Jurnal Manajemen Terapan dan Keuangan (Mankeu) Vol. 14 No. 03, September 2025
P-ISSN: 2252-8636, E-ISSN: 2685-9424

PENGARUH SOCIAL ENGINEERING DAN CYBER CRIME TERHADAP PERSEPSI KEAMANAN PADA APLIKASI BSI MOBILE

Nadya Ananda Efendi[1)], Muhammad Ikhsan Harahap[2)], Muhammad Syahbudi[3)]

Fakultas Ekonomi Bisnis Islam, Universitas Islam Negeri Sumatera Utara[1,2,3)]
nadyaananda2105@gmail.com[1)], m.ihsan.harahap@uinsu.ac.id[2)], bode.aries@uinsu.ac.id[3)]

Abstrak.

Penelitian ini bertujuan untuk mengetahui pengaruh Sosial Engineering dan Cyber Crime terhadap Persepsi Keamanan Pengguna Aplikasi BSI Mobile. Latar belakang penelitian ini didasari oleh meningkatnya kasus kejahatan siber yang menyasar layanan perbankan digital, khususnya melalui teknik manipulatif seperti sosial engineering dan kejahatan siber lainnya. Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei terhadap 100 responden pengguna aktif aplikasi BSI Mobile. Analisis data dilakukan menggunakan regresi linear berganda. Hasil uji secara parsial menunjukkan bahwa baik Sosial Engineering maupun Cyber Crime memiliki pengaruh signifikan terhadap persepsi keamanan pengguna. Hasil uji simultan juga menunjukkan bahwa kedua variabel tersebut secara bersama-sama berpengaruh signifikan terhadap persepsi keamanan. Temuan ini mengindikasikan bahwa aspek keamanan siber yang melibatkan faktor manusia dan teknis harus menjadi perhatian utama dalam pengembangan dan pengelolaan aplikasi mobile banking.

Kata kunci*: Social Engineering, Cyber Crime, persepsi keamanan*

Abstract.

This study aims to examine the influence of Social Engineering and Cyber Crime on the Security Perception of BSI Mobile Application Users. The background of this research is based on the increasing number of cybercrime cases targeting digital banking services, particularly through manipulative techniques such as social engineering and other cyber threats. A quantitative approach was employed, using a survey method involving 100 respondents who are active users of the BSI Mobile application. The data were analyzed using multiple linear regression. Partial test results indicate that both Social Engineering and Cyber Crime have a significant influence on users' security perception. Simultaneous testing also reveals that the two variables jointly have a significant effect on security perception. These findings suggest that both human and technical aspects of cybersecurity must be a primary concern in the development and management of mobile banking applications.

Keywords: *Social Engineering, Cyber Crime, Security Perception*

1. PENDAHULUAN

Pada pertengahan 2023, BSI mengalami sebuah gangguan layanan mobile bankingdan ATM BSI (Bank Syariah Indonesia) selama sepekan. Awalnya, BSI memberi penjelasan bahwa gangguan tersebut disebabkan oleh adanya pemiliharaan sistem sehingga layanan tidak dapat digunakan. Namun, fakta baru terungkap bahwa ganguan layanan disebabkan oleh sebuah serangan yang dinamakan dengan ransomwaredari sekelompok hacker. Peretasan ini tidak hanya mengakibatkan semua layanan BSI berhenti namun ada pencurian data yang dilakukan. Data yang dicuri mencakup berbagai informasi pribadi dan keuangan, termasuk nama, alamat, nomor kartu, nomor telepon, dan transaksi nasabah, serta dokumen keuangan, dokumen hukum, dan kata sandi (password) untuk layanan internal dan eksternal yang digunakan oleh bank(Kompas.com., 2023).Situasi

menjadi kompleks ketika kelompok peretas yang dikenal dengan nama LockBit 3.0mengklaim bahwa mereka adalah pelaku di balik serangan tersebut. Mereka mengancam akan merilis data pribadi 1,5 TB yang mencakup informasi nasabah dan karyawan BSI jika tuntutan mereka tidak dipenuhi. Ancaman ini menciptakan kepanikan dan kekhawatiran di antara nasabah dan memaksa manajemen BSI untuk mengatasi masalah ini dengan serius.

Meskipun, BSI bersikeras bahwa data dan dana nasabah aman namun publik tetap merasa cemas tentang potensi kebocoran data dan dampak serius yang dapat terjadi. Pasalnya, BSI tidak menyampaikan pemberitahuan secara langsung kepada nasabah terkait data nasabah yang terikat dengan penyerangan siber yang berdambak pada peretasan data nasabah. Sementara BSI mengklaim gangguan hacker ini dengan berdalih adanya proses perbaikan sistem yang terganggu(Cnnindonesia.com., 2023).Seperti hal yang terjadi di Aceh dengan pengguna terbesar bank BSI turut merasakan dampak dari gangguan yang terjadi, kekecewaan terjadi terhadap pengguna yang muncul akibat gangguan jaringan yang disebabkan oleh serangan hacker dan layanan pelanggan yang kurang memuaskan. Hal ini, memicu terjadinya rencana perubahan kebijakan yang terjadi, seperti yang disampaikan oleh ketua DPR Aceh Saiful Bahri bahwa ia akan berkodinator dengan berbagai pihak untuk merevisi kebijakan Qanun Lembaga Keuangan Syariah (LKS) yang beroperasi di tanah rencong dan juga merencanakan agar perbankan konvensional bisa beroperasi di Aceh."Kami sudah bermusyawarah di lembaga kami menilai ini harus ditinjau ulang Qanun LKS supaya bank konvensional bisa tetap beroperasi di Aceh. Biarlah nanti masyarakat yang memilih mau bank syariah atau konvensional," kata Saiful kepada wartawan,(Detik.com, 2023).

Media memberikan perhatian besar pada isu peretasan data BSI, menjadikannya fokus utama dalam berita mereka. Spekulasi dan narasi negatif yang berkembang dalam liputan media dapat memperburuk citra BSI dan mengurangi kepercayaan masyarakat terhadap bank syariah, tetapi juga menciptakan tantangan serius bagi reputasi perbankan syariah di tingkat nasional. Dalam konteks ini, respons yang cepat dan efektif dari BSI menjadi kunci untuk memulihkan kepercayaan nasabah dan merestorasi citra perbankan syariah secara keseluruhan. Perbaikan sistem dan kebijakan perlindungan data yang lebih kuat juga menjadi langkah penting untuk mencegah terulangnya insiden serupa di masa depan. Media memiliki peran krusial dalam membentuk opini masyarakat terhadap suatu peristiwa, dan isu peretasan data yang melibatkan Bank Syariah Indonesia (BSI) menjadi sorotan utama. Spekulasi dan narasi negatif yang tersebar melalui liputan media dapat menciptakan dampak jangka panjang terhadap kepercayaan masyarakat terhadap perbankan syariah(Ritonga, 2018). Keberlanjutan pemberitaan ini dapat merugikan operasional BSI dan bahkan menciptakan tantangan serius bagi reputasi perbankan syariah di tingkat nasional. Berita mengenai serangan hacker terhadap BSI diberitakan secara dramatis, menciptakan narasi yang menekankan berbagai aspek serius dari peristiwa ini.

Freaming pemberitaan yang terjadi, memberikan kesan bahwa serangan ini bukan hanya mengancam satu lembaga keuangan, melainkan juga menjadi ujian berat bagi sektor perbankan Indonesia secara keseluruhan. Fokus media pada dampak luas dariserangan, baik dari segi operasional BSI maupun reputasi perbankan syariah secara umum, meningkatkan kekhawatiran bahwa keamanan perbankan syariah secara menyeluruh terancam. Kurangnya informasi tentang langkah-langkah yang diambil oleh BSI untuk menangani situasi ini juga dapat meninggalkan kesan bahwa bank tidak mampu mengatasi masalah tersebut secara efektif. Spekulasi yang muncul tanpa sadar dapat menciptakan

sentimen negatif di kalangan masyarakat.

Dari penelitian terdahulu yang dilakukan oleh Irwan Dermawan, Asmat Baidawi, Iksan, Selly Mellyana Dewi, Sektor perbankan dan keuangan merupakan sektor besar dengan jumlah nasabah yang besar di seluruh dunia.

Sepanjang tahun ini, aksesibilitas layanan perbankan kepada kelompok masyarakat yang paling lemah atau paling rentan terus meningkat. Menurut database Findex globe tahun 2017, ditemukan bahwa terdapat 1,2 miliar orang dewasa yang memiliki rekening bank. Selain itu, terlihat bahwa sebagian besar negara beralih ke pendekatan digital; sekitar 51% lebih memilih saluran perbankan online sementara 26% mengakses layanan melalui situs web bank dan menggunakan layanan mobile banking.

Karena pesatnya pertumbuhan digitalisasi di bank, risiko dan serangan cyber telah berkembang menjadi area utama yang menjadi perhatian. Selama beberapa dekade terakhir, telahterjadi peningkatan serangan siber yang sangat besar, dan serangan tersebut menyebabkan serangkaian kerusakan pada proses perbankan yang kritis dan menyebabkan kerugian finansial yang besar pada sistem. Sangat penting bagi sektor perbankan atau keuangan untuk menerapkan strategi keamanan cyber yang efektif. Strategi keamanan siber yang efektif seperti kecerdasan buatan (AI) untuk mengatasi semua masalah ini. Dengan demikian, studi saat ini akan menjelaskan kondisi keamanan siber di bank-bank swasta Indonesia dan apakah bank-banktersebut menawarkan tingkat yang dapat diterima untuk melindungi dirinya sendiri dan menjaga basis data pelanggannya.

Dan juga Dari penelitian yang dilakukan oleh Koteswara Ivaturi,. Lech Janczewski,mengatakan Rekayasa sosial adalah strategi utama peretas saat ini, terutama dengan berkembangnya e-commerce dan layanan perbankan online yang menjadi target utama. Bank harus menangani masalah ini untuk tetap bersaing dan menguntungkan. Meski banyak bank memiliki kebijakan keamanan, serangan rekayasa sosial masih sering terjadi. Penelitian ini mengevaluasi kebijakan keamanan bank online di 11 negara Asia-Pasifik dan menemukan bahwa informasi tentang tren serangan baru terbatas, kecuali phishing. Praktik keamanan yang ada sering disajikan sebagai tips umum tanpa konteks yang jelas, sehinggakurang efektif.

Dari penelitian terdahulu yang telah dilakukan oleh Indra Ava Dianta dan Edwin Zusrony pada tahun 2019, Penelitian dilakukan di PT. XYZ cabang Salatiga. Penelitian ini menunjukkan menunjukkan bahwa bagi hampir seluruh karyawan PT. XYY Salatiga sebesar 80%, menyatakan bahwa dimensi *availability* dengan indikator *access speed* adalah yang paling mempengaruhi keamanan sistem informasi fitur *Internet Banking*.Hal ini menjadi rekomendasi bagi Bank BCA dalam hal peningkatan *data security* khususnya terkait *Internet Banking*. Sebagai contoh, BCA bisa memulai menggunakan teknologi *criptography* yang lebih canggih untuk mencegah terjadinya kerentanan terhadap *datasecurity*.

Dan juga penelitian yang dilakukan oleh Putri Amalia dan Anna Zakiyah Hastriana pada tahun 2022 tentang Pengaruh Kemanfaatan, Kemudahan Keamanan, dan Fitur M-BankingTerhadap Kepuasan Nasabah dalam Bertransaksi Pada Bank Syariah Indonesia (Studi Kasus BSI KCP Sumenep).Temuan penelitian ialah keamanan mbanking berpengaruh positif signifikan terhadap kepuasan nasabah dalam bertransaksi pada Bank Syariah Indonesia KCP Sumenep. Nilai koefisien regresi variabel keamanan m-banking sebesar 0,332. Nilai koefisien positif menunjukkan adanya hubungan yang searah antara keamanan m-banking dengan kepuasan nasabah. Hasil penelitian ini diperkuat dengan hasil penelitian Sukmawati(2020) bahwa keamanana M-Banking berpengaruh positif dan signifikan terhadap kepuasan nasabah Bank BRI Syariah Cabang Kediri secara parsial.

Hasil penelitian inidapat disimpulkan bahwa variabel Keamanan berpengaruh positif dan signifikan terhadap Kepuasan Nasabah. Dengan demikian dapat diartikan bahwa keamanan merupakan faktor yang sangat penting dengan sistem keamanan yang memumpuni dan terupdate, sehingga nasabah tidak khawati dengan keamanan data pada m-banking mereka.

Dalam konteks digital banking, ancaman *Social Engineering* tidak lagi bersifat umum, tetapi semakin spesifik, seperti melalui modus *vishing* (voice phishing) yang mengatasnamakan call center bank, serta *smishing* (SMS phishing) yang menyamar sebagai notifikasi resmi. Kasus pencurian kode OTP dan informasi pribadi telah beberapa kali menimpa nasabah BSI, menunjukkan bahwa pengguna kerap tidak menyadari bahwa mereka sedang menjadi target penipuan.

Di sisi lain, *Cyber Crime* juga semakin berkembang melalui berbagai bentuk kejahatan, seperti penyebaran malware, hacking akun mobile banking, dan pembobolan data pribadi. Serangan siber terhadap BSI pada tahun 2023 yang menyebabkan gangguan layanan menjadi bukti nyata bahwa kejahatan siber bukan lagi potensi ancaman, tetapi sudah menjadi kejadian riil yang memengaruhi kepercayaan masyarakat.

Masalah-masalah inilah yang kemudian menjadi dasar penting bagi penelitian ini, untuk mengetahui sejauh mana *persepsi keamanan pengguna* dipengaruhi oleh dua bentuk ancaman tersebut — baik dari aspek manipulasi psikologis (*social engineering*) maupun dari sisi serangan teknis (*cyber crime*).

Berdasarkan uraian di atas penulis tertarik untuk meringkas dalam sebuah penelitian dengan rumusan masalah Apakah Cyber crime berpengaruh terhadap persepsi keamanan?

2. KAJIAN TEORITIS

Social Engineering

Menurut SANS Institute, *social engineering* adalah serangan psikologis di mana penyerang menipu korban untuk melakukan sesuatu yang seharusnya tidak dilakukan. Konsep *social engineering* bukanlah hal baru; namun yang membuat teknologi saat ini jauh lebih efektif bagi para penyerang dunia maya adalah korban tidak dapat melihatnya secara fisik; pelaku dapat dengan mudah berpura-pura menjadi apa pun atau siapa pun yang mereka inginkan dan menargetkan jutaan orang di seluruh dunia.

Selain itu, serangan *social engineering* dapat melewati banyak teknologi keamanan. Kesalahpahaman umum yang dimiliki kebanyakan orang tentang penyerang dunia maya adalah bahwa pelaku menggunakan alat dan teknik yang sangat canggih untuk meretas ke komputer atau akun korban. Padahal, penyerang dunia maya telah belajar bahwa seringkali cara termudah untuk mencuri informasi pribadi, meretas akun, atau menginfeksi sistem korban adalah dengan menipu korban agar melakukan kesalahan.Serangan *social engineering* datang dalam berbagai bentuk dan dapat dilakukan di mana saja dengan melibatkan interaksi manusia.

Dalam penelitian ini, variabel *Social Engineering* diukur melalui beberapa indikator yang disusun berdasarkan teori social engineering yang dikemukakan oleh Mitnick dan Simon (2002), serta disesuaikan dengan konteks perbankan digital. Social engineering merupakan metode manipulasi psikologis yang bertujuan mengecoh pengguna agar memberikan informasi rahasia atau melakukan tindakan yang merugikan dirinya sendiri. Oleh karena itu, indikator dalam penelitian ini difokuskan pada aspek kewaspadaan, kesadaran, dan pengetahuan pengguna terhadap berbagai bentuk rekayasa sosial digital.

Cyber Crime

Cyber crime adalah perilaku kejahatan yang beroperasi di ruang maya, dimana

pelaku mengambil keuntungan secara paksa dari korban. *Cyber crime* dalam Bahasa Indonesia diartikan sebagai kejahatan dunia maya, dimana pelau melakukan aksinyadengan melakukan penyadapan pada data-data yang terhubung dengan elektronik. *Cyber crime* merupakan tindak kejahatan yang masuk dalam hukum pidana yang dilakukan dengan memanfaatkan teknologi

maupun perangkat jaringan lainnya.*Cyber crime* banyak menimbulkan keresahan karena mengakibatkan kerugian besar, *cyber crime* bisa terjadi pada siapapun. Berbagai motif baru kejahatan ini terus berkembang dan mencari celah disaat korban sedang lengah.

Cyber crime atau kejahatan siber adalah segala bentuk aktivitas ilegal yang dilakukan melalui perangkat digital dan jaringan internet, dengan tujuan untuk merusak, mencuri, atau mengakses data tanpa izin. Dalam konteks teknologi informasi, cyber crime merupakan bentuk kejahatan modern yang tidak lagi dilakukan secara fisik, melainkan menggunakan manipulasi sistem digital untuk menyerang individu, institusi, atau organisasi.

Menurut Wall (2001), cyber crime mencakup tindakan kriminal seperti akses ilegal ke sistem komputer (hacking), pencurian data pribadi, penyebaran malware, penipuan online, serta serangan terhadap infrastruktur digital yang bersifat rahasia atau penting. Dalam konteks perbankan digital, kejahatan siber dapat merugikan pengguna secara langsung melalui pembobolan rekening, pencurian informasi finansial, atau penyalahgunaan identitas.

Lebih lanjut, Furnell (2002) menekankan bahwa cyber crime tidak hanya menimbulkan kerugian teknis, tetapi juga berdampak pada psikologis pengguna, khususnya pada persepsi terhadap keamanan dan kepercayaan terhadap sistem digital yang digunakan. Oleh karena itu, literasi keamanan digital menjadi hal yang krusial untuk mencegah pengguna menjadi korban dari kejahatan siber.

Perkembangan teknologi yang semakin kompleks telah menciptakan bentuk-bentuk baru dari cyber crime, seperti serangan *ransomware*, *social engineering-based intrusion*, dan *pharming*, di mana pelaku berusaha mengelabui pengguna untuk mendapatkan akses atau informasi berharga. Dalam penelitian ini, cyber crime diposisikan sebagai variabel yang memengaruhi persepsi keamanan pengguna dalam menggunakan aplikasi BSI Mobile.

Dalam penelitian ini, variabel *Cyber Crime* diukur melalui lima indikator utama yang merepresentasikan kesadaran dan kewaspadaan pengguna terhadap kejahatan digital.

Indikator pertama adalah pengetahuan pengguna terhadap jenis-jenis kejahatan siber, seperti peretasan akun, pencurian data, dan penipuan melalui situs palsu. Indikator kedua mengukur tingkat kekhawatiran pengguna terhadap ancaman cyber saat melakukan aktivitas finansial digital.

Indikator ketiga adalah pengalaman langsung atau tidak langsung menjadi korban kejahatan siber, yang berpengaruh pada kewaspadaan pengguna. Indikator keempat berkaitan dengan penggunaan fitur keamanan digital, seperti autentikasi ganda dan penghindaran akses dari jaringan publik.

Sementara indikator kelima adalah tingkat kepercayaan pengguna terhadap sistem keamanan aplikasi yang digunakan, termasuk keyakinan bahwa sistem mampu menangkal serangan digital secara efektif.

Persepsi Keamanan

Persepsi keamanan (*security perception*) adalah penilaian subjektif individu terhadap seberapa aman suatu sistem teknologi, layanan digital, atau aplikasi dalam melindungi informasi pribadi serta transaksi yang mereka lakukan dari berbagai potensi

ancaman, seperti pencurian data, penyalahgunaan akses, hingga serangan siber. Konsep ini merupakan turunan dari teori *perceived risk*, yang menyatakan bahwa dalam setiap keputusan menggunakan teknologi, individu mempertimbangkan potensi risiko yang mungkin mereka hadapi, termasuk risiko keamanan.

Menurut Flavián dan Guinalíu (2006), persepsi keamanan didefinisikan sebagai keyakinan pengguna bahwa sistem akan melindungi data dan interaksi digital mereka dari pihak yang tidak bertanggung jawab. Persepsi ini sangat erat kaitannya dengan rasa percaya (trust), kenyamanan (comfort), serta pengalaman pengguna sebelumnya dalam berinteraksi dengan teknologi. Dalam konteks digital banking, persepsi keamanan sangat penting karena menyangkut aktivitas yang bersifat sensitif, seperti penyimpanan data pribadi, transaksi keuangan, serta akses terhadap rekening nasabah.

Gefen et al. (2003) menekankan bahwa persepsi keamanan merupakan komponen kunci dalam model penerimaan teknologi, karena seseorang hanya akan menggunakan layanan digital jika mereka merasa sistem tersebut mampu memberikan jaminan keamanan terhadap data dan privasinya. Oleh karena itu, banyak penelitian menyebut bahwa persepsi keamanan menjadi mediator penting antara sistem teknologi dan perilaku pengguna (Wang et al., 2003).

Faktor-faktor yang memengaruhi persepsi keamanan dapat berasal dari kualitas teknologi (seperti sistem enkripsi, firewall, otentikasi dua faktor), pengalaman pengguna sebelumnya (baik positif maupun negatif), serta literasi keamanan digital yang dimiliki pengguna. Misalnya, seseorang yang pernah menjadi korban kejahatan digital seperti *phishing* atau *data breach* akan memiliki persepsi keamanan yang lebih rendah terhadap sistem yang tidak menunjukkan transparansi atau tidak memberikan kontrol keamanan yang cukup kepada pengguna.

Dalam konteks penelitian ini, persepsi keamanan berkaitan dengan bagaimana pengguna aplikasi BSI Mobile menilai sistem tersebut dari aspek perlindungan data, risiko kehilangan akses, serta potensi ancaman lainnya. Semakin tinggi persepsi keamanan yang dirasakan oleh pengguna, maka semakin besar pula kemungkinan mereka akan merasa nyaman dan percaya untuk menggunakan layanan mobile banking secara rutin.

Dalam penelitian ini, persepsi keamanan diukur melalui beberapa indikator yang disesuaikan dengan studi-studi terdahulu, seperti yang dikembangkan oleh Gefen et al. (2003) dan Wang et al. (2003). Indikator-indikator tersebut mencerminkan keyakinan pengguna bahwa aplikasi BSI Mobile dapat melindungi data pribadinya, menjaga kerahasiaan transaksi, serta mencegah akses ilegal dari pihak ketiga. Pengukuran persepsi keamanan mencakup aspek seperti keyakinan terhadap keamanan sistem, kepercayaan terhadap mekanisme otentikasi, serta rasa aman saat memasukkan data pribadi ke dalam aplikasi. Dengan demikian, indikator ini secara keseluruhan menggambarkan sejauh mana pengguna merasa aplikasi yang digunakan dapat diandalkan dari segi keamanan.

***Technology Acceptance Model*(TAM)**

Technology Acceptance Model (TAM) dikembangkan oleh Davis pada tahun 1989 melalui adaptasi dari Theory of Reasoned Action (TRA) yang lebih dulu dikenal- kan oleh oleh Ajzen dan Fishbein pada tahun 1975. Technology Acceptance Model digunakan untuk memodelkan penerimaan pemakai (user acceptance) terhadap teknologi. TAM menjelaskan bagaimana proses adopsi mengenai teknologi informasi dengan pendekatan teori perilaku (behavior theory). Pada saat ini TAM menjadi model yang penggunanya paling banyak untuk memprediksi para penerima teknologi informasi dengan alasan karena dianggap mudah diaplikasikan dan sederhana.

Technology Acceptance Model merupakan teori yang digunakan untuk

memprediksi tingkat penerimaan pemakaian teknologi yang berdasarkan persepsi terhadap kemudahan penggunaan teknologi informasi dan mempertimbangkan manfaatnya. TAM menjelaskan secara sederhana hubungan sebab akibat antara perilaku dan keyakinan (manfaat suatu sistem informasi dan kemudahan), tujuan, serta penggunaan aktual dari pengguna sistem informasi. Kegunaan persepsi (perceived usefulness) dan kemudahan penggunaan persepsian (perceived ease of use) keduanya mempunyai pengaruh ke minat perilaku (behavioral intention). Pemakai teknologi akan mempunyai minat menggunakan teknologi (minat perilaku) jika merasa sistem teknologi bermanfaat dan mudah digunakan.

Aspek-aspek Technology Acceptance Model

Technology Acceptance Model (TAM) memiliki lima dimensi, yaitu kemudahaan penggunaan (perceived ease of use), kemanfaatan (perceived usefulness), sikap dalam
menggunakan (attitude toward using), perilaku untuk tetap menggunakan (behavioral intention to use), dan kondisi nyata penggunaan sistem (actual system usage). Adapun hubungan antar variabel dapat digambarkan dan dijelaskan sebagai berikut:

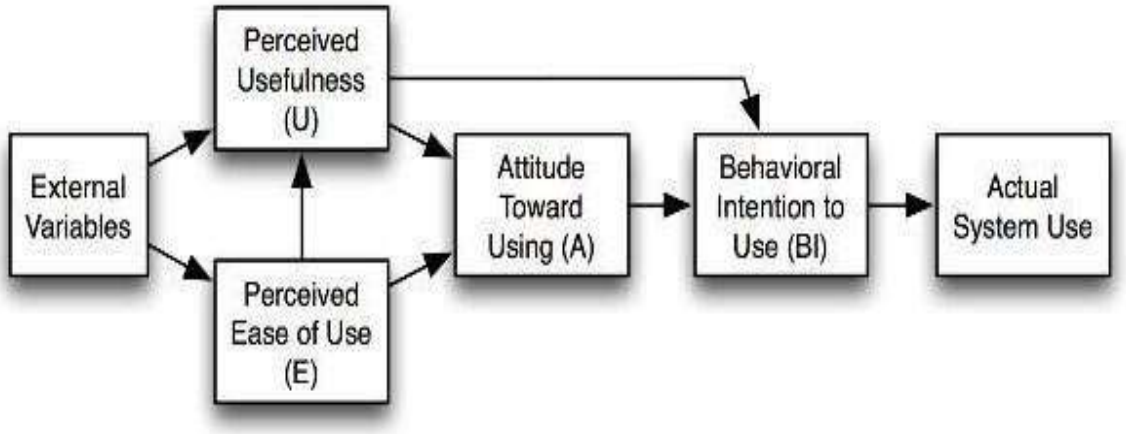

Diagram Aspek Aspek Teori TAM

a. Percieved Ease of Use (Persepsi Kemudahan Penggunaan)

Percieved Ease of Use atau persepsi kemudahan penggunaan adalah persepsi yang menerangkan mengenai seberapa besar seseorang memiliki kepercayaan bahwasanyadengan menggunakan teknologi, seseorang tersebut akan dapat terbebas dari segala bentuk usaha. Percieved ease of use merupakan sebuah tingkatan seberapa jauh kepercayaan seseorang bahwa teknologi adalah suatu hal yang mudah untuk dipahami. Perceived ease of use adalah sebuah ukuran seberapa besar kepercayaan seorang pengguna sistem dalam mempercayai bahwa sebuah teknologi bisa dengan mudah dipahami dan dapat dipergunakan untuk membantu meringankan beban pekerjaan yang dimiliki dengan mudah dan lebih cepat sehingga dapat meningkatkan kinerja para pengguna.

1. *Clear* (jelas), artinya bahwa layanan yang terdapat dalam teknologi tepat sesuai dengan kegunaan.
2. *Understandable* (sudah dipahami**)**, artinya bahwa fungsi dalam teknologi telekomunikasi mudah dipahami dan tidak menimbulkan kesalahpahaman.
3. *Does not require a lot of mental effort* (tidak memerlukan banyak usaha**)**, artinya bahwa dalam penggunaan teknologi tidak diperlukan usaha yang berat.*Easy of use* (mudah digunakan), artinya fitur yang ada didalam teknologi mudah untuk dioperasikan dan tidak menimbulkan kesulitan.

4. *Easy to get the system to do what he/she want to do* (mudah didapatkan saat akan digunakan), artinya bahwa sistem teknologi dapat dengan mudah didapatkan, pengguna hanya perlu untuk mengunduhnya melalui internet dan dapat langsung menggunakannya.

b. Percieved Usefulness (Persepsi kegunaan)

Percieved Usefulness atau persepsi kegunaan adalah sejauh-mana seseorang percaya bahwa menggunakan suatu teknologi akan meningkatkan kinerja pekerjaannya. Persepsi terhadap kegunaan merupakan sebuah kemampuan subjektif para pengguna untuk masa yang akan datang dimana dengan menggunakan sistem aplikasi yang spesifik akan meningkatkan kinerja dalam konteks organisasi. Percieved usefulness menunjukkan bahwa jika pengguna mempunyai rasa kepercayaan terhadap teknologi informasi dapat secara

mudah digunakan dan tidak sukar untuk dimengerti, maka percieved usefulness akan menyebabkan dampak positif terhadap minat untuk menggunakan sebuah teknologi. Seseorang akan dapat menggunakan sebuah teknologi informasi, apabila pengguna mempunyai pemahaman tentang apa yang bisa didapatkan, kegunaan, dan manfaat (usefulness) yang menguntungkan atas keputusan seseorang tersebut saat menggunakan teknologi.

Adapun aspek-aspek dan indikator dari Percieved Usefulness atau persepsi kegunaan adalah:

1. Mempercepat pekerjaan yang artinya dalam penggunaan teknologi dapat dapat membantu pekerjaan yang dimiliki oleh seorang konsumen menjadi lebih cepat.
2. Efektivitas artinya pada saat penggunaan sebuah teknologi konsumen dapat melakukan segala bentuk pekerjaan dalam waktu yang lebih singkat dari biasanya.
3. Bermanfaat yang berarti dalam menggunakan teknologi, para pengguna dapat merasakan manfaat dalam mempermudah pekerjaan.
4. Meningkatkan produktivitas yang memiliki arti bahwa dengan menggunakan sebuah teknologi, para pengguna akan dapat meningkatkan Produktivitas dalam bekerja.

c. Attitude Toward Using (Sikap Terhadap Pengaplikasian)

Attitude Toward Using atau sikap terhadap pengaplikasian adalah sikap terhadap penggunaan sistem yang berbentuk penerimaan atau penolakan sebagai dampak bila seseorang menggunakan suatu teknologi dalam pekerjaannya. Sikap seseorang terdiri atas unsur kognitif/cara pandang (cognitive), afektif (affective) dan komponen-komponen yang berkaitan dengan perilaku (behavioral components). Faktor sikap (attitude) sebagai salah satu aspek yang mempengaruhi perilaku individu. Sikap merupakan salah satu bentuk evaluasi terhadap konsekuensi setelah melaksanakan suatu perilaku.

d. Behavioral Intention to Use (Minat Perilaku Menggunakan)

Behavioral Intention to Use atau minat perilaku menggunakan adalah bentuk dari keinginan pengguna saat ingin menggunakan suatu obyek pada pertama kali atau menggunakan kembali obyek tersebut. Behavioral Intention to use adalah satu dari sekian aspek psikis dalam manusia yang memiliki kecenderungan untuk memberikan perhatian dan perasaan senang yang lebih besar terhadap obyek tersebut, yang mana perasaan ini bisa menimbulkan dorongan bagi seseorang untuk mencapai tujuan. Intention to use dapat dijadikan sebagai gambaran tentang situasi seseorang sebelum bertindak, dan intention to use juga bisa menjadi faktor dasar untuk memprediksi tindakan dan perilaku seseorang.

e. Actual System Use (Kondisi Nyata Penggunaan Sistem)

Actual System Use atau kondisi nyata penggunaan sistem adalah bentuk pengukuran terhadap frekuensi dan durasi waktu penggunaan teknologi. Dengan kata lain, pengukuran penggunaan sesungguhnya (actual use) diukur sebagai jumlah waktu yang

digunakan untuk berinteraksi dengan suatu teknologi dan besarnya frekuensi penggunaannya. Seseorang akan puas menggunakan sistem jika meyakini bahwa sistem tersebut mudah digunakan dan akan meningkatkan produktivitas-nya, yang tercermin darikondisi nyata penggunaan.

3. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian kuantitatif. Sumber data dalam penelitian ini adalah data primer. Data primer yang digunakan penulis yaitu melalui kuisioner yang dibagikan secara daring menggunakan *google form* yang diberikan langsung kepada responden. Menurut (Sugiyono dalam Galih,2020) populasi merupakan objek atau subjek yang memiliki kualitas dan karakteristik yang diinginkan peneliti untuk mengambil untuk diambil kesimpulan dalam wilayah tertentu. Sampel adalah bagian dari populasi yang jawabannya dapat mewakili populasi yang ditentukan. Populasi dalam penelitian ini adalah seluruh nasabah BSI yang memiliki Bsi mobile di Kota Medan. Penelitian ini menggunakan Purposive sampling adalah sebuah teknik penentuan sampel non-probabilitas (non-random) yang dilakukan oleh peneliti berdasarkan kriteria atau pertimbangan tertentu yang dianggap relevan dan sesuai dengan tujuan penelitian, sehingga informasinya spesifik dan kaya. Untuk mengetahui jumlah responden untuk jumlah populasi yang terlalu besar,untuk mencari jumlah sampel penelitian menggunakan rumus slovin yaitu:

$$n = \frac{N}{1 + Ne^2}$$

Keterengan:
n = Ukuran Sampel N= Ukuran Populasi
e = Tingkat Kesalahan yang di toleransi (0,1)

$$n = \frac{7{,}120.000}{1 + 7{,}120.000(0{,}1)^2}$$

$$n = \frac{7{,}120.000}{71{,}201}$$

$$n = 99{,}99$$

Maka jumlah sampel yang didapatkan untuk penelitian adalah 99,99 atau digenapkan menjadi 100 responden. Teknik pengambilan sampel dilakukan dengan purposive sampling, yaitu pemilihan responden berdasarkan kriteria tertentu:

(1) pengguna aktif BSI Mobile,
(2) berusia minimal 17 tahun, dan
(3) bersedia mengisi kuesioner secara mandiri dan lengkap.

Variabel independen (X) pada penelitian ini adalah Sosial Engineering dan Cyber Crime. dan variabel dependen (Y) Pada penelitian ini adalah Persepsi Keamanan Pada Aplikasi BSI Mobile. Teknik analisis data dalam penelitian ini adalah menggunakan Uji regresi linear berganda untuk melihat pengaruh variable independen terhadap dependen. Dan Uji asumsi klasik (normalitas, multikolinearitas, heteroskedastisitas).

4. HASIL DAN PEMBAHASAN

Hasil Analisis Statistik Deskriptif

Variabel	N	Minimum	Maksimum	Mean	Std. Dev
Social Engineering	100	2	10	5,49	1,432
Cyber Crime	100	1	5	4,03	0,745
Persepsi Keamanan	100	4	10	6,96	1,197

Berdasarkan tabel di atas, variabel Social Engineering memiliki rata-rata 5,49 dengan standar deviasi 1,432, menunjukkan bahwa tingkat kewaspadaan terhadap ancaman sosial relatif sedang. Variabel Cyber Crime memiliki rata-rata 4,03, yang menunjukkan bahwa sebagian besar responden cukup menyadari bahaya kejahatan siber. Sedangkan persepsi keamanan berada pada nilai rata-rata 6,96, yang menunjukkan bahwa mayoritas responden merasa cukup aman dalam menggunakan aplikasi BSI Mobile.

Uji Reliabilitas

Cronbach's Alpha	Jumlah Item	Keterangan
0,741	3	Reliabel

Nilai Cronbach's Alpha sebesar 0,741 mengindikasikan bahwa instrumen kuesioner yang digunakan memiliki tingkat reliabilitas yang baik dan layak digunakan dalam penelitian ini.

Uji Normalitas

Z K-S	Sig. (2-tailed)	Keterangan
1,320	0,061	Data berdistribusi normal

Nilai signifikansi Kolmogorov-Smirnov sebesar 0,061 > 0,05 menunjukkan bahwa data residual berdistribusi normal. Maka, asumsi normalitas terpenuhi.

Uji Multikolinearitas

Variabel	Tolerance	VIF
Social Engineering	0,996	1,004
Cyber Crime	0,996	1,004

Nilai Tolerance > 0,1 dan VIF < 10 menunjukkan bahwa tidak terdapat gejala multikolinearitas antara variabel independen.

Uji Heteroskedastisitas (Glejser)

Variabel	Sig.	Keterangan
Social Engineering	0,274	Heteroskedastisitas tidak terjadi
Cyber Crime	0,431	Heteroskedastisitas tidak terjadi

Karena nilai signifikansi kedua variable > 0,05, maka tidak terdapat indikasi heteroskedastisitas. Hal ini menunjukkan bahwa varians residual tidak konstan.

Hasil Uji Regresi Linear Berganda

Uji F (Simultan)

F-hitung	Sig.	Keterangan
45,213	0,000	Signifikan (berpengaruh simultan)

Model regresi menunjukkan bahwa Social Engineering dan Cyber Crime secara

simultan berpengaruh signifikan terhadap persepsi keamanan pengguna.

Koefisien Determinasi (R^2)

R Square	Adjusted R^2	Keterangan
0,600	0,591	60% variasi dijelaskan oleh model

Nilai R Square sebesar 0,600 menunjukkan bahwa kedua variabel independen menjelaskan 60% perubahan dalam variabel persepsi keamanan, sedangkan sisanya dipengaruhi oleh faktor lain di luar model.

Pembahasan Hasil Penelitian

Pengaruh Social Engineering terhadap Persepsi Keamanan

Berdasarkan hasil uji t, variabel Social Engineering memiliki nilai signifikansi sebesar 0,006 (< 0,05) dan nilai t sebesar 0,312. Hal ini menunjukkan bahwa Social Engineering berpengaruh positif dan signifikan terhadap Persepsi Keamanan. Artinya, secara parsial, semakin tinggi kewaspadaan pengguna terhadap ancaman seperti phishing atau penipuan digital, maka semakin tinggi pula persepsi keamanan yang dirasakan saat menggunakan aplikasi digital seperti BSI Mobile. Hubungan positif ini dapat dijelaskan secara logis melalui tingkat literasi keamanan digital pengguna. Ketika pengguna memiliki pengetahuan yang cukup untuk mengenali pola-pola serangan siber, mereka akan merasa lebih mampu melindungi diri, sehingga muncul rasa percaya diri dan rasa aman dalam berinteraksi dengan aplikasi. Dalam konteks ini, persepsi keamanan tidak hanya dibentuk oleh teknologi atau sistem aplikasi itu sendiri, tetapi juga oleh *self-awareness* pengguna dalam menghadapi potensi risiko. Temuan ini menunjukkan bahwa edukasi mengenai ancaman cyber dan peningkatan kewaspadaan pengguna memiliki peran penting dalam menciptakan rasa aman di era digital. Mungkin para pengguna yang lebih sering melakukan transaksi ke bank langsung kurang memperhatikan mobile banking nya sehingga tidak berfikir ke hal ini.

Dari mulai jangan mengklik file yang dikirim oleh nomor tidak dikenal,dan juga jangan mendownload dari situs-situs yang memiliki virus,sehingga tidak akan terjadinya hack dari hp pemilik. Mungkin bagi mereka yang sudah paham pasti mungkin sudah tau car mencegahnya,walaupun dari hal-hal kecil,mulai dari memisahkan email mobile banking dengan email sehari-haro,dan juga nomor telfon yang terdaftar di mobile banking dipisahkan dengan yang digunakan untuk sehari-hari.

Hasil ini sejalan dengan penelitian Ramadhan dan Sari (2021) yang menunjukkan bahwa kesadaran terhadap ancaman rekayasa sosial dapat meningkatkan sikap protektif pengguna dalam aktivitas digital. Namun, berbeda dengan temuan Fauzan (2020) yang menyatakan bahwa pengaruh social engineering tidak signifikan pada pengguna yang memiliki tingkat literasi keamanan digital rendah.

Pengaruh Cyber Crime terhadap Persepsi Keamanan

Hasil uji t menunjukkan bahwa variabel Cyber Crime memiliki nilai signifikansi sebesar 0,003 (< 0,05) dan nilai t sebesar 2,165. Ini berarti Cyber Crime berpengaruh positif dan signifikan terhadap Persepsi Keamanan. Semakin tinggi pemahaman atau kesadaran individu terhadap kejahatan siber, maka semakin besar pula persepsi mereka akan pentingnya keamanan saat menggunakan layanan digital.

Hal ini menunjukkan bahwa pemahaman dan kesadaran pengguna terhadap berbagai bentuk cyber crime seperti pencurian data, peretasan akun, penyebaran malware, dan modus penipuan digital berkontribusi secara nyata dalam membentuk persepsi mereka terhadap pentingnya keamanan saat menggunakan aplikasi layanan keuangan digital. Semakin tinggi pengetahuan individu terhadap ancaman tersebut, semakin tinggi pula

kewaspadaan mereka, sehingga menumbuhkan rasa aman karena merasa mampu mengendalikan risiko. Secara logis, hubungan positif ini dapat dijelaskan melalui tingkat literasi keamanan digital pengguna. Ketika pengguna memahami potensi risiko dan langkah-langkah pencegahannya, seperti penggunaan autentikasi ganda, penghindaran akses melalui jaringan publik, serta kemampuan mengenali aktivitas mencurigakan, maka mereka tidak hanya lebih siap secara teknis, tetapi juga merasa lebih percaya diri dalam menggunakan aplikasi. Misalnya, pengguna yang paham bahwa menggunakan Wi-Fi publik tanpa VPN bisa membuka risiko penyadapan data, akan menghindarinya. Tindakan ini memberi rasa aman secara psikologis, karena pengguna merasa tahu cara melindungi dirinya sendiri, bukan hanya bergantung pada sistem.

Temuan ini menunjukkan bahwa persepsi keamanan tidak hanya dipengaruhi oleh sistem dan fitur keamanan yang disediakan oleh pihak penyedia aplikasi, tetapi juga sangat dipengaruhi oleh pemahaman dan kesiapan pengguna itu sendiri. Oleh karena itu, peningkatan literasi keamanan siber merupakan aspek penting yang harus diperhatikan oleh lembaga perbankan digital dalam menciptakan rasa aman bagi para penggunanya.

Penemuan ini sejalan dengan penelitian dari Aziz dan Nurhaliza (2022) yang menyebutkan bahwa kekhawatiran terhadap risiko kejahatan siber mendorong individu lebih sadar terhadap pentingnya keamanan sistem informasi. Berbeda dengan Kurniawan (2018**)** yang menyatakan bahwa persepsi keamanan lebih banyak dipengaruhi oleh aspek kenyamanan dan desain antarmuka aplikasi, bukan oleh pemahaman tentang cyber crime.

Pengaruh Social Engineering dan Cyber Crime terhadap Persepsi Keamanan secara Simultan

Berdasarkan hasil uji F (ANOVA), diperoleh nilai F hitung sebesar 45,213 dengan nilai signifikansi 0,000 (< 0,05). Ini menunjukkan bahwa variabel Social Engineering dan Cyber Crime secara simultan berpengaruh signifikan terhadap Persepsi Keamanan. Artinya, kedua variabel secara bersama-sama mampu menjelaskan variasi yang terjadi pada persepsi keamanan pengguna aplikasi.

Hal ini berarti bahwa kedua variabel tersebut, ketika digabungkan dalam satu model analisis, secara bersama-sama mampu menjelaskan perubahan atau variasi yang terjadi pada persepsi keamanan pengguna. Dengan kata lain, persepsi pengguna terhadap keamanan digital dipengaruhi oleh kombinasi antara kewaspadaan terhadap manipulasi sosial dan pemahaman terhadap ancaman kejahatan siber.

Temuan ini menegaskan bahwa pendekatan keamanan digital tidak cukup hanya fokus pada teknologi, tetapi juga harus memperhatikan faktor manusia. Oleh karena itu, peningkatan keamanan aplikasi perbankan digital seperti BSI Mobile harus dilakukan secara holistik, yaitu dengan memperkuat sistem keamanan internal sekaligus meningkatkan kesadaran dan literasi pengguna terhadap ancaman yang bersifat teknis maupun manipulatif.

Hasil ini diperkuat oleh temuan Maulana dan Dewi (2021) yang menyatakan bahwa kombinasi antara kewaspadaan terhadap ancaman digital dan pemahaman terhadap risiko kejahatan siber akan membentuk persepsi yang lebih kuat mengenai pentingnya perlindungan data dan keamanan informasi pribadi.

5. KESIMPULAN DAN SARAN

Kesimpulan

1. Berdasarkan hasil penelitian yang telah dilakukan terhadap 100 responden pengguna aplikasi BSI Mobile, dapat disimpulkan bahwa Sosial Engineering dan Cyber Crime memiliki pengaruh signifikan terhadap Persepsi Keamanan Pengguna.

2. Hasil uji parsial menunjukkan bahwa masing-masing variabel independen, yaitu Sosial Engineering dan Cyber Crime, berpengaruh secara signifikan terhadap persepsi keamanan. Selain itu, hasil uji simultan memperkuat temuan bahwa kedua variabel tersebut secara bersama-sama berkontribusi dalam membentuk persepsi keamanan pengguna terhadap aplikasi BSI Mobile.
3. Dengan demikian, penting bagi pihak pengembang dan penyedia layanan perbankan digital untuk meningkatkan perlindungan terhadap ancaman sosial engineering dan kejahatan siber guna menjaga kepercayaan dan rasa aman pengguna.

Saran

Berdasarkan hasil penelitian, penulis menyarankan agar Bank Syariah Indonesia (BSI) meningkatkan sistem keamanan aplikasi BSI Mobile, baik melalui penguatan teknologi maupun edukasi pengguna terkait ancaman seperti social engineering dan cyber crime. Pengguna juga diharapkan lebih waspada serta memahami fitur keamanan digital yang tersedia. Penelitian selanjutnya dapat menambahkan variabel lain seperti kepercayaan pengguna atau kualitas sistem untuk memperoleh hasil yang lebih komprehensif. Selain itu, temuan ini diharapkan dapat menjadi referensi akademik dalam studi keamanan digital dan perilaku pengguna layanan perbankan syariah.

DAFTAR PUSTAKA

Amalia, P., & Hastriana, A. Z. (2022). Pengaruh kemanfaatan, kemudahan keamanan, dan fitur m-banking terhadap kepuasan nasabah dalam bertransaksi pada bank syariah indonesia (studi kasus BSI KCP sumenep). *Alkasb: Journal of Islamic Economics, 1*(1), 70- 89.

Darmaningrat, E. T., Ali, A. H. N., Herdiyanti, A., Subriadi, A. P., Muqtadiroh, F. A., Astuti, H. M., & Susanto, T. D. (2022). Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi. *Sewagati*, *6*(2), 159-168.

Dianta, I. A., & Zusrony, E. (2019). Analisis Pengaruh Sistem Keamanan Informasi Perbankan pada Nasabah Pengguna Internet Banking. *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, *3*(1), 1-9.

Fahlevi, P., & Dewi, A. O. P. (2020). Analisis Aplikasi Ijateng Dengan Menggunakan Teori Technology Acceptance Model (TAM). *Jurnal Ilmu Perpustakaan*, *8*(2), 103-111.

Hendarsyah, D. (2012). Keamanan Layanan Internet Banking Dalam Transaksi Perbankan. *IQTISHADUNA: Jurnal Ilmiah Ekonomi Kita*, *1*(1), 12-33.

Maulana, L., & Fitriana, N. (2023). Analisis dampak Insiden BSI Eror dan Dugaan Hacking Bank Syariah Indonesia (BSI) terhadap kepercayaan dan loyalitas nasabah Bank Syariah Indonesia di Kabupaten Subang. *Rayah Al-Islam*, *7*(3), 1755-1768.

Maulana, N., Laurens, T., Faiz, D. H. A., & Patrianti, T. (2024). Manajemen Krisis PT. BSI Tbk Pasca Peretasan Data Nasabah. *INNOVATIVE: Journal Of Social Science Research*, *4*(1), 8244-8258.

Mauliza, A. Y. I., Machmudi, R. D. S., & Indrarini, R. (2022). Pengaruh Perlindungan Data Dan Cyber Security Terhadap Tingkat Kepercayaan Menggunakan Fintech Masyarakat Di Surabaya. *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan*, *1*(11), 2497-2516.

Putri, D. F., Sari, W. R., & Nabbila, F. L. (2023). Analisis Perlindungan Nasabah Bsi Terhadap Kebocoran Data Dalam Menggunakan Digital Banking. *Jurnal Ilmiah Ekonomi Dan Manajemen*, *1*(4), 173-181.

Rahayu, A. D. OPTIMALISASI SISTEM KEAMANAN BANK DALAM PENCEGAHAN PENCURIAN DATA NASABAH.

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).

Ratulangi, C. H. (2021). Tindak pidana cyber crime dalam kegiatan perbankan. *Lex Privatum*, *9*(5).

Setyaningrat, D., Mushlihin, I. A., & Zunaidi, A. (2023). Strategi digitalisasi untuk mendorong inklusi keuangan nasabah bank syariah: Pendekatan Technology Acceptance Model (TAM). *Proceedings of Islamic Economics, Business, and Philanthropy*, *2*(1), 53-76.

Sulisrudatin, N. (2018). Analisa kasus cybercrime bidang perbankan berupa modus pencurian data kartu kredit. *Jurnal Ilmiah Hukum Dirgantara*, *9*(1).

Wandi, J., Bachri, S., & Parubak, B. (2020). Pengaruh Persepsi Kegunaan, Persepsi Keuntungan, Persepsi Keamanan Terhadap Minat Nasabah Bni Menggunakan Mobile Banking. *Jurnal Ilmu Manajemen Universitas Tadulako (JIMUT)*, *6*(1), 88-96.

Kesuma, P., & Nurbaiti, N. (2023). Minat Menggunakan E-Wallet Dana Di Kalangan Mahasiswa Di Kota Medan. *Jesya (Jurnal Ekonomi dan Ekonomi Syariah)*, *6*(1), 694-703.

Nasution, M. I. P., Nurbaiti, N., Nurlaila, N., Rahma, T. I. F., & Kamilah, K. (2020, September). Face recognition login authentication for digital payment solution at COVID-19 pandemic. In *2020 3rd International Conference on Computer and Informatics Engineering (IC2IE)* (pp. 48-51). IEEE.

Rahma, T. I. F. (2018). Persepsi masyarakat Kota Medan terhadap penggunaan financial technology. *At-tawassuth: jurnal ekonomi islam*, *3*(1), 184-203.

Seputri, W., Soemitra, A., & Rahmani, N. A. B. (2023). Pengaruh Technolgy Acceptance Model terhadap Minat Mahasiswa Menggunakan Quick Response Code Indonesian Standard (QRIS) sebagai Cashless Society. *MES Management Journal*, *2*(1), 116-126.

Soemitra, A. (2022). Perlindungan konsumen terhadap kebocoran data pada jasa keuangan di Indonesia. *Juripol (Jurnal Institusi Politeknik Ganesha Medan)*, *5*(1), 288-303.

Nurhayani, N., Kamilah, K., & Rahmani, N. A. B. (2024). Pengaruh Penggunaan Digital Banking Sebagai Layanan Transaksi Online Terhadap Kepuasan Nasabah Bank Bsi Syariah Kabupaten Langkat. *JURNAL ILMIAH EDUNOMIKA*, *8*(1).

Fadhillah, N., Nasution, M. I. P., & Syahbudi, M. (2023). Peranan Penting Internet Terhadap Peningkatan Pendapatan Gen-Z Pada Usaha Technopreneurship. *Student Research Journal*, *1*(5), 57-73.