INNOVATIVE: Journal Of Social Science Research
Volume 4 Nomor 2 Tahun 2024
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Analisis Perilaku Pengguna Mobile Banking Terhadap Keamanan Informasi Menggunakan Metode Human Aspects of Information Security Questionnaire (HAIS-Q)

Maria Anastasiah[1], Henry Pandia[2]✉
Program Studi S1 Sistem Informasi Universitas Advent Indonesia
Email: 2082025@unai.edu[2]✉

Abstrak

Penelitian ini merupakan studi tentang perilaku para pengguna mobile banking terhadap keamanan informasi di Indonesia. Tujuan studi ini adalah untuk mengevaluasi apakah perilaku pengguna mobile banking telah memadai dalam menjaga keamanan informasi mereka dari ancaman kejahatan di sektor jasa keuangan yang mungkin memanfaatkan kelalaian atau kelemahan dari pengguna mobile banking. Penelitian ini diukur menggunakan metode HAIS-Q. Populasi untuk penelitian ini adalah 100 responden yang menggunakan layanan aplikasi mobile banking di Indonesia. 30 responden menjadi sampel dalam penelitian ini. Instrumen penelitian ini adalah angket pertanyaan bedasarkan instrumen HAIS-Q. Angket pertanyaan terdiri dari 15 butir pertanyaan yang meliputi instrumen HAIS-Q. Teknik pengumpulan data menggunakan kuesioner yang disebarkan melalui platform google form. Tentang hasil penelitian ini, diharapkan bahwa perilaku pengguna mobile banking dalam menjaga keamanan informasi data pribadi dapat mencapai tingkat yang optimal dan penelitian ini bisa Memberikan referensi atau pemahaman kepada masyarakat dalam berprilaku menjaga keamanan informasi data pribadinya. Dari hasil perhitungan beberapa nilai focus area yang bernilai rendah terdapat pada focus area “password management” dengan sub area “Sharing Password” (M=2,83) dan “mobile device” dengan sub area “Sending sensitive information via WI-FI” (M=2,68).

Kata Kunci : *Mobile banking, keamanan, informasi*

Abstract

This research is a study of the behavior of mobile banking users towards information security in Indonesia. Theaim of this study is to evaluate whether the behavior of mobile banking users is adequate in maintaining the security of their information from the threat of crime in the financial services sector which may take advantage of the negligence or weaknesses of mobile banking users. This research was measured using the HAIS-Q method. The population for this research is 100 respondents who use mobile banking application services in Indonesia. 30 respondents were the sample in this research. The instrument of this research is a questionnaire based on the HAIS-Q instrument. The questionnaire consists of 15 questions covering the HAIS-Q instrument. The data collection technique uses a questionnaire distributed via the Google Form platform. Regarding the results of this research, it is hoped that the behavior of mobile banking users in maintaining the security of personal data information can reach an optimal level and this research can provide a reference or understanding to the public in their behavior in maintaining the security of their personal data information. From the calculation results, several focus area values with low value are in the focus area "password management" with the sub area "Sharing Passwords" (M=2.83) and "mobile devices" with the sub area "Sending sensitive information via WI-FI" (M=2.68).

Keyword : *mobile banking, security, information*

PENDAHULUAN

Seiring berkembangnya internet, layanan keuangan juga semakin berkembang karena pengaruh teknologi informasi yang mendorong transformasi digital. Menurut data dari *Visa Consumer Payment Attitudes Study*, padsa tahun 2022, 88 persen orang Indonesia memilih digital banking untuk bertransaksi. Ini meningkat dari 86% pada tahun 2021 dan 75% pada tahun 2020. Pengguna layanan keuangan yang terus meningkat dengan adanya teknologi yang semakin canggih dengan mayoritas pengguna *digital banking* berasal dari generasi muda dan mapan finansial(Ahmad Fikri Noor & Novita Intan, 2023).

Perkembangan digital dan *mobile banking* ini berdampak besar bagi masyarakat global, khususnya indonesia. *Mobile banking* memberikan manfaat bagi pengguna nya seperti mudah kirim uang ke orang lain,cepat dan mudah bayar tagihan, bisa dipantau 24 jam, transaksi lebih aman. Meskipun memiliki keuntungan, *mobile banking* juga rentan terhadap risiko karena pelaku kejahatan *siber* atau *fraud cyber crime* dibidang jasa keuangan berusaha memanfaatkan kelemahan atau kelalaian pengguna seperti kejahatan pada eksploitasi oleh *social engineers* dan bentuk kejahatan lainnya(Ramadhan & Purwandari, 2023). Oleh sebab itu sangat penting menjadikan pengguna sebagai prioritas dalam hal keamanan, karena pengguna bisa berperan sebagai penghubung para pelaku kejahatan untuk mendapatkan informasi ke dalam sistem tersebut. Walaupun telah

memiliki sistem pengaman yang ada di aplikasi, hal tersebut tidak menjadi penghalang bagi para pelaku untuk membuat strategi agar bisa mengakses sistem yang sudah terlindungi(Magister et al., 2022)

Banyak ancaman yang ditimbulkan dari tindakan kejahatan dan sering sekali terjadi kasus-kasus penipuan dibidang jasa keuangan yang menjadi sasaran utama bagi pelaku kejahatan. Oleh karena itu, tidak sedikit nasabah atau pengguna layanan aplikasi *mobile banking* ketika menjadi korban penipuan menyalahkan pihak bank. Karena salah satu penyebabnya adalah pengetahuan yang kurang dan kelalaian dari pengguna. Maka dari itu, nasabah atau pengguna perlu mengetahui dan mewaspadai modus kejahatan penipuan yang sering terjadi seperti(Farodilah Muqoddam, 2019):

1. *Phising* melalui aplikasi *mobile banking*

   penipuan melalui pesan teks atau email yang dikirim dengan modus meminta nasabah memasukan data pribadi, nomor rekening dan *PIN* melalui *website* samaran yang seolah-olah mirip dengan *website* aslinya.

2. *Skimming*

   Skimming adalah tindakan mencuri informasi kartu kredit internet. Pengguna kartu kredit internet memasukkan nomor kartu kreditnya, dibagian belakang kartu kredit terdapat kode rahasia. Namun hal ini dapat dieksploitasi oleh oknum yang tidak bertanggung jawab.

3. *Social Engineering*

   Memanipulasi psikolog korban untuk mendapatkan informasi pribadi korban.

4. *Social Engineering (Vhishing)*

   Menggunakan teknik *social engineering* melalui telepon yang mengiming-imingi korban mendapat hadiah atau memberikan desakan untuk memberikan data pribadi agar korban tidak mengalami kerugian.

5. *Malware* dan aplikasi palsu

   Penggunaan *malware* atau aplikasi palsu yang dapat mencurui informasi keuangan dari perangkat nasabah yang digunakan untuk mengakses layanan *mobile banking*.

(Chevers, 2019), Pemberian edukasi tentang kejahatan internet dapat meningkatkan kewaspadaan dan menjaga perilaku terhadap kejahatan internet seperti phising. Untuk membantu masyarakat mengenali tingkah laku kejahatan secara dini, pemberian edukasi lewat informasi akan dibagikan melalui media sosial dan situs web resmi perusahaan.

Dengan menggunakan metode HAIS-Q atau *Human Aspects of Information Security Questionnaire* adalah komponen penting keamanan informasi yang melibatkan peran manusia dalam penggunaan teknologi informasi dan sistem keamanan informasi(Kör

& Metin, 2021). penelitian ini menargetkan pengguna *mobile banking* Indonesia berusia 16 hingga 65 tahun. Semua aplikasi *mobile banking* yang tersedia di Indonesia secara legal dan resmi dipilih untuk penelitian ini. Oleh karena itu, penelitian ini dilakukan untuk menilai perilaku pengguna *mobile banking* terhadap keamanan informasi dan mengetahui apakah langkah-langkah keamanan telah diikuti. Hasil penelitian ini diharapkan bahwa perilaku pengguna *mobile banking* dalam menjaga keamanan informasi data pribadi dapat mencapai tingkat yang optimal dan penelitian ini bisa Memberikan referensi atau pemahaman kepada masyarakat dalam berprilaku menjaga keamanan informasi data pribadinya(Ramadhan & Purwandari, 2023).

METODE PENELITIAN

Metode HAIS-Q

Penelitian ini menggunakan metode HAIS-Q. Metode penelitian ini bertujuan untuk mengetahui analisis perilaku pengguna *mobile banking* terhadap keamanan informasi. Teknik pengumpulan data menggunakan instrumen pada 7 area fokus HAIS-Q, area fokus tersebut adalah area fokus tersebut adalah *(1) password management, (2) email use, (3) internet use, (4) social media use, (5) mobile device, (6) information handling, dan (7) incident reporting*. Dalam penelitian ini tidak diikut sertakan fokus area *(4) social media use* dan *(6) information handling*, karena menurut peneliti fokus area tersebut tidak berpengaruh pada perilaku oengguna mobile banking dalam menjaga keamanan informasinya.(Parsons et al., 2017).

Populasi dan Sampel

Populasi adalah keseluruhan subjek penelitian (Suharsimi Arikunto, 2011). Populasi yang digunakan dalam penelitian ini adalah masyarakat yang menggunakan aplikasi layanan *mobile banking* di Indonesia. Penelitian ini menggunakan populasi yang menggunakan aplikasi layanan *mobile banking* di Indonesia karena tidak ada informasi yang relevan dan akurat tentang jumlah pengguna *mobile banking* di Indonesia. Akibatnya, peneliti tidak dapat menentukan besarnya populasi. Untuk mengumpulkan data secara acak dari populasi pengguna *mobile banking* penelitian ini menggunakan metode *Simple Random Sampling*. Sampel dilakukan secara acak dari seluruh populasi pengguna *mobile banking*. (Hayuningtyas, 2015) Karena populasi ini tersebar luas dan sulit untuk menemukan jumlah sampel yang tepat, rumus (1) berikut digunakan untuk menghitung jumlah sampel

$$\mathrm{n} = \frac{Z^2}{4(Moe)^2} \quad (1)$$

Dimana n merupakan Jumlah sampel. Z adalah tingkat keyakinan yang dibutuhkan dalam pengambilan sampel, biasanya 90% sehingga Z=1,96. Dan Moe atau yang disingkat sebagai *Margin of error* adalah kesalahan maksimum yang bisa ditoleransi, biasanya 10% atau 0,1. Sesuai rumus diatas jadi dapat dilihat Ukuran sampel minimum yang diperlukan untuk penelitian ini adalah :

$$\mathrm{n} = \frac{1{,}96^2}{4(0{,}1)^2} = 96{,}04 \approx 100 \quad (2)$$

Berdasarkan perhitungan di atas(2) maka jumlah sampel minimum yang harus diteliti sebanyak 96,04 responden, bila dibulatkan banyaknya sampel adalah 100 responden.

Jenis dan Teknik Pengambilan Data.

Data primer adalah jenis data yang digunakan dalam penelitian ini karena sumber data penelitian ini diperoleh secara langsung dari sumber asli (Andika et al., n.d.).

(Sugiyono, 2017), Angket, juga dikenal sebagai kuesioner, adalah metode pengumpulan data yang melibatkan memberi responden seperangkat pertanyaan atau pernyataan tertulis untuk dijawab. Peneliti menggunakan kuesioner untuk mendapatkan informasi dan memudahkan mereka. Tujuan utama penulisan kuesioner adalah untuk membantu responden memberi jawaban yang akurat.

Mekanisme pengumpulan datanya adalah dengan memberikan kuesioner berupa *Google Form* kepada responden. Kuesioner disebar ke media sosial seperti *WhatsApp, Line* dan *Instagram*. Setiap pertanyaan terdiri dari 5 pilihan jawaban berdasarkan *skala Likert* dari 1 hingga 5—di mana 1 adalah tidak pernah dan 5 adalah selalu. (1) demografi dan (2) perilaku keamanan adalah bagian dari kuesioner. Kuesioner terdiri dari lima belas pertanyaan yang mencakup area fokus HAIS-Q dan dirancang untuk mengukur kesadaran perilaku pengguna tentang keamanan informasi saat menggunakan layanan perbankan *mobile*.

Tahapan Penelitian

Dalam penelitian diperlukan tahapan penelitian untuk memperoleh hasil yang diharapkan. Langkah awal yang dillakukan oleh peneliti yaitu mengidentifikasikan masalah yang akan diteliti. Selanjutnya peneliti menyelusuri dan mempelajari beberapa sumber seperti jurnal-jurnal ilmiah. *Studi literatur* dilakukan dalam upaya untuk mengungkapkan berbagai teori yang relevan dengan masalah dan tujuan penelitian. Tahap berikutnya pengumpulan data dengan cara penyebaran kuesioner kepada pengguna *mobile banking* di Indonesia menggunakan platform *google form* dan terakhir pada tahap pengelolahan dan analisis data dari kuesioner yang diberikan kepada responden. Setelah itu peneliti

membuat kesimpulan dari penelitian yang harus diperbaiki.

HASIL DAN PEMBAHASAN

Hasil

Uji Validitas dan Reabilitas

Penelitian ini menggunakan analisis *Partial Least Square* untuk menguji validitas dan reabilitas dengan bantuan aplikasi PLS Algorithm. Model yang digunakan untuk menganalisis semua variabel laten dari *partial least square* ini terdiri dari *Inner model* dan *Outer Model*, dalam penelitian ini peneliti menggunakan *Outer model*. Tujuan dari *Outer model* adalah untuk menentukan bagaimana variabel laten dan indikatornya berinteraksi satu sama lain(Dash & Paul, 2021). Uji yang dilakukan mencakup:

Nilai convergen validitas adalah nilai *loading faktor* pada variabel dan indikatornya, yang menunjukkan seberapa besar korelasi antara indikator dan variabel laten. Nilai pengisian 0,5–0,6 dianggap cukup, tetapi diharapkan lebih dari 0,7(Memon et al., 2021). Bedasarkan hasil perhitungan nilai *convergen validitas* pada penelitian ini semua item atau indikator nilai *outer loading* > 0,5 walaupun masih < 0,7. Dengan demikian, validitas *outer loading* menunjukkan bahwa semua item atau indikator telah valid secara validitas butir.

Tabel 1. Convergent Validity

Focus Area	*Sub-Area*	*Mean*	*Standar Devition*	*Standarized Loading*
Password Management	*Using the same password*	3,66	1,35	0,879
	Sharing passwords	2,63	1,56	0,636
	Using a strong password	3,60	1,20	0,913
Email Use	*Clicking on links in emails from known senders*	2,46	1,20	0,771
	Clicking on links in emails from unknown senders	3	1,15	0,747
	Opening attachments in email from unknown senders	2,23	1,20	0,739
Internet Use	*Downloading files*	3,86	1,14	0,776
	Accessing dubious websites	3,56	1,17	0,678
	Entering information online	3,76	1,02	0,735

	Physically securing mobile devices	2,1	1,13	0,762
Mobile Devices	*Sending sensitive information via WI-FI*	2,43	1,11	0,714
	Shoulder surfing	3,66	1,24	0,648
Incident Reporting	*Reporting suspicious behavior*	3,33	1,7	0,994
	Ignoring poor security behavior by colleagues	3,63	1,56	0,920
	Reporting all incidents	3,46	1,70	0,859

Konstruksi Reliabilitas adalah ukuran reliabilitas struktur variabel laten. *Reliabilitas Counstruc* sama dengan nilai *cronbach alfa*. Nilai harus di atas 0,70 untuk dianggap reliabel.(Julius Nursyamsi et al., 2023). Bedasarkan hasil perhitungan *Contruct Reability* pada penelitian ini bahwa semua konstruk memiliki nilai *Cornbach's Alpha* >0,6 dan bahkan semuanya >0,7, maka dapat dikatakan bahwa semua konstruk tersebut telah reliable.

Average Variance Extracted- AVE digunakan untuk menentukan apakah syarat validitas diskriminan telah dipenuhi. Keandalan harus minimal 0,50(Guenther et al., 2023). Bedasarkan nilai nilai *Average Variance Extracted* (AVE) maka semua konstruk telah tercapai syarat validitas diskriminan sebab nilai AVE semuanya >0,50.

Tabel 2. *Contruct Reliability dan AVE*

Item	*Cronbach's Alpha*	*AVE*
Focus Area : Password Management	0,846	0,670
Focus Area : Email Use	0,796	0,566
Focus Area : Internet Use	0,773	0,534
Focus Area : Mobile Devices	0,750	0,504
Focus Area : Incident Reporting	0,946	0,857

Tujuan dari validitas diskriminatif adalah untuk menentukan seberapa jauh konstruk laten benar berbeda dengan konstruk lainnya. Metode alternatif untuk menilai validitas diskriminan adalah *heterotrit-monotriat ratio of correlations* (HTMT). Menurut perhitungan HTMT, nilai HTMT <0.9 menunjukkan bahwa konstruk itu valid secara diskriminan

(Guenther et al., 2023). Bedasarkan tabel 3 menunjukkan bahwa semua nilai HTMT < 0,9, yang berarti bahwa semua konstruk memiliki validitas diskriminan.

Tabel 3. *Disriminant Validity*

	Password	*Email*	*Internet*	*Mobile Device*	*Incident Reporting*
Password					
Email	0,285				
Internet	0,501	0,292			
Mobile Device	0,221	0,142	0,284		
Incident Reporting	0,265	0,302	0,429	0,206	

Hasil

Bedasarkan Jenis kelamin, usia, pendidikan terakhir, dan jenis perbankan seluler yang digunakan untuk mengumpulkan demografi responden.

Tabel 4. Demografi Responden

Kriteria	Kategori	Presentasi
Jenis Kelamin	Laki-laki	46%
	Perempuan	54%
Usia	16-25	60%
	26-35	20%
	36-45	13%
	>45	7%
Pendidikan	SMA atau dibawahnya	26%
	D3/S1	70%
	S2	3%
	S3	1%
Mobile banking yang digunakan	*BCA Mobile/MyBCA*	44%
	Livin by Mandiri	35%
	BNI Mobile Banking	11%
	BRImo BRI	33%
	Jenius by BTPN	2%

	Octo Mobile by CIMB Niaga	4%
	Other…	6%

Tabel 5. Hasil

Focus Area	*Sub-Area*	*Mean*	*Standar Devition*
Password Management	*Using the same password*	3,69	1,32
	Sharing passwords	2,83	1,47
	Using a strong password	3,78	1,20
Email Use	*Clicking on links in emails from known senders*	3,29	1,26
	Clicking on links in emails from unknown senders	3,54	1,35
	Opening attachments in email from unknown senders	4	1,17
Internet Use	*Downloading files*	4,18	1,17
	Accessing dubious websites	3,59	1,4
	Entering information online	3,71	1,15
Mobile Devices	*Physically securing mobile devices*	3,43	1,43
	Sending sensitive information via WI-FI	2,68	1,14
	Shoulder surfing	3,97	1,09
Incident Reporting	*Reporting suspicious behavior*	3,34	1,63
	Ignoring poor security behavior by colleagues	3,59	1,49
	Reporting all incidents	3,66	1,58

100 responden telah membantu menjawab kuesioner HAIS-Q, pada tabel 7 menyajikan hasil dari perhitungan rata-rata dan devisiasi standar untuk masing-masing sub-bidang HAIS-Q. Skor responden yang terendah untuk manajemen *password* adalah pada sub-area *"sharing password"* (M = 2,83, SD = 1,47). Responden sepertinya menganggap aman untuk berbagi *password mobile banking* dengan keluarga atau bahkan dengan temannya. Pada fokus area penggunaan *email* skor responden terendah pada sub-

area *"Clicking on links in emails from known senders"* (M = 3,29, SD = 1,26). Berbeda dengan skor responden sub-area *email "Clicking on links in emails from unknown senders"* (M = 3,54, SD =1,35) perilaku responden cenderung lebih sadar dalam mengenali sub-area tersebut. Namun, jika *email* dari orang yang dikenal dipalsukan, itu bisa dianggap sebagai *email phising*. Skor responden terendah selanjutnya untuk fokus area penggunaan internet adalah pada sub-area *"Accessing dubious websites"* (M = 3,59, SD = 1,4). Responden menganggap aman bahwa perilaku mengakses situs *web* yang meragukan tidak berbahaya bagi keamanan *mobile banking*, responden tidak menyadari bahwa bisa saja tertular virus melalui akses ke *website* tertentu. Fokus area untuk *mobile device* skor terendah pada sub-area *"Sending sensitive information via WI-FI"* (M =2,68 , SD = 1,14) responden tidak menyadari bahwa perilaku mengakses *mobile banking* dengan *WI-FI public* dapat beresiko mengalami pencurian data. Dan terakhir untuk fokus area *Incident reporting*, skor terendah pada sub-area *"Reporting suspicious behavior"* (M = 3,34, SD = 1,63). Responden kurang memperhatikan perilaku seseorang yang tidak berhak sedang berusaha mendapatkan hak akses ke akun *mobile banking*.

SIMPULAN

Hasil penelitian, yang bertujuan untuk mengukur perilaku pengguna *mobile banking* terhadap keamanan data pribadi, menunjukkan bahwa responden memahami dan bertindak sesuai dengan prosedur yang digunakan untuk melindungi data pribadi mereka. Hasil kuesioner menunjukkan bahwa tingkat pengetahuan keamanan data (ISA) yang dimiliki sudah cukup baik. Namun, tingkat pemahaman dan pengetahuan individu perlu ditingkatkan, dan fokus area yang bernilai rendah juga perlu ditingkatkan. Beberapa nilai fokus area yang bernilai sangat rendah terdapat pada fokus area *"password management"* dengan sub area *"Sharing Password"* (M=2,83) dan *"mobile device"* dengan sub area *"Sending sensitive information via WI-FI"* (M=2,68).

Hasil penelitian ini membantu masyarakat memahami sikap atau tindakan terhadap keamanan informasi yang harus dilindungi, meningkatkan kesadaran masyarakat dengan memahami *social engineering* dan ancaman yang ditimbulkannya. Masyarakat seharusnya memahami tentang *social engineering* agar Masyarakat bisa lebih waspada terhadap kejahatan tersebut. Perilaku masyarakat harus berhati-hati, teliti, dan berhati-hati untuk mencegah penipuan *social engineering* atau kejahatan lainnya. Mereka harus berhati-hati saat menghubungi orang yang tidak dikenal atau yang mengaku sebagai staf bank yang mengajak mereka untuk memberikan informasi pribadi klien mereka karena bank resmi tidak mungkin meminta informasi pribadi klien mereka. Jika mereka menjadi korban

penipuan *social engineering*, masyarakat harus segera menghubungi bank atau polisi. Mereka tidak perlu takut atau malu untuk melakukan penyidikan. Penulis berharap dapat melakukan penelitian lebih lanjut tentang perilaku pengguna mobile banking yang menggunakan media sosial populer seperti *Facebook, YouTube, Instagram, Telegram, WhatsApp*, dan *TikTok*, antara lain.

DAFTAR PUSTAKA

329-Article Text-1249-2-10-20211001. (n.d.).

Ahmad Fikri Noor, & Novita Intan. (2023, June 20). *Riset Visa: 88 persen Masyarakat Gemar Gunakan Digital Banking*. Republika. https://ekonomi.republika.co.id/berita/rwjb8m490/riset-visa-88-persen-masyarakat-gemar-gunakan-digital-banking

Carlin Tan, C. (n.d.). *HUBUNGAN BODY IMAGE DENGAN POLA MAKAN PADA REMAJA PUTRI*.

Chevers, D. A. (2019). *Association for Information Systems AIS Electronic Library (AISeL) The impact of cybercrime on e-banking: A proposed model*. https://aisel.aisnet.org/confirm2019

Dewi Noviyanti, R., Marfuah, D., Gizi, S., Pku, S., & Surakarta, M. (n.d.). *Hubungan Pengetahuan Gizi, Aktivitas Fisik, dan Pola Makan Terhadap Status Gizi Remaja Di Kelurahan Purwosari Laweyan Surakarta*.

Dewi, R. K., & Martini, S. (2021). *HUBUNGAN TINGKAT PENGETAHUAN REMAJA PUTRI TENTANG GIZI DENGAN KEJADIAN KEKURANGAN ENERGI KRONIK (KEK) PADA USIA REMAJA* (Vol. 9, Issue 3).

Ertiana, D., Suryani Wahyuningsih, P., Studi, P. S., Karya Husada Kediri, S., Timur, J., & Studi DIV Kebidanan, P. (2019). ASUPAN MAKAN DENGAN KEJADIAN KEK PADA REMAJA PUTRI DI SMAN 2 PARE KABUPATEN KEDIRI (Food Intake with Chronic Energy Deficiency in Young Women in Public Senior High School 2 Pare, Kediri Regency). In *Jurnal Gizi KH* (Vol. 1, Issue 2).

Farodilah Muqoddam. (2019, March 28). *Mengenal Modus Kejahatan Keuangan, Definisi Skimming, Phising, dan Vishing*. Bisnis.Com. https://finansial.bisnis.com/read/20190328/90/905444/mengenal-modus-kejahatan-keuangan-definisi-skimming-phising-dan-vishing

Hafiza, D., Utami, A., Niriyah, S., Studi Keperawatan, P., Hang Tuah Pekanbaru Corresponding Author, Stik., & Hang Tuah, Stik. (n.d.). *HUBUNGAN KEBIASAAN MAKAN DENGAN STATUS GIZI PADA REMAJA SMP YLPI PEKANBARU*.

Ika Wardhani, P., Ery, M. S., Ilmu Kesehatan, F., & Pembangunan Nasional, U. (2020). HUBUNGAN BODY IMAGE DAN POLA MAKAN DENGAN KEKURANGAN ENERGI KRONIS (KEK) PADA REMAJA PUTRI SMAN DI JAWA BARAT The Correlation Between Body Image and Diet with Chronic Energy Deficiency (Ced) on Female Adolescents in SMAN in West Java. In *RECODE Maret* (Vol. 3, Issue 2). http://e-journal.unair.ac.id/JPHRECODE

Irnani, H., & Sinaga, T. (2017). Pengaruh pendidikan gizi terhadap pengetahuan, praktik gizi seimbang dan status gizi pada anak sekolah dasar. In *Jurnal Gizi Indonesia (The Indonesian Journal of Nutrition)* (Vol. 6, Issue 1).

Kör, B., & Metin, B. (2021). Understanding Human Aspects for an Effective Information Security Management Implementation. *International Journal of Applied Decision Sciences*, *14*(1). https://doi.org/10.1504/ijads.2021.10030447

Magister, P., Diajukan, A., Rahmadani, O., & Sekar Putri, N. (2022). *Analisa Pola-Pola Sosialisasi Pencegahan Modus Social Engineering Oleh Bank Melalui Media Website dan Media Sosial Twitter Tesis S2*.

pdf-gizi-reproduksi_compress. (n.d.).

pdf-hubungan-pengetahuan-gizi-dan-kebiasaan-makan-dengan-kejadian-kek-pada-remaja-putri-di-model-agency-elmode-management-kota-medan_compress. (n.d.).

Ramadhan, T., & Purwandari, B. (2023). Analisis Tingkat Kesadaran Keamanan Informasi: Studi Kasus Pengguna Aplikasi Perbankan Digital di Indonesia Guna Mencegah Social Engineering. *Syntax Idea*, *5*(1). https://doi.org/10.46799/syntax-idea.v5i1.2113

Riskesdas 2018 dalam angka, Indonesia ii. (n.d.).

Sari, N., Kelana, D., Sopiah, P., Studi III Keperawatan, P. D., & Pendidikan Indonesia, U. (n.d.). *HUBUNGAN CITRA TUBUH (BODY IMAGE) DENGAN STATUS GIZI KEK PADA SISWI SMKN SUKASARI*.

Šivert, Š. Š., & Sinanović, O. (2008). *BODY DISSATISFACTION-IS AGE A FACTOR?* https://www.researchgate.net/publication/279749767