e-ISSN:2829-4580, p-ISSN: 2829-4599
DOI: https://doi.org/10.38035/jim.v2i1
Received: 17 Mei 2023, Revised: 1 Juni 2023, Publish: 2 Juni 2023

JIM
JURNAL ILMU MULTIDISIPLIN
E-ISSN:2829-4580, P-ISSN=2829-4599
https://greenpub.org/JIM
editor@greenpub.org
0811 7401 455

Pencegahan Penipuan Social Engineering pada Massa 4.0

Dimas Ryan Triwahono[1], Achmad Fauzi[2], Adzansyah Adzansyah[3], Belva Yulivio[4], Muhammad Yusuf Fito[5], Reynaldo Ghifari Putra Yuntama[6], Satrio Waliyudin Azhar[7]
[1.] Universitas Bhayangkara Jakarta Raya, Indonesia, ryantwhn@gmail.com
[2.] Universitas Bhayangkara Jakarta Raya, Indonesia, achmad.fauzi@dsn.ubharajaya.ac.id
[3.] Universitas Bhayangkara Jakarta Raya, Indonesia, adzansyah11@gmail.com
[4.] Universitas Bhayangkara Jakarta Raya, Indonesia, yulivio.belva@gmail.com
[5.] Universitas Bhayangkara Jakarta Raya, Indonesia, m.yusuffito@gmail.com
[6.] Universitas Bhayangkara Jakarta Raya, Indonesia, aldozuper1@gmail.com
[7.] Universitas Bhayangkara Jakarta Raya, Indonesia, satriowaliyudin13@gmail.com

Corresponding Author: Dimas Ryan Triwahono

Abstract: *This paper intends to explore three social design related online protection issues facing organizations and develop techniques to stop human trickery in friendly design attacks. Twenty experts in Branch Security Information Structures took part in a three-round Delphi study to unify and refine the feeling of high quality. The three rounds move the individual towards a setting for guidelines against attacks with friendly plans in affiliates. Three basic problems: compromised data; inadequate training; and the lack of sophisticated training drives the three target areas to apply best practices against social plan attacks. The invention provides countermeasures by coordinating high-level training, techniques, cycles, and preparation into safety exercises. This study adds to the field of organizational security with an emphasis on trust and human creativity to examine counter-accommodation counter-accommodation attack plans. This paper adds to the set of underrepresented underrepresented social program monitoring implementation of social programs.*

Keyword: *IT Strategy, Security, Trust, Human-computer interaction (HCI).*

Abstrak: Makalah ini bermaksud untuk mengeksplorasi tiga masalah perlindungan online terkait desain sosial yang dihadapi organisasi dan mengembangkan teknik untuk menghentikan tipu daya manusia dalam serangan desain ramah. Dua puluh ahli dalam Struktur Informasi Keamanan Cabang mengambil bagian dalam studi Delphi tiga putaran untuk menyatukan dan menyempurnakan perasaan berkualitas tinggi. Tiga putaran menggerakkan individu menuju pengaturan untuk pedoman melawan serangan dengan rencana persahabatan dalam afiliasi. Tiga masalah dasar: data yang disusupi; latihan yang tidak memadai; dan kurangnya pelatihan canggih mendorong tiga bidang target untuk menerapkan praktik terbaik terhadap serangan rencana sosial. Penemuan ini memberikan

penanggulangan dengan mengoordinasikan pelatihan tingkat tinggi, teknik, siklus, dan persiapan ke dalam latihan keamanan. Studi ini menambah bidang keamanan organisasi dengan penekanan pada kepercayaan dan kreativitas manusia untuk memeriksa balasan terhadap rencana penyerangan kontra-akomodasi. Makalah ini menambahkan untuk mengatur penelitian penjaminan yang kurang terwakili dalam pelaksanaan pemantauan program sosial yang dibatasi.

Kata Kunci: Strategi TI, Keamanan, Kepercayaan, Interaksi manusia-komputer (HCI).

PENDAHULUAN

Dalam kejahatan dunia maya, ada kecenderungan yang berkembang ke arah rekayasa sosial, suatu bentuk serangan dunia maya yang unik, karena biayanya yang sederhana dan keuntungan yang tinggi dalam melakukan kejahatan. Untuk melewati jaringan dan kontrol teknis, peretas memanfaatkan serangan rekayasa sosial melalui berbagai bentuk komunikasi online, teknologi, dan teknik penipuan untuk membujuk dan mengelabui individu agar memberikan akses ke jaringan perusahaan (Blacbkbourne N, 2016). Rekayasa sosial berupaya mempengaruhi pekerja untuk melakukan tindakan yang dapat merugikan organisasi (S.D.A, 2009), Dengan menargetkan individu yang seringkali tidak mengetahui nilai informasi yang mereka berikan (Conteh N. Y. and Schmick P.J, 2016), pekerja dapat salah menafsirkan maksud bahwa memberikan informasi membawa sedikit biaya kepada penolong (Lohani S, 2018), gagal menjaga sistem komputer yang aman aman dari niat jahat (Hasanuddin W.Z.B, 2020)

Memanfaatkan kepercayaan dan psikologi perilaku manusia dan pengambilan keputusan, insinyur sosial bertujuan untuk menembus jaringan keamanan dengan memanipulasi orang dalam untuk mendapatkan informasi rahasia (Akbar, S., Rabi', A., Minggu, D., &Mujahidin, 2019). Sementara banyak perusahaan menyadari peretasan eksternal atau serangan dunia maya, banyak perusahaan gagal menangani kontrol keamanan secara internal di tingkat karyawan (Februariyanti, 2006). Setelah dikompromikan, organisasi dapat kehilangan data, keunggulan kompetitif, dan menderita kerugian finansial. Yang diperlukan agar kejahatan dunia maya berhasil hanyalah satu eksploitasi atau kerentanan keamanan.

Meningkatnya serangan kejahatan dunia maya yang menargetkan penipuan manusia mendukung penelitian pendekatan pertahanan balik terhadap rekayasa sosial dalam organisasi. Berbeda dari peretasan jaringan langsung, serangan rekayasa sosial mengeksploitasi pengambilan keputusan dan kepercayaan manusia untuk membujuk korban agar secara tidak sengaja membocorkan informasi sensitif (Herjanto, E., & Kristiningrum, 2006). Serangan-serangan ini berkisar pada pengambilan keputusan instan untuk mempercayai suatu tindakan atau tidak dengan membuka atau mengklik tautan. Ada hubungan antara tingkat kepercayaan individu dan kinerja individu dalam lingkungan yang didukung komputer (Perwita, 2008).

Dibandingkan dengan ketersediaan literatur untuk keamanan TI untuk kejahatan dunia maya, kurangnya publikasi peer-review untuk pertahanan rekayasa sosial untuk serangan rekayasa sosial membenarkan perlunya penelitian. Google Cendekia mengembalikan 2,5 juta artikel peer-review untuk keamanan TI dalam kejahatan dunia maya yang diterbitkan selama dekade terakhir. Menyempurnakan pencarian untuk mencerminkan literatur yang berkaitan secara khusus dengan serangan rekayasa sosial untuk periode yang sama, Google Cendekia mengembalikan 496.000 artikel peer-review, seperlima dari jumlah referensi untuk topik luas keamanan TI. Sejak 2016, Google Cendekia mencerminkan hanya 22.000 artikel peer-reviewed yang diterbitkan tentang topik pertahanan atau pencegahan rekayasa sosial dan

39.000 artikel peer-review terkait keberhasilan serangan rekayasa sosial. Kesenjangan dalam literatur khusus untuk solusi yang diterapkan untuk melawan serangan rekayasa sosial yang menargetkan penipuan manusia. Kesenjangan dalam penelitian ini dalam memberikan pertahanan dan solusi rekayasa sosial yang efektif untuk menangkal serangan yang menjadi tujuan penelitian ini.

1. Bagaimana Cara pencegahan sosial enggering pada massa 4.0?
2. Apa saja metode untuk melakukan pencegahan sosial enggering ?

METODE

Metodologi eksplorasi menggunakan strategi subjektif untuk mengkaji kekhasan orang miskin yang terkonsentrasi secara luas. Tujuan dari desain Delphi adalah untuk mengumpulkan pendapat ahli menjadi tiga strategi dan solusi masa depan yang paling mungkin untuk menempatkan pertahanan rekayasa sosial ke dalam tindakan untuk menghentikan dan menggagalkan serangan rekayasa sosial. Menurut Linstone dan Turoff (2002), konfigurasi Delphi adalah metode terkenal untuk mengatur korespondensi profesional di mana komitmen yang signifikan dibuat dan evaluasi yang memenuhi syarat dicari. Akibatnya, ini memberikan kerangka kerja yang tepat untuk anggapan peristiwa sosial yang merupakan hasil terbaik dari mengumpulkan kesepakatan untuk strategi dan pengaturan. masa depan. untuk menggagalkan upaya rekayasa sosial (Aliyhafiz.com, 2020) Menurut (Gondohanindijo, 2010) desain Delphi sangat cocok untuk menentukan penilaian subyektif kolektif peserta kelompok dan membantu mereka dalam membuat keputusan dan mencapai konsensus tentang topik yang sedang diselidiki. Tanggapan kolektif para ahli dapat mengarah pada praktik terbaik yang disarankan di masa depan (Gondohanindijo, 2010), dan pertanyaan penelitian mencari penilaian dan pendapat pemimpin mengenai praktik terbaik di masa depan (kemungkinan pendekatan, solusi, strategi, dan kebijakan yang efektif). Hal ini membuat penelitian Delphi kredibel (Aliyhafiz.com, 2020). dan metode).

Peserta diberi kebebasan untuk mengirimkan pendapat ahli mereka secara elektronik dan asinkron selama tiga putaran survei, terlepas dari zona waktu atau lokasi mereka, terlepas dari fakta bahwa penelitian dilakukan dalam pengaturan virtual online. Itu dilakukan dengan sampling yang disengaja. Audiens target untuk komunitas Asosiasi Keamanan Sistem Informasi (ISSA) dipilih berdasarkan pengalaman dan keahlian keamanan TI, sertifikasi, publikasi tentang rekayasa sosial, penelitian keamanan informasi, dan keterlibatan sebelumnya dengan program keamanan TI. Hanya anggota ISSA AS dengan setidaknya sepuluh tahun pengalaman kepemimpinan keamanan TI, CISSP atau sertifikasi keamanan IS lainnya, lima tahun keanggotaan aktif ISSA, dan artikel atau presentasi yang dipublikasikan tentang rekayasa sosial di tingkat konferensi ISSA nasional yang memenuhi syarat untuk ikut serta dalam belajar. Untuk kelompok ini, studi tentang potensi strategi dan solusi rekayasa sosial tingkat perusahaan pemimpin TI adalah ideal. Ada 25 orang dari populasi sasaran dalam kerangka sampling. Signifikansi penemuan ditingkatkan dengan membatasi populasi tinjauan sesuai dengan standar ini. Ada 25 orang dari populasi sasaran dalam kerangka sampling. Ketika populasi penelitian dibatasi sesuai dengan kriteria ini, temuannya lebih relevan. Ada 25 orang dari populasi sasaran dalam kerangka sampling. Ketika populasi penelitian dibatasi sesuai dengan kriteria ini, temuannya lebih relevan.

HASIL DAN PEMBAHASAN

Dalam draf Delphi, terdapat pertanyaan penelitian, komentar, dan partisipasi dari para ahli tentang potensi strategi dan solusi untuk mencegah dan menghentikan serangan rekayasa sosial. Dengan mengirimkan undangan peserta melalui email dan menampilkan notifikasi email untuk pertanyaan, metode survei elektronik membuat pengumpulan data menjadi lebih mudah.

Gambaran Umum Monkey memberikan tata letak yang mudah dipahami untuk membuat rencana studi yang diperluas untuk menyematkan teks untuk reaksi terbuka di Babak 1 dan 3. Di Babak 2, Survey Monkey menyediakan templat kotak teks tarik dan tarik yang dapat disesuaikan untuk memberi peringkat atau mengurutkan respons secara otomatis dalam urutan. Anonimitas melalui penggunaan internet untuk pengiriman melalui situs web yang aman.

Para panelis diminta untuk memberikan pendapat ahli mereka tentang tiga isu paling signifikan mengenai organisasi rekayasa sosial yang harus ditangani sekarang dan di masa mendatang sebagai jawaban atas pertanyaan terbuka di Putaran 1. Saat respons survei Survey Monkey baru diterima, peneliti menerima peringatan pemberitahuan survei otomatis melalui email. Di Babak 2, sepuluh tanggapan teratas dimasukkan dari kumpulan semua tanggapan. Putaran 2 meminta panelis untuk memberi peringkat sepuluh tanggapan teratas dalam urutan abjad dan mengurutkan masalah dari yang paling penting hingga yang paling tidak penting, dengan opsi untuk berkomentar untuk klarifikasi. Pemeringkatan dari tiga item survei peringkat paling penting dari Putaran 2 berfungsi sebagai dasar untuk survei Putaran 3. Peserta diminta untuk menjelaskan bagaimana mereka akan mengimplementasikan tiga solusi teratas dalam teks tertulis yang menjelaskan implementasinya. Bagian prosedur pengumpulan dan analisis data memberikan gambaran ringkasan reduksi data.

Di Babak 2, Daftar sepuluh isu teratas yang diidentifikasi oleh kelompok tersebut dipresentasikan kepada 23 panelis di Putaran 2. Panelis tidak diberi tahu mana dari sepuluh isu teratas yang paling sering dicatat; sebaliknya, daftar tersebut disusun menurut abjad. Hal ini dilakukan untuk mencegah agar peserta tidak terpengaruh oleh opini mayoritas, atau bias kelompok. Sepuluh isu dalam daftar mencerminkan kata-kata panelis yang paling sering digunakan. Para panelis diinstruksikan untuk mengambil daftar sepuluh item ini dan menyusunnya dalam urutan kepentingan, dimulai dengan No. 1 dan yang paling tidak krusial sebagai No. 10, mengingat pentingnya kesepuluh isu tersebut. Untuk menghindari duplikasi, panelis diinstruksikan untuk tidak menetapkan nomor yang sama untuk lebih dari satu terbitan. 21 dari 23 panelis menyelesaikan Putaran 2 dengan mengurutkan masalah menurut kepentingannya. Peringkat mereka kemudian dimasukkan ke dalam spreadsheet Excel, di mana rata-rata untuk masing-masing sepuluh masalah dihitung. Peringkat keseluruhan grup untuk sepuluh masalah potensial diberikan oleh rata-rata.

Di Babak 3, anggota panel diberi peringkat untuk tiga masalah teratas dan diminta untuk memberikan solusi spesifik dan mendetail yang dapat memecahkan atau memperbaiki masalah tersebut. Mereka juga diberi instruksi untuk memperluas detail apa pun yang menurut mereka penting untuk solusi.

Metode InVivo dan Focused Coding Saldana, bersama dengan perangkat lunak NVivo 8, menyediakan metode pengkodean tematik untuk menganalisis hasil panel pakar kolektif dari setiap putaran dan data yang diprioritaskan. Tiga tanggapan teratas dikategorikan dan diberi kode menggunakan komentar kontekstual (Nasution, 2008). Menggunakan pengkodean Siklus Pertama InVivo untuk memeriksa lebih lanjut tanggapan untuk melihat apakah ada peluang untuk pengurangan data atau pengkodean tambahan. Pengkodean siklus kedua menggunakan metode Focused Coding untuk mengatur ulang dan menganalisis kembali data yang dikodekan menggunakan metode siklus pertama memberikan peluang tambahan untuk pengkodean (Nasution, 2008)

Pertanyaan survei putaran 1 menghasilkan 69 hal besar yang berkaitan dengan perancangan sosial yang dicatat dan dikaji ke dalam empat wilayah yang berkaitan dengan soal ujian: pendidikan pengguna; prosedur, kebijakan, dan program keamanan; data yang terkontaminasi; dan pendidikan dan pelatihan yang berkelanjutan. 78% ahli mengidentifikasi jaringan yang disusupi dari serangan phishing yang berhasil sebagai salah satu masalah utama dalam hal serangan desain sosial. Kesadaran pengguna tertinggi dan informasi yang

dikompromikan dikutip oleh 69% panelis sebagai masalah paling signifikan yang terkait dengan serangan rekayasa sosial. Masalah yang paling mendesak, menurut 60% panelis, adalah nama dan reputasi yang dikompromikan, informasi yang dibobol, serta praktik dan kebiasaan karyawan yang buruk..

Putaran kedua survei digunakan untuk menentukan peringkat dan memprioritaskan sepuluh masalah teratas. Panelis menggunakan skala satu sampai sepuluh untuk menetapkan skor numerik. Untuk setiap panelis, semua rating dijumlahkan dan dibagi dengan jumlah isu. Berdasarkan peringkat panelis dalam urutan kepentingan, ini memberikan peringkat rata-rata keseluruhan untuk setiap item. Tabel II menunjukkan 10 penilaian reaksi terbaik dengan penilaian tipikal dari yang paling patut diperhatikan hingga yang paling tidak dinilai. Karena urutan peringkat didasarkan pada 1 (paling penting) dan 10 (paling tidak penting), masalah dengan rata-rata yang lebih rendah menunjukkan tingkat kepentingan yang lebih besar.

Pada skala satu sampai sepuluh, para panelis mendefinisikan tiga isu paling signifikan terkait rekayasa sosial sebagai berikut sebagai titik balik dalam penelitian: data yang dikompromikan dari organisasi; kurangnya langkah-langkah keamanan organisasi atau ketidakefektifannya; serta pelatihan dan pendidikan berkelanjutan bagi karyawan. Sembilan dari 21 panelis memeringkat data yang dikompromikan sebagai perhatian paling penting atau peringkat teratas. Dari 21 spesialis, 7 memposisikan ketidakcukupan atau kurangnya latihan keselamatan sebagai faktor pemosisian terbesar kedua. Pendidikan berkelanjutan dan pelatihan karyawan non-tech-savvy, seperti eksekutif dan asisten, dinobatkan sebagai isu rekayasa sosial terpenting ketiga oleh enam panelis. Tiga panelis menilai praktik dan kebiasaan buruk karyawan sebagai masalah paling signifikan dengan serangan rekayasa sosial untuk bisnis.

Temuan ini mencakup tiga pendekatan potensial untuk menggagalkan atau mencegah serangan rekayasa sosial dalam bisnis: Kontrol teknologi dan perilaku harus seimbang dalam solusi keamanan; Langkah-langkah keamanan harus diberlakukan, menurut temuan. Ada tiga kemungkinan cara untuk menghentikan serangan rekayasa sosial dalam bisnis: Kontrol teknologi dan perilaku harus seimbang dalam solusi keamanan; Penting untuk menerapkan langkah-langkah keamanan dan terus melatih perilaku pengguna.

KESIMPULAN

Serangan rekayasa sosial kini menjadi komponen umum dari serangan siber terhadap perusahaan, dan saat ini menjadi salah satu ancaman terbesar bagi keamanan siber semua orang. (Hermawan, 2014). Karena manipulasi sifat manusia daripada kontrol teknologi, pertahanan rekayasa sosial terus menjadi titik lemah dalam mengendalikan keamanan ISIS. (Hermawan, 2014). Penetrasi organisasi oleh serangan teknis yang umum telah digagalkan oleh alat teknologi dan perangkat lunak keamanan, tetapi serangan rekayasa sosial yang menargetkan orang-orang tertentu belum. Penelitian ini didasarkan pada masalah menggagalkan serangan rekayasa sosial, dengan masalah khusus apa yang dapat dilakukan oleh para ahli keamanan siber di masa depan sebagai pertahanan balik dalam serangan rekayasa sosial.

Menurut sebuah panel spesialis keamanan, tiga masalah terbesar dalam rekayasa sosial adalah data organisasi yang dikompromikan, praktik keamanan organisasi yang tidak memadai atau tidak ada sama sekali, serta pendidikan dan pelatihan rekayasa sosial staf yang sedang berlangsung. Panel tersebut merekomendasikan solusi keamanan berlapis berupa otentikasi dan pendidikan keamanan, pendidikan dan pelatihan berkelanjutan, praktik, kebijakan, dan prosedur keamanan, komunikasi yang sering dengan berbagai media, pengembangan pendidikan karyawan, dan akuntabilitas untuk mengatasi masalah-masalah ini.

Metode untuk mencegah penipuan oleh manusia dan dampak dari penerapan kebijakan dan program keamanan yang efisien, serta pendidikan dan pelatihan yang konsisten, memiliki implikasi untuk praktik di masa depan. Arah penelitian di masa depan mungkin akan melihat berapa biaya yang dibutuhkan untuk menerapkan solusi dari sudut pandang keuangan dan operasional di perusahaan. Penelitian di masa depan dapat meningkatkan pemahaman kita untuk membuat rencana tindakan menyeluruh yang mencakup sumber daya manusia dan keuangan untuk memajukan penyertaan pendidikan dan pelatihan rekayasa sosial dalam praktik keamanan informasi. Biaya aktual untuk menciptakan dan menerapkan solusi organisasi untuk bisnis dari berbagai ukuran dapat diselidiki oleh para peneliti di masa depan.

Meskipun serangan rekayasa sosial hanya merupakan bagian kecil dari keseluruhan kejahatan siber, efeknya bisa sangat menghancurkan bagi organisasi. Kejahatan dunia maya terus menjadi salah satu masalah yang paling mendesak bagi masyarakat. Temuan penelitian ini memajukan bidang keamanan siber dengan menekankan pelatihan keamanan semacam ini, praktik dan prosedur yang berkelanjutan, komunikasi yang sering, dan pengembangan karyawan dengan akuntabilitas sebagai solusi organisasi untuk memerangi penipuan manusia untuk menghentikan atau mengurangi serangan rekayasa sosial. Penelitian ini menyoroti pentingnya memasukkan teknik rekayasa sosial ke dalam rencana kejahatan siber strategis yang komprehensif bagi organisasi.

Karena kesimpulan didasarkan pada penilaian kolektif dari kelompok yang lengkap, penelitian memiliki keterbatasan. (Rafizan O., 2011). Kelemahan dari desain Delphi yang muncul pada desain penelitian yang hasilnya bergantung pada konsensus telah diteliti secara mendalam. Tata letak yang tepat dan signifikansi dari putaran pertama pertanyaan adalah salah satu kelemahan Delphi. (Junaedi D.I, 2017) Keterbatasan dapat muncul jika keselarasan mengenai putaran pertama tidak mewakili komponen penting karena kuesioner kedua dan selanjutnya bergantung pada kuesioner pertama. (Fadlil A, 2020)

REFERENSI

Akbar, S., Rabi', A., Minggu, D., &Mujahidin, I. (2019). FrequencyHopping Video Real Time UntukPengamanan Data Pengintaian Operasi Inteligence TNI. *JASIEK*, *1*(19–27), 3.

Aliyhafiz.com. (2020). *SocialEngineering, Pengertian, Langkah-Langkah,DanCaraMenghindarinya.*

Blacbkbourne N. (2016). The Dark Side of Social Engineering,. *EDPACS*, *53*(8–9), 4.

Conteh N. Y. and Schmick P.J. (2016). Cybersecurity:risks, vulnerabilities andcountermeasures to prevent social engineering attacks. *International Journal OfAdvanced Computer Research*, *1*(31–38).

Fadlil A, R. I. and N. A. (2020). Data Security for School Service Top-UpTransactions Based on AES Combination Blockchain Technology Modification,. *Lontar Komputer*, *11*(155–166), 3.

Februariyanti, H. (2006). Standar danManajemen Keamanan Komputer. *Teknologi InformasiDINAMIK*, *11*(134–142), 2.

Gondohanindijo, J. (2010). *Pengamanan Sistem Berkas.*

Hasanuddin W.Z.B. (2020). Improving Network Performanceof IP PBX Based Telecommunication System. *Lontar Komputer*, *11*(101–113), 2.

Hasibuan, M. S. & Gultom, L. M. (2018). Analisis Serangan Deface MenggunakanBackdoor Shell Pada Website. *Techno.COM*, 415–423.

Herjanto, E., & Kristiningrum, E. (2006). KAJIAN STANDARBIDANG KEAMANAN. *KAJIAN STANDARBIDANG KEAMANAN.*, *8*(18–26), 1.

Hermawan, R. (2014). Analisis Konsep Dan Cara Kerja Serangan KomputerDistributed Denial Of Service (DDOS). *Faktor Exacta*, *5*(1–14).

Junaedi D.I. (2017). "Antisipasi Dampak Social Engineering Pada Bisnis Perbankan,." *Ilmu-Ilmu Informatika Dan Manajemen STMIK*, *11*(1).

Lohani S. (2018). Social Engineering: Hacking into Humans,. *4th International Conferenceon Cyber Security (ICCS)*, *1*(385–393), 2.

Nasution, M. I. P. (2008). Urgensi Keamanan Pada Sistem Informasi. *Jurnal Iqra'*, *2*, 41–53.

Perwita, A. A. (2008). DinamikaKeamanan Dalam HubunganInternasional Dan ImplikasinyaBagiIndonesia. *Universitas Katolik Parahyangan*.

Rafizan O. (2011). "Analisis Penyerangan Social Engineering,." *4th International Conferenceon Cyber Security (ICCS)*, *2*(115–126).

S.D.A, M. (2009). "Social Engineering: Hacking the Wetware! *Information SecurityJournal: A Global Perspective*, *18*(40–46), 1.

Seskoau. (2020). Prosedur TetapTentang Mata Pelajaran SeskoauYang Tidak Diikuti Oleh PasisNegaraSahabat. *Markas BesarAngkatan Udara Sekolah Staf DanKomando*.

Suherman, Widodo, P., & Gunawan, D. (2017). Efektivitas KeamananInformasi Dalam MenghadapiBahaya Social Engineering. *JurnalProdi Peperangan Asimetris*, *73–90*, 1.

Susetyo, H. (2008). Menuju ParadigmaKeamananKomprehensifBerperspektif Keamanan Manusiadalam Kebijakan KeamananNasional. *Lex Jurnalica*, 1–2.

Velicia, V., Wisanjaya, I., & Widiatedja, I. (2015). Perlindungan HukumTerhadap Indonesia Dalam KasusPenyadapan Oleh Australia. *Program Kekhususan HukumInternasional Dan Hukum Bisnis*.