas tentang kecurian identiti termasuk bil untuk item yang anda tidak beli di mana ini boleh dilihat pada kad kredit anda atau diterima melalui e-mel serta pesanan ringkas yang diterima (Hussain, 2022).

2.4. Gangguan Psikologikal, mental dan buli siber

Gangguan psikologikal, mental dan buli siber boleh berlaku melalui peranti digital seperti komputer, telefon bimbit, laptop dan juga tablet. Gangguan-gangguan ini boleh berlaku melalui pesanan ringkas, forum, permainan dan paling banyak berlaku ialah di laman sosial yang membolehkan orang ramai melihat, mengambil bahagian atau berkongsi kandungan berbahaya,negatif, palsu dan jahat tentang orang lain. Ia boleh termasuk berkongsi maklumat peribadi tentang orang lain yang menyebabkan rasa malu atau kehinaan. Sesetengah buli siber melampaui batas kepada tingkah laku yang menyalahi undang-undang atau jenayah. Gangguan psikologikal, mental dan buli siber boleh mengakibatkan masalah mental kepada mereka yang mengalaminya. Beberapa kajian keratan rentas dan juga membujur telah melaporkan bahawa penganiayaan buli siber dikaitkan dengan peningkatan risiko idea untuk membunuh diri, mencederakan diri sendiri dan percubaan membunuh diri. Perkara ini ditambah lagi dengan kurangnya sokongan rakan sebaya, kecerdasan emosi, tingkah laku ganas serta penggunaan bahan yang menjadi akses kepada media sosial dan internet yang akhirnya mempengaruhi perkaitan antara penganiayaan buli siber dan gangguan kesihatan mental. Mesch (2009) dalam kajiannya menyatakan bahawa wanita dua kali lebih berkemungkinan menjadi mangsa buli siber sekurang-kurangnya sekali daripada lelaki. Hal ini demikian kerana corak jantina ini mungkin digariskan oleh stereotaip budaya di mana responden lelaki cuba menangani masalah itu sendiri dan mengelak daripada melaporkan penganiayaan kerana berbuat demikian boleh merosakkan rasa maskulin mereka. Dalam Sebaliknya, wanita mungkin menggalakkan pelaporan penganiayaan kerana mereka menganggap buli siber sebagai masalah serius dan lebih mementingkan hubungan rakan sebaya juga (Maurya et al., 2022).

2.5. Kepura-puraan mendapatkan data berdasarkan organisasi yang terkenal

Jenayah ini berlaku apabila penjenayah menelefon mangsa dan mendakwa mereka daripada sesebuah organisasi tertentu seperti Polis, Pihak Kerajaan atau Pihak bank. Penjenayah akan memberitahu mangsa bahawa mangsa terlibat dalam sesuatu jenayah atau telah melanggar undang-undang dan meminta mangsa untuk melakukan pembayaran tertentu supaya kes ini tidak berlarutan dan ditimpa lebih banyak masalah. Kebanyakan yang menjadi mangsa oleh penjenayah ini adalah dari golongan warga emas yang kurang mahir dalam teknologi. Namun begitu, terdapat juga mangsa yang terdiri dari warga muda. Oleh yang demikian, kes jenayah ini berlaku tidak mengira umur, dan juga jantina. Terdapat pelbagai penyamaran yang dilakukan sebagai contoh Pihak polis atau Kerajaan yang kebiasaannya dari pihak Lembaga Hasil Dalam Negeri (LHDN) yang menyatakan mangsa terlibat dalam kegiatan jenayah atau menyalahi undang-undang percukaian. Menurut Boateng et al. (2011), untuk mengukuhkan lagi dakwaan mereka,

© 2023 by the authors. Published by Secholian Publication. This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

mereka akan memaklumkan segala identiti mangsa seperti nombor kad pengenalan, nama dan nombor akaun bank. Hal ini jelas akan membuatkan mangsa berasa percaya dan kemudian membayar denda seperti yang diminta (Boateng et al., 2011).

3. Metod Kajian

Kajian ini menggunakan kaedah kualitatif di mana dalam mengumpul data, paradigma penyelidikan abduktif telah digunakan. Paradigma abuktif merupakan satu strategi yang digunakan untuk menerangkan mengenai realiti sosial serta memahami kehidupan sosial dari segi cerita serta motif aktor sosial berdasarkan segala pengalaman yang dialami oleh aktor sosial itu sendiri (Blaikie, 2000). Pengkaji juga menggunakan temu bual secara mendalam dengan mendapatkan seberapa banyak maklumat yang boleh berkenaan perspektif informan dan juga pengalaman mereka sendiri. Dalam kajian ini, temu bual mendalam yang telah dilaksanakan terhadap 16 orang responden adalah secara bersemuka. 16 orang informan dipilih adalah terdiri daripada pengguna yang aktif dalam pembelian dalam talian, pernah menjadi mangsa jenayah siber dan menetap di Lembah Klang. Mereka dipilih adalah kerana untuk menjawab persoalan kajian mengenai pemahaman mereka mengenai jenayah siber dan kriteria yang mereka ada dapat membantu mereka menjawab setiap persoalan yang ditanya. Prosedur persampelan "*Snowball"* telah dilakukan dalam mendapatkan maklumat melalui informan. Prosedur ini digunakan terutamanya apabila pengkaji mengalami kesukaran atau tidak memperoleh senarai subjek yang mempunyai ciri-ciri yang sama dalam populasi yang dipilih. Dalam menjalankan kajian ini, Satu kawasan telah dipilih oleh pengkaji dalam menjalankan kajian ini dan kawasan tersebut ialah di sekitar Lembah Klang yang terdiri daripada Cheras, Putrajaya dan juga Shah Alam. Seterusnya data yang diperoleh daripada temu bual secara mendalam yang dilakukan bersama 16 orang informan dianalisis menggunakan analisis tema. Tema dibina apabila pengkaji melakukan proses mengkategorikan dan menyeragamkan data-data temu bual kesemua informan mengikut susunan soalan kajian yang merangkumi konsep-konsep yang dikaji. Dalam menentukan tema, data telah diperiksa, disusun dan ditapis terlebih dahulu supaya bersesuaian dengan tema serta melindungi data-data yang sensitif.

4. Hasil Kajian

4.1. Memahami Jenayah Siber Sebagai Aktiviti Peras Ugut Siber

Hampir kesemua informan yang ditemu bual menyatakan bahawa pemahaman mereka mengenai jenayah siber adalah peras ugut siber yang berlaku atas talian dan bukannya secara fizikal ataupun komersial seperti jenayah-jenayah lain yang mempunyai bukti-bukti fizikal yang memudahkan pihak berkuasa untuk melakukan analisis dan mampu menangkap penjenayah tersebut. Seperti yang diketahui umum, jenayah siber merupakan jenayah yang berlaku di negara-negara yang maju dan moden seperti negara Amerika, negara-negara Eropah dan juga negara Jepun. Jenayah siber ini jenayah yang sukar mendapatkan bukti-bukti fizikal dan perkara ini menyukarkan pihak berkuasa untuk menangkap serta mengenal pasti suspek. Hal ini disebabkan oleh pembangunan teknologi yang semakin rancak. Oleh yang demikian, pihak-pihak yang tidak bertanggungjawab mengambil kesempatan untuk melakukan jenayah siber ini dengan memperdaya masyarakat pada hari ini. Peras ugut siber merupakan jenayah yang kerap berlaku terhadap sesebuah syarikat yang besar dan jarang berlaku terhadap individu. Kebiasaannya, modus operandi yang dilakukan terhadap peras ugut siber ini ialah penjenayah akan mengancam untuk melumpuhkan operasi perniagaan yang menjadi

© 2023 by the authors. Published by Secholian Publication. This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

sasaran dengan menjejaskan sistem atau data sesebuah syarikat. Kemudian setelah mereka melumpuhkan sistem sesebuah syarikat itu, mereka akan mengugut meminta bayaran bagi membaik pulih godam yang mereka lakukan terhadap sistem yang telah mereka lakukan. Satu contoh mudah yang boleh dilihat ialah terdapat seorang lelaki bernama A yang menggodam sistem syarikat Coca-Cola. Kini dia mempunyai akses kepada resipi rahsia untuk minuman ringan Coca-Cola. Kini, A mengancam syarikat itu perlu membayar wang tebusan yang banyak untuk pemulihan resipi, jika tidak, ia akan dibocorkan ke domain awam atau dihantar kepada pesaing lain. Ini merujuk kepada contoh mudah yang boleh difahami mengenai jenayah peras ugut siber ini.

Dalam satu kajian yang dilakukan oleh Mahawar (2022) menyatakan bahawa Penjenayah siber biasanya melakukan pemerasan siber sama ada menyekat akses kepada komputer mangsa atau membebankan rangkaiannya dengan menjalankan atau memperkenalkan sejumlah besar trafik. Dalam kes trafik yang padat pada rangkaian, mangsa tidak dapat menjalankan perniagaannya sama sekali kerana rangkaian biasanya gagal di muat naik kerana trafik yang berterusan. Mangsa mengalami ketidakupayaan untuk menjalankan perniagaannya. selain itu, mangsa akan menanggung perbelanjaan yang besar untuk pemulihannya, yang juga merupakan proses panjang yang mengganggu kewangan perniagaan. Dalam kes pemerasan siber seperti yang dinyatakan, mangsa terpaksa membayar wang tebusan dan biasanya dari segi kewangan atau data pentingnya sama ada peribadi atau komersial dibocorkan kepada orang ramai yang boleh memudaratkan mangsa. Lebih-lebih lagi dalam kes sedemikian, mangsa tidak boleh menghubungi pihak berkuasa untuk mendapatkan bantuan yang diperlukan kerana terdapat risiko besar kehilangan maklumat peribadinya di laman rangkaian sosial kepada orang ramai. Akibatnya, boleh difahami bahawa peras ugut siber atau pemerasan adalah salah satu bentuk kezaliman yang berlaku dalam bentuk jenayah yang melanggar prinsip privasi dan menyebabkan mangsa mengalami penyeksaan mental dan fizikal yang hebat.

4.2. Jenayah Siber Merupakan Aktiviti Pelanggaran Data Peribadi Pengguna

Pelanggaran data merupakan aktiviti mendedahkan maklumat sulit, sensitif dan dilindungi kepada orang yang tidak sepatutnya tanpa kebenaran. Pelanggaran data ini boleh berlaku kepada sesiapa sahaja sama ada individu, perusahaan yang besar dan juga kerajaan. Hal ini jelas menunjukkan bahawa sesiapa sahaja boleh menjadi mangsa pelanggaran data jika mereka tidak mempunyai perlindungan. Secara umumnya, pelanggaran data ini berlaku adalah disebabkan oleh kelemahan teknologi perlindungan dalam melindungi data yang sedia ada. Hal ini berlaku adalah disebabkan oleh alatan komputer dan peranti mudah alih mempunyai lebih banyak ciri penghubung dan tempat untuk data dihubungi yang menyebabkan ia memberi kelebihan kepada penjenayah untuk melakukan pelanggaran data. Selain itu, kepesatan teknologi baru menyebabkan data yang sedia ada sukar untuk dilindungi dan penjenayah mempunyai kepakaran yang lebih baik untuk melakukan aktiviti pelanggaran data. Oleh yang demikian, pengguna dan juga perusahaan syarikat mempunyai risiko yang tinggi untuk menghadapi pelanggaran data tanpa keselamatan sistem yang menyeluruh.

Menerusi temu bual yang dilakukan, informan menyatakan pelanggaran data peribadi pengguna merupakan pemahaman mereka mengenai jenayah siber ini. Mereka menyatakan bahawa penjenayah melakukan pelanggaran data ini melalui sistem oleh sebab kepakaran yang mereka ada melebihi pengguna. Informan juga berpendapat bahawa pelanggaran data peribadi ini boleh berlaku terhadap individu dan juga syarikat

© 2023 by the authors. Published by Secholian Publication. This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

kecil ataupun organisasi yang besar malahan ia juga boleh melibatkan negara. Data yang dicuri mungkin melibatkan maklumat sensitif atau sulit seperti nombor kad kredit, data pelanggan, rahsia perdagangan atau hal keselamatan negara. Informan juga berpendapat bahawa pelanggaran data ini melibatkan kebocoran orang dalam yang mempunyai akses istimewa untuk mencuri data, penipuan kad pembayaran, kehilangan atau kecurian seperti komputer riba dan fail, pendedahan yang tidak disengajakan melalui kesilapan atau kecuaian, dan pelanggaran data yang tidak diketahui puncanya atau tidak didedahkan.

Menurut kajian yang dilakukan oleh Brunst (2008), pelanggaran data boleh berlaku dalam 4 cara. Cara yang pertama ialah pelanggaran data berlaku kepada orang dalam tanpa sengaja. Contohnya ialah pekerja yang menggunakan komputer rakan sekerja dan membaca fail tanpa mempunyai kebenaran yang sepatutnya. Akses adalah tidak disengajakan, dan tiada maklumat dikongsi. Walau bagaimanapun, kerana ia dilihat oleh orang yang tidak dibenarkan, data tersebut dianggap dilanggar. Cara yang kedua ialah, pelanggaran data boleh berlaku pada orang dalam yang berniat jahat. Orang ini dengan sengaja mengakses dan berkongsi data dengan niat untuk mendatangkan bahaya kepada individu atau syarikat. Orang dalam yang berniat jahat mungkin mempunyai kebenaran yang sah untuk menggunakan data, tetapi niatnya adalah untuk menggunakan maklumat itu dengan cara yang jahat. Cara yang ketiga ialah pelanggaran data berlaku apabila peranti hilang atau dicuri dan yang keempat ialah penjenayah luar berniat jahat. Penjenayah ini adalah penggodam yang menggunakan pelbagai vektor serangan untuk mengumpulkan maklumat daripada rangkaian atau individu.

4.3. Memahami Jenayah Siber Sebagai Aktiviti Kecurian Identiti Pengguna

Kecurian identiti juga merupakan salah satu pemahaman pengguna dalam talian mengenai jenayah siber. Kecurian identiti ini berlaku apabila maklumat peribadi mangsa dicuri dan digunakan oleh penjenayah siber atau penipu untuk mendapatkan akses ke pelbagai bidang kehidupan digital mangsa. Kecurian identiti pengguna ini juga berlaku oleh sebab berlakunya tumbuhan yang pesat terhadap transaksi digital dan penerimaan e-dagang dalam urusan harian pengguna. Oleh hal yang demikian, penjenayah mengambil kesempatan terhadap pertumbuhan ini untuk melakukan jenayah dan mencuri identiti pengguna demi mengaut keuntungan dengan cara yang menyalahi undang-undang. Tambahan lagi, penjenayah siber ini melakukan kecurian identiti pengguna ini bukan sahaja untuk tujuan kewangan, malahan boleh memusnahkan kerjaya dan juga nyawa mangsa oleh sebab aktiviti penyalahgunaan identiti mangsa ini.

Terdapat dua objektif yang dilakukan oleh penjenayah semasa menyalahgunakan identiti atau nama mangsa. Penjenayah akan melakukan salah satu objektif ini apabila mereka mencuri data mangsa. Objektif pertama penjenayah ialah penjenayah akan mendapatkan faedah dari segi kewangan tidak kira membuat pinjaman bank, penyalahgunaan kad kredit dan pembelian barang e-dagang menggunakan nama palsu. Objektif kedua penjenayah ialah mereka berniat untuk mencederakan mangsa oleh sebab motif rendah yang dihadapi oleh penjenayah seperti cemburu, cinta iri hati, dengki, dendam dan juga rasa benci. Dalam hal ini, penjenayah akan menerbitkan sesuatu yang negatif di laman-laman sosial dengan nama mangsa dan juga membuat serangan siber atau pengumuman yang negatif.

Penjenayah juga boleh menjual identiti mangsa yang dicuri di web gelap atau lebih dikenali sebagai *dark web.* Web gelap ini merupakan pasaran di mana penjenayah boleh

© 2023 by the authors. Published by Secholian Publication. This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

membeli atau menjual maklumat peribadi yang dicuri. Terdapat tiga pasaran yang dijadikan tempat penjenayah untuk melakukan aktiviti mencuri identiti mangsa. Pasaran yang pertama ialah *Surface web* di mana ia merupakan pasaran yang kandungannya mudah diakses oleh sesiapa sahaja dan ia dipantau oleh pihak kerajaan secara amnya. Pasaran ini tidak memberi risiko yang besar kepada pengguna. Antara pasaran *surface web* ini ialah laman berita, rangkaian sosial dan juga e-dagang. Selain itu, pasaran yang digunakan ialah *deep web*. *Deep web* merupakan apa-apa kandungan ataupun maklumat yang memerlukan kata laluan untuk diakses, mempunyai keselamatan dan memerlukan log masuk. Antara contoh *deep web* ini ialah forum, pengkalan data dan juga fail polis. Pasaran yang ketiga ialah *dark web* yang merupakan web yang mempunyai kandungan-kandungan yang negatif serta persekitaran di mana ia mempunyai kandungan yang terlarang di dalamnya dan boleh berlaku aktiviti menjual beli barang yang dicuri, senjata, dadah dan pornografi kanak-kanak.

Kecurian data pengguna ini juga boleh menyebabkan penjenayah mencederakan mangsa oleh sebab motif rendah yang dihadapi oleh penjenayah seperti cemburu, cinta iri hati, dengki, dendam dan juga rasa benci. Dalam hal ini, penjenayah akan menerbitkan sesuatu yang negatif di laman-laman sosial dengan nama mangsa dan juga membuat serangan siber atau pengumuman yang negatif. Perkara ini telah diterangkan di dalam teori kriminologi di bawah hipotesis kekecewaan-pencerobohan oleh ahli psikologi universiti Yale. Mereka percaya bahawa kemarahan datang sebelum kekecewaan, dan kekecewaan boleh nyata dalam kedua-dua tingkah laku yang agresif dan tidak agresif (Runions et al., 2013). Sebaliknya, emosi negatif ini memerlukan tindak balas mengatasi sebagai cara untuk melegakan tekanan dalaman. Mengatasi melalui tingkah laku dan keganasan yang menyalahi undang-undang mungkin benar terutamanya untuk remaja kerana sumber yang terhad dan ketidakupayaan mereka untuk melarikan diri dari persekitaran yang mengecewakan.

Menurut kajian yang dilakukan oleh Zainab (2015) terdapat 5 jenis aktiviti yang dilakukan oleh penjenayah selepas melakukan kecurian identiti mangsa. Salah satunya ialah melakukan pembelian barang, penyalahgunaan dalam bentuk forum dan media sosial, mencipta profil palsu dalam rangkaian sosial, salah nyata atau fakta palsu dan kecurigaan palsu dan tuduhan kesalahan jenayah. Kelima-lima aktiviti ini merupakan aktiviti yang dilakukan oleh penjenayah apabila mereka mencuri data pengguna yang memberikan kesan yang buruk kepada mangsa dan memberikan keuntungan kepada para penjenayah. Kesemua aktiviti yang dilakukan oleh penjenayah ini tiada objektif lain selain memberikan keuntungan kepada mereka tanpa memikirkan apa yang dilalui oleh mangsa.

4.4. Jenayah Siber Merupakan Jenayah Gangguan Psikologikal, Mental dan Buli

Gangguan psikolologikal, mental dan buli merupakan salah satu aktiviti jenayah siber yang sangat popular dan kerap berlaku pada masa kini. Gangguan psikologikal terbahagi kepada dua iaitu ia berkaitan dengan gangguan kognitif dan juga gangguan afektif. Gangguan kognitif ini melibatkan kepada aspek intelektual ataupun perkembangan minda manakala gangguan afektif pula ia melibatkan aspek emosi sepenuhnya. Bagi aktiviti jenayah siber yang berlaku ini, gangguan psikologikal melibatkan aspek gangguan afektif dimana ia mengganggu emosi seseorang mangsa yang akhirnya menyebabkan mangsa tidak dapat mengawal emosi dan seterusnya melakukan perkara yang di luar pertimbangan kita sebagai manusia seperti bunuh diri dan mencederakan diri. Hal ini demikian kerana, apabila berlaku gangguan psikologikal terhadap aspek

© 2023 by the authors. Published by Secholian Publication. This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

afektif ataupun emosi ia akan menyebabkan mangsa berasa marah, sedih, dendam dan benci. Emosi ini jika tidak dapat dikawal ia akan menjadi negatif dan apabila dapat dikawal ia akan menjadi positif yang membuatkan emosi seseorang menjadi gembira, riang, kasih dan seronok. Jadi fokus jenayah siber ini ialah dengan mengganggu psikologikal mangsa sehingga mangsa tidak dapat mengawal emosi dan seterusnya melakukan perkara yang tidak diingini.

Bagi gangguan mental pula, ia berlaku apabila seseorang tidak dapat mengawal perasaan yang akhirnya menyebabkan perlakuan serta tingkah laku yang berisiko dan juga negatif. Gangguan mental ini juga boleh berlaku kepada sesiapa sahaja tanpa mengira umur, jantina, bangsa dan juga status kesihatan. Gangguan mental ini boleh mencapai tahap kritikal sehinggan mangsa tidak dapat berfikir dengan waras dan normal seperti orang lain. Ia berlaku disebabkan beberapa perkara iaitu faktor sosial, biologi dan psikologi. Jenayah siber menurut pemahaman pengguna ialah penjenayah melakukan jenayah di atas talian dengan melakukan gangguan mental kepada mangsa. Gangguan ini dilakukan di dalam laman-laman sosial sehingga menyebabkan mangsa hilang pertimbangan dan seterusnya melakukan perkara yang negatif. Oleh hal yang demikian ia diklasifikasikan sebagai jenayah alaf baru iaitu jenayah siber.

Seterusnya, jenayah siber ini juga boleh berlaku terhadap aspek buli siber. Buli siber merupakan satu aktiviti komunikasi dengan menggunakan teknologi dan berlaku di alam maya dengan tujuan mengganggu, mengecam, memalukan dan mengugut mangsa melalui aktiviti penyebaran berita palsu, menghamburkan perkataan yang negatif kepada mangsa dan membuat perkongsian mengenai video dan juga gambar yang boleh memalukan mangsa. Kesemua aktiviti buli siber ini akan memberikan kesan yang negatif kepada mangsa dan seterusnya akan menyebabkan mangsa mengalami gangguan psikologikal dan juga gangguan mental. Hal ini jelas menunjukkan buli siber ini merupakan satu jenayah yang boleh mendatangkan kesan yang negatif terhadap mental mangsa. Jadi ia merupakan perkara yang dilarang dan menjadi aktiviti jenayah yang boleh membawa kepada kes yang serius.

Menurut satu kajian yang dilakukan oleh Zainab (2015) menyatakan bahawa gangguan psikologikal dan mental ini berlaku terhadap seseorang apabila mereka tidak dapat bertoleransi terhadap sesuatu tekanan yang mereka hadapi dalam pelbagai sudut. Seperti kita sedia maklum, toleransi merupakan satu proses dimana seseorang itu dapat mengadaptasi kemampuan seseorang dalam menghadapi situasi yang sulit atau sukar dan penuh dengan tekanan. Menurut Zainab (2015) lagi, terdapat tiga aspek yang mendasari aspek kemampuan diri seseorang. Aspek yang pertama ialah kemampuan seseorang dalam memilih perkara yang sesuai dalam mengatasi masalah tekanan diri sebagai contoh mengatasi masalah tekanan dengan melakukan perkara yang sesuai dan efektif terhadap diri , mengetahui cara apa yang perlu dilakukan dan cara untuk melaksanakannya supaya ia berhasil dalam mengatasi masalah tekanan yang dihadapi. Aspek kedua ialah mengenal pasti perubahan yang berlaku terhadap diri dalam mengatasi sesuatu masalah dengan baik supaya ia berhasil dan kecenderungan terhadap sesuatu pengalaman yang baru secara optimistik. Aspek yang ketiga pula ialah bagaimana seseorang itu dapat mengatasi masalah yang dihadapi dengan melakukan perkara seperti menenangkan diri, sentiasa sabar dan memastikan diri sentiasa tenang apabila menghadapi sesuatu masalah atau kesulitan tanpa ada sebarang kuasa negatif yang mampu memberi kesan terhadap diri seseorang.

© 2023 by the authors. Published by Secholian Publication. This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

4.5. Jenayah Siber Merupakan Aktiviti Kepura-Puraan Mendapatkan Data Berdasarkan Organisasi Yang Terkenal

Dalam mengenal pasti pemahaman pengguna mengenai jenayah siber ini, sesi temu bual telah dilakukan bersama informan dan salah satu pemahaman informan mengenai jenayah siber ini ialah informan menyatakan bahawa penjenayah melakukan aktiviti kepura-puraan mendapatkan data ataupun melakukan penipuan berdasarkan organisasi yang terkenal dan juga pihak-pihak yang berautoriti di sesebuah negara untuk merompak wang simpanan mangsa dan melakukan penipuan. Namun begitu, kes jenayah siber yang disebut oleh informan semasa sesi temu bual yang dilakukan ini telah diklasifikasikan sebagai sindiket *Macau Scam* atau *Telecommunication Fraud*. Sindiket ini telah dilabel atau dikategorikan sebagai penipuan telekomunikasi yang berlaku yang melibatkan penjenayah dan juga mangsa.

Sindiket *Macau Scam* atau *Telecommunication Fraud* ini sebenarnya didalangi oleh warga asing dan juga warga tempatan yang cuba menipu mangsa dengan melalukan panggilan secara rambang dan rawak dengan berpura-berpura mewakili organisasi-organisasi yang terkenal seperti Polis Di Raja Malaysia (PDRM), Lembaga Hasil Dalam Negeri (LHDN) dan Pihak Bank. Mereka juga berpura-pura sebagai pegawai yang mempunyai autoriti serta mampu menimbulkan rasa panik, was-was yang menyebabkan mangsa ingin membela diri mereka serta mengelak daripada dikenakan tindakan undang-undang. Taktik serta cara yang digunakan oleh penjenayah ini adalah bertujuan untuk memperdaya mangsa yang boleh mendatangkan kerugian yang besar kepada mangsa jenayah ini. Melalui jenayah siber Macau Scam ini, terdapat beberapa modus operandi yang digunakan oleh penjenayah dalam menipu pengguna. Modus operandi yang pertama ialah membuat panggilan dengan menyatakan pengguna memenangi cabutan bertuah, membuat penipuan mengenai penculikan dan meminta wang tebusan kepada mangsa, modus operandi yang ketiga ialah *Spoofing* yang menyamar sebagai pegawai kerajaan seperti Polis, SPRM, dan pihak mahkamah serta *spoofing* yang seterusnya ialah menyamar sebagai pegawai Bank Negara Malaysia ataupun bank komersial.

Dalam melakukan jenayah ini, penjenayah menggunakan elemen psikologi apabila membuat panggilan bersama mangsa. Sebagai contoh, apabila melakukan panggilan telefon, penjenayah akan menggunakan elemen kepatuhan terhadap organisasi yang dilakonkan. Mangsa kepada jenayah siber ini akan cepat berasa cemas dan takut apabila mendapat panggilan daripada pihak PDRM ataupun pihak mahkamah seolah-olah mereka melakukan kesalahan yang melanggar undang-undang negara. Perkara ini telah menjadikan penjenayah mendapat kelebihan untuk melakukan proses seterusnya untuk mendapat wang melalui penipuan yang dilakukan apabila mangsa patuh dan berasa cemas apabila berpura menjadi organisasi tersebut. Selain itu, penjenayah tersebut merupakan seorang yang terlatih kerana penggunaan ayat yang baik semasa melakukan perbualan dan perkara ini secara tidak langsung dapat meyakinkan mangsa bahawa mereka merupakan pihak yang benar dan bukanlah dari pihak yang membuat penipuan.

Namun begitu, terdapat beberapa undang-undang yang diwujudkan oleh pihak kerajaan dalam memastikan perkara ini dapat dikawal dan melindungi pengguna dalam menjadi mangsa kepada penipuan yang berpura-pura dalam mendapatkan data berdasarkan organisasi yang terkenal ini. Antaranya ialah Sekseyn 420 Kanun Keseksaan, Seksyen 416 Kanun Keseksaan dan Akta Pencegahan Pengubahan Wang Haram, Pencegahan Pembiayaan Keganasan aan Hasil Daripada Aktiviti Haram 2001 (Akta 613). Bagi

© 2023 by the authors. Published by Secholian Publication. This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

Sekseyn 420 Kanun Keseksaan, peruntukan ini dikenakan terhadap kesalahan menipu secara curang bagi memaksa pengguna menyerahkan wang atau harta benda pengguna kepada diri mereka. Jika disabitkan kesalahan, mereka akan dikenakan penjara tidak melebihi 10 tahun, hukuman sebat dan juga denda. Bagi Seksyen 416 Kanun Keseksaan pula, peruntukan akan dilakukan terhadap seseorang yang melakukan penipuan dengan menyamar sebagai orang lain atau pihak yang berautoriti demi melakukan penipuan. Jika perkara ini disabitkan kesalahan, pesalah akan dihukum penjara tidak lebih 7 tahun dan denda atau kedua-duanya sekali. Akhirnya bagi Akta Pencegahan Pengubahan Wang Haram, Pencegahan Pembiayaan Keganasan dan Hasil Daripada Aktiviti Haram 2001 (Akta 613) pula, ia melibatkan kesalahan membabitkan penggubahan wang haram seperti melibatkan diri secara langsung atau tidak langsung terhadap transaksi daripada aktiviti haram dan menerima, memperoleh, menyembunyikan, memiliki, memindahkan menukar, mengubah, melupuskan, membawa dan menggunakan hasil daripada perbuatan yang salah atau haram. Jika disabitkan, mereka akan dikenakan penjara tidak lebih daripada 15 tahun dan denda daripada hasil yang diterima. Hal ini jelas menunjukkan bawah aktiviti berpura-pura dalam mendapatkan data sebagai organisasi yang popular merupakan satu jenayah siber yang sangat popular dan jika disabitkan kesalahan ia akan memberikan hukuman yang setimpal dengan perbuatan yang dilakukan.

5. Kesimpulan

Menerusi hasil kajian yang diperoleh, dapat disimpulkan bahawa pengguna memahami jenayah siber itu secara dasarnya dan mampu menterjemahkan pemahaman mereka apabila sesi temu bual berlangsung. Secara keseluruhannya, hasil analisis dapatan kajian berjaya menungkai pemahaman pengguna dalam talian tentang jenayah siber. Terdapat 5 aspek yang disebut oleh informan mengenai pemahaman mereka mengenai tema utama dalam kajian ini iaitu jenayah siber. Antaranya ialah jenayah siber merupakan aktiviti peras ugut siber, jenayah siber merupakan aktiviti pelanggaran data peribadi pengguna, memahami jenayah siber sebagai aktiviti kecurian identiti pengguna, jenayah siber merupakan jenayah gangguan psikologikal, mental dan buli dan aktiviti kepura-puraan mendapatkan data berdasarkan organisasi yang terkenal. Kemajuan Internet pada masa kini telah menyebabkan berlakunya peningkatan dalam kes jenayah siber pada hari ini. Walaupun begitu, masih lagi ramai pengguna yang masih tidak menghiraukan kes jenayah siber yang semakin meningkat dari tahun ke tahun. Hal ini demikian kerana adalah disebabkan oleh kurangnya pemahaman mengenai jenayah siber dan kurang mengambil berat mengenai kes jenayah siber yang semakin meningkat. Informan memahami, mengetahui dan menyedari mengenai jenayah siber itu sendiri tetapi hanyalah secara asas dan bukanlah secara keseluruhan. Namun begitu mereka mampu menterjemahkan pemahaman mereka dengan baik semasa sesi temu bual. Hal ini telah menyebabkan kajian ini berjaya dilakukan dan dapat menjawab persoalan kajian mengenai pemahaman pengguna mengenai jenayah siber.

Kelulusan Etika dan Persetujuan untuk Menyertai Kajian (*Ethics Approval and Consent to Participate*)

Kajian ini dilakukan mengikut etika yang telah ditetapkan dan setiap data yang diperolehi dari informan menggunakan etika yang betul dan sebelum melakukan pengumpulan data telah mendapat persetujuan dari Supervisor dan Pihak Universiti Kebangsaan Malaysia (UKM)

© 2023 by the authors. Published by Secholian Publication. This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

Penghargaan (*Acknowledgement*)

Ribuan terim kasih diucapkan kepada Supervisor saya Prof Madya Dr. Novel yang banyak membantu saya dalam menyiapkan artikel ini serta terima kasih kepada informan yang terlibat dalam kajian ini.

Kewangan (*Funding*)

Kajian ini tidak menerima sebarang pembiayaan sepanjang melaksanakan kajian ini.

Konflik Kepentingan (*Conflict of Interest*)

Kajian ini tidak menerima sebarang pembiayaan sepanjang melaksanakan kajian ini.

Rujukan

Anita, A. R., & Nazura, A. M. (2004). *Jenayah Berkaitan Dengan Komputer: Perspektif Undang-Undang Malaysia*. Kuala Lumpur: Dewan Bahasa Dan Pustaka.

Bernama. (2022, September 26). Jenayah siber: 12,092 kes, kerugian RM414.8 juta. *Harian Metro*. https://www.hmetro.com.my/itmetro/2022/09/885795/jenayah-siber-12092-kes-kerugian-rm4148-juta

Blaikie, N. (2000). *Designing social research*. Cambridge: Polity Press.

Boateng, R., Longe, O. babatope, Isabalija, R. S., & Budu, J. (2011). Sakawa – Cybercrime and Criminality in Ghana. *Journal of Information Technology Impact, 11*(2), 85–100.

Brunst , P. W. (2008). *Use of the Internet by Terrorists a Threat Analysis*. IOS Press Ebooks. https://ebooks.iospress.nl/volumearticle/24328

Hussain, A. (2022, September 21). What Is Identity Theft? Definition, Types and Examples. London: *SSRN Electronic Journal*.

Mahawar, S. (2022, January 10). Criminal Conspiracy under I.P.C. Criminal Conspiracy. *Ipleaders*. https://blog.ipleaders.in/criminal-conspiracy-under-ipc/

Maurya, C., Muhammad, T., Dhillon, P., & Maurya, P. (2022). The Efects of Cyberbullying Victimization on Depression and Suicidal Ideation among Adolescents and Young Adults: A Three Year Cohort Study from India. *Bmc Psychiatry,* 22, 599. https://doi.org/10.1186/s12888-022-04238-x

Mesch, G. S. (2009). Parental Mediation, Online Activities, and Cyberbullying. *Cyberpsychology & Behavior, 12*(4), 387–93. https://doi.org/10.1089/cpb.2009.0068

Natsui, T. (2003). Cybercrimes in Japan: Recent Cases, Legislations, problems and perspectives. *Kertas kerja, NetSafe II Conference, Auckland, Newzealand*. http://cyberlaw.la.coocan.jp/Documents/netsafepapers_takatonatsui_japan.pdf

Pitchan, M. A., Omar , S. Z., Bolong, J., & ghazali, A. H. (2017). Analisis Keselamatan Siber Dari Perspektif Persekitaran Sosial: Kajian Terhadap Pengguna Internet Di Lembah Klang. *Jurnal Sains Sosial Dan Kemanusiaan, 12*(2), 016–029.

Ramsey, C. E., & Rickson, R. E. (2010). Environmental knowledge and attitudes. *Journal of environmental education, 8*(11), 10–18. https://doi.org/10.1080/00958964.1976.9941552

Runions, K., Shapka, J. D., Dooley, J., & Modecki, K. L. (2013). Cyber Aggression, Victimization, and Social Information Processing: Adressing the Medium and the Message. *Psychology of Violence, 3*(1), 9–26. DOI:10.1037/a0030511

© 2023 by the authors. Published by Secholian Publication. This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

Sulkowski, A. J., & Shea , T. (2007). Cyber-Extortion: The Elephant in the Server Room. *SSRN Electronic Journal*. DOI:10.2139/ssrn.955969

World Stats. (2021, Disember 28). Internet 2021 Usage in Asia. *World Stats.* https://www.statista.com/statistics/265153/number-of-internet-users-in-the-asia-pacific

Zainab Ismail (2015). Faktor Gangguan Psikologi Dalam Kalangan Mahasiswa Universiti. *Al-Himah Journal of Islamik Dakwah, 7*(2), 55–71. http://spaj.ukm.my/jalhikmah/index.php/jalhikmah/i

Zaini Othman & Wan Shawaluddin (2009). *Dunia tanpa sempadan: Teknologi maklumat dan persoalan keselamatan negara*. Penerbit UKM.

© 2023 by the authors. Published by Secholian Publication. This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).