Edukasi Bahaya *Social Engineering* Menggunakan Media Belajar Quizizz Untuk Meningkatkan Kesadaran Keamanan Informasi Nasabah Perbankan

Tabina Dea Anindya[a1], Gusti Made Arya Sasmita[a2], I Putu Agus Eka Pratama [b3]
[a]Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Udayana
Kampus Bukit Jimbaran, Bali, Indonesia, 0361-701806
e-mail: [1]deanindya13@gmail.com, [2]aryasasmita@it.unud.ac.id , [3]eka.pratama@unud.ac.id

Abstrak

Menanggulangi ancaman keamanan informasi nasabah, bank telah berperan dengan menerapkan prinsip kepercayaan dan prinsip kerahasiaan yang diwujudkan melalui pengamanan teknologi informasi yang kuat serta pemberdayaan SDM yang baik. Keamanan bank yang sulit ditembus ini membuat pelaku kejahatan siber beralih menggunakan teknik social engineering yang menargetkan nasabah bank. Teknik yang juga disebut dengan human hacking ini menjadi salah satu ancaman keamanan informasi dalam sektor perbankan yang patut diwaspadai. Penelitian ini bertujuan untuk meningkatkan kesadaran keamanan informasi nasabah perbankan melalui edukasi bahaya social engineering menggunakan media belajar Quizizz. Hasil penelitian menunjukkan adanya peningkatan awareness pada kelompok kontrol dari 33% (poor) menjadi 63,2% (average) dan pada kelompok eksperimen dari 22,3% (poor) menjadi 66,8% (average). Penggunaan media belajar Quizizz efektif membantu kelompok eksperimen memperoleh peningkatan nilai yang signifikan dengan melihat gain score antar kelompok, serta dibuktikan secara statistik melalui uji independent sample t-test.

Kata-kata kunci: *Data Pribadi,* Social Engineering, Information Security Awareness, *Quizizz*

Abstract

Overcoming information security threats, the bank has implemented the principle of trust and confidentiality which are realized by a strong information technology securement and good HR empowerment. Strongly protected banking system made cybercriminals turn to social engineering technique targetting banking customers. This technique, also called human hacking, aims for confidential information by manipulating its victim's psychology, making it as one of the hazardous information security threats in the banking sector. This research aimed to increase banking customers' information security awareness through education on the dangers of social engineering using Quizizz learning media. Results showed that there's an increase in awareness level in the control group from 33% (poor) to 63,2% (average) and in the experimental group from 22,3% (poor) to 66,8% (average). The use of Quizizz effectively helped experimental group obtain a significant increase in scores by looking at the gain scores comparison between groups and independent sample t-test result.

Keywords: *Personal Data, Social Engineering, Information Security Awareness, Quizizz*

1. Pendahuluan

Perkembangan teknologi informasi yang pesat mengarah pada peningkatan kecepatan dan mobilitas akses informasi.[1] Hal tersebut juga membuat manusia menjadi sangat mengandalkan teknologi dalam kesehariannya hingga timbul sifat ketergantungan. Masyarakat semakin mudah terhubung untuk saling berinteraksi, berperilaku, bekerja, bertransaksi, dan berpikir sebagai masyarakat digital. [2] Berkembangnya teknologi informasi membuat persebaran informasi menjadi lebih mudah, cepat, dan jangkauannya pun meluas. Persebaran informasi yang cepat ini menjadikan adanya keharusnya untuk memahami jenis informasi mana yang layak dan tidak layak untuk dibagikan. Terdapat informasi yang bila tidak dibagikan secara terbuka akan

menghalangi kepentingan publik, tetapi adapun informasi yang kerahasiannya wajib dilindungi seperti data pribadi yang apabila disatukan dapat mengidentifikasi seorang individu atau dikenal juga dengan *personally identifiable information* (PII). Adapun data pribadi selain PII, yaitu data pribadi spesifik seperti data keuangan.

Bank merupakan salah satu lembaga keuangan yang dalam pemenuhan kegiatan organisasi dan nasabahnya memerlukan teknologi informasi. Sebagai pihak yang memberikan berbagai macam pelayanan keuangan, bank berkewajiban untuk menjaga kerahasiaan informasi para nasabahnya dengan tidak diungkapkan kepada siapapun tanpa seizin pemilik data. Tanggung jawab bank ini tercerminkan dalam dua prinsip penting yang diterapkan, yaitu prinsip kepercayaan (*fiduciary principle*) dan prinsip kerahasiaan (*confidential principle*). [3] Prinsip kepercayaan fidusia mengatur tentang pengalihan hak kepemilikan suatu benda atas dasar kepercayaan dengan ketentuan bahwa benda yang hak kepemilikannya dialihkan tersebut masih dalam penguasaan pemilik benda asli (Pasal 1 angka 1 UU No.42/1999 tentang jaminan Fidusia). Prinsip kerahasiaan mewajibkan bank merahasiakan segala sesuatu yang berhubungan dengan keadaan keuangan serta data pribadi milik nasabah penyimpan dana. Rahasia bank adalah segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpan dan simpanannya (Pasal 1 angka 28 UU No.10/1998 tentang perubahan atas UU No.7/1992 tentang perbankan). Dilihat dari penerapan kedua prinsip tersebut, bank telah menjalankan porsinya untuk melindungi data pribadi nasabah agar data keuangan dan dana simpanan milik nasabah tidak terungkap ke sembarang orang tanpa seizin nasabah. Perlindungan tersebut juga diwujudkan dengan pengamanan teknologi informasi melalui penerapan sistem keamanan siber yang kuat serta pemberdayaan SDM yang baik. Keamanan sistem bank yang sulit ditembus membuat pelaku kejahatan siber beralih dari eksploitasi atau pengrusakan sistem ke penggunaan teknik *social engineering* yang menargetkan nasabah bank.

Social engineering atau yang disebut pula dengan *human hacking* adalah teknik yang digunakan pelaku kejahatan siber untuk mengeksploitasi kelemahan psikologis manusia dengan harapan mendapat akses ke informasi rahasia. *Social engineering* merupakan ancaman keamanan informasi yang patut diwaspadai sebab pelaku memahami bahwa manusia adalah mata rantai terlemah dalam sistem keamanan jaringan dikarenakan kondisi psikologisnya yang dinamis dan rentan terhadap teknik manipulasi psikologis. Diberitakan oleh CNN Indonesia [4], sebanyak 2000 nasabah bank swasta tiap bulannya menjadi korban kejahatan siber dengan modus *social engineering*. *Social engineering* paling umum menargetkan nasabah perbankan, pemilik dompet digital, serta pengguna *e-commerce* dan media sosial. [5] *Social engineering* marak terjadi di tengah masyarakat Indonesia dan masih memakan banyak korban diakibatkan oleh kurangnya pengetahuan kesadaran keamanan informasi masyarakat. Disampaikan pula oleh Amirudin selaku Kaprodi Antropologi Fakultas Ilmu Budaya Universitas Diponegoro, bahwa masih adanya perbedaan tafsir setiap orang akan data yang tergolong pribadi dengan data terbuka sehingga timbul keambiguan tentang kapan suatu data bersifat pribadi atau terbuka. [6] Keambiguan ini dapat menjadi salah satu faktor keberhasilan serangan *social engineering*, di mana masyarakat dengan pemahaman yang kurang tentang keamanan data pribadi cenderung melakukan *oversharing* pada media sosialnya bahkan secara sukarela memberikan informasi pribadi ke pihak yang asal-usulnya tidak jelas.

Kurangnya pemahaman masyarakat Indonesia terkait keamanan informasi pribadinya juga dibuktikan pada tren “Add Yours” di Instagram yang sempat marak pada bulan November tahun 2021 lalu. Diberitakan oleh CNN Indonesia [7], seorang pengguna Twitter @ditamoechtar_ menceritakan pengalaman buruk temannya yang menjadi korban penipuan *online* dengan modus meminta sejumlah uang untuk ditransfer. Korban percaya terhadap pelaku sebab pelaku menggunakan panggilan “Pim” yang mana adalah panggilan kecil korban. Korban kemudian teringat bahwa dirinya sempat mengikuti *challenge* Add Yours di Instagram dengan topik “nama panggilan kecil”. Peristiwa ini ditanggapi oleh Alfons Tanujaya selaku Pakar Keamanan Siber dari Vaksin.com bahwa fitur bukan merupakan akar permasalahan, tetapi kecerobohan penggunalah yang menyebabkan maraknya kejahatan *social engineering*. Pemerintah melalui Kominfo telah melakukan usaha dalam antisipasi kejahatan penipuan *online* dengan menciptakan situs cekrekening.id. Situs tersebut dapat digunakan untuk memeriksa nomor rekening dan penyeedia dompet digital yang terindikasi dengan tindak pidana, akan tetapi situs tersebut bukanlah tempat untuk memproses pengambalian uang maupun melakukan pembekuan rekening pelaku.

Anggota Dewan Komisioner Otoritas Jasa Keuangan (OJK) Bidang Edukasi dan Perlindungan Konsumen, Friderica Widyasari Dewi, turut mengingatkan perbankan akan

pentingnya sosialisasi dan edukasi tentang modus kejahatan di era digital. *Social engineering* termasuk kejahatan di sektor perbankan yang marak terjadi di Indonesia dengan memanfaatkan kelengahan nasabah dalam menjaga data pribadi. Dewi juga berkata OJK akan terus mengacu pada prinsip kehati-hatian dalam kerangka pengawasan mikro guna melindungi nasabah, tetapi hal ini juga perlu didukung oleh nasabah yang belajar dan memahami bagaimana melakukan serangkaian pencegahan terhadap kejahatan tersebut.

Berdasarkan latar belakang di atas, penelitian ini berupaya meningkatkan pengetahuan *information security awareness* nasabah perbankan melalui edukasi bahaya *social engineering* menggunakan media belajar game edukasi Quizizz. Hasil yang diharapkan adalah edukasi dapat meningkatkan *awareness level* nasabah dan dapat mengenalkan nasabah tentang apa itu *social engineering* beserta upaya pencegahan yang tepat.

2. Metode Penelitian

Penelitian ini menggunakan metode kuantitatif bentuk *quasi experimental* dengan desain *nonequivalent control group*. Desain eksperimen diilustrasikan sebagai berikut.

Tabel 1. Desain Eksperimen

Kelompok	Pretest	Perlakuan	Posttest
Eksperimen	O_1	X	O_2
Kontrol	O_3		O_4

(Sumber: Sugiyono, 2022:122)

Keterangan

O_1 dan O_3	:	*Pretest* sebelum diberi perlakuan
X	:	Perlakuan diberikan dengan edukasi bahaya *social engineeering* menggunakan media belajar Quizizz
O_2	:	*Posttest* setelah diberikan perlakuan X
O_4	:	*Posttest* setelah tidak diberi perlakuan X

Populasi yang digunakan dalam penelitian ini adalah mahasiswa aktif dan alumni prodi Teknologi Informasi Unud angkatan 2018 sebanyak 126 orang. Sampel yang digunakan berjumlah 50 orang dan dipilih menggunakan teknik sampling kuota. Pengambilan data penelitian dilakukan menggunakan instrumen tes (*pretest-posttest*) menggunakan Google Form dan menerapkan metode *vocabulary test* [8] untuk pengukuran level kesadaran keamanan informasi yang selanjutnya disebut dengan *awareness level*. Metode *vocabulary test* terdiri dari dua bagian tes, yaitu *knowledge test* dan *behavior test*. Pembuatan instrumen tes menyesuaikan metode tersebut. Instrumen tes kemudian diujicobakan terlebih dahulu untuk menguji validitas dan reliabilitasnya.

2.1 Uji Validitas

Uji validitas dilakukan untuk menentukan apakah instrumen bersifat valid (sah) dan dapat digunakan sebagai alat ukur dalam penelitian. [9] Pada instrumen tes, validitasnya diuji dengan validitas isi dan validitas konstruk. Validitas isi dilakukan dengan menyelaraskan isi instrumen dengan materi yang diajarkan, sedangkan validitas konstruk dilakukan dengan analisis faktor menggunakan aplikasi SPSS 26 untuk mencari korelasi antar item dengan skor totalnya. [9] Butir instrumen untuk N = 20 dan taraf signifikansi 5% dapat dikatakan valid jika nilai $r_{hitung} > 0{,}444$. Hasil uji coba validitas instrumen adalah sebagai berikut.

Tabel 2. Hasil Uji Validitas

Jenis Tes	Butir Soal	Keterangan
Knowledge	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20	Valid
Behavior	24, 25, 26, 27, 29	Valid
	21, 22, 23, 28, 30	Tidak Valid

Hasil uji menunjukkan 20 soal *knowledge test* sudah valid, tetapi 5 dari 10 soal *behavior test* tidak valid. Sebanyak 25 soal tes kemudian digunakan sebagai soal *pretest* dan *posttest*.

2.2 Uji Reliabilitas

Uji reliabilitas dilakukan untuk menentukan apakah bersifat reliabel (handal) yang berarti instrumen dapat memberikan hasil yang konsisten meski digunakan berulang kali untuk mengukur objek yang sama di waktu dan dengan subjek penelitian yang berbeda. [9] Uji reliabilitas dilakukan menggunakan aplikasi SPSS 26 terhadap butir instrumen yang telah teruji validitasnya. Instrumen penelitian dikatakan reliabel apabila nilai Cronbach Alpha hitung > 0,60. Hasil uji reliabilitas instrumen tes adalah sebagai berikut.

Tabel 3. Hasil Uji Reliabilitas

Cronbach Alpha Hitung	Keterangan
0,901	Instrumen Reliabel

Hasil uji reliabilitas menunjukkan instrumen tes teruji bersifat reliabel dengan nilai Cronbach Alpha hitung sebesar 0,901 dan dapat digunakan untuk pengambilan data penelitian.

3. Tinjauan Pustaka

3.1 Penelitian Sebelumnya

Penelitian oleh [10] membahas dampak *social engineering* pada lembaga perbankan. Terdapat empat kelompok atau individu yang diincar pelaku *social engineer* dalam perbankan, yaitu resepsionis, IT *support*, administrator, mitra kerja atau vendor, dan karyawan baru. *Social engineering* sendiri mengincar informasi seperti *username* dan *password*, data pegawai dan nasabah, strategi bisnis, laporan perusahaan, kebijakan internal, hingga dokumen rahasia.

Ancaman *social engineering* yang menargetkan organisasi lain dijelaskan pada [11] yang membahas ancaman *social engineering* dalam organisasi kesehatan. Pada penelitiannya dikatakan serangan *social engineering* tidak akan berhasil kecuali korban menunjukkan ciri-ciri kerentanan yang dibutuhkan pelaku. Wanita dikatakan lebih rentan terhadap serangan *social engineering* daripada pria. Menurut [12] dalam [11], sifat-sifat seperti suka bicara (*talkative*), komunikatif (*conversational*), terbuka (*open*), dan ramah (*positive*) berpotensi membuat seseorang menjadi sasaran *social engineering*. Akhirnya dapat disimpulkan bahwa keamanan informasi secara teknis saja tidak cukup untuk mencegah serangan *social engineering* sehingga dibutuhkan edukasi *awareness* kepada nasabah untuk perbankan atau kepada kolega, karyawan, dan pasien untuk organisasi kesehatan.

Penggunaan pendekatan game untuk edukasi bahaya *social engineering* pernah dilakukan oleh [13] yang membandingkan pendekatan game dengan pendekatan *paper-based* untuk penyampaian edukasi bahaya *social engineering*. Penelitian ini menciptakan prototipe *social engineering awareness game* (SEAG) menggunakan Construct2, sebuah *software* pengembangan game *open source*. Hasil penelitian menyatakan pendekatan game untuk penyampaian materi yang kompleks seperti *social engineering* dinilai lebih efektif daripada pendekatan *paper-based* ditandai dengan peningkatan pengetahuan partisipan sebesar 71% dibandingkan sebelum partisipan memainkan game edukasi.

Penelitian oleh [14] membahas efektivitas pemanfaatan media belajar Quizizz terhadap peningkatan nilai siswa kelas X SMK Ketintang Surabaya pada mata pelajaran Teknologi Perkantoran. Penelitian ini menggunakan metode kuantitatif eksperimen dan membandingkan dua metode belajar yang diterapkan sebagai perlakuan, yaitu media papan tulis dan penugasan untuk kelompok kontrol dan media belajar game edukasi Quizizz untuk kelompok eksperimen. Hasil penelitian menyatakan bahwa penggunaan media belajar Quizizz untuk mata pelajaran Teknologi Perkantoran pada kelas X OTKP SMK Ketintang Surabaya berhasil meningkatkan hasil belajar siswa dengan rata-rata hasil *posttest* sebesar 85,3 dibandingkan media papan tulis yang memperoleh rata-rata hasil *posttest* sebesar 80,7, serta memperoleh taraf signifikansi Sig. (*2-tailed*) 0,036 pada uji *independent sample t-test* yang berarti terdapat perbedaan signifikan pada rata-rata *posttest* kelompok eksperimen dan kelompok kontrol.

3.2 Data Pribadi

Menurut UU PDP No. 27 Tahun 2022 data pribadi dibagi menjadi data pribadi spesifik dan data pribadi umum. Data pribadi spesifik mencakup data dan informasi kesehatan, data

biometrik, data genetika, catatan keuangan, data anak, data keuangan pribadi, dan/atau data lainnya sesuai dengan ketentuan peraturan perundang-undangan. Data pribadi umum mencakup nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan/atau data lainnya sesuai dengan ketentuan peraturan perundang-undangan. Data pribadi spesifik memiliki dampak yang lebih besar terhadap subjek data pribadi karena dapat menimbulkan tindakan diskriminasi dan kerugian besar lainnya apabila diungkapkan kepada selain pemilik data pribadi.

3.3 Keamanan Informasi

Pentingnya informasi melahirkan istilah "keamanan informasi" berupa sekumpulan metodologi, praktik, atau proses yang dirancang dan diterapkan untuk melindungi data atau informasi pribadi dari akses, penggunaan, penyalahgunaan, atau modifikasi yang tidak sah. Keamanan informasi bertujuan untuk melindungi data dalam proses penyimpanan, transfer, atau penggunaan informasi. Keamanan informasi berfokus dan merujuk pada aspek CIA *triad*, yaitu *confidentiality*, *integrity*, dan *availability*. [15] *Confidientality* (kerahasiaan) yang berarti informasi hanya dapat diakses oleh individu yang berwenang. *Integrity* (integritas) yang berarti informasi tidak dapat diubah tanpa seizin pemilik informasi. *Availability* (ketersediaan) yang berarti informasi selalu tersedia ketika dibutuhkan.

Beberapa metodologi pengamanan informasi adalah dengan menerapkan manajemen risiko seperti yang dilakukan oleh [16] sebagai proses pelaksanaan kegiatan manajemen untuk mengatasi timbulnya risiko, baik yang dihadapi perusahaan ataupun dihadapi masyarakat. Pengamanan informasi dapat pula dilakukan dengan menerapkan teknologi *blockchain* dalam transaksi keuangan *online* yang dilakukan dalam penelitian oleh [17]. Keamanan informasi juga didukung melalui pemberdayaan sumber daya manusia dan perangkat teknologi informasi, karena itu pemberlakuan audit keamanan teknologi informasi pada lembaga atau perusahaan menjadi hal yang wajib dilakukan secara berkala seperti yang diteliti oleh [18] dan [19]. Keandalan metode pengamanan informasi pada suatu organisasi maupun institusi dapat diujicobakan dengan melakukan *penetration testing* seperti yang dilakukan oleh [20]. Melalui *penetration testing* dapat diketahui seberapa andal pengamanan informasi yang telah diterapkan, di samping itu juga dapat menilai kerentanan sistem untuk diberikan rekomendasi perbaikan yang dapat diterapkan nantinya.

3.4 Kesadaran Keamanan Informasi

Sementara keamanan informasi berfokus pada CIA *triad* (*confidentiality*, *integrity*, dan *availability*), kesadaran keamanan informasi atau yang selanjutnya disebut ISA menurut ISF (2003) dalam [21] didefinisikan sebagai tingkat atau sejauh mana seseorang memahami pentingnya keamanan informasi, tingkat suatu keamanan informasi, tanggung jawab keamanan individu, dan apakah mereka sudah bertindak dengan sesuai. Oleh [22] juga mendefinisikan ISA sebagai tingkat pengetahuan akan pentingnya keamanan informasi dan sejauh mana pemahaman seseorang akan tanggung jawabnya terhadap keamanan informasi.

Kesadaran keamanan informasi dapat diukur dari pengetahuan (*knowledge*), sikap (*attitude*), dan perilaku (*behavior*). [21] Peningkatan ISA bertujuan untuk membuat perubahan positif agar pengguna tersadar akan risiko yang sedang dihadapi dan mengetahui upaya pencegahan yang tepat sehingga dapat mengontrol keamanan informasi guna melindungi data dan jaringan dalam organisasi. [22] Menurut Kruger, ISA dibagi menjadi tiga tingkatan sebagai berikut.

Tabel 4. Kriteria *Awareness Level*

Awareness	Measurement (%)
Good	80 – 100
Average	60 – 79
Poor	59 and less

(Sumber: Kruger, 2010)

Tingkat ISA yang *good* (baik) memiliki persentase 80% – 100%, tingkat *average* (rata-rata) memiliki persentase 60% – 79%, dan tingkat yang *poor* (buruk) memiliki persentase 59% ke bawah.

3.5 Social Engineering

3.5.1 Pengertian Social Engineering

Menurut [23], *social engineering* merupakan teknik peretasan yang menargetkan manusia dalam suatu sistem dengan mengeksploitasi kelemahan psikologisnya untuk mendapatkan informasi. Tujuan *social engineering* sama dengan peretasan pada umumnya, yaitu memperoleh akses tidak sah ke sistem untuk melakukan *fraud*, pencurian, pengubahan atau pengrusakan sistem, atau sekadar menimbulkan gangguan. Dilihat dari bagaimana *social engineering* hendak mengekstrak informasi dari manusia, teknik ini dapat disebut sebagai *human hacking*. Lembaga keuangan beserta nasabahnya menjadi salah satu sasaran khas *social engineering*. [24]

Menurut [25] kategori *social engineering* ada dua, yaitu *technology-based deception* dan *human-based deception* yang kemudian disebut dengan pendekatan sosio-teknikal dan pendekatan sosial. Serangan *social engineering* memanfaatkan dua aspek, yaitu *sensory level* dan *psychologial level*. *Sensory level* berhubungan dengan lingkungan yang rawan terhadap serangan *social engineering*, seperti tempat kerja, tempat pembuangan dokumen atau perangkat penting, dan internet. *Psychological level* mengacu pada kondisi psikologis tertentu yang dapat dimanfaatkan pelaku untuk mengelabui korban.

3.5.2 Penyebab dan Tahapan Soceng

Salah satu alasan dipilihnya teknik *social engineering* untuk meretas sistem adalah selain karena tekniknya memerlukan biaya sedikit, risiko rendah, tetapi potensi kesuksesannya bisa sangat tinggi [23], pelaku mengetahu manusia merupakan komponen terlemah dalam sistem keamanan jaringan karena memiliki kondisi psikologis yang dinamis sehingga rentan terhadap teknik manipulasi. Andress dalam bukunya [26] merumuskan komponen utama keamanan informasi dengan manusia ditempatkan di prioritas kedua setelah proses dan sebelum teknologi.

Keberhasilan serangan *social engineering* disebabkan oleh beberapa faktor pendukung. Wawancara yang dilakukan oleh Hadnagy membahas mengenai mode *alpha* dan *beta* pada otak yang mempengaruhi proses pengambilan keputusan pada manusia. Mode *alpha* merupakan keadaan otak yang ditandai dengan sifat *daydreaming*, santai, dan fokus terputas. Mode ini setara dengan kemampuan *automatic processing*, yaitu kemampuan otak untuk mengabaikan informasi berlebih terutama pada hal yang dianggap familier. Mode inilah yang dimanfaatkan pelaku *social engineering* karena korban umumnya sedang tidak dalam kondisi waspada dan cenderung berpikir atau bertindak spontan. Berpikir secara irasional yang didasarkan pada emosi dan perasaan jugalah hal yang dimanfaatkan oleh pelaku. Sebaliknya, mode *beta* adalah keadaan otak yang ditandai dengan sifat waspada, penglihatan tajam, dan kritis akan segala hal yang terjadi di sekitarnya. Pelaku *social engineering* sangat bergantung pada mode *alpha* sebab dalam keadaan otak ini korban lebih mungkin untuk membuat keputusan secara spontan.

A. Tahapan Social Engineering

1. Research (Pengumpulan Informasi)

Tahap *research* digunakan untuk mengumpulkan informasi sebanyak mungkin terkait apa yang ingin pelaku peroleh dari korban. [23] Pengumpulan informasi dilakukan dengan melakukan riset pada korban, seperti mencari tahu struktur organisasi, mengumpulkan daftar nama orang dalam, atau informasi tambahan lainnya yang mendukung. [10] Pada tahap ini pelaku menentukan tujuan apa yang hendak dicapai, target seperti apa yang diinginkan, dan bagaimana cara terbaik untuk mencapai tujuan tersebut.

2. Pengembangan Pretext dan Relasi

Setelah memperoleh cukup informasi dan tujuan telah ditetapkan, selanjutnya pengembangan *pretext* dan relasi. [23] *Pretext* merupakan skenario atau situasi yang dibuat-buat oleh pelaku agar terkesan meyakinkan jika pelaku berhak atas informasi rahasia yang diminta. *Pretext* dilakukan dengan pendekatan impersonasi atau penyamaran/peniruan untuk mengelabui korban dengan identitas baru. Langkah berikutnya setelah *pretext* ditentukan adalah pemilihan target yang ingin dikenai serangan dengan mengidentifikasi mata rantai terlemah dalam sistem keamanan.

Target yang telah ditentukan akan selanjutnya dihubungi dan pelaku mulai mengembangkan relasi dengan calon korban. Pengembangan relasi bertujuan untuk memperoleh kepercayaan korban agar tidak menaruh curiga terhadap pelaku. Sering kali pelaku menggunakan skenario dengan melaporkan hal mendesak untuk membuat korban merasa syok dan khawatir.

3. Eksploitasi

Korban yang psikologisnya dalam pengaruh manipulasi akan dieksploitasi oleh pelaku dengan diberikan perintah untuk memberikan informasi rahasia miliknya. Informasi rahasia yang umumnya diminta pelaku dari nasabah perbankan adalah nomor kartu kredit atau debit, nomor PIN, nomor CVV atau CVV, hingga tanggal kadaluwarsa kartu. Pada kasus yang bersangkutan dengan *e-wallet*, pelaku akan meminta kode *one-time password* (OTP). [10]

4. Eksekusi

Tahap terakhir setelah seluruh informasi rahasia yang dibutuhkan terkumpul, pelaku akan memutus interaksi dengan korban untuk menjalankan aksinya. Eksekusi dilakukan dengan mencuri, melakukan transaksi tidak sah, hingga mengubah atau merusak sistem beserta data yang tersimpan di dalamnya. Setelah tahap ini pelaku biasanya sulit untuk dilacak. [24]

3.5.3 Jenis-jenis Social Engineering

Terdapat berbagai jenis serangan *social engineering* yang digunakan menyesuaikan skenario buatan pelaku. Jenis-jenis serangna *social engineering* berdasarkan kategorinya adalah sebagai berikut.

A. Pendekatan Sosio-Teknikal

Pendekatan sosio-teknikal adalah jenis serangan yang menggabungkan unsur teknikal dan sosial. Jenis serangan dari kategori ini umumnya sering dijumpai secara digital.

***Phishing*:** Jenis serangan yang menggunakan tautan berbahaya dan umumnya dikirim melalui *email*, tetapi dapat dijumpai pula di pesan teks dan media sosial. Tautan berbahaya yang dikirim pelaku akan mengarahkan korban ke situs palsu yang terlihat meyakinkan lalu korban diminta untuk mengisi form halaman *login* palsu dengan data pribadi miliknya. Tujuan utama serangan ini adalah untuk mencuri data pribadi korban.

***Spear phishing*:** Mirip dengan *phishing*, *spear phishing* juga merupakan serangan yang menggunakan tautan berbahaya yang dikirimkan melalui *email*, pesan teks, dan media sosial untuk mencuri data pribadi korban. Perbedaannya terletak pada target *spear phishing* yang telah ditentukan secara spesifik, sedangkan *phishing* masih menargetkan korban secara acak (*random*). Terdapat dua jenis *spear phishing*: 1) *Whaling*, yaitu serangan yang menargetkan eksekutif perusahaan, dan 2) CEO *Fraud*, yaitu serangan di mana pelaku berpura-pura menjadi eksekutif perusahaan.

***Baiting*:** Jenis serangan yang menggunakan umpan (*bait*) untuk menarik korban ke dalam jebakan yang dapat mencuri informasi rahasia hingga menginfeksi perangkat dengan *malware*. Umpan yang digunakan bisa berbentuk fisik, misalnya USB *drive* yang terkontaminasi *malware* digeletakkan sembarangan menunggu untuk diakses oleh calon korban yang pensaran, dan umpan bentuk digital, misalnya saat korban ingin mengunduh suatu file dari internet, korban diminta untuk mengizinkan permintaan izin akses ke perangkat.

***Watering hole*:** Meskipun jarang dijumpai dalam kasus umum, *watering hole* merupakan jenis serangan yang sangat berbahaya. Pelaku menentukan target dan mengidentifikasi satu atau lebih situs web sambil mencari kerentanannya. Pelaku kemudian menginfeksi situs web yang peluang keberhasilan serangnnya paling tinggi. Pelaku juga dapat membuat situs klon untuk mengelabui korban. Dikarenakan kompleksitasnya, sernagan ini menjadi salah satu yang membutuhkan kehalian teknis dan observasi tinggi.

B. Pendekatan Sosial

Pendekatan sosial adalah jenis serangan yang melibatkan interaksi langsung dengan korban. Datang ke lokasi sasaran, bertemu tatap muka, atau menghubungi via telepon masuk dalam kategori pendekatan sosial.

Impersonation**:** *Impersonation* atau peniruan adalah teknik dasar yang digunakan pelaku *social engineering* agar tidak terlihat mencurigakan. Pelaku dapat menyamar sebagai pihak berwajib, petugas, hingga sebagai orang biasa yang perlu bantuan. *Impersonation* merupakan terapan dari prinsip dasar *social engineering*, yaitu untuk tampil sebagai *non-hacker* yang berhak atas informasi rahasia.

Vishing**:** *Vishing* atau *voice phishing* adalah jenis serangan yang dilakukan melalui panggilan telepon dan sering dikenali sebagai *fake call*. Pelaku ingin mengeksploitasi emosi korban dengan melaporkan hal mendesak atau memberikan kabar baik, lalu saat korban sedang dalam pengaruh manipulasi pelaku akan meminta korban untuk memberikan data pribadinya.

Shoulder surfing**:** Jenis serangan yang dilakukan dengan mengintip atau pengamatan langsung terhadap korban untuk mengetahui informasi rahasia. [safitri] Serangan ini dilakukan untuk mencari tahu data otentikasi seperti PIN, *password*, pola, atau jenis data otentikasi lainnya.

Eavesdropping**:** *Eavesdropping* pada pendekatan sosial dilakukan secara langsung di mana pelaku hadir secara fisik di tempat calon korban berada, misalnya di lingkungan perkantoran. Individu atau kelompok dapat berperilaku ceroboh dengan membicarakan informasi rahasia di tempat umum hingga di dalam perusahaan, maka pada tempat dan waktu yang tepat pelaku dapat mengeksploitasi kesalahan ini.

Reverse social engineering **(RSE):** Jenis serangan yang bertujuan membuat calon korban meminta tolong pelaku untuk menyelesaikan suatu masalah. Serangan ini membutuhkan persiapan dan *pre-hacking* cukup banyak, misalnya melakukan kerusakan pada sistem atau perangkat calon korban, kemudian menawarkan jasanya dengan berpura-pura menjadi teknisi atau membiarkan calon korban datang sendiri kepadanya.

Tailgating**:** Tindakan membuntuti (*tailgate*) seseorang yang memiliki akses sah melewati pihak keamanan agar pelaku dapat masuk ke area terbatas tanpa menimbulkan kecurigaan. Pelaku dapat menyamar sebagai orang yang berkepentingan atau hendak mengantarkan barang ke perkantoran lalu meminta dipinjamkan akses menuju area terbatas.

Dumpster diving**:** Tindakan mengacak-acak tong sampah untuk mencari sampah dokumen atau peralatan yang belum dihancurkan dan berpotensi memuat informasi penting. Sampah-sampah yang diincar dapat berupa *printout* data-data penting, *printout source code*, manual sistem, memo, jadwal kegiatan atau pertemuan, hingga perangkat keras usang. [10] Sampah-sampah rumahan juga dapat mengandung informasi pribadi, seperti sampah bungkus paket yang tidak dirusak dan masih memperlihatkan data pribadi penerima paket (nama, nomor telepon, alamat).

3.6 Game Edukasi Quizizz

Quizizz merupakan aplikasi pendidikan berbasis game yang diciptakan oleh Ankit Gupta dan Deepak Joy Cheenath di Bengaluru, India pada tahun 2015. Pada Desember 2020, Quizizz telah mencapai sebanyak 65 juta pengguna aktif. Quizizz membawa aktivitas multi pemain ke ruang kelas sehingga aktivitas belajar menjadi lebih interaktif dan menyenangkan. [27]

Quizizz sebagai aplikasi pendidikan berbasis game memiliki beberapa fitur unggulan yaitu pelajaran (*lessons*), kuis (*quiz*), ruang kelas (*classroom*), dan laporan (*report*). Quizizz tersedia dalam bentuk aplikasi web *desktop* maupun *mobile* dan tersedia pula dalam bentuk aplikasi yang dapat diunduh ke perangkat Android maupun iOS.

4. Hasil

4.1 Pelaksanaan Penelitian

Kegiatan penelitian dilaksanakan bertempatan di Zodiac XII Coffee & Eatery, Renon pada tanggal 14 Mei 2023 untuk pertemuan kelompok kontrol dan 15 Mei 2023 untuk pertemuan kelompok eksperimen.

Urutan kegiatan pada pertemuan dengan tiap kelompok dimulai dengan pengerjaan *pretest* menggunakan Google Form selama 25 menit untuk mengukur kemampuan awal partisipan sebelum diberikan perlakuan. Tahap berikutnya setelah *pretest* dilanjutkan dengan sesi belajar mandiri menggunakan *textbook* untuk kelompok kontrol dan game edukasi Quizizz untuk kelompok eksperimen. Kegiatan penelitian kemudian diakhiri dengan pengerjaan *posttest* menggunakan Google Form selama 25 menit.

4.2 Analisis Hasil Belajar

Hasil tes diuji menggunakan uji normalitas, uji homogenitas, dan uji t terhadap *gain score*. Uji normalitas dilakukan terhadap data hasil tes dan data *gain score* menggunakan aplikasi SPSS 26 dan mendapatkan hasil sebagai berikut.

Tabel 5. Hasil Uji Normalitas Hasil Tes

Kelompok	*Kolmogorov-Smirnov*		Keterangan
	Pretest	***Posttest***	
Kontrol	0,200	0,079	Normal
Eksperimen	0,200	0,200	Normal

Tabel 6. Hasil Uji Normalitas *Gain Score*

Data	*Kolmogorov-Smirnov*	Keterangan
Gain Kontrol	0,173	Normal
Gain Eksperimen	0,078	Normal

Hasil taraf signifikansi (Sig.) uji normalitas terahdap data *pretest* dan *posttest* kelompok kontrol adalah 0,200 dan 0,079. Hasil taraf signifikansi (Sig.) untuk *pretest* dan *posttest* kelompok eksperimen adalah 0,200. Hasil taraf signifikansi (Sig.) uji normalitas terhadap data *gain score* kelompok kontrol adalah 0,173 dan 0,078 untuk *gain score* kelompok eksperimen. Hasil taraf signifikansi > 5% (0,05) menandakan bahwa data tes dan data *gain score* kedua kelompok telah teruji berdistribusi normal. Uji homogenitas dilakukan terhadap data *gain score* kedua kelompok menggunakan aplikasi SPSS 26 dan memperoleh taraf signifikansi (Sig.) 0,023 < 0,05 yang berarti varians data *gain score* kedua kelompok teruji tidak bersifat homogen.

Analisis hasil dimulai dengan melakukan uji *paired sample t-test* pada data hasil tes masing-masing kelompok. Hasil uji *paired sampe t-test* adalah sebagai berikut.

Tabel 7. Hasil Uji *Paired Sample T-test*

Paired Sample		N	Mean Tes	Sig. (2-*tailed*)
Pair 1	Pre Kontrol	25	33	0,000
	Post Kontrol	25	63,2	
Pair 2	Pre Eksperimen	25	22,3	0,000
	Post Eksperimen	25	66,8	

Hasil *paired sample t-test* untuk sampel berpasangan kelompok kontrol (*Pair* 1) dengan N = 25 memperoleh nilai taraf signifikansi Sig. (*2-tailed*) = 0,000 dan hasil uji untuk sampel berpasangan kelompok eksperimen (*Pair* 2) dengan N = 25 memperoleh nilai taraf signifikansi Sig. (*2-tailed*) = 0,000. Taraf signifikansi Sig. (*2-tailed*) < 0,05 berarti bahwa terdapat perbedaan rata-rata yang signifikan antara *pretest* dan *posttest* baik pada kelompok kontrol maupun kelompok eksperimen. Hal ini berarti kedua kelompok terbukti memiliki perbedaan nilai yang signifikan antara *pretest* sebelum menerima edukasi bahaya *social engineering* dan *posttest* setelah menerima edukasi bahaya *social engineering*.

Analisis hasil tes dilanjutkan dengan mengujikan *gain score* antar kelompok dengan uji *independent sample t-test*. Hasil uji tersebut ditunjukkan sebagai berikut.

Tabel 8. Hasil Uji *Independent Sample T-test*

Kelompok	N	Mean *Gain Score*	Sig. (2-*tailed*)
Kontrol	25	30,2	0,001
Eksperimen	25	44,5	

Pada keluaran SPSS 26 dikarenakan varians data *gain score* tidak bersifat homogen maka hasil uji yang dibaca adalah *equal varians not assumed*. Hasil uji *independent sample t-test* terhadap rata-rata *gain score* kedua kelompok memperoleh nilai taraf signifikansi Sig. (*2-tailed*) = 0,001 < 0,05 yang menandakan terdapat perbedaan yang signifikan antara rata-rata *gain score* kelompok eksperimen dan kelompok kontrol. Hal ini berarti pemanfaatan media belajar Quizizz untuk edukasi bahaya *social engineering* efektif membantu kelompok eksperimen memperoleh peningkatan hasil belajar yang signifikan.

Peningkatan *awareness level* sebelum dan sesudah edukasi bahaya *social engineering* ditampilkan sebagai berikut menggunakan tingkat ISA yang dirumuskan oleh Kruger.

Tabel 9. Peningkatan *Awareness Level* Kelompok Kontrol

Kelompok Kontrol	K	B	Mean	Awareness Level
	100	100	100	
Pretest	41,2	24,8	33	*Poor*
Posttest	74,4	52	63,2	*Average*

Kelompok kontrol memperoleh ketuntasan *knowledge test* 41,2%, ketuntasan *behavior test* 24,8%, dan rata-rata ketuntasan 33% pada *pretest* (sebelum edukasi) kemudian memperoleh ketuntasan *knowledge test* 74,4%, ketuntasan *behavior test* 52%, dan rata-rata ketuntasan 63,2% pada *posttest* (setelah edukasi). Hasil kelompok eksperimen ditunjukkan sebagai berikut.

Tabel 10. Peningkatan *Awareness Level* Kelompok Eksperimen

Kelompok Kontrol	K	B	Mean	Awareness Level
	100	100	100	
Pretest	28,6	16	22,3	*Poor*
Posttest	75,2	58,4	66,8	*Average*

Kelompok eksperimen memperoleh ketuntasan *knowledge test* 28,6%, ketuntasan *behavior test* 16%, dan rata-rata ketuntasan 22,3% pada *pretest* (sebelum edukasi) kemudian memperoleh ketuntasan *knowledge test* 75,2%, ketuntasan *behavior test* 58,4%, dan rata-rata ketuntasan 66,8% pada *posttest* (setelah edukasi). Berdasarkan hasil di atas, *gain score* kelompok kontrol untuk aspek *knowledge* sebesar 74,4 – 41,2 = 33,2 poin, sedangkan untuk kelompok eksperimen sebesar 75,2 – 28,6 = 46,6 poin. *Gain score* kelompok kontrol untuk aspek *behavior* sebesar 52 – 24,8 = 27,2 poin, sedangkan untuk kelompok eksperimen sebesar 58,4 – 16 = 42,4 poin. Hasil tersebut menunjukkan bahwa kelompok eksprimen yang melakukan pembelajaran dengan game edukasi Quizizz mengalami peningkatan persentase rata-rata ketuntasan ISA lebih tinggi dibandingkan dengan kelompok kontrol yang melakukan pembelajaran dengan *textbook*.

4.3 Pembahasan

Pada peningkatan *awareness level* dapat dilihat bahwa aspek *knowledge* mengalami peningkatan cukup tinggi jika dibandingkan dengan aspek *behavior*. Hal ini dapat mengacu pada teori kognitif yang mendasari metode *vocabulary test* [8] di mana *knowledge* memiliki kognitif tindakan di antaranya mengingat dan mengenali. Hal ini berarti pengetahuan erat kaitannya dengan pikiran, oleh karena itu peningkatan *knowledge* yang cukup tinggi tersebut diprediksi karena pengetahuan yang dipelajari dapat diingat dan dikenali dengan lebih cepat. Aspek *behavior* memiliki kognitif tindakan di antaranya menganalisis dan memecahkan masalah yang mana hal ini memiliki bobot lebih berat daripada *knowledge* karena saat menjawab *behavior test* terdapat proses timbang-menimbang terkait mana tindakan yang benar, bisa diterima, hingga salah. Dikarenakan perilaku merupakan sesuatu yang dibentuk, terdapat intervensi dengan beberapa pengaruh lainnya seperti pengetahuan dan kebiasaan lama yang sudah menempel pada keseharian sehingga berimbas pada peningkatan *behavior* yang kurang baik. Menurut [28] perilaku terbentuk karena kebiasaan dan [29] menyatakan bahwa berapa lama waktu untuk membentuk kebiasaan baru bisa sangat bervariasi tergantung pada perilaku, individu, dan keadaan. Berdasarkan pembahasan tersebut, aspek *behavior* yang mengalami peningkatan tidak sebaik aspek *knowledge* diprediksi karena pembentukan *behavior* memerlukan latihan yang tidak hanya sekali dan perlu dipraktikkan sampai terbentuk kebiasaan yang baru.

Penelitian yang telah dilakukan dengan kedua kelompok penelitian menunjukkan hasil bahwa kelompok eksperimen yang melakukan pembelajaran dengan Quizizz mengalami peningkatan hasil belajar yang signifikan dengan hasil *independent t-test* memperoleh taraf signifikansi Sig. (*2-tailed*) 0,001. Peningkatan hasil belajar yang signifikan oleh kelompok eksperimen yang menggunakan pendekatan game edukasi didukung pula dengan hasil penelitian [14] yang menunjukkan bahwa terdapat perbedaan signifikan antara *gain score* kelompok eksperimen yang menggunakan media belajar Quizizz dan *gain score* kelompok

kontrol yang menggunakan media papan tulis dan penugasan dengan hasil *independent t-test* menunjukkan taraf signifikansi Sig. (*2-tailed*) 0,002. Hasil penelitian oleh [13] menunjukkan pula bahwa pendekatan SEAG untuk menyalurkan materi jauh lebih efektif daripada pendekatan *paper-based* ditandai dengan rata-rata peningkatan *awareness* mencapai 71%. Mengacu pada kedua hasil penelitian tersebut maka dapat dikatakan media belajar berbasis game edukasi seperti Quizizz dapat secara nyata membantu kelompok eksperimen memperoleh peningkatan hasil belajar yang signifikan.

Pada penelitian ini, penggunaan game edukasi Quizizz memperoleh hasil taraf signifikansi Sig. (*2-tailed*) 0,001 yang berarti hasil penelitian sedikit lebih signifikan dari [14] serta rata-rata persentase peningkatan *awareness level* kelompok eksperimen mencapai 119,552% yang berarti juga sudah melampaui [13]. Berkaitan dengan perolehan hasil yang tinggi tersebut diprediksi karena penggunaan populasi nasabah perbankan yang hanya berasal dari mahasiswa TI Unud angkatan 2018. Metode ini apabila diterapkan ke populasi yang lebih luas atau masyarakat umum yang tidak dapat sepenuhnya dikondisikan untuk mempelajari sesuatu secara detail akan sangat mungkin memberikan hasil yang berbeda. Berdasarkan analisis tersebut dapat disimpulkan bahwa: 1) Quizizz dapat menjadi alternatif media belajar yang lebih ideal dan menyenangkan untuk pemberian edukasi bahaya *social engineering* kepada masyarakat umum karena sifatnya yang lebih praktis, dan 2) hasil penelitian ini sangat dipengaruhi oleh pemilihan populasi dan sampel nasabah perbankan yang hanya terbatas pada mahasiswa TI Unud angkatan 2018. Oleh karena itu pada penelitian yang akan datang dapat mencoba menggunakan populasi yang lebih beragam agar hasil penelitian dapat lebih komprehensif.

4.4 Rekomendasi

Penelitian tugas akhir ini telah mengujicobakan game edukasi Quizizz sebagai media pembelajaran untuk edukasi bahaya *social engineering* dan telah menunjukkan peningkatan hasil belajar yang signifikan, akan tetapi *awareness level* yang dicapai kelompok eksperimen masih belum maksimal. Aspek *knowledge* masih memperoleh persentase ketuntasan sebesar 75,2% (*average*) dan aspek *behavior* sebesar 58,4% (*poor*). Hal ini berarti dari kedua aspek belum ada yang mencapai level *good* (80%-100%) sehingga diperlukannya beberapa rekomendasi untuk meningkatkan *awareness level*.

4.4.1 Peningkatan Aspek *Knowledge* dan *Behavior*

Peningkatan aspek *knowledge* dapat dilakukan dengan proaktif mencari arti dari istilah terkait keamanan informasi yang baru ditemui. Hal ini seperti yang dikemukakan oleh [8] bahwa mendengar atau mempelajari konsep atau istilah baru adalah sama halnya dengan mempelajari pengetahuan baru. Rekomendasi pertama untuk peningkatan aspek *behavior* adalah dengan menganalisis lebih lanjut terhadap konsekuensi dari macam-macam tindakan yang dipilih saat menjawab pertanyaan skenario dalam *behavior test*. Analisis ini dapat menambah wawasan partisipan terkait mengapa tindakan tersebut tergolong benar, masih bisa diterima, atau bahkan salah. Rekomendasi berikutnya adalah melakukan pembiasaan perilaku baru yang dapat dimulai dengan memeriksa dan mengurangi informasi pribadi yang terpampang di media sosial, mulai mengurangi membagikan atau menceritakan hal-hal personal ke internet, menyimpan dengan baik berkas atau dokumen pribadi, dan perilaku sesuai lainnya.

4.4.2 Penyempurnaan Penelitian

Terkait dengan rekomendasi untuk peningkatan ISA melalui penyempurnaan penelitian yang dapat dilakukan pertama adalah pengembangan media belajar yang lebih mendalam. Hal tersebut dapat diwujudkan dengan meningkatkan level interaktivitas permainan dan memperbanyak bahasan terkait skenario sebagai tambahan bahan ajar aspek *behavior*. Rekomendasi berikutnya ditujukan terhadap proses belajar yang dilakukan. Adapun rekomendasi untuk proses belajar adalah menambah lama waktu belajar dan meningkatkan keterlibatan aktif partisipan selama proses belajar. Penambahan waktu belajar dapat membantu partisipan menjalani proses belajar dengan lebih santai sehingga berpengaruh pada tingkat konsentrasi, sementara keterlibatan aktif dapat membuka sesi tanya jawab atau diskusi agar partisipan dapat lebih memahami permasalahan dan menemukan jawaban untuk kesulitan yang dihadapi.

5. Kesimpulan

Terdapat peningkatan *awareness level* dari *poor* menjadi *average* pada kelompok kontrol maupun kelompok eksperimen setelah diberikan edukasi bahaya *social engineering*. Ketuntasan *knowledge test* masih berada di level *average*, sedangkan ketuntasan *behavior test* masih berada di level *poor*. Pemaksimalan capaian *awareness level* dapat menerapkan rekomendasi yang telah disusun khusus untuk peningkatan aspek *knowledge* dan aspek *behavior*, serta dalam rangka penyempurnaan penelitian selanjutnya.

Penggunaan media belajar Quizizz untuk edukasi bahaya *social engineering* dapat secara efektif meningkatkan hasil belajar kelompok eksperimen. Hasil ini ditunjukkan secara deskriptif pada perolehan *gain score* kelompok eksperimen yang lebih tinggi dibandingkan *gain score* kelompok kontrol, serta didukung dengan hasil uji *independent sample t-test* yang menyatakan bahwa terdapat perbedaan signifikan antara rata-rata *gain score* kelompok eksperimen yang menggunakan Quizizz dan rata-rata *gain score* kelompok kontrol yang tidak menggunakan Quizizz. Perolehan hasil penelitian tersebut dapat disebabkan oleh pemilihan populasi penelitian yang terbatas hanya pada mahasiswa dan alumni TI Unud angkatan 2018 sehingga hasil penelitian ini bisa saja ditentukan oleh hal tersebut.

Referensi

[1] A. A. B. A. Wiradarma and G. M. A. Sasmita, “IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study: X Company),” *International Journal of Computer Network and Information Security*, vol. 11, no. 12, pp. 17–29, Dec. 2019, doi: 10.5815/ijcnis.2019.12.03.

[2] Uji, “Perkembangan Teknologi, Manusia Semakin Tergantung Kepada Internet,” http://www.cakrawalanews.co.id/artikel/5713/Perkembangan-Teknologi-Manusia-Semakin-Tergantung-Kepada-Internet/.

[3] M. Rani, “PERLINDUNGAN OTORITAS JASA KEUANGAN TERHADAP KERAHASIAAN DAN KEAMANAN DATA PRIBADI NASABAH BANK,” *Jurnal Selat*, vol. 2, no. 1, pp. 168–181, 2014, [Online]. Available: http://www.republika.co.id/berita,

[4] CNN Indonesia, “Per Bulan, 2 Ribu Nasabah Bank Jadi Korban Kejahatan Siber,” https://www.cnnindonesia.com/teknologi/20220826193538-185-839667/per-bulan-2-ribu-nasabah-bank-jadi-korban-kejahatan-siber.

[5] Kompas.com, “Mengenal Kejahatan Social Engineering dan Modus-modusnya,” https://money.kompas.com/read/2022/09/11/230215926/mengenal-kejahatan-social-engineering-dan-modus-modusnya?page=all.

[6] H. Qur’ani, “Simak Beda Data Pribadi Dengan Informasi Terbuka,” https://www.hukumonline.com/berita/a/simak-beda-data-pribadi-dengan-informasi-terbuka-lt5d5dcad4d55fd?page=all.

[7] CNN Indonesia, “Fitur Add Yours Instagram Buka Celah Penipuan dan Curi Data,” https://www.cnnindonesia.com/teknologi/20211123101840-185-724774/fitur-add-yours-instagram-buka-celah-penipuan-dan-curi-data.

[8] H. Kruger, L. Drevin, and T. Steyn, “A vocabulary test to assess information security awareness,” *Information Management & Computer Security*, vol. 18, no. 5, pp. 316–327, Nov. 2010, doi: 10.1108/09685221011095236.

[9] Sugiyono, *Metode Penelitian Kuantitatif*. Bandung: Alfabeta, 2022.

[10] D. I. Junaedi, “Antisipasi Dampak Social Engineering Pada Bisnis Perbankan,” *Jurnal Ilmu-ilmu Informatika dan Manajemen STMIK*, vol. 11, no. 1, 2017.

[11] N. Patel, “SOCIAL ENGINEERING AS AN EVOLUTIONARY THREAT TO INFORMATION SECURITY IN HEALTHCARE ORGANIZATIONS,” *Indonesian Journal of Health Administration*, vol. 8, no. 1, pp. 56–64, Jun. 2020, doi: 10.20473/jaki.v8i1.2020.56-64.

[12] R. Heartfield, G. Loukas, and D. Gan, “You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks,” *IEEE Access*, vol. 4, pp. 6910–6928, 2016, doi: 10.1109/ACCESS.2016.2616285.

[13] A.-S. Temitope Olanrewaju and N. H. Zakaria, “SOCIAL ENGINEERING AWARENESS GAME (SEAG): AN EMPIRICAL EVALUATION OF USING GAME TOWARDS IMPROVING INFORMATION SECURITY AWARENESS,” in *5th International Conference*

on Computing and Informatics, Instanbul, Aug. 2015, pp. 187–193. [Online]. Available: http://www.uum.edu.my

[14] C. A. Citra and B. Rosy, "Keefektifan Penggunaan Media Pembelajaran Berbasis Game Edukasi Quizizz Terhadap Hasil Belajar Teknologi Perkantoran Siswa Kelas X SMK Ketintang Surabaya," *Jurnal Pendidikan Administrasi Perkantoran (JPAP)*, vol. 8, no. 2, pp. 261–272, 2020, [Online]. Available: https://journal.unesa.ac.id/index.php/jpap

[15] F. NKD, "Definisi Keamanan Informasi dan 3 Aspek di Dalamnya (CIA Triad)," https://www.logique.co.id/blog/2021/02/18/keamanan-informasi/#Definisi_Keamanan_Informasi.

[16] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. Sri Arsa, "Information technology risk management using ISO 31000 based on issaf framework penetration testing (Case study: Election commission of x city)," *International Journal of Computer Network and Information Security*, vol. 12, no. 4, pp. 30–40, Aug. 2020, doi: 10.5815/ijcnis.2020.04.03.

[17] A. Fadlil, I. Riadi, and A. Nugrahantoro, "Data Security for School Service Top-Up Transactions Based on AES Combination Blockchain Technology," *Lontar Komputer : Jurnal Ilmiah Teknologi Informasi*, vol. 11, no. 3, p. 155, Dec. 2020, doi: 10.24843/lkjiti.2020.v11.i03.p04.

[18] A. D. Purba, I. K. A. Purnawan, and I. P. A. E. Pratama, "Audit Keamanan TI Menggunakan Standar ISO/IEC 27002 dengan COBIT 5," *MERPATI*, vol. 6, no. 3, pp. 148–158, 2018.

[19] I. Riadi, Sunardi, and E. Handoyo, "Security Analysis of Grr Rapid Response Network using COBIT 5 Framework," *Lontar Komputer : Jurnal Ilmiah Teknologi Informasi*, p. 29, May 2019, doi: 10.24843/lkjiti.2019.v10.i01.p04.

[20] R. T. N. Yamin, I. M. A. D. Suarjaya, and I. P. A. E. Pratama, "Penetration Testing on the SISAKTI Application at Udayana University Using the OWASP Testing Guide Version 4," *MERPATI*, vol. 10, no. 3, pp. 155–166, 2022.

[21] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput Secur*, vol. 25, no. 4, pp. 289–296, Jun. 2006, doi: 10.1016/j.cose.2006.02.008.

[22] E. W. Tyas Darmaningrat *et al.*, "Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi," *Sewagati*, vol. 6, no. 2, Feb. 2022, doi: 10.12962/j26139960.v6i2.92.

[23] C. Hadnagy, "A Look into the New World of Professional Social Engineering," in *Social Engineering: The Science of Human Hacking*, 2nd ed., United Kingdom: Wiley, 2018, pp. 18–43.

[24] E. M. Safitri, Z. Ameilindra, and R. Yulianti, "Analisis Teknik Social Engineering Sebagai Ancaman Dalam Keamanan Sistem Informasi: Studi Literatur," *JIFTI-Jurnal Ilmiah Teknologi Informasi dan Robotika*, vol. 2, no. 2, pp. 21–26, 2020.

[25] I. A. M. Abass, "Social Engineering Threat and Defense: A Literature Survey," *Journal of Information Security*, vol. 09, no. 04, pp. 257–264, 2018, doi: 10.4236/jis.2018.94018.

[26] A. Andress, *Surviving Security: How to Integrate People, Process, and Technology*. London: Taylor and Francis, 2004.

[27] L. S. L. Purba, "PENINGKATAN KONSENTRASI BELAJAR MAHASISWA MELALUI PEMANFAATAN EVALUASI PEMBELAJARAN QUIZIZZ PADA MATA KULIAH KIMIA FISIKA I," *Jurnal Dinamika Pendidikan*, vol. 12, no. 1, 2019, doi: 10.33541/jdp.v12i1.1028.

[28] H. Koyimah, L. Hidayah, and M. Huda, "Pertemuan Ilmiah Bahasa dan Sastra Indonesia | 293 (PIBSI) XL," 2018.

[29] J. Clear, "How Long Does it Actually Take to Form a New Habit? (Backed by Science)," https://jamesclear.com/new-habit#:~:text=On%20average%2C%20it%20takes%20more,to%20form%20a%20new%20habit.