HUMANITIS: Jurnal Humaniora, Sosial dan Bisnis
Vol. 2 No. 7 Juli 2024, hal. 748-752 e-ISSN: 2988-6287

JURNAL REVIEW : KONSEP KEAMANAAN PERBANKAN DI ERA DIGITAL

Putra Dena Pangestu[1], Hagi Vander Khan[2], Ghani Irfan Susanto[3], Ayub Trisna Mukti[4], Mochammad Rifan Arkaan[5], Muhammad Bimo Ferlyando[6]
Teknik Industri, Fakultas Teknik UBJ, Bekasi, Indonesia
e-mail: [1]202210215006@ubharajaya.ac.id, [2]202210215022@ubharajaya.ac.id,
[3]202210215026@ubharajaya.ac.id, [4]202210215035@ubharajaya.ac.id,
[5]202210215014@ubharajaya.ac.id, [6]202210215011@ubharajaya.ac.id
Corresponding author* : **Tubagus Hedi Saepudin
e-mail : tubagus.hedi@dsn.ubharajaya.ac.id

Abstract

Increased use of the internet and smartphones in Indonesia, driven by the development of e-commerce and strong digital transformation efforts at banks, has accelerated the migration towards digital banking services. This is demonstrated by the high adoption of digital technology, especially in terms of digital banking. However, there are no clear standards for how well digital banking app users are aware of the security of their data. The aim of this study is to evaluate the level of awareness that digital banking service users have regarding the security of their data to prevent social engineering incidents. In this research, the Knowledge-Attitude-Behavior (KAB) model is used in the Questionnaire of Human Aspects of Information Security (HAIS-Q), as well as a nomenclature for understanding cellular customer information security. The data was combined through a questionnaire distributed to 299 people who met the requirements as respondents. The research results show that digital banking application users in Indonesia have quite good information security awareness, with a score of 81.30% in the knowledge dimension, 84.45% (good), attitude 84.68% (good), and behavior 78.06 % (Enough). Based on these findings, to reduce the threat of social engineering, it is recommended to strengthen regulations relating to the installation of illegal applications and increase awareness training materials on data security. Overall, this study succeeded in testing the level of understanding of digital banking application users in Indonesia regarding the security of their data, with a final score of 81.30%.

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

Abstrak

Peningkatan penggunaan internet dan smartphone di Indonesia, didorong oleh perkembangan e-commerce dan upaya kuatnya transformasi digital pada bank-bank, telah mempercepat migrasi menuju layanan perbankan digital. Ini ditunjukkan oleh adopsi tinggi teknologi digital, terutama dalam hal perbankan digital. Namun, tidak ada standar yang jelas tentang seberapa baik pengguna aplikasi perbankan digital menyadari keamanan data mereka. Tujuan studi ini adalah agar mengevaluasi tahap kesadaran yang dimiliki pemakai layanan perbankan digital tentang keamanan data mereka untuk mencegah insiden rekayasa sosial. Dalam penelitian ini, model Knowledge-Attitude-Behavior (KAB) digunakan pada *Questionnaire of Human Aspects of Information Security* (HAIS-Q), serta tata nama pemahaman tentang keamanan informasi pelanggan seluler. Data dijadikan satu melalui kuesioner yang dibagikan kepada 299 orang yang memenuhi syarat sebagai responden. Hasil penelitian menunjukkan bahwa pengguna aplikasi perbankan digital di Indonesia memiliki kesadaran keamanan informasi yang cukup baik, dengan nilai 81,30% pada dimensi pengetahuan, 84,45% (baik), sikap 84,68% (baik), dan

perilaku 78,06% (cukup). Berdasarkan temuan ini, untuk mengurangi ancaman rekayasa sosial, disarankan untuk memperkuat regulasi yang berkaitan dengan penginstalan aplikasi ilegal dan meningkatkan materi pelatihan kesadaran tentang keamanan data. Secara keseluruhan, studi ini berhasil menguji tingkat pemahaman pengguna aplikasi perbankan digital di Indonesia tentang keamanan data mereka, dengan nilai akhir 81,30%.
Kata kunci: Pemahaman Data Keamanan; Perbankan Aplikasi; Rekayasa Sosial; Pengetahuan Sikap-Perilaku (KAB).

PENDAHULUAN

Studi yang dilakukan oleh Company & McKinsey yang menyertakan 17.000 individu dari 15 negara Asia menemukan sampai Indonesia adalah negara yang paling cepat mengadopsi teknologi digital, terutama dalam sektor perbankan digital. Menurut penelitian, dua hingga tiga produk layanan perbankan digital digunakan secara aktif oleh penduduk di perkotaan Indonesia. Selain itu, peningkatan yang signifikan dalam penggunaan internet dan ponsel pintar, bersama dengan lonjakan e-commerce, telah mendorong sektor perbankan di Indonesia untuk mendorong digitalisasi, yang pada gilirannya mempercepat peralihan mereka ke layanan perbankan digital.

Dalam beberapa tahun terakhir, transaksi perbankan digital telah meningkat seiring dengan meningkatnya jumlah pengguna. Transaksi digital tercatat meningkat 45,64 persen pada tahun 2021, menjadi Rp39.841,4 triliun (Fiona & Rahmayanti, 2022) Namun, peningkatan ini juga diikuti oleh peningkatan ancaman keamanan digital. Dilaporkan bahwa terdapat lima kali lipat jumlah serangan siber pada tahun 2020 dibandingkan tahun sebelumnya. Laporan World Economic Forum (2021) dalam Global Risk Report 2021 menyatakan bahwa serangan siber menggunakan berbagai metode, termasuk phishing, penipuan OTP, pertukaran SIM, kelemahan sistem keuangan dan perbankan, dan rekayasa sosial.

Meskipun pemakaian teknologi unit seluler telah meningkat dengan cepat di seluruh dunia, ada juga risiko keamanan yang signifikan. Dalam hal ini, kesadaran pengguna sangat penting untuk menjaga keamanan. Pengguna sering dihalangi oleh malware, phishing, aplikasi berbahaya, spam, pencurian identitas, jaringan internet yang tidak aman, dan rekayasa sosial. Ketidaktahuan dapat menyebabkan ancaman seperti mengungkapkan data pribadi, perilaku penjelajahan web, penggunaan kata sandi yang buruk, dan penggunaan beberapa perangkat sekaligus.

Salah satu contoh rekayasa sosial yang terjadi pada pengguna aplikasi perbankan digital adalah ketika pengguna memberikan OTP kepada orang yang mengaku petugas bank. Selain itu, ada laporan bahwa pengguna kehilangan barang setelah membuka aplikasi perbankan digital, yang kemudian dianggap tidak sah (Putri et al., 2022). Studi Utaminingsih (2014) mendemonstrasikan model evaluasi kesadaran keamanan informasi yang memberikai ulasai menjadi tiga aspek: Pengetahuan, Sikap, dan Perilaku (KAB). Parsons dan rekannya (2017) menggunakan model KAB untuk membangun Kuisioner Aspek Manusia Keamanan Informasi (HAIS-Q), yang mengukur kesadaran keamanan informasi pengguna. Selain itu, taksonomi juga digambarkan dengan model KAB.

METODE PENELITIAN

Studi ini bertujuan untuk mengukur tingkat kesadaran pengguna aplikasi perbankan tentang keamanan data mereka dengan tujuan mencegah rekayasa sosial. Studi ini berfokus pada pengguna

perbankan digital di Indonesia. Ada 15 aplikasi perbankan digital yang sah dan resmi dipilih dalam penelitian ini: NeoBank, Bank Allo, OCTO Mobile oleh CIMB Niaga, Aladin oleh Bank Aladin Syariah, Permata Mobile X oleh CIMB Niaga, Seabank, BNI Mobile Banking, BCA Mobile atau MyBCA, Jago oleh Jago Bank Jago, BSI Mobile, Livin oleh Mandiri, BRImo BRI, Jenius oleh BTPN, Digibank Indonesia, dan Motion Perbankan oleh MNC Bank. Diharapkan bahwa penelitian ini akan berkontribusi besar pada upaya untuk menghentikan rekayasa sosial di kalangan pemakaian aplikasi perbankan.

HASIL DAN PEMBAHASAN

Menurut Mattord & Whitman (2011), keamanan informasi adalah upaya untuk melindungi informasi, termasuk semua bagian pentingnya, serta sistem dan *hardware* yang diaplikasikan untuk mengirim, mengaksesnya, dan menyimpan. Kerahasiaan, integritas, dan ketersediaan adalah tiga sifat penting dari informasi yang memberikan nilai bagi organisasi.

Ketika karyawan suatu organisasi menyadari dan memahami tujuan organisasi untuk menjaga keamanan data mereka, itu disebut kesadaran keamanan data (Tiatama, 2016). Pengertian ini mencakup pemahaman individu tentang keamanan informasi dalam organisasi dan kebijakan keamanan informasi. (Bauer & Bernroider, 2017).

Penelitian sering menggunakan model dimensi pengetahuan, sikap, dan perilaku untuk mengukur kesadaran keamanan informasi. Model ini menetapkan bahwa pengetahuan adalah apa yang didapati atau dipahami manusia, sikap ialah apa yang dirasakan atau dipikirkan oleh seseorang, serta perilaku adalah apa yang mereka lakukan. (Mukhtaruddin et al., 2019). Mengubah perilaku adalah tujuan utama dari inisiatif kesadaran keamanan informasi. Memahami tingkat pengetahuan dan perilaku dapat membantu mencapai tujuan ini.

Selain itu, pendapat lain dari Bitton yaitu membuat kerangka dimensi KAB untuk mengukur kesadaran keamanan pengguna ponsel. Mereka memberi keamanan seluler dijadikan 4 bidang pusat: eksplorasi dan komunikasi, perangkat, saluran komunikasi, dan aplikasi.

a.Mary J. Cronin menjelaskan bahwa Internet Banking merupakan layanan keuangan dalam bentuk aplikasi yang memungkinkan lembaga keuangan untuk menyediakan produk dan layanan perbankan tradisional seperti pengecekan saldo tabungan, rekening pasar uang, dan sertifikat deposito melalui internet.

b. David Whiteley menggambarkan Internet Banking adalah layanan yang diberikan oleh bank kepada nasabahnya. dengan tujuan memungkinkan nasabah untuk melakukan pengecekan saldo rekening dan pembayaran tagihan secara online selama 24 jam tanpa perlu mengunjungi kantor cabang.

c. Menurut Steve Clarke dan Mahmood Shah, Internet Banking merupakan penyediaan informasi tentang bank dan layanannya melalui halaman website di World Wide Web (WWW). Layanan yang tersedia termasuk akses pelanggan terhadap rekening mereka, kemampuan untuk mentransfer dana antar rekening yang berbeda, dan kemampuan untuk melakukan pembayaran atau mengajukan pinjaman melalui saluran elektronik. Internet Banking memiliki tiga tingkatan definisi berdasarkan layanan yang ditawarkan oleh bank kepada nasabah:

a.Tingkat Entry :
Dalam konteks Internet Banking adalah tingkatan yang paling dasar, di mana hanya menyajikan informasi statistik tentang bank, layanan atau produk yang ditawarkan, dan juga layanan dasar seperti perhitungan estimasi pembayaran pinjaman. Pada tingkat ini, fokus utamanya adalah pada tampilan situs yang baik di browser web.
b.Tingkat Intermediate:
Pada tingkat ini, Anda menyediakan semua layanan informasi keuangan yang tersedia pada tingkat awal, bersama dengan layanan interaktif dasar yang mencakup perhitungan pembayaran kredit dan kemampuan untuk menampilkan rincian simpanan klien.
c.Tingkat Advanced:
Pada tingkat Advanced, Internet Banking dapat dikarakterisasi sebagai tingkat layanan yang paling lengkap, yang mencakup seluruh fungsionalitas dan aspek keamanan. Pada tingkat ini, nasabah bank memiliki kemampuan untuk melakukan transfer dana antar bank, membayar tagihan, serta membuka simpanan baru.

Fasilitas Internet Banking

Fasilitas Internet Banking seringkali hampir identik dengan fasilitas transaksi tradisional di bank, tetapi transaksi tradisional memerlukan kehadiran fisik di bank. Secara umum, layanan pembayaran melalui internet dapat dibagi menjadi 2 kategori:

A. Fasilitas Transaksional

Fasilitas Transaksional adalah layanan yang secara langsung terkait dengan rekening dan setiap transaksi dicatat dalam rekening tersebut. Fasilitas ini mencakup:

1. Transaksi pembelian dan penjualan investasi
2. Aplikasi dan transaksi pinjaman
3. Pembelian tiket
4. Proses kliring
5. Pembayaran zakat, sedekah, dan wakaf
6. Proses persetujuan transaksi
7. Pembayaran tagihan (seperti listrik, telepon/handphone, dan air)
8. Dan layanan lainnya.

B. Fasilitas Non Transaksional

layanan yang dipakai ialah melakukan tugas administratif yang tidak berkaitan dengan transaksi rekening atau melihat data rekening. Ini termasuk fitur berikut:

1. Mengunduh aplikasi Mobile Bangking
2. Memesan buku cek
3. Mengganti sandi
4. Memeriksa saldo rekening
5. Daftar rekening
6. Unduh laporan transaksi
7. Melihat riwayat transaksi terakhir
8. Dan layanan lainnya.

Manfaat Internet Banking

Manfaat Internet Banking: Setiap layanan yang ditawarkan oleh bank memiliki keuntungan bagi kedua pihak, bank dan pelanggannya. Berikut adalah beberapa manfaat dari Internet Banking:

A. Biaya operasional seperti kertas, percetakan, dan alat tulis dapat dikurangi dengan menggunakan internet banking.
B. Memungkinkan pelanggan bank melakukan transaksi seperti memeriksa saldo, mentransfer dana, memeriksa transaksi, membayar tagihan, dan lainnya tanpa perlu pergi ke bank atau ATM, kecuali untuk setoran tunai atau penarikan tunai. Sebagai contoh, pelanggan yang menjalankan bisnis online mereka dapat langsung melihat apakah uang yang ditransfer oleh klien atau pelanggan mereka telah masuk atau tidak.
C. Bagi bank, hal ini memungkinkan pengurangan jumlah karyawan atau staf operasional, yang menghasilkan efisiensi dalam penggunaan ruang.
F. Bank dapat memperluas cakupannya ke seluruh dunia, memungkinkan nasabah untuk mengakses layanan bank dari mana pun di dunia dengan fleksibilitas waktu yang tidak terbatas.

Jenis Serangan Terhadap Internet Banking

Karena selalu ada orang yang berusaha memanfaatkan atau menguji keamanan perangkat yang terkoneksi ke Internet, yang berpotensi menghadapi ancaman keamanan. Pengaplikasian perbankan seperti internet banking juga bisa diserang dalam segi keamanan, terutama karena langsung terhubung dengan rekening nasabah yang memiliki jumlah uang tertentu, yang membuat mereka menjadi sasaran bagi orang yang ingin merusak keamanan mereka. Beberapa jenis gangguan keamanan yang melibatkan perbankan online meliputi:

a. Remote attacks :

Serangan jarak jauh (remote attacks) adalah upaya untuk mengambil alih atau mengendalikan akses tanpa izin dari pihak asing atau yang tidak bertanggung jawab. Jenis-jenis serangan jarak jauh ini dapat diklasifikasikan sebagai berikut:

1) Phishing :

Serangan jarak jauh yang umumnya menyerang layanan keuangan online. Penyerang menciptakan situs web yang mirip persis dengan situs aslinya dan menggunakan alamat web yang serupa untuk mengelabui korban. Mereka kemudian mengirimkan email ke sejumlah akun email, berisi tautan (yang merupakan alamat situs palsu yang tersembunyi) yang harus diklik oleh korban. Penyerang meyakinkan korban bahwa ada masalah dengan server atau memberikan alasan lain yang masuk akal, sering kali dengan janji hadiah atau uang. Karena itu, korban tergoda untuk mengklik tautan palsu dan memberikan data pribadi mereka untuk fasilitas keuangan khusus. Penyerang lalu menggunakan informasi ini untuk pencurian atau tujuan yang tidak diinginkan lainnya.

2) Interception:

Penyadapan adalah ketika pihak yang tidak sah berhasil mengakses aset atau informasi. Contoh dari penyerangan penyadapan:

a. Local attacks :

Serangan lokal, juga disebut sebagai serangan lokal, terjadi pada komputer lokal dan dapat dilakukan oleh virus seperti trojan atau perangkat lunak yang dapat merekam kunci atau keylogger. Meskipun situs web menggunakan Secure Socket Layer (SSL), Trojan dapat mengambil data pengguna. Keylogger sekarang lebih canggih. Mereka sekarang dapat merekam setiap klik mouse saat mengunjungi situs web, meskipun situs web tersebut memiliki keyboard virtual.

b. Hybrid attacks

Serangan hibrida (hybrid attacks) tidak dibatasi oleh penggunaan hanya satu jenis serangan keamanan dalam jaringan komputer. Penyerang mampu menggabungkan berbagai metode serangan baik yang bersifat lokal maupun jarak jauh (remote) untuk mencapai tujuannya.

3) DNS (Domain Name System) attacks :

DNS attacks terbagi atas dua bagian antara lain:

a) DNS Cache Poisoning :

DNS Cache Poisoning adalah metode penyerangan DNS Cache Poisoning menggunakan informasi IP Address yang salah terkait dengan suatu host untuk mengarahkan lalu lintas data ke lokasi yang tidak seharusnya. Serangan ini sering digunakan untuk menargetkan situs web e-commerce dan layanan internet banking. Teknik ini memungkinkan pembuatan server palsu yang sangat mirip dengan server asli layanan Internet Banking. Akibatnya, DNS cache poisoning mengganggu server DNS asli, mengarahkan pengguna internet ke situs yang sangat mirip dengan situs asli, memungkinkan data dikirim ke server palsu.

b) DNS Hijacking :

Serangan DNS Hijacking adalah serangan keamanan jaringan komputer di mana penyerang memposisikan dirinya di antara klien dan server DNS, mencuri informasi klien dan mengirimkan informasi palsu sebelum informasi asli sampai ke server DNS. Keberhasilan serangan ini bergantung pada kecepatan respons penyerang, karena Penyerang perlu merespons informasi klien sebelum informasi asli mencapai server DNS.

KESIMPULAN

Menurut Whitman & Mattord (2011), keamanan informasi merujuk pada cara perlindungan terhadap informasi serta infrastruktur kritisnya, tercantum sistem dan *hardware* yang dipakai untuk mengelola, menyimpan, dan mengirimkan informasi. Pemahaman akan keamanan informasi, sebagaimana yang disampaikan oleh (Tiatama, 2016) mencerminkan pemahaman dan komitmen individu terhadap kebijakan keamanan organisasi, yang bertujuan untuk mengubah perilaku melalui peningkatan pengetahuan, sikap, dan perilaku terhadap keamanan informasi. Internet Banking, yang didefinisikan oleh David Whiteley, Mary J. Cronin, dan Mahmood Shah & Steve Clarke, mencakup layanan perbankan dari informasi dasar hingga transaksi kompleks yang dapat diakses melalui internet. Layanan Internet Banking dibagi menjadi 2 jenis, antara lain non-transaksional (seperti melihat saldo) dan transaksional (contohnya, transfer dana), memberikan keuntungan dalam efisiensi operasional bagi bank dan kenyamanan akses bagi nasabah. Namun, layanan ini rentan terhadap

berbagai jenis serangan seperti phishing dan serangan DNS yang dapat membahayakan keamanan data dan dana nasabah.

DAFTAR PUSTAKA

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.

Mukhtaruddin, M., Ubaidillah, U., Dewi, K., Hakiki, A., & Nopriyanto, N. (2019). Good corporate governance, corporate social responsibility, firm value, and financial performance as moderating variable. *Indonesian Journal of Sustainability Accounting and Management*, *3*(1), 55â – 64.

Putri, A. D., Novita, D., & Maskar, S. (2022). Pengenalan Wawasan Bisnis Di Era Digital Bagi Siswa/I Smk Yadika Bandarlampung. *Journal of Social Sciences and Technology for Community Service (JSSTCS)*, *3*(2), 213–217.

Tiatama, A. (2016). Perencanaan Tata Kelola Manajemen Keamanan Informasi Menggunakan Information Technology Infrastructure Library (Itil) V3. Pada D~ Net Surabaya. *Repository. Its. Ac. Id*, *3*.

DIGITAL MARKETING. *Volume 17, No.2, Oktober 2022, 17*, 316-322.