JURNAL SYNTAX IDEA
p–ISSN: 2723-4339 e-ISSN: 2548-1398
Vol. 5, No. 1, Januari 2023

ANALISIS TINGKAT KESADARAN KEAMANAN INFORMASI: STUDI KASUS PENGGUNA APLIKASI PERBANKAN DIGITAL DI INDONESIA GUNA MENCEGAH SOCIAL ENGINEERING

Taufiq Ramadhan, Betty Purwandari
Fakultas Ilmu Komputer Universitas Indonesia, Jawa Barat, Indonesia
Email: taufiq.ramadhan91@ui.ac.id, bettyp@cs.ui.ac.id

Abstrak

Adopsi internet dan smartphone yang meningkat pesat, pertumbuhan e-commerce, dan dorongan digitalisasi yang kuat oleh bank-bank di Indonesia menjadi kombinasi faktor yang mempercepat proses migrasi ke layanan perbankan digital in. Perkembangan tersebut dibuktikan dengan tingginya adopsi digital terutama di perbankan digital. Permasalahan yang ditemukan adalah belum adanya acuan tingkat kesadaran keamanan informasi pada pengguna aplikasi perbankan digital. Penelitian ini dilakukan untuk mengukur tingkat kesadaran keamanan informasi pengguna aplikasi perbankan digital guna mencegah kasus *social engineering*. Jenis penelitian ini menggunakan model *Knowledge-Attitude-Behaviour* (KAB) yang diterapkan pada *Human Aspects of Information Security Questionnaire* (HAIS-Q) dan taksonomi kesadaran keamanan pengguna selular. Data penelitian dikumpulkan menggunakan kuesioner dan mendapat 299 responden valid. Hasil dari penelitian ini menunjukkan bahwa tingkat kesadaran keamanan informasi pengguna aplikasi layanan perbankan di Indonesia berada pada level baik dengan nilai 81,30%. Nilai masing-masing dimensi kesadaran keamanan informasi adalah dimensi pengetahuan sebesar 84,45% (baik), dimensi sikap sebesar 84,68% (baik) dan dimensi perilaku sebesar 78,06% (cukup). Berdasarkan hasil tersebut, ada beberapa rekomendasi yaitu regulasi terhadap installasi aplikasi ilegal dan materi peningkatan kesadaran keamanan informasi guna mencegah *social engineering*. Kesimpulan, Penelitian ini berhasil menghitung tingkat kesadaran keamanan informasi pengguna aplikasi layanan perbankan. Nilai akhir kesadaran keamanan informasi yang didapat adalah sebesar 81,30% atau pada level baik.

Kata kunci: Kesadaran Keamanan Informasi; Aplikasi Perbankan; Pengetahuan-Sikap-Perilaku (KAB); Rekayasa Sosial.

Abstract

The rapidly increasing adoption of the internet and smartphones, the growth of e-commerce, and the strong drive for digitalization by banks in Indonesia are a combination of factors that have accelerated the migration process to digital banking services. This development is evidenced by the high digital adoption, especially in digital banking. The problem found is that there is no reference to the level of information security awareness among users of digital banking applications. This research was conducted to measure the level of information security awareness of users of digital banking applications to prevent cases of

How to cite: Taufiq Ramadhan, Betty Purwandari (2023) Analisis Tingkat Kesadaran Keamanan Informasi: Studi Kasus Pengguna Aplikasi Perbankan Digital di Indonesia Guna Mencegah *Social Engineering*, *(5) 1*, https://doi.org/10.36418/syntax-idea.v3i6.1227
E-ISSN: 2684-883X
Published by: Ridwan Institute

social engineering. This type of research uses the Knowledge-Attitude-Behaviour (KAB) model which is applied to the Human Aspects of Information Security Questionnaire (HAIS-Q) and the taxonomy of security awareness of mobile users. Research data was collected using a questionnaire and obtained 299 valid respondents. The results of this study indicate that the level of information security awareness of users of banking service applications in Indonesia is at a good level with a value of 81.30%. The value of each dimension of information security awareness is the knowledge dimension of 84.45% (good), the attitude dimension is 84.68% (good) and the behavioral dimension is 78.06% (enough). Based on these results, there are several recommendations, namely controlling the installation of illegal applications and information security education materials to prevent social engineering. In conclusion, this study succeeded in calculating the level of information security awareness of users of banking service applications. The final value of information security awareness obtained is 81.30% or at a good level.

Keywords: *Information Security Awareness; Banking Applications; Knowledge-Attitude-Behavior (KAB); Social Engineering*.

PENDAHULUAN

Menurut penelitian (Barquin, Gantès, HV, & Shrikhande, 2019) dalam riset McKinsey & Company yang melibatkan 17.000 orang di 15 negara di Asia menyatakan bahwa Indonesia merupakan negara tercepat yang melakukan adopsi digital utamanya di perbankan digital. Riset tersebut menyebutkan bahwa masyarakat yang tinggal di perkotaan di Indonesia menggunakan dua sampai tiga produk layanan perbankan digital. Adopsi internet dan smartphone yang meningkat pesat, pertumbuhan e-commerce, dan dorongan digitalisasi yang kuat oleh bank-bank di Indonesia menjadi kombinasi faktor yang mempercepat proses migrasi ke layanan perbankan digital ini (Barquin et al., 2019).

Seiring tumbuhnya jumlah pengguna, jumlah transaksi perbankan digital juga ikut naik. Setidaknya pada dua tahun terakhir, terjadi peningkatan jumlah transaksi perbankan digital. Pada tahun 2021, kenaikan transaksi digital juga terjadi senilai Rp39.841,4 triliun atau tumbuh 45,64 persen jika dibandingkan dengan tahun sebelumnya (Fiona & Rahmayanti, 2022).

Peningkatan jumlah utilisasi layanan perbankan digital tersebut dihadapkan dengan ancaman keamanan digital. Pada tahun 2020, (Nasional, 2021) mengungkapkan bahwa sepanjang tahun 2020 terjadi 495 juta serangan siber atau naik 5 kali lipat dibanding tahun sebelumnya. Catatan tersebut senada dengan apa yang disampaikan oleh *World Economic Forum* (2021) dalam laporan *Global Risk* Report 2021. Serangan siber memanfaatkan social engineering, OTP fraud, SIM swap, kelemahan pada sistem keuangan dan perbankan, dan juga *phishing* (Wicaksana, Munandar, & Samputra, 2020).

(Scheffauer, Goyanes, & de Zúniga, 2021) menyatakan bahwa peningkatan penggunaan teknologi perangkat bergerak dalam skala global yang sangat cepat juga memunculkan ancaman keamanan dari penggunaan teknologi tersebut. Kesadaran

pengguna menjadi sebuah faktor manusia yang sangat penting untuk keamanan dalam konteks ini. Berbagai ancaman seperti *malware, phishing, malicious applications, spam, hijacking, untrusted wi-fi*, dan *social engineering* kerap ditemui oleh pengguna selain beberapa ancaman yang disebabkan oleh tidak cukupnya kesadaran dan pengetahuan seperti memberikan data pribadi, navigasi web, penggunaan password yang buruk, dan penggunaan banyak perangkat sekaligus. Dalam keamanan informasi, manusia adalah rantai terlemah yang sifat-sifatnya dapat dieksploitasi oleh social engineers untuk mendapatkan akses atau informasi rahasia. Satu-satunya cara yang ampuh untuk mencegah social engineering adalah dengan program kesadaran keamanan informasi yang baik (Tolle, Kurniawan, & Zakaria, 2012).

Beberapa catatan mengenai kasus *social engineering* yang menyasar pengguna aplikasi perbankan digital antara lain: seorang pengguna layanan perbankan digital mengalami social engineering hingga memberikan OTP pada pihak yang mengaku sebagai petugas bank (Putri, 2022). Pengguna membuka aplikasi perbankan digital yang kemudian diketahui invalid hingga kemudian mengalami sejumlah kerugian materil, dan pengguna bank digital yang jatuh dalam kasus penipuan terutama *social engineering* hingga mengalami kerugian materi.

Pada penelitian sebelumnya, (Utaminingsih, 2014) telah memperkenalkan prototipe untuk penilaian kesadaran keamanan informasi dengan membagi pengukuran menjadi tiga dimensi: *Knowledge-Attitude-Behaviour* (KAB). (Parsons et al., 2017) menggunakan model KAB ini sebagai acuan metode pengukuran kesadaran keamanan informasi pengguna (*Human Aspects of Information Security Questionnaire HAIS-Q*). Selain itu model KAB juga digunakan untuk menjabarkan taksonomi keamanan informasi pengguna selular oleh (Bitton, Boymgold, Puzis, & Shabtai, 2020).

Penelitian ini dimaksudkan untuk mengetahui tingkat kesadaran keamanan informasi pengguna aplikasi perbankan guna mencegah *social engineering*. Target populasi dari penelitian ini adalah pengguna aplikasi perbankan digital di Indonesia. Dala, penelitian ini dipilih lima belas aplikasi perbankan digital yang legal dan resmi: BCA Mobile atau MyBCA, Livin by Mandiri, BNI Mobile Banking, BRImo BRI, BSI Mobile, Jenius by BTPN, Jago by Bank Jago, Digibank Indonesia, Seabank, Motion Banking by MNC Bank, OCTO Mobile by CIMB Niaga, Permata Mobile X, Aladin by Bank Aladin Syariah, Allo Bank, dan NeoBank. Hasil penelitian ini diharapkan dapat menjadi input guna mencegah terjadinya *social engineering* pada pengguna aplikasi perbankan.

Penelitian ini bertujuan untuk mengetahui nilai kesadaran keamanan informasi pengguna aplikasi layanan perbankan di Indonesia. Target penelitian ini adalah pengguna aplikasi layanan perbankan di Indonesia yang berusia 16 sampai 65 tahun. Aplikasi layanan perbankan yang menjadi objek adalah aplikasi perbankan yang dikeluarkan oleh Bank secara legal dan tersedia di Google Play Store maupun *Apple App Store.*

METODE PENELITIAN

Jenis metode yang digunakan dalam penelitian ini adalah kuesioner. Kuesioner tersebut berisi pertanyaan yang mempunyai pilihan jawaban berupa skala Likert 1 – 5, yang mana 1 satu merupakan sangat tidak setuju (*strongly disagree*) hingga 5 yang merupakan sangat setuju (*strongly agree*) (Joshi, Kale, Chandel, & Pal, 2015). Kuesioner terdiri dari empat bagian, yaitu (1) pengantar kuesioner berisi tujuan penelitian dan komitmen keamanan informasi, (2) profiling pengguna aplikasi perbankan digital, (3) pertanyaan mengenai profil responden, dan (4) kriteria dari area fokus keamanan. Kuesioner dibuat menggunakan *platform survey* ui dan akan disebar melalui media sosial dan grup perpesanan sehingga diharap dapat mengumpulkan data secara acak dengan populasi pengguna aplikasi perbankan digital.

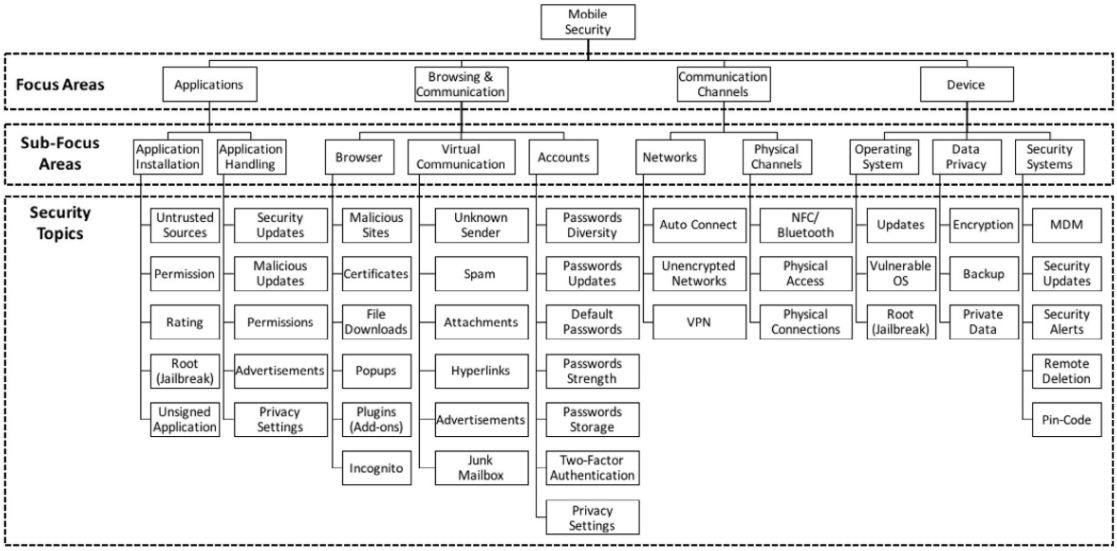
HASIL DAN PEMBAHASAN

Menurut penelitian (Whitman & Mattord, 2011) mendefinisikan keamanan informasi sebagai perlindungan informasi dan segala elemen kritisnya, beserta sistem dan *hardware* yang menggunakan, menyimpan, dan mengirimkan informasi tersebut. Model keamanan informasi tersebut didasarkan pada karakteristik informasi yang memberi nilai kepada organisasi yaitu: *Confidentiality*, *Integrity*, dan *Availability*.

Kesadaran keamanan informasi dapat didefinisikan sebagai keadaan di mana pengguna dalam sebuah organisasi sadar dan berkomitmen pada misi keamanannya (Tiatama, 2016). Definisi ini meliputi keadaan kognitif saat persepsi individu mengenai keamanan informasi berada di dalam konteks organisasi yang relevan dan dibingkai dalam kebijakan keamanan informasi (Bauer & Bernroider, 2017).

Pengukuran kesadaran keamanan informasi jamak menggunakan model dari (Amin, 2014a). Model penelitian (Amin, 2014b) menggunakan tiga dimensi yang menjadi basis pengukuran, yaitu *knowledge*, *attitude*, dan *behaviour*. *Knowledge* atau pengetahuan didefinisikan sebagai apa yang diketahui atau dipahami seseorang, *attitude* atau sikap adalah apa yang mereka rasakan atau pikirkan, dan *behavior* atau perilaku yaitu tindakan yang dilakukan (Ubaidillah, 2019). Fokus utama inisiatif kesadaran keamanan informasi adalah untuk mengubah perilaku, tetapi memahami tingkat pengetahuan dan perilaku adalah panduan yang paling efektif untuk mengubah perilaku (Utaminingsih, 2014).

(Bitton et al., 2020) juga mengembangkan kerangka dari dimensi KAB untuk mengukur tingkat kesadaran keamanan pengguna selular. (Bitton et al., 2020) membagi keamanan selular menjadi empat are fokus yaitu (1) aplikasi, (2) penjelajahan dan komunikasi, (3) kanal komunikasi, dan (4) perangkat.



Gambar 1. **Taksonomi Keamanan Selular** (Bitton et al., 2020)

Tabel 1
Level Kesadaran KAB

Level	Hasil (%)
Baik	80 - 100
Cukup	60 – 79
Kurang	< 60

Berdasarkan model KAB dari (Amin, 2014);(Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014) mengembangkan tujuh area fokus dari tiga dimensi pengetahuan, sikap, dan perilaku. Area fokus tersebut adalah (1) manajemen *password*, (2) penggunaan email, (3) penggunaan internet, (4) penggunaan media sosial, (5) perangkat seluler, (6) penanganan informasi, dan (7) pelaporan insiden. Kerangka kerja ini dikenal sebagai *Human Aspects of Information Security* (HAIS-Q). HAIS-Q dikembangkan untuk mengukur kesadaran keamanan informasi karyawan maupun anggota organisasi (Parsons et al., 2014). Masing-masing area fokus tersebut akan diukur dalam dimensi KAB. Pembobotan nilai kesadaran didasarkan pada bobot dimensi dari (Amin, 2014). Bobot masing-masing dimensi disajikan pada tabel 2.

Tabel 2
Bobot Dimensi KAB

Level	Nilai (%)
Knowledge	30
Attitude	20
Behaviour	50

Penelitian ini menggunakan komponen HAIS-Q dan area fokus keamanan selular, sehingga. Penggabungan tersebut digunakan untuk mengurangi aspek keamanan di

lingkup *desktop* pada HAIS-Q, dan menambah aspek keamanan selular. Pemetaan HAIS-Q dan area fokus keamanan selular ada pada tabel 3.

Tabel 3
Bobot Dimensi KAB

HAIS-Q	Area Fokus Keamanan Selular	Area Fokus yang Digunakan
Manajemen password	Penjelajahan dan Komunikasi	Penjelajahan dan komunikasi,
Penggunaan email		
Penggunaan internet	Kanal Komunikasi	Kanal komunikasi
Media sosial		Media Sssial
Perangkat seluler	Aplikasi, Perangkat	Aplikasi
Penanganan informasi		Perangkat
Pelaporan insiden		Pelaporan insiden

Area fokus yang digunakan kemudian dinilai bobotnya guna menentukan nilai perbandingan pada area fokus tersebut. Pada penelitian ini nilai bobot diambil dari pembobotan pembobotan yang telah dilakukan (Arisya, Ruldeviyani, Prakoso, & Fadhilah, 2020) dan kemudian memetakannya berdasarkan padanan area fokus tersebut di area fokus yang digunakan. Hal ini dilakukan karena pada adanya kesamaan dengan penelitian tersebut, yang juga mengukur nilai kesadaranan keamanan informasi pengguna aplikasi perbankan (*mobile banking).*

Tabel 4
Pembobotan Area Fokus

Area Fokus HAIS-Q	Nilai	Area Fokus yang Digunakan	Nilai
Manajemen password	17,36%	Penjelajahan dan komunikasi	25,05%
Penggunaan email	7,69%		
Penggunaan internet	5,22%	Kanal komunikasi	5,22%
Penanganan informasi	25,30%	Aplikasi	25,30%
Penggunaan perangkat	15,40%	Perangkat	15,40%
Penggunaan media sosial	15,40%	Media sosial	15,40%
Pelaporan insiden	13,63%	Pelaporan insiden	13,63%
Total Kesadaran (dimensi psikologis)	100%	Total Kesadaran (dimensi psikologis)	100%

A. Tahapan Penelitian

Tahapan yang dilakukan dalam penilitian ini ada pada gambar 2.

Gambar 2. Tahapan Penelitian

Berdasarkan jenis kelamin, usia, latar belakang, dan domisili didapat demografi responden yang dilihat pada tabel 5.

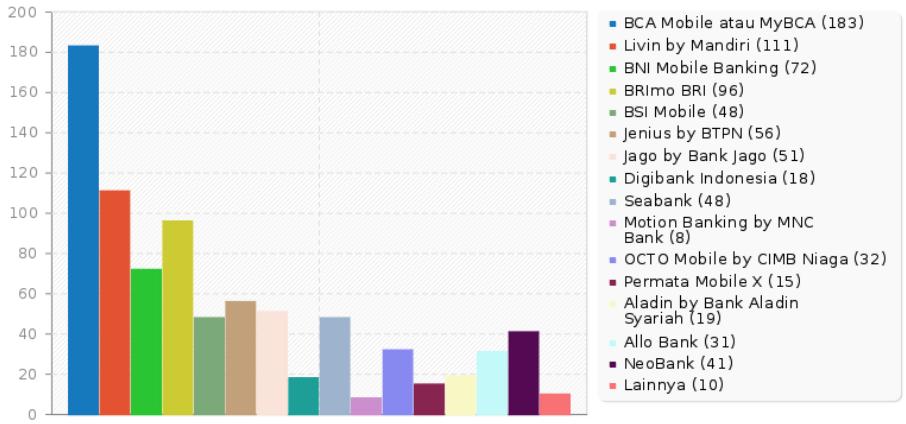
Tabel 5
Demografi Responden

Kriteria	Kategori	Prosentase
Jenis Kelamin	Laki-laki	38%
	Perempuan	62%
Usia	16 - 25	69%
	26 - 35	28%
	36 - 45	3%
	> 45	0%
Latar Belakang Pendidikan	SMA	38%
	Diploma	14%
	S1	44%
	S2	4%
Pulau Domisili	Jawa	86.29%
	Sumatera	9.7%
	Kalimantan	1.67%
	Sulawesi	1.34%
	Bali & Kep. Nusa Tenggara	1%
	Kep. Maluku & Papua	0%

Berdasarkan tabel 5, penelitian ini belum mendapat pengguna aplikasi perbankan yang berusia di atas 45 tahun maupun yang berdomisili di Indonesia bagian timur.

B. Karakteristik Penggunaan Aplikasi Perbankan Digital

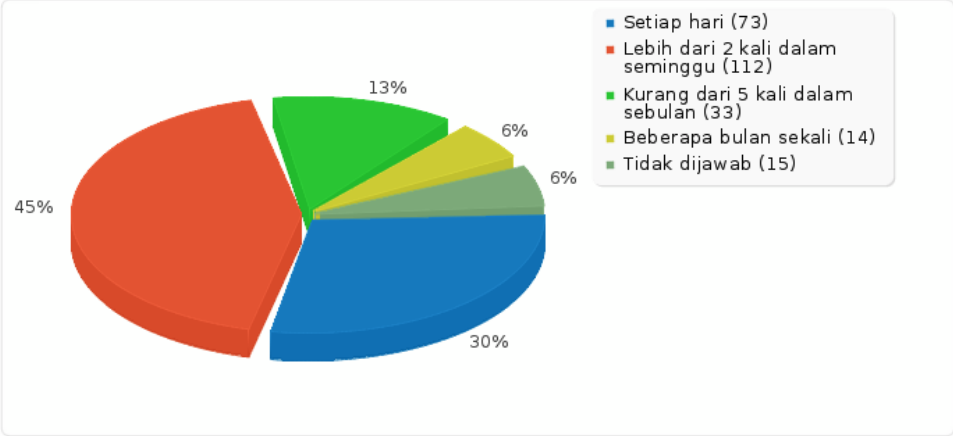
Pada sebaran aplikasi perbankan yang digunakan, aplikasi perbankan yang paling banyak digunakan adalah BCA Mobile atau MyBCA. Kemudian diikuti oleh Livin by Mandiri 111 responden, BRImo BRI sebanyak 96 responden, BNI Mobile Banking dengan 72 responden, dan Jenius by BTPN sejumlah 16 responden. Data disajikan pada gambar 3.



Gambar 3. Aplikasi Perbankan yang Digunakan

Selain lima belas aplikasi perbankan yang disajikan, ada sebanyak empat aplikasi masukan dari responden yaitu TMRW by UOB oleh 2 responden, DBank Pro Danamon 2 responden, BPDDIY Mobile 1 responden, BTN Mobile Banking 1 responden, Blu by BCA Digital 1 responden, CommBank Mobile by Bank Commonwealth 1 responden, dan D-Bank Pro Danamon 1 responden.

Sementara dari sisi frekuensi penggunaan aplikasi perbankan, didapatkan data seperti pada Gambar 4. Sejumlah 123 responden mengaku menggunakan aplikasi perbankan antara 2 kali hingga 6 kali seminggu, kemudian ada 101 responden yang menggunakan aplikasi perbankan setiap hari.



Gambar 4. Frekuensi penggunaan aplikasi

C. Hasil Pengukuran Tingkat Kesadaran Keamanan Informasi

Berdasarkan analisis data kuesioner kesadaran keamanan informasi yang telah dilakukan didapat tingkat kesadaran keamanan informasi pada tabel 6.

Tabel 6
Tingkat Kesadaran Keamanan Informasi

Area Fokus	Knowledge	Attitude	Behaviour	Kesadaran
Aplikasi	83,74%	88,60%	75,33%	80,51%
Penjelajahan dan Komunikasi	86,42%	86,85	82,22%	84,41%
Perangkat	88,27%	85,80%	84,60%	85,94%
Kanal Komunikasi	80,30%	76,90%	70,40%	74,67%
Media Sosial	88,90%	89,30%	87,30%	88,18%
Pelaporan Insiden	83,40%	84,60%	77,84%	80,86%
Kesadaran Informasi (Dimensi)	84,45%	84,68%	78,06%	81,30%

Perbedaan warna pada tabel 6 menunjukan tingkat kesadaran keamanan informasi dan informasi yang diberikan. Pedoman nilai dan informasi pada tabel 7.

Tabel 7
Tingkat Kesadaran Keamanan Informasi

Warna	Nilai (%)	Kategori	Informasi
Biru	80-100	Baik	Memuaskan tidak memerlukan tindakan
Kuning	60-79	Cukup	Pengawasan, ada kemungkinan dibutuhkan Tindakan
Merah	< 60	Kurang	Tidak memuaskan, membutuhkan tindakan

Pada perhitungan kesadaran keamanan informasi, didapat nilai akhir 84,45% untuk dimensi pengetahuan, 84,68% pada dimensi sikap, dan 78,06% pada dimensi perilaku, dan didapat nilai total sebesar 81,30%. Jika dibaca menggunakan level kesadaran keamanan informasi, nilai akhir menunjukkan level baik, adapun pada masing-masing dimensi, pengetahuan dan sikap mendapat level baik, namun pada perilaku mendapat cukup. Dimensi perilaku perlu mendapat perhatian berupa pengawasan. Area fokus aplikasi dan kanal komunikasi merupakan dua area fokus yang mendapat nilai kesadaran keamanan informasi cukup. Kedua area fokus ini harus mendapat perhatian khusus dari pemerintah dan penyedia layanan.

Aplikasi kerap menjadi jalan masuk upaya *social engineering* dengan memanfaatkan kelengahan pengguna yang menginstall aplikasi dari sumber tidak resmi atau tidak terpercaya. Contoh kasus telah terjadi adalah seorang nasabah membuka aplikasi perbankan digital yang ternyata diketahui *invalid* hingga kemudian mengalami sejumlah kerugian materil (Kalbuadi, 2015). Regulasi dari pemerintah diperlukan guna mencegah pengguna menginstall aplikasi ilegal. Sementara itu penyedia layanan perbankan harus ada edukasi untuk tidak menginstall aplikasi tidak resmi maupun memasukkan data-data akun finansial dalam aplikasi lain.

Area fokus kanal komunikasi meliputi penggunaan jaringan wifi publik dan pemanfaatan VPN. Wifi publik didefinisikan sebagai akses jaringan internet terbuka yang menggunakan teknologi WiFI. Penggunaan jaringan wifi publik memungkinkan terjadi pencurian data melalui serangan *man-in-the-middle* dan *spoofing* atau penyadapan (Kurniawan, 2021). Pencegahan dapat dilakukan dengan cara menggunakan VPN saat terhubung dengan jaringan wifi publik. Responden

cukup memahami pemanfaatan VPN, namun tidak mengadopsinya karena layanan VPN tersebut berbayar.

Sebagai upaya pencegahan *social engineering* dan *man-in-the-middle*, pemerintah dan penyedia layanan diharapkan melakukan kampanye dan edukasi keamanan informasi yang meliputi materi berikut ini:

1. Risiko dan bahaya melakukan instalasi dan pembaruan aplikasi dari sumber yang tidak terpercaya.
2. Pengamanan data pribadi dan data-data finansial dengan tidak menyimpan dalam catatan maupun menginputnya dalam aplikasi lain.
3. Panduan membedakan aplikasi resmi dan tidak resmi.
4. Panduan transaksi atau penggunaan aplikasi perbankan saat berada pada jaringan wifi publik.
5. Pemanfaatan VPN.

Sementara itu rekomendasi untuk menjaga tingkat kesadaran keamanan informasi pengguna tetap baik, antara lain:

1. Penyedia layanan bisa memanfaatkan fitur notifikasi pada aplikasi untuk memberi pemberitahuan secara berkala untuk mengingatkan pengguna akan bahaya apa saja yang harus dihindari pengguna dan hal-hal lain yang dapat menuntut kepatuhan pengguna dalam menjaga keamanan informasi.
2. Penyedia layanan dan pemerintah harus tetap melakukan kampanye dan edukasi baik melalui media komunikasi konvensional seperti pelatihan ataupun seminar dan media komunikasi online yang interaktif seperti video interaktif, media sosial, maupun permainan yang berisi materi-materi dari dimensi dan area fokus yang membutuhkan perhatian sehingga dapat naik menjadi level baik.
3. Perlu adanya evaluasi tingkat kesadaran keamanan informasi bagi pengguna secara berkala.

KESIMPULAN

Penelitian ini berhasil menghitung tingkat kesadaran keamanan informasi pengguna aplikasi layanan perbankan. Nilai akhir kesadaran keamanan informasi yang didapat adalah sebesar 81,30% atau pada level baik. Berdasarkan masing-masing dimensi adalah dimensi pengetahuan sebesar 84,45% (baik), dimensi sikap sebesar 84,68% (baik), dan dimensi perilaku sebesar 78,06% (cukup).

Dimensi dan area fokus yang memiliki nilai cukup harus mendapat perhatian dan tindakan lanjutan jika diperlukan. Beberapa rekomendasi mengenai peningkatan kesadaran keamanan informasi dalam upaya pencegahan *social engineering* antara lain regulasi instalasi aplikasi ilegal dari pemerintah, edukasi perlindungan data finansial dari penyedia layanan, program kampanye yang berisi materi dari area fokus yang masih berada pada level cukup. Selain itu guna menjaga agar tingkat kesadaran keamanan pengguna tetap baik, diperlukan evaluasi berkala baik dari pemerintah maupun penyedia layanan.

BIBLIOGRAFI

Amin, Mukhlis. (2014a). Information Security Awareness Level Measurement Using Multiple Criteria Decision Analysis (Mcda). *Jurnal Penelitian Dan Pengembangan Komunikasi Dan Informatika*, *5*(1).Google Scholar

Amin, Mukhlis. (2014b). Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (Mcda) Information Security Awareness Level Measurement Using Multiple Criteria Decision Analysis (Mcda). *Jurnal Penelitian Dan Pengembangan Komunikasi Dan Informatika Vol*, *5*(1). Google Scholar

Arisya, Khairunnisa Firsty, Ruldeviyani, Yova, Prakoso, Rahardi, & Fadhilah, Amanda Lailatul. (2020). Measurement Of Information Security Awareness Level: A Case Study Of Mobile Banking (M-Banking) Users. *2020 Fifth International Conference On Informatics And Computing (Icic)*, 1–5. Ieee. Google Scholar

Barquin, Sonia, Gantès, G. De, Hv, Vinayak, & Shrikhande, Duhita. (2019). Digital Banking In Indonesia: Building Loyalty And Generating Growth. *Mckinsey & Company, February*, *6*. Google Scholar

Bauer, Stefan, & Bernroider, Edward W. N. (2017). From Information Security Awareness To Reasoned Compliant Action: Analyzing Information Security Policy Compliance In A Large Banking Organization. *Acm Sigmis Database: The Database For Advances In Information Systems*, *48*(3), 44–68. Google Scholar

Bitton, Ron, Boymgold, Kobi, Puzis, Rami, & Shabtai, Asaf. (2020). Evaluating The Information Security Awareness Of Smartphone Users. *Proceedings Of The 2020 Chi Conference On Human Factors In Computing Systems*, 1–13. Google Scholar

Fiona, Febzi, & Rahmayanti, Dewi. (2022). Analisis Dampak Pandemi Covid-19 Bagi Umkm Dan Implementasi Strategi Digital Marketing Pada Umkm Indonesia. *Managament Insight: Jurnal Ilmiah Manajemen*, *17*(2), 298–322. Google Scholar

Joshi, Ankur, Kale, Saket, Chandel, Satish, & Pal, D. Kumar. (2015). Likert Scale: Explored And Explained. *British Journal Of Applied Science & Technology*, *7*(4), 396. Google Scholar

Kalbuadi, Putra. (2015). *Jual Beli Online Dengan Menggunakan Sistem Dropshipping Menurut Sudut Pandang Akad Jual Beli Islam (Studi Kasus Pada Forum Kasus)*. Google Scholar

Kurniawan, Reza. (2021). *Analisis Keamanan Fasilitas Jaringan (Wifi) Terhadap Serangan Packet Sniffing Pada Protocol Http Dan Https*. Universitas Islam Riau. Google Scholar

Nasional, Pusat Operasi Keamanan Siber. (2021). Laporan Tahunan Hasil Monitoring Keamanan Siber 2020. *Buletin Jendela Data Dan Informasi Kesehatan*. Google Scholar

Parsons, Kathryn, Calic, Dragana, Pattinson, Malcolm, Butavicius, Marcus, Mccormac, Agata, & Zwaans, Tara. (2017). The Human Aspects Of Information Security Questionnaire (Hais-Q): Two Further Validation Studies. *Computers & Security*, *66*, 40–51. Google Scholar

Parsons, Kathryn, Mccormac, Agata, Butavicius, Marcus, Pattinson, Malcolm, & Jerram, Cate. (2014). Determining Employee Awareness Using The Human Aspects Of Information Security Questionnaire (Hais-Q). *Computers & Security*, *42*, 165–176. Google Scholar

Putri, Rahmadani Ningtyas Sekar. (2022). *Analisa Pola–Pola Sosialisasi Pencegahan Modus Social Engineering Oleh Bank Melalui Media Website Dan Media Sosial Twitter*. Google Scholar

Scheffauer, Rebecca, Goyanes, Manuel, & De Zúniga, Homero Gil. (2021). Beyond Social Media News Use Algorithms: How Political Discussion And Network Heterogeneity Clarify Incidental News Exposure. *Online Information Review*. Google Scholar

Tiatama, Adi. (2016). *Perencanaan Tata Kelola Manajemen Keamanan Informasi Menggunakan Information Technology Infrastructure Library (Itil) V3. Pada D~ Net Surabaya*. Institut Teknologi Sepuluh Nopember. Google Scholar

Tolle, Herman, Kurniawan, Tri Astoto, & Zakaria, Andi. (2012). Peningkatan Keamanan Web Terhadap Serangan Cross Site Scripting (Xss). *Tekno*, *9*(1). Google Scholar

Ubaidillah, Muhammad Septian. (2019). *Pengaruh Pengetahuan Keuangan Terhadap Perilaku Keuangan Dengan Sikap Keuangan Dan Self-Efficacy Sebagai Variabel Mediasi (Studi Empiris Pada Mahasiswa Jurusan Akuntansi Universitas Airlangga)*. Universitas Airlangga. Google Scholar

Utaminingsih, Alifiulahtin. (2014). *Perilaku Organisasi: Kajian Teoritik & Empirik Terhadap Budaya Organisasi, Gaya Kepemimpinan, Kepercayaan Dan Komitmen*. Universitas Brawijaya Press. Google Scholar

Whitman, Michael E., & Mattord, Herbert J. (2011). *Principles Of Information Security 4th Edition*. Cengage Learning. Google Scholar

Wicaksana, Ratnadi Hendra, Munandar, Adis Imam, & Samputra, Palupi Lindiasari. (2020). Studi Kebijakan Perlindungan Data Pribadi Dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 (A Narrative Policy Framework Analysis Of Data Privacy Policy: A Case Of Cyber Attacks During The Covid-19 Pandemic). *Jurnal Iptekkom (Jurnal Ilmu Pengetahuan & Teknologi*

Informasi), *22*(2), 143–158. Google Scholar