JPEK (Jurnal Pendidikan Ekonomi dan Kewirausahaan)
Vol. 8, No. 3 Desember 2024, Hal. 1483-1498
DOI: 10.29408/jpek.v8i3.29304
E-ISSN: 2549-0893

Analisis Tingkat Security Awareness Dalam Password Behavior Mahasiswa (Studi Kasus Mahasiswa FEBI UINSU Medan)

Muhammad Resty Fauzi[1], Atika[2], Nursantri Yanti[3]

[1,2,3,] Fakultas Ekonomi dan Bisnis Islam, Universitas Islam Negeri Sumatera Utara
Correspondence: muhammadrestyfauzi31@gmail.com
Received: 27 November 2024 | Revised: 21 Desember 2024 | Accepted: 30 Desember, 2024

Keywords:
Awareness; Behavior; Passwords; Security

Abstract
Analysis of security awareness in password behavior in mobile banking is very important to ensure the security of financial transactions through digital platforms. The purpose of this study is to analyze the level of security awareness in student password behavior, especially in the use of mobile banking. This type of research uses the Knowledge-Attitude-Behavior (KAB) model applied to the Human Aspects of Information Security Questionnaire (HAIS-Q) and the security awareness taxonomy of mobile users. The research data was collected using a questionnaire and received 61 valid respondents. The results of this study show that the level of information security awareness of users of banking service applications in Indonesia is at a sufficient level with a value of 70%. The value of each dimension of information security awareness is the knowledge dimension of 72% (sufficient), the attitude dimension of 69% (sufficient), and the behavior dimension of 69% (sufficient). This study successfully calculated the level of information security awareness of banking service application users. The final value of information security awareness obtained is 70% or at a sufficient level.

Kata Kunci:
Kesadaran; Tingkah Laku; Kata Sandi; Keamanan.

Abstrak
Analisis kesadaran keamanan pada perilaku password pada mobile banking sangat penting untuk menjamin keamanan transaksi keuangan melalui platform digital. Tujuan dari penelitian ini adalah untuk menganalisis tingkat kesadaran keamanan pada perilaku password mahasiswa khususnya dalam penggunaan mobile banking. Jenis penelitian ini menggunakan model Knowledge-Attitude-Behavior (KAB) yang diterapkan pada taksonomi kesadaran keamanan pengguna smartphone dan Human Aspects of Information Security Assessment (HAIS-Q). Data penelitian dikumpulkan melalui kuesioner yang melibatkan 61 partisipan yang valid. Hasil penelitian ini menunjukkan bahwa pengguna aplikasi layanan perbankan di Indonesia mempunyai kesadaran keamanan informasi sebesar 70%, dengan nilai pengetahuan sebesar 72%, sikap sebesar 69%, dan perilaku sebesar 69%. Penelitian ini berhasil mengetahui tingkat kesadaran pengguna aplikasi layanan perbankan terhadap keamanan datanya. Sekitar 70% orang mengetahui tentang keamanan data mereka, atau pada tingkat yang memadai.

PENDAHULUAN

Munculnya globalisasi dan kemajuan teknologi menjadi katalis utama bagi metamorfosis di berbagai bidang kehidupan manusia, khususnya yang berkaitan dengan mekanisme pembayaran (Syahira dkk., 2024). Mayoritas nasabah Muslim memilih perbankan syariah sebagai mitra pilihan mereka untuk menabung dan mengembangkan bisnis mereka. Karena populasi Muslimnya yang terbesar di dunia, Indonesia mendapatkan manfaat dari leverage untuk merangsang pertumbuhan ekonominya. Menurut penelitian terbaru (Nasution et al., 2024),... Menurut penelitian yang dilakukan oleh With McKinsey & Company yang melibatkan Dengan populasi 17.000 orang di 15 negara Asia, Indonesia menonjol sebagai pemimpin yang tak terbantahkan dalam transisi menuju adopsi digital, khususnya di sektor perbankan online. Penduduk di Indonesia kini tergiur dengan dua hingga tiga layanan perbankan digital untuk memudahkan kehidupan sehari-hari mereka. Dengan meningkatnya penggunaan internet dan ponsel pintar, pertumbuhan e-commerce, dan kuatnya dorongan menuju digitalisasi lembaga perbankan di Indonesia, semua hal ini dapat membantu mempercepat transisi ke perbankan digital (Barquin et al., 2019). Bank saat ini mulai meningkatkan layanan mereka sehingga pelanggan dapat memperoleh berbagai layanan perbankan secara mandiri tanpa harus mengunjungi kantor bank.(Syahira et al., 2024). Layanan keuangan berbasis digital seperti crowd funding, peer-to-peer (P2P) lending, digital banking, online digital insurance, dan payment channel system telah berkembang pesat di Indonesia. (Zuhra & Nasution, 2024). Untuk meningkatkan kenyamanan nasabah, bank telah mengimplementasikan sistem mobile banking. Pelanggan memanfaatkan perangkat seluler (tablet, ponsel pintar, dll) untuk mengakses seluruh layanan perbankan melalui mbanking(Syahira et al., 2024). Seiring dengan meningkatnya jumlah pengguna perbankan digital, volume transaksi perbankan digital juga mengalami pertumbuhan. Dalam dua tahun terakhir, terdapat peningkatan jumlah transaksi perbankan digital. Pada tahun 2021, transaksi digital meningkat sebesar Rp39.841,4 triliun, mencatat pertumbuhan 45,64 persen dibandingkan tahun sebelumnya (Fiona & Rahmayanti, 2022).

Mobile banking adalah layanan perbankan yang memungkinkan nasabah melakukan transaksi perbankan, mengakses informasi rekening, dan terlibat dalam berbagai aktivitas keuangan melalui perangkat seluler, seperti telepon pintar dan tablet. Mobile banking memungkinkan warga negara untuk melakukan berbagai transaksi, termasuk transfer uang, pembayaran tagihan, pemantauan rekening, pembelian produk atau layanan, dan bahkan investasi, semuanya melalui aplikasi seluler bank. Layanan perbankan adalah aplikasi yang memungkinkan nasabah melakukan transaksi langsung melalui telepon pintar mereka(Inayah, 2023). Keamanan adalah kemampuan untuk mengatur data dengan cara yang tidak menguntungkan. Mayoritas umat Islam sudah mulai menggunakan layanan M-banking, karena transaksi yang dilakukan secara daring lebih mungkin dilakukan dengan informasi yang akurat. Oleh karena itu, bank harus terus berinovasi untuk memastikan bahwa transaksi daring seaman mungkin dan mendorong nasabah untuk menggunakan layanan M-banking(Anita Pramadani Lubis et al., 2023). Perbankan digital ibarat memiliki bank di saku Anda: semuanya terjadi secara online, tanpa perlu pergi ke cabang. Salah satu keunggulan perbankan digital adalah nasabah tidak memerlukan rekening bank untuk mengakses informasi, melakukan penyetoran, membuka rekening, melakukan transaksi, dan mentransfer dana. Produk bank seperti giro, investasi, dan perbankan operasional juga dapat diakses oleh Nasabah, yang dapat melihat informasi terkait dan melakukan transaksi terkait (Syahira et al., 2024). Peningkatan penggunaan layanan perbankan digital menghadapi ancaman keamanan siber. Di tahun 2020, terungkap bahwa sepanjang tahun tersebut terjadi 495 juta serangan siber, meningkat lima kali lipat dibandingkan tahun sebelumnya. Catatan tersebut sejalan dengan pernyataan yang diungkapkan oleh World Economic Forum (2021) dalam laporan Global Risk Report 2021. Serangan siber memanfaatkan rekayasa sosial, penipuan OTP, pertukaran SIM, kelemahan dalam sistem keuangan dan perbankan, serta phishing (Hendra Wicaksana et al., 2020)

.

Pesatnya penggunaan teknologi perangkat dalam skala global telah menimbulkan kekhawatiran tentang keamanannya. Agar dapat mengimbangi kemajuan ilmu pengetahuan dan teknologi, diperlukan sumber daya untuk melanjutkan kemajuan ini(Nurhaliza et al., 2023). Kesadaran pengguna

JPEK (Jurnal Pendidikan Ekonomi dan Kewirausahaan)
Vol. 8, No. 3 Desember 2024, Hal. 917–926
DOI: 10.29408/jpek.v8i2.27646
E-ISSN: 2549-0893

telah muncul sebagai faktor manusia yang penting dalam memastikan keselamatan dalam konteks ini. Dalam hal keamanan informasi, manusia merupakan target rentan yang dapat dimanfaatkan oleh para insinyur sosial untuk memperoleh akses atau informasi sensitif. Salah satu metode yang paling efektif untuk mencegah rekayasa sosial adalah melalui program keamanan informasi yang baik (Tolle et al., 2008). Kesadaran keamanan mobile banking sangat penting dalam meningkatkan keamanan transaksi keuangan melalui perangkat mobile. Kesadaran keamanan meliputi pengetahuan dan kesadaran individu tentang ancaman keamanan dan cara-cara untuk menghindari atau mengatasi mereka. Dalam konteks mobile banking, kesadaran keamanan melibatkan kemampuan pengguna untuk memahami risiko yang terkait dengan penggunaan aplikasi mobile banking untuk transaksi dan mengambil langkah-langkah yang tepat untuk melindungi informasi pribadi dan keuangan mereka. (Shofia et al., 2024). Di era digital yang berkembang pesat seperti saat ini, penerapan teknologi informasi menjadi semakin penting dalam kehidupan sehari-hari. Salah satu teknologi yang paling sering digunakan adalah mobile banking, yang memungkinkan pengguna melakukan transaksi perbankan melalui perangkat seluler mereka. Namun, dengan semakin seringnya aktivitas kejahatan dunia maya, keamanan informasi menjadi isu yang semakin kritis dan harus ditangani. Penggunaan data pribadi merupakan salah satu aspek terpenting dari dunia digital, di mana sebagian besar informasi disediakan oleh organisasi dan biasanya digunakan dalam proses verifikasi identitas (AK, 2015).

Dapat disimpulkan bahwa pengumpulan data merupakan akses ilegal ke data pribadi seseorang oleh organisasi yang bersangkutan, sehingga mendorong pencurian identitas. Tanggung jawab mendasar masyarakat untuk menjaga informasi identitas, verifikasi identitas dapat dilakukan melalui berbagai metode dan pendekatan, dan ini harus diakui. Informasi yang telah diperoleh akan dijual di pasar gelap daring atau dimodifikasi untuk menciptakan identitas sintetis. Salah satu aspek keamanan informasi yang sangat penting adalah tingkat *security awareness*, terutama dalam hal penggunaan password. Password merupakan salah satu lapisan pertahanan pertama dalam melindungi informasi pribadi pengguna. Namun, masih banyak pengguna yang tidak menyadari pentingnya keamanan password dan seringkali menggunakan password yang lemah atau mudah ditebak. Oleh karena itu, tujuan dari penelitian ini adalah untuk menguji tingkat kesadaran keamanan dalam perilaku penggunaan kata sandi oleh mahasiswa, khususnya dalam konteks perbankan seluler BSI. Berdasarkan hasil penelitian dari Ibnu Maulana (2021), Hasil penelitian menunjukan bahwa Bank-bank sudah memberikan layanan yang lebih kuat dibandingkan dengan pesaingnya untuk menciptakan kepuasan nasabah. Oleh karena itu, diharapkan Teknologi Layanan Mandiri (SST) akan memberikan solusi kepada penerima manfaat utama, yaitu mahasiswa, untuk memudahkan transaksi sehari-hari tanpa perlu mengalokasikan waktu untuk mengunjungi bank. Dalam Penelitian Annisa Shofia (2019), hasil penelitian menunjukkan bahwa dalam konteks mahasiswa, penggunaan mobile banking juga semakin meningkat seiring dengan perkembangan teknologi. Namun, belum banyak penelitian yang mengkaji tingkat *security awareness* dalam *password behavior* mahasiswa, terutama dalam penggunaan *mobile banking*. (Shofia et al., 2024).

Dalam hal ini peneliti juga akan melaksanakan dan melakukan penelitian kepada mahasiswa FEBI UINSU untuk mengetahui secara langsung bagaimana fenomena kesadaran mahasiswa dalam penggunaan mobile banking. Dan diketahui 8 dari 10 mahasiswa FEBI UINSU menggunakan layanan banking yakni mobile banking. Hal ini menunjukkan tingginya tingkat penggunaan mobile banking di mahasiswa FEBI, Tentu ini menjadikan bahwa pentingnya Security Awareeness mobile banking di kalangan mahasiswa khususnya mahasiswa FEBI UINSU. Berdasarkan latar belakang masalah tersebut, maka penulis tertarik untuk melakukan penelitian lebih mendalam dengan mengangkat judul "Analisis Tingkat *Security Awereness* dalam *Password Behavior* Mahasiswa (Studi Kasus Mahasiswa FEBI UINSU Medan)".

Kata Sandi (*Password*)

Kata sandi adalah metode otentikasi terbanyak digunakan dalam berbagai sistem keamanan (Sudiarto Raharjo et al., 2017). Password banyak digunakan karena mudah diimplementasi.

JPEK (Jurnal Pendidikan Ekonomi dan Kewirausahaan)
Vol. 8, No. 3 Desember 2024, Hal. 917–926
DOI: 10.29408/jpek.v8i2.27646
E-ISSN: 2549-0893

National Institute of Standards and Technology (NIST) mengemukakan bahwa standar kata sandi sebenarnya cukup sederhana. Kata sandi yang diberikan oleh pengguna setidaknya harus terdiri dari delapan karakter alfanumerik, kata sandi yang dibuat secara acak oleh sistem harus terdiri dari setidaknya enam karakter dan seluruhnya dapat berupa angka. Tetapi baru-baru ini NIST telah memperbarui standarnya dan persyaratan baru yang paling signifikan. Sistem harus memeriksa kata sandi prospektif terhadap daftar yang berisi kata sandi yang umum digunakan, mudah ditebak, atau disusupi, lalu NIST secara eksplisit merekomendasikan persyaratan kata sandi kompleksitas tinggi. Dalam dunia keamanan ada beberapa faktor-faktor yang mempengaruhi otentikasi yaitu *Something you know* – Ini adalah bentuk paling dasar dari otentikasi yang akrab dengan Sebagian pengguna, sesuatu yang diketahui pengguna misalnya: kata sandi atau kode PIN. *Something you have* – Bentuk otentikasi ini diwakili oleh barang yang dimiliki pengguna misalnya smartphone atau kartu identitas. *Something you are* – Otentikasi ini direpresentasikan sebagai tanda identitas dari fisik pengguna misalnya: sidik jari atau iris mata. *Someplace you are* – Bentuk otentikasi ini sesuai dengan lokasi pengguna untuk memverifikasi misalnya lokasi pengguna atau alamat IP.

Beberapa jurnal atau *paper* yang telah membuktikan bahwa kata sandi adalah faktor otentikasi di antaranya yang ditulis oleh Nilesh A. Lal, S. Prasad, & Mohammed Farik. Dalam judul A Review of Authentication Method, dan dipublikasikan pada tahun 2016. Dalam penelitiannya mereka melakukan tinjauan dalam metode otentikasi dimana kata sandi adalah salah satunya, dalam penelitiannya kata sandi merupakan metode otentikasi yang mengharuskan mengingat apa yang diketahuinya dan tidak diketahui orang lain, dengan ini kata sandi termasuk faktor keamanan yang rentan apabila pengguna lupa ataupun membocorkan kata sandinya kepada orang lain. Jurnal atau paper kedua yang ditulis oleh Pamela R. Mc,C. Bell, Linda C. M., & Ronald F. DeMara. yang berjudul Evaluation of the Human Impact of Password Authentication Practices on Information Security dipublikasikan pada tahun 2004, dalam penelitiannya mereka mengevaluasi dampak kata sandi sebagai faktor otentikasi keamanan informasi (Lal et al., 2016)

Kesadaran keamanan *(Security Awereness)*

Kesadaran keamanan sangatlah penting dalam hidup manusia dikarenakan banyaknya cara yang bisa dimanfaatkan untuk memperoleh keuntungan maupun merusak informasi seseorang. Pengetahuan akan kesadaran keamanan seharusnya diajarkan dari jenjang sekolah serta implementasinya (Amin, 2014). Kesadaran keamanan informasi dapat dirancang sebagai penilaian pemahaman, komitmen seseorang, dan perilaku berdasarkan informasi yang berlaku Kebijakan, pedoman, dan aturan keamanan. Ada tiga metode penilaian kesadaran keamanan informasi pengguna, yaitu kuesioner, pasif Pengukuran, dan simulasi serangan.

Kesadaran keamanan sangatlah penting dalam hidup manusia dikarenakan banyaknya cara yang bisa dimanfaatkan untuk memperoleh keuntungan maupun merusak informasi seseorang. Pengetahuan akan kesadaran keamanan seharusnya diajarkan dari jenjang sekolah serta implementasinya (Kusumaningrum et al., 2022). Program pelatihan dan kesadaran keamanan dapat dibagi dalam tiga bagian yang berbeda : Pendidikan: Subjek harus memahami bahwa keamanan informasi sangat penting bagi organisasi. Setiap orang harus bertanggung jawab atas keamanan yang mempengaruhi lingkungan organisasi. Kesadaran keamanan bisa dipelajari melalui kursus atau juga pendidikan keamanan informasi dasar di sekolah atau perguruan tinggi. Pelatihan: Subjek harus mengetahui cara agar bisa merasa aman. Subjek harus mengetahui cara menggunakan fitur keamanan suatu aplikasi dan begitupun sebaliknya dimana aplikasi menyediakan pembelajaran cara menggunakan fitur keamanan. *Something you are* – Otentikasi ini direpresentasikan sebagai tanda identitas dari fisik pengguna misalnya: sidik jari atau iris mata. Kesadaran: Gerakan menyerukan kesadaran keamanan juga perlu dilakukan. Program insentif akan mendorong subjek untuk berpartisipasi dengan

JPEK (Jurnal Pendidikan Ekonomi dan Kewirausahaan)
Vol. 8, No. 3 Desember 2024, Hal. 917–926
DOI: 10.29408/jpek.v8i2.27646
E-ISSN: 2549-0893

fasi “menjadi sadar” lalu “menyadari” hingga “sadar” secara naluri atau terbiasa.

Perilaku *(Behavior)*

Bagian dari melakukan adalah perencanaan, pengorganisasian, dan komunikasi. Jika tindakan adalah suatu perubahan fisik dalam jangka waktu singkat, maka kegiatan adalah suatu tindakan yang diulang-ulang dalam jangka waktu yang relatif lama. Perilaku muncul karena perilaku yang menerapkan perilaku adalah perilaku untuk bertahan hidup. (Ginting, 2015). Keamanan informasi melindungi bisnis dari berbagai bahaya untuk mengurangi risiko, meningkatkan investasi, dan peluang bisnis (Dola Ramalinda et al., 2024). Tiga aspek keamanan informasi ialah: *Confidentialy* (Kerahasiaan), Data yang menghasilkan informasi harus dilindungi dari pihak yang tidak berwenang untuk mengaksesnya. *Integerity* (Integritas), Informasi yang dimiliki tidak boleh diubah oleh individu yang tidak memiliki hak. Ini bertujuan untuk memastikan bahwa informasi yang dimiliki dan diakses adalah benar, akurat, dan komprehensif. *Aviability* (Ketersediaan), Memastikan tersedianya informasi yang diperlukan agar aspek ketersediaan ini terpenuhi dalam sebuah organisasi menerapkan cadangan data atau menyediakan backup untuk data yang akan menghasilkan informasi (Parhusip, 2024). Kesadaran ini mencakup perlindungan terhadap keamanan informasi pribadi serta informasi organisasi tempat individu tersebut bernaung. Membagi kesadaran menjadi tiga dimensi, yaitu:

A. Knowledge

Pengetahuan mengacu pada pemahaman individu terhadap keamanan informasi yang dimilikinya. Pembelajaran memiliki beberapa tingkatan: Paham, mengacu pada pemahaman individu terhadap suatu subjek berdasarkan tindakannya terhadap aspek materi atau situasi tertentu. Memahami merupakan kemampuan untuk menjelaskan secara benar mengenai suatu objek, menginterpretasi materi yang ada secara benar, menjelaskan, dan menyebutkan contoh. Aplikasi, mengacu pada kemampuan untuk menggunakan materi yang diperoleh sebelumnya dalam situasi tertentu. Analisis, Kemampuan mengelompokkan bahan atau benda ke dalam komponen-komponen yang saling berkaitan satu sama lain. Sintesis, meningkatkan kemampuan menangani dan menghubungkan informasi baru.

B. Attitude

Attitude adalah cara seseorang berinteraksi dan berkomunikasi dengan orang lain. Sikap adalah bagaimana seseorang bertindak terhadap situasi tertentu. Komponen sikap terdiri dari beberapa hal, di antaranya: 1. Kognitif: data yang diterima seseorang dalam hidupnya digunakan untuk membuat keputusan tentang apa yang harus mereka lakukan. 2. Efektif Afektif berkaitan dengan masalah emosional subjektif yang dialami suatu objek. Sebagai aturan umum, pose yang dimiliki suatu objek dikaitkan dengan komponen afektifnya. 3. Deskriptif menunjukkan bagaimana kegagalan individu dalam mencapai suatu tujuan berkaitan dengan cara mereka menangani objek yang dipegangnya.

C. Behavior

Perilaku mengacu pada cara seseorang menggunakan teknologi informasi. Setiap orang memiliki kemampuan untuk menentukan apa yang akan dilakukan atau dimbilnya dalam respons terhadap stimulus. Perilaku alami, juga dikenal sebagai perilaku innate dalam psikologi, terbagi menjadi dua kategori: Perilaku Alami: Perilaku alami adalah perilaku yang dibawa sejak lahir. Perilaku Operan: Perilaku operan, juga disebut perilaku operan, adalah perilaku yang dibentuk melalui proses belajar.

JPEK (Jurnal Pendidikan Ekonomi dan Kewirausahaan)
Vol. 8, No. 3 Desember 2024, Hal. 917–926
DOI: 10.29408/jpek.v8i2.27646
E-ISSN: 2549-0893

Orang-orang akan belajar tentang keamanan data, kemudian mereka akan memahami dan menerapkan pengetahuan ini untuk melindungi data mereka, sehingga kesadaran tentang keamanan data dapat membantu mereka menjalani kehidupan sehari-hari. (Parhusip, 2024) mengembangkan kesadaran tentang keamanan data pada tingkat kesadaran berikut:

Tabel. 1 ***Level of Awareness***

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

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif deksriptif, Penelitian ini menggunakan kuesioner, yang terdiri dari pertanyaan dengan pilihan jawaban berdasarkan skala Likert dari 1 hingga 5. Studi ini memiliki 45 pertanyaan untuk menguji perspektif pengguna terhadap sikap, pengetahuan, dan perilaku smartphone. Beberapa pertanyaan diberi tanggapan berdasarkan skala Likert 1–5, yang berarti sangat tidak setuju, tidak setuju, netral, setuju, dan sangat setuju dengan tiga dimensi sikap, pengetahuan, dan perilaku (Attitude, Knowledge dan Behavior). Nama, jenis kelamin, usia, dan program studi adalah beberapa pertanyaan demografis dalam penelitian ini. Selain itu, model kerangka KAB (Knowledge, Atittude, and Behavior) digunakan untuk membuat 45 pertanyaan untuk mengukur kesadaran keamanan pengguna selular (Amin, 2014).

Tabel 2. Daftar Pertanyaan

Dimensi	Pertanyaan	Opsi
Knowledge	1. mobile banking penting untuk dijaga keamanannya . 2. Saya mencari informasi atau bantuan melalui komunitas online atau forum ketika mengalami masalah keamanan dengan mobile banking saya 3. saya selalu logout setelah selesai menggunakan mobile banking saya 4. Perangkat mobile harus dilengkapi dengan kunci layar (PIN, pola, sidik jari, atau pengenalan wajah) untuk mencegah akses tidak sah. 5. saya selalu menggunakan kanal komunikasi yang aman dalam konteks mobile banking 6. bagi saya pentingnya untuk menggunakan kata sandi yang kuat dan unik untuk akun media sosial Anda dalam konteks perlindungan mobile banking 7. Saya mengerti yang dimaksud dengan pelaporan insiden dalam konteks mobile banking 8. saya mengetahui apa itu phishing dan bagaimana cara mengidentifikasinya dalam konteks mobile banking? 9. Menggunakan password atau PIN yang mudah diingat, seperti nama, tanggal lahir, atau angka berurutan, merupakan hal yang perlu diperhatikan.	• Sangat Tidak Setuju • Tidak Setuju • Netral • Setuju

JPEK (Jurnal Pendidikan Ekonomi dan Kewirausahaan)
Vol. 8, No. 3 Desember 2024, Hal. 917–926
DOI: 10.29408/jpek.v8i2.27646
E-ISSN: 2549-0893

	10. Menggunakan lockscreen pada smartphone, baik berupa biometrik, PIN, pola, maupun password, merupakan suatu masalah. 11. Penggunaan aplikasi M-Banking yang terhubung ke jaringan Wi-Fi publik 1. Password/PIN M-Banking tidak boleh dibagikan kepada orang lain. 2. Letakkan dan simpan smartphone hanya di tempat yang aman 3. Menyimpan password/PIN dalam bentuk catatan berupa teks adalah sesuatu yang perlu dihindari. 4. Kode OTP adalah sesuatu yang tidak boleh dibagikan kepada siapa pun.	• Sangat Setuju

Tabel 3. Daftar Pertanyaan

Dimensi	Pertanyaan	Opsi
Atittude	1. Selalu logout dari aplikasi mobile banking setelah selesai menggunakannya 2. Saya selalu menghindari akses mobile banking dari perangkat umum atau komputer publik 3. Saya selalu memeriksa dan memastikan keaslian notifikasi transaksi yang dikirim oleh bank melalui SMS atau email 4. Saya selalu memperbarui sistem operasi perangkat seluler untuk memastikan mendapatkan pembaruan keamanan terbaru 5. Selalu memverifikasi keaslian kontak atau saluran komunikasi yang mengatasnamakan bank sebelum memberikan informasi pribadi 6. Penting bagi saya untuk menjaga privasi informasi akun mobile banking Anda ketika menggunakan media sosial 7. Penting bagi saya untuk menyimpan bukti atau dokumentasi terkait insiden keamanan sebelum melaporkannya 8. Saya merasa bahwa pendidikan dan pelatihan tentang keamanan mobile banking penting untuk meningkatkan kesadaran 9. Saya ingin menggunakan kunci layar pada ponsel pintar saya, baik berupa kata sandi, PIN, pola, atau biometrik agar lebih aman. 10. Saya ingin menggunakan kata sandi atau PIN yang berbeda untuk setiap akun yang digunakan. 11. Saya ingin menggunakan M-Banking hanya dengan data seluler dari kartu SIM itu sendiri. 12. Saya tidak memberikan kata sandi atau PIN M-Banking saya kepada orang lain selain diri saya sendiri. 13. Saya hanya ingin menggunakan dan membawa ponsel pintar di tempat yang aman.	• Sangat Tidak Setuju • Tidak Setuju • Netral • Setuju • Sangat Setuju

JPEK (Jurnal Pendidikan Ekonomi dan Kewirausahaan)
Vol. 8, No. 3 Desember 2024, Hal. 917–926
DOI: 10.29408/jpek.v8i2.27646
E-ISSN: 2549-0893

	14. Sebagai kata sandi, saya menggunakan tanggal lahir dan tanggal khusus. 15. Saya membatasi konten-konten yang saya akses menggunakan	

Tabel 4. Daftar Pertanyaan

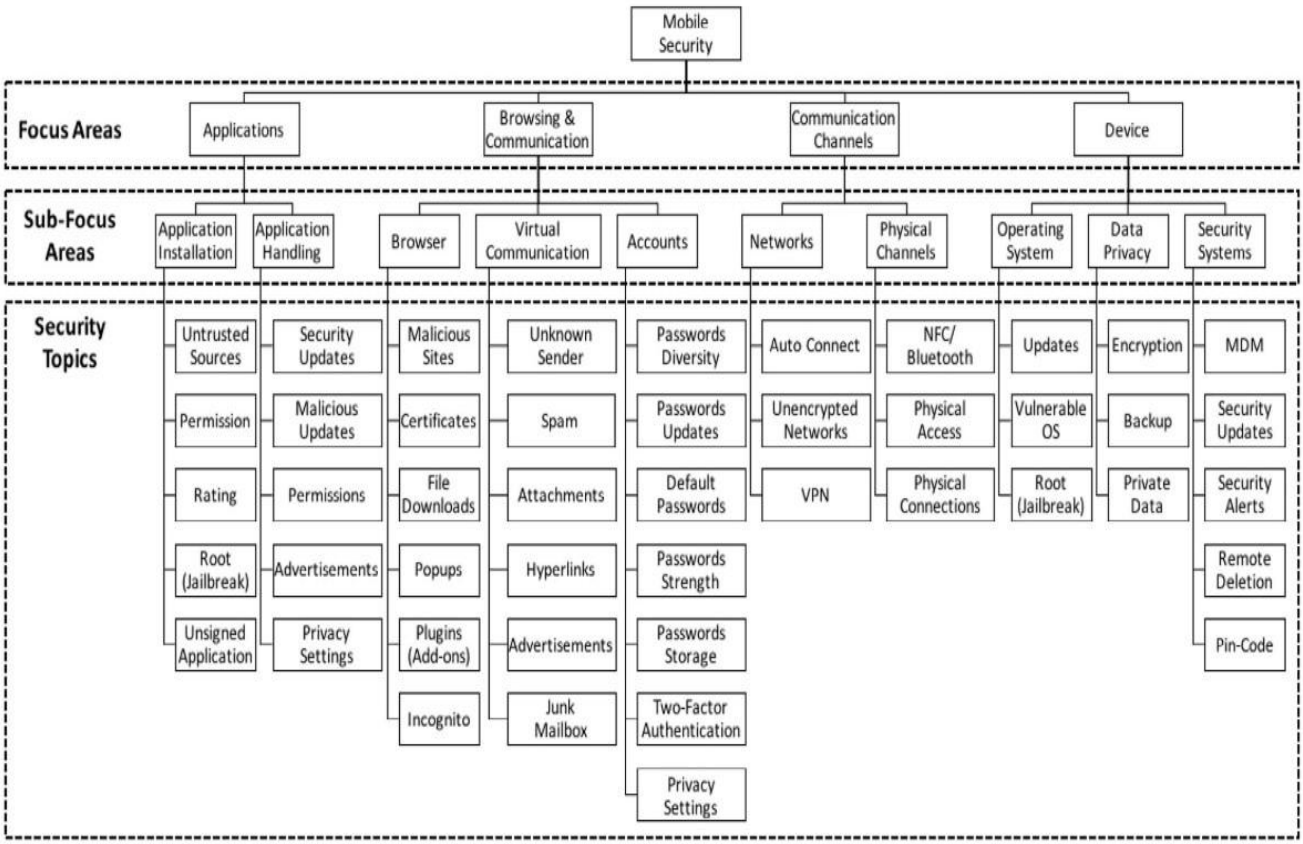
Dimensi	Pertanyaan	Opsi
Behavior	1. Data pribadi sangat penting untuk dilindungi dalam penggunaan mobile banking 2. perlu untuk selalu membersihkan riwayat penjelajahan dan cache setelah melakukan transaksi mobile banking 3. Menginformasikan orang lain (misalnya, keluarga, teman) tentang pentingnya keamanan dalam berkomunikasi terkait mobile banking? 4. penting bagi saya untuk memastikan bahwa perangkat seluler Anda dilindungi dengan kata sandi atau PIN 5. saya selalu memeriksa enkripsi atau keamanan saluran komunikasi (seperti HTTPS) ketika mengakses informasi mobile banking melalui web 6. selalu membagikan informasi tentang rekening bank atau transaksi keuangan di media social 7. mengetahui saluran komunikasi atau nomor kontak khusus untuk melaporkan insiden keamanan mobile banking kepada bank adalah hal yang diharuskan 8. penting bagi saya untuk memahami cara melindungi perangkat seluler Anda dari malware dan serangan siber? 9. Saya enggan menggunakan kata sandi atau PIN yang sama untuk beberapa akun yang berbeda. 10. Saya enggan menggunakan M-Banking saat terhubung ke jaringan Wi-Fi publik. 11. Saya enggan membagikan kata sandi atau PIN M-Banking saya dengan orang lain. 12. Saya enggan meninggalkan kode OTP kepada siapa pun. 13. Saya ragu menggunakan kata sandi atau PIN dalam format yang mirip dengan 15. Saya ragu membiarkan orang lain menggunakan ponsel pintar pribadi saya tanpa persetujuan saya.	• Sangat Tidak Setuju • Tidak Setuju • Netral • Setuju Sangat Setuju

JPEK (Jurnal Pendidikan Ekonomi dan Kewirausahaan)
Vol. 8, No. 3 Desember 2024, Hal. 917–926
DOI: 10.29408/jpek.v8i2.27646
E-ISSN: 2549-0893

HASIL PENELITIAN DAN PEMBAHASAN

Pelanggan organisasi yang sadar akan tujuan keamanan informasinya disebut kesadaran keamanan informasi(ADI TIATAMA, 2016). Pengukuran kesadaran keamanan informasi jamak dilakukan dengan menggunakan model penelitian. (Amin, 2014) menggunakan tiga dimensi sebagai dasar pengukuran: pengetahuan, sikap, dan perilaku. Pengetahuan atau pengetahuan adalah apa yang diketahui atau dipahami seseorang, dan sikap atau sikap adalah apa yang mereka rasakan atau pikirkan. Perilaku atau perilaku adalah apa yang dilakukan seseorang. (Ubaidillah, 2019) Fokus utama inisiatif kesadaran keamanan informasi adalah untuk mengubah perilaku; namun, panduan terbaik untuk mengubah perilaku adalah memahami tingkat pengetahuan dan perilaku. Kami melakukan survei kepada mahasiswa FEBI UINSU (Universitas Islam Negeri Sumatera Utara) untuk menilai tingkat kesadaran mereka tentang keamanan menggunakan layanan perbankan mobile. Hasil kuesioner menunjukkan beberapa kesimpulan penting. Ada tiga dimensi dalam penelitian ini: pengetahuan (pengetahuan) mengukur apa yang diketahui pengguna M-Banking tentang keamanan dan privasi, perspektif (sikap) mengukur perasaan mereka tentang keamanan dan privasi, dan perilaku (perilaku) mengukur apa yang dilakukan pengguna M-Banking terkait masalah keamanan dan privasi. Untuk penelitian ini, responden adalah mahasiswa Universitas Islam Negeri Sumatera Utara Medan, seperti yang ditunjukkan di bawah ini:

(Bitton et al., 2020) juga membuat kerangka dimensi KAB untuk mengukur tingkat kesadaran keamanan pengguna selular, yang membagi keamanan selular menjadi empat area fokus: (1) aplikasi; (2) penjelajahan dan komunikasi; (3) kanal komunikasi; dan (4) perangkat.



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

JPEK (Jurnal Pendidikan Ekonomi dan Kewirausahaan)
Vol. 8, No. 3 Desember 2024, Hal. 917–926
DOI: 10.29408/jpek.v8i2.27646
E-ISSN: 2549-0893

Tabel 5. Level Kesadaran KAB

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

(Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014). Pertama, penggunaan sandbox; kedua, email; ketiga, internet; keempat, media sosial; kelima, penggunaan telepon seluler; keenam, pengelolaan informasi; dan ketujuh, komunikasi internal. Faktor Manusia dalam Keamanan Informasi (HAIS-Q) mengacu pada bidang pekerjaan ini. Bertujuan untuk meningkatkan keamanan informasi karyawan dan anggota organisasi, HAIS-Q dikembangkan (Parsons et al. 2014). Dimensi KAB dapat digunakan untuk menempelkan jari pada suatu area fokus. Nilai kesadaran pembobotan ditentukan oleh dimensi bobot (Amin, 2014). Tabel 2 menampilkan dimensi Bobot.

Tabel 6. Bobot Dimensi KAB

Level	Nilai (%)
Knowledge	30
Attitude	20
Behaviour	50

Kruger dan Kerney (2005) menentukan tingkat bobot yang tepat untuk setiap dimensi pengetahuan, keterampilan, dan kinerja. Dimensi ketiga ditunjukkan pada tabel 2. Studi ini menggunakan komponen HAIS-Q dan area fokus untuk keamanan, yang menghasilkan. Fitur ini digunakan untuk meningkatkan keamanan lingkungan desktop pada HAIS-Q dan keamanan secara keseluruhan. Tabel 3 menunjukkan hasil HAIS-Q dan area fokus untuk keamanan.

Tabel 7. Bobot Dimensi KAB

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

Area fokus kemudian digunakan untuk menentukan ambang perbandingan. Temuan penelitian ini didasarkan pada penelitian sebelumnya (Arisya, Ruldeviyani, Prakoso, &

JPEK (Jurnal Pendidikan Ekonomi dan Kewirausahaan)
Vol. 8, No. 3 Desember 2024, Hal. 917–926
DOI: 10.29408/jpek.v8i2.27646
E-ISSN: 2549-0893

Fadhilah, 2020) dan selanjutnya diterapkan pada area fokus yang dipilih. Hal ini kami lakukan karena ada korelasinya dengan penelitian ini yang turut mengangkat tingkat keamanan informasi bagi pengguna aplikasi perbankan (mobile banking).

Tabel 8. Pembobotan Area Fokus

Area Fokus HAIS-Q	Nilai(%)	Area Fokus	Nilai(%)
Manajemen Password dan Email	25,05%	Penjelajahan dan komunikasi	25,05%
Penggunaan Internet	5,22%	Kanal komunikasi	5,22%
Penanganan Informasi	25,30%	Aplikasi	25,30%
Penggunaan perangkat	15,40%	Perangkat	15,40%
Penggunaan media social	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 9. Demografi Responden

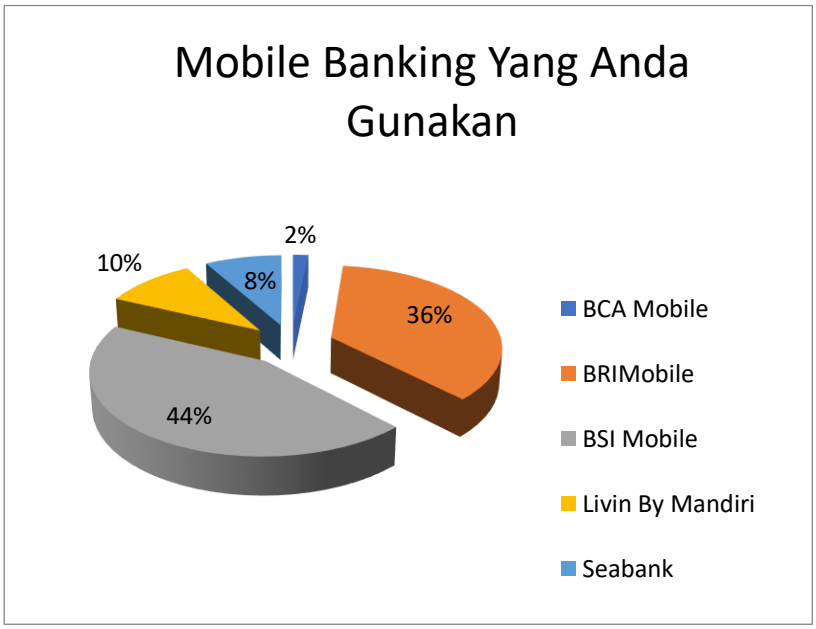
Kriteria	Kategori	Prosentase
Jenis Kelamin	Laki-laki	31%
	Perempuan	69%
Usia	18 - 20	34%
	21 - 25	66%

JPEK (Jurnal Pendidikan Ekonomi dan Kewirausahaan)
Vol. 8, No. 3 Desember 2024, Hal. 917–926
DOI: 10.29408/jpek.v8i2.27646
E-ISSN: 2549-0893

Program Studi	Perbankan Syariah	56%
	Manajemen	11%
	Ekonomi Islam	13%
	Asuransi Syariah	3%
	Akuntansi Syariah	16%
Total Responden	61	100%

B. Karakteristik Penggunaan Aplikasi Perbankan Digital

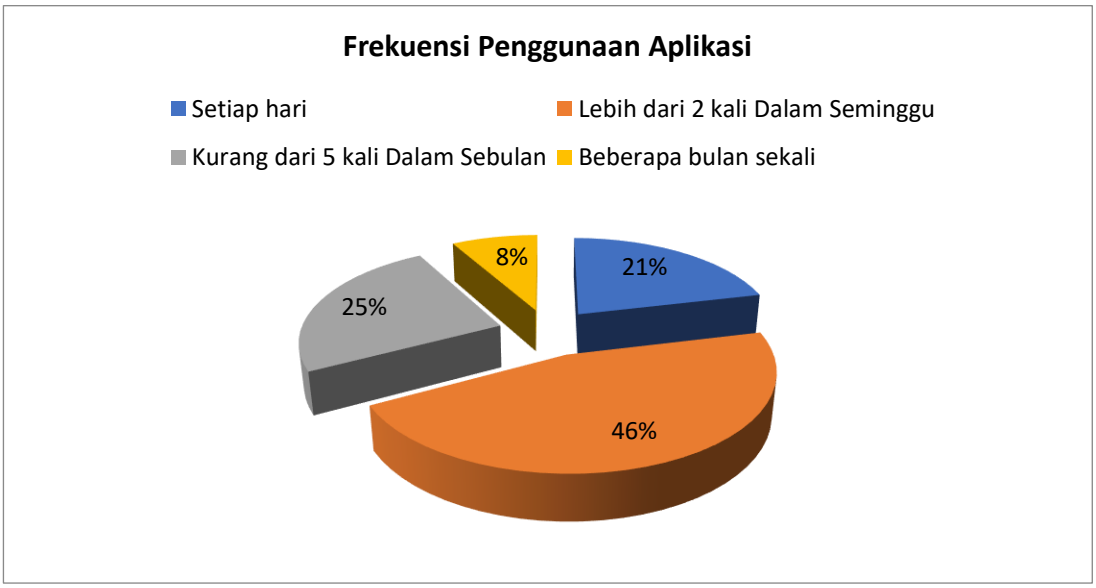
Pada sebaran aplikasi perbankan yang digunakan, aplikasi perbankan yang paling banyak digunakan adalah BSI Mobile 27 responden. Kemudian diikuti oleh BRImo Mobile 22 responden, Livin By Mandiri sebanyak 6 responden, Seabank dengan 5 responden, dan BCA Mobile sejumlah 1 responden. Data disajikan pada Gambar 3.



Gambar 3. Aplikasi Perbankan yang Digunakan

Data seperti yang ditunjukkan pada Tabel 4 dikumpulkan berdasarkan frekuensi penggunaan aplikasi perbankan. Sebanyak 13 responden mengatakan bahwa mereka menggunakan aplikasi perbankan setiap hari.kemudian ada 28 responden yang menggunakan Lebih dari 2 kali Dalam Seminggu,kemudian ada 15 responden yang menggunakan Kurang dari 5 kali Dalam Sebulan, dan ada 5 responden yang menggunakannya Beberapa bulan sekali.

JPEK (Jurnal Pendidikan Ekonomi dan Kewirausahaan)
Vol. 8, No. 3 Desember 2024, Hal. 917–926
DOI: 10.29408/jpek.v8i2.27646
E-ISSN: 2549-0893



Gambar 4. Frekuensi penggunaan aplikasi

Langkah selanjutnya adalah mengumpulkan data dan menganalisis hasil kuesioner. Kuesioner terdiri dari 45 pertanyaan tentang keamanan informasi dan 15 pertanyaan tentang sikap, perilaku, dan pengetahuan di masa mendatang. Keamanan Mobile banking Salah satu aspek terpenting dalam memberikan edukasi berdasarkan prinsip keamanan informasi dan privasi adalah tersedianya umpan balik dan komunikasi terbuka dengan nasabah, yang memungkinkan mereka mempelajari apa yang perlu dipelajari. Populasi atau objek studi dalam penelitian ini adalah mahasiswa yang menggunakan layanan mobile banking. Setelah pengumpulan data dengan kuisioner, data kemudian ditransformasikan menggunakan metode Deskriptif untuk menangkap perubahan dimensi. Tahap akhir penelitian melibatkan pemberian umpan balik pada semua langkah sebelumnya.

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 10. Tingkat Kesadaran Keamanan Informasi

Area Fokus	Knowledge	Atittude	Behavior	Kesadaran (Dimensi)
Aplikasi	73%	70%	68%	70%
Penjelajahan dan Komunikasi	64%	66%	71%	67%
Perangkat	**81%**	70%	68%	73%
Kanal Komunikasi	73%	72%	69%	71%
Media Sosial	71%	64%	70%	68%
Pelaporan Insiden	68%	73%	70%	70%
Kesadaran Keamanan Informasi (Dimensi)	72%	69%	69%	70%

Berdasarkan hasil pengukuran Tingkat keamanan informasi pada table 6 diperoleh nilai akhir rata-rata sebesar 72% untuk dimensi pengetahuan (*knowledge*), 69% pada dimensi sikap (*attitude*), 69% pada

JPEK (Jurnal Pendidikan Ekonomi dan Kewirausahaan)
Vol. 8, No. 3 Desember 2024, Hal. 917–926
DOI: 10.29408/jpek.v8i2.27646
E-ISSN: 2549-0893

dimensi perilaku (*behavior*), dan 70% pada dimensi kesadaran. Hasil tersebut didapat dari rata-rata yang berasal dari keenam area fokus diatas.

Berbagai warna pada tabel 6 menunjukkan tingkat keamanan informasi dan informasi yang diberikan yang lebih tinggi. Nilai dan informasi ditunjukkan 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

Berdasarkan hasil pengukuran Tingkat keamanan informasi pada table 6 diperoleh nilai akhir rata-rata sebesar 72% untuk dimensi pengetahuan (*knowledge*), 69% pada dimensi sikap (*attitude*), 69% pada dimensi perilaku (*behavior*), dan 70% pada dimensi kesadaran. Hasil tersebut didapat dari rata-rata yang berasal dari keenam area fokus diatas. Jika dibaca menggunakan level kesadaran keamanan informasi, nilai akhir menunjukkan level cukup yang artinya memerlukan pengawasan. Dari hasil yang didapatkan dari tingkat kesadaran pada area focus hanya area focus yang mendapatkan nilai 81% yang artinya baik dan memuaskan. Area focus penjelajahan & komunikasi dimensi knowledge dan media sosial dimensi attitude mendapatkan nilai paling rendah yang artinya memerlukan Pengawasan serta tindakan maupun yang masih berpotensi (Tingkat rata-rata dan kurang) hal ini harus mendapatkan perhatian khusus dari pemerintah dan penyedia layanan. Bidang yang menjadi fokus penelitian ini meliputi : Aplikasi, Perangkat, Saluran Komunikasi, Media Sosial, Browsing dan Komunikasi. Studi ini menemukan bahwa proses perlindungan informasi pengguna mobile banking memiliki implikasi keamanan yang signifikan. Hal ini menyoroti pentingnya bank mengintegrasikan aktivitas pengguna ke dalam strategi keamanan informasi yang komprehensif. Studi ini berkontribusi untuk meningkatkan praktik keamanan informasi mobile banking dengan menyediakan data tentang tindakan pengguna dan demografi.

Berdasarkan hasil analisis data responden, artikel ini berpendapat bahwa layanan perbankan dan pemerintah harus memiliki kemampuan untuk meningkatkan kesadaran dalam penggunaan m-banking melalui media cetak dan televisi. Mereka harus mengedukasi agar nasabah mereka mengetahui dan menyadari penggunaan m-banking karena merupakan salah satu produk bank yang sangat penting bagi nasabah. Dengan demikian untuk tetap menjaga kesadaran pengguna akan pentingnya menjaga keamanan informasinya, berikut ini beberapa rekomendasi yang dapat dilakukan :

1. Gunakan fitur notifikasi aplikasi untuk memberi tahu pengguna apa yang harus dihindari dan faktor lain yang dapat memengaruhi keputusan mereka tentang perlindungan informasi mereka.
2. Penyedia layanan dan lembaga pemerintah harus terus meningkatkan kesadaran dan mendidik melalui cara konvensional seperti pelatihan dan seminar, serta media online

JPEK (Jurnal Pendidikan Ekonomi dan Kewirausahaan)
Vol. 8, No. 3 Desember 2024, Hal. 917–926
DOI: 10.29408/jpek.v8i2.27646
E-ISSN: 2549-0893

interaktif seperti video, media sosial, dan permainan. Fokus pada dimensi dan area utama untuk meningkatkan kualitas.

3. Evaluasi evaluasi menyeluruh terhadap tingkat kesadaran pengguna mengenai keamanan informasi diperlukan .pengguna tingkat kesadaran yang lebih tinggi mengenai keamanan informasi sangatlah diperlukan.

KESIMPULAN

Hasil dari penelitian ini menunjukkan bahwa mahasiswa FEBI UINSU memiliki Tingkat kesadaran keamanan informasi dalam kategori cukup dan mengetahui dampak yang terjadi apabila menggunakan system teknologi informasi dan layanan perbankan. Terlihat pada hasil Dimensi *Knowledge* area fokus Perangkat mendapatkan hasil sebesar 81% dan ini masuk dalam kategori Tingkat kesadaran Baik yang artinya memuaskan dan tidak memerlukan Tindakan. Area fokus perangkat pada dimensi perangkat itu seperti "Perangkat mobile harus dilengkapi dengan kunci layar (PIN, pola, sidik jari, atau pengenalan wajah) untuk mencegah akses tidak sah". Selanjutnya pada Dimensi area fokus *Atittude* dengan nilai tertinggi yakni area fokus pelaporan insiden sebesar 73%, tetapi nilai ini masuk kedalam kategori cukup yang artinya butuh pengawasan dan ada kemungkinan dibutuhkan Tindakan. Area fokus perangkat pada dimensi atittude itu seperti "penting bagi saya untuk menyimpan bukti atau dokumentasi terkait insiden keamanan sebelum melaporkannya". Dan terakhir pada Dimensi *Behavior* are fokus media sosial dan pelaporan insiden mendapatkan nilai yang sama-sama tinggi sebesar 70% tetapi nilai ini juga masih dalam kategori cukup yang artinya masih butuh sebuah pengawasan serta Tindakan. Dimensi *behavior* Area fokus media sosial seperti, "selalu membagikan informasi tentang rekening bank atau transaksi keuangan di media sosial" dan area fokus pelaporan insiden seperti "mengetahui saluran komunikasi atau nomor kontak khusus untuk melaporkan insiden keamanan mobile banking kepada bank adalah hal yang diharuskan". Saran untuk peneliti selanjutnya adalah responden tidak hanya di kalangan mahasiswa saja tetapi juga dikalangan civitas akademika di lingkungan UINSU untuk mengetahui seberapa besar tingkat kesadaran keamanan informasinya, dikembangkan untuk menganalisis faktor-faktor tersebut seperti mengapa ketidaksadaran keamanan informasi terhadap pengguna mobile banking masih tergolong tinggi.

REFERENSI

ADI Tiatama. (2016). Perencanaan Tata Kelola Manajemen Keamanan Informasi Menggunakan Information Technology Infrastructure LIBRARY (ITIL) v3. pada D~NET SURABAYA. *Repository.Its.Ac.Id*, *3*.

AK. (2015). No Title空間像再生型立体映像の 研究動向. *Nhk技研*, *151*, 10–17.

Amin, M. (2014). Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (Mcda). *Jurnal Penelitian Dan Pengembangan Komunikasi Dan Informatika*, *5*(1), 15–24.

Anita Pramadani Lubis, Sri Ramadhani, & Nurul Inayah. (2023). Pengaruh Kemudahan, Keamanan, Dan Kenyamanan Mobile Banking Syariah Terhadap Customer Intention (Minat Nasabah) Dengan Lifestyle Sebagai Variabel Moderating. *Surplus : Jurnal Ekonomi Dan Bisnis*, *2*, 14–30.

Bitton, R., Boymgold, K., Puzis, R., & Shabtai, A. (2020). Evaluating the Information Security Awareness of Smartphone Users. *Conference on Human Factors in Computing Systems - Proceedings*, 1–20. https://doi.org/10.1145/3313831.3376385

Dola Ramalinda, Jayadi, & Agung Rachmat Raharja. (2024). Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi. *Journal of International Multidisciplinary Research*, *2*(6), 665–671. https://doi.org/10.62504/jimr679

Fiona, F., & Rahmayanti, D. (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.

Ginting, I. M. (2015). Jurnal Manajemen Jurnal Manajemen. *Pengaruh Celebrity Endorsement, Brand Image, Dan Testimoni Terhadap Minat Beli Konsumen Produk Mie Instan Lemonilo Pada Media Sosial Instagram*, *6*(1), 131–143.

Hendra Wicaksana, R., Imam Munandar, A., Samputra, P. L., Salemba, J., No, R., & Indonesia, J. (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 Ilmu Pengetahuan Dan Teknologi Komunikasi*, *22*(2), 143–158. http://dx.doi.org/10.33164/iptekkom.22.2.2020.143-158

Inayah, I. S. S. S. J. N. (2023). Pengaruh E-Trust Dan E-Service Quality Terhadap E-Loyalty Menggunakan Layanan Mobile Banking Bank Syariah Indonesia Dengan Kepuasan Nasabah Sebagai Variabel Intervening (Studi Kasus Mahasiswa FEBI UINSU Tahun 2019). *Jurnal Nuansa*, *1*(4), 221–233. https://doi.org/10.61132/nuansa.v1i4.399

Kusumaningrum, A., Wijayanto, H., & Raharja, B. D. (2022). Pengukuran Tingkat Kesadaran Keamanan Siber di Kalangan Mahasiswa saat Study From Home dengan Multiple Criteria Decision Analysis (MCDA). *Jurnal Ilmiah SINUS*, *20*(1), 69. https://doi.org/10.30646/sinus.v20i1.586

Lal, N. A., Prasad, S., & Farik, M. (2016). *A Review Of Authentication Methods*. *5*(11), 246–249.

Nasution, S. E. H., Atika, A., & Daulay, A. N. (2024). Pengaruh Pendekatan Emosional Dan Rasionalitas Terhadap Keputusan Mahasiswa Memilih Menabung Di Bank Syariah (Studi Kasus Pada Mahasiswa Febi Uinsu). *Jesya*, *7*(1), 291–304. https://doi.org/10.36778/jesya.v7i1.1400

Nurhaliza, Muhammad Irsyad Fadhil, Deri Kurniawan, & Nurbaiti. (2023). Analisis Persepsi Mahasiswa FEBI UINSU Mengenai Mobile Banking Bank Syariah Di Indonesia. *OPTIMAL Jurnal Ekonomi Dan Manajemen*, *4*(1), 22–29. https://doi.org/10.55606/optimal.v4i1.2559

Parhusip, T. (2024). Jurnal Sistem dan Teknologi Informasi. *Penerapan Visual Novel Dari Cerita Rakyat Asal Usul Kota Pontianak*, *1*(2), 1–5.

Shofia, P. A., Yafiz, M., & Jannah, N. (2024). Terhadap Kepuasan Mahasiswa Febi UIN Sumatera Utara Dalam Penggunaan Layanan Digital Bank Syariah. *INNOVATIVE: Journal Of Social Science Research Volume*, *4*(3), 10098–10112.

Sudiarto Raharjo, W., E.K. Ratri, I. D., & Susilo, H. (2017). Implementasi Two Factor Authentication Dan Protokol Zero Knowledge Proof Pada Sistem Login. *Jurnal Teknik Informatika Dan Sistem Informasi*, *3*(1). https://doi.org/10.28932/jutisi.v3i1.579

Syahira, T., Indra, A. P., & Anggraini, T. (2024). PENGARUH PENGALAMAN NASABAH DALAM PENGGUNAAN MBANKING TERHADAP LOYALITAS NASABAH BANK SYARIAH INDONESIA (Studi Kasus Masyarakat Sei Mencirim). *Jurnal Ilmiah Ekonomi Islam*, *10*(01), 1216–1220.

Tolle, H., Tri, A., Kurniawan, S. T., Mt, A., & Zakaria, S. T. (2008). Peningkatan Keamanan Web Terhadap Serangan Cross Site Scripting (XSS). *Tekno*, *9*, 1693–8739. http://www.owasp.

Ubaidillah, M. S. (2019). Pengaruh Literasi Keuangan Terhadap Perilaku Keuangan Dengan Sikap Keuangan Dan Self-Efficacy Sebagai Variabel Mediasi. *Perpustakaan Universitas Airlangga*, 310–320. http://repository.unair.ac.id/88317/

Zuhra, A., & Nasution, M. L. I. (2024). Penyelesaian Masalah M-Banking Nasabah Pt. BSI. *Musytari: Neraca Manajemen, Akuntansi, Dan Ekonomi*, *3*(9), 81–90.