PENGARUH KESADARAN PENGGUNA TERHADAP KEBERHASILAN SERANGAN PHISHING DI JARINGAN PERBANKAN

Harry Pribadi Fitrian, Lulu Abidah, Khabibah Wiendie Zahra, Wildan Hanif Hafidudin
Tenik Informatika, Universitas Teknologi Digital
Jl. Raya Janti Karang Jambe No. 143, Yogyakarta
harrypribadi@digitechuniversity.ac.id

ABSTRAK

Phishing adalah ancaman keamanan siber yang signifikan di sektor perbankan, di mana serangan ini memanfaatkan manipulasi psikologis untuk memperoleh informasi sensitif, seperti kata sandi dan data keuangan, yang dapat merugikan baik pengguna maupun institusi. Meskipun berbagai upaya mitigasi telah dilakukan, kesadaran pengguna terhadap ancaman phishing, smishing, dan vishing masih rendah, terutama di kelompok dengan literasi digital terbatas, yang meningkatkan kerentanannya terhadap serangan siber yang semakin kompleks. Hal ini berpotensi menyebabkan kebocoran data pribadi dan finansial yang merugikan, serta merusak kepercayaan terhadap sistem perbankan digital. Penelitian ini bertujuan untuk menganalisis pengaruh kesadaran pengguna terhadap keberhasilan serangan phishing dalam sektor perbankan, dengan mengevaluasi pola serangan, strategi mitigasi seperti pelatihan keamanan siber, serta faktor-faktor yang memengaruhi keberhasilan serangan, termasuk literasi digital dan kebijakan keamanan. Dengan menggunakan tinjauan literatur, penelitian ini diharapkan dapat memberikan rekomendasi yang membantu meningkatkan kesadaran keamanan informasi di kalangan pengguna dan mengurangi risiko serangan phishing.

Kata kunci : *phishing*, kesadaran pengguna, keamanan informasi, sektor perbankan, literasi digital, mitigasi, *cybersecurity*.

1. PENDAHULUAN

Phishing merupakan salah satu ancaman keamanan siber yang sering dihadapi oleh sektor perbankan. Serangan ini memanfaatkan teknik manipulasi psikologis untuk mengelabui pengguna agar memberikan informasi sensitif, seperti kata sandi atau data keuangan. Salah satu bentuk kejahatan siber yang umum dilakukan oleh para penipu adalah phishing[1]. Dalam konteks keamanan jaringan, penerapan kontrol akses yang tepat, seperti Network Access Control (NAC), dapat membantu meminimalkan risiko serangan siber, termasuk phishing[2]. Namun, kesadaran pengguna terhadap ancaman phishing, smishing, dan vishing masih menjadi tantangan signifikan, sebagaimana ditunjukkan oleh studi yang dilakukan di Kota Cimahi, yang mengungkapkan rendahnya tingkat kesadaran masyarakat terhadap keamanan informasi [3].

Jaminan keamanan informasi sangat penting di era digital ini, terutama bagi organisasi yang menyimpan data sensitif, seperti sektor perbankan. Studi mengenai keamanan informasi di BPJS Kesehatan menunjukkan bahwa peningkatan kesadaran akan pentingnya perlindungan data dapat membantu menjaga kerahasiaan, integritas, dan ketersediaan informasi[4]. Selain itu, kesadaran keamanan informasi memainkan peran krusial dalam meminimalkan risiko serangan siber dan memastikan kepatuhan terhadap kebijakan keamanan, baik di sektor publik maupun swasta[5].

Meskipun berbagai upaya telah dilakukan, penelitian sebelumnya menunjukkan bahwa perbedaan individu dalam hal pendidikan, pengalaman, dan pemahaman terhadap keamanan informasi dapat memengaruhi kesadaran seseorang [5]. Sebagai contoh, institusi pendidikan tinggi sering kali menghadapi tantangan dalam meningkatkan kepatuhan pengguna terhadap kebijakan keamanan informasi, sehingga memerlukan pendekatan strategis yang lebih efektif[6].

Serangan phishing sering memanfaatkan pola tertentu, seperti manipulasi tautan dan rekayasa sosial, yang membuat pengguna kesulitan membedakan situs web asli dari palsu. Media komunikasi seperti email dan aplikasi pesan instan juga sering dimanfaatkan untuk menyebarkan tautan palsu yang mengarahkan pengguna ke situs phishing. Selain itu, kelompok dengan tingkat literasi digital rendah, seperti remaja dan perempuan, sering menjadi target utama karena kerentanannya terhadap teknik manipulasi semacam ini.

Penelitian ini menggunakan metode tinjauan literatur (literature review) untuk menganalisis pengaruh kesadaran pengguna terhadap keberhasilan serangan phishing dalam jaringan perbankan. Literatur yang digunakan mencakup artikel jurnal, laporan industri, dan buku yang diterbitkan dalam 10 tahun terakhir. Sumber-sumber ini diperoleh dari basis data akademik seperti IEEE Xplore, ScienceDirect, Sinta Kemdikbud, dan Google Scholar, dengan kata kunci pencarian seperti "phishing", "keamanan informasi", dan "cybersecurity".

Tujuan dari penelitian ini adalah untuk menganalisis dan mengidentifikasi pola serangan phishing yang paling sering digunakan dalam sektor perbankan serta mengevaluasi strategi mitigasi yang efektif, seperti pelatihan keamanan siber dan simulasi serangan, yang dapat meningkatkan kesadaran

pengguna. Penelitian ini juga bertujuan untuk mengkaji faktor-faktor yang memengaruhi keberhasilan serangan phishing, seperti literasi digital, kompleksitas serangan, dan kebijakan keamanan perbankan yang diterapkan. Dengan demikian, hasil penelitian ini diharapkan dapat memberikan rekomendasi strategis yang dapat membantu sektor perbankan dalam meningkatkan kesadaran keamanan informasi di kalangan pengguna dan mengurangi risiko keberhasilan serangan phishing.

2. TINJAUAN PUSTAKA

2.1. Phishing dalam Keamanan Siber

Phishing merupakan salah satu bentuk kejahatan siber yang memanfaatkan manipulasi psikologis untuk memperoleh informasi sensitif pengguna, seperti kata sandi dan data keuangan. Penelitian sebelumnya menunjukkan bahwa phishing sering dilakukan melalui email atau situs web palsu yang menyamar sebagai institusi terpercaya. Dengan semakin canggihnya teknologi, ancaman phishing kini semakin kompleks dan sulit dikenali oleh pengguna biasa.

2.2. Kesadaran Pengguna terhadap Ancaman Phishing

Kesadaran pengguna memainkan peran yang sangat penting dalam upaya mitigasi serangan phishing. Penelitian oleh [2] mengungkapkan bahwa rendahnya kesadaran akan ancaman siber dapat meningkatkan risiko serangan phishing, smishing, dan vishing. Sebagai contoh, 37% pengguna WhatsApp diketahui menyebarkan informasi tanpa verifikasi lebih lanjut, yang membuka celah bagi serangan siber. Oleh karena itu, meningkatkan kesadaran pengguna terhadap ancaman ini menjadi salah satu langkah utama dalam mengurangi risiko serangan phishing.

2.3. Strategi Mitigasi Phishing

Terdapat berbagai strategi mitigasi yang telah dibahas dalam literatur untuk mengurangi keberhasilan serangan phishing, antara lain:

a. Teknologi Keamanan: Penggunaan autentikasi dua faktor (seperti OTP) dan perangkat lunak anti-phishing dapat mengurangi dampak dari serangan phishing. Penelitian oleh [2] menunjukkan bahwa penerapan protokol keamanan seperti 802.1X dapat meningkatkan tingkat keamanan jaringan.
b. Pelatihan Keamanan Siber: Pelatihan keamanan siber dan simulasi serangan phishing terbukti efektif dalam meningkatkan kesadaran dan kewaspadaan pengguna. Beberapa studi menunjukkan bahwa simulasi serangan phishing dapat meningkatkan deteksi dan pencegahan serangan.
c. Pengelolaan Risiko Keamanan Informasi: Menurut studi oleh [5], pengelolaan risiko yang sistematis, termasuk identifikasi, pemantauan, dan pengendalian risiko, sangat penting untuk melindungi informasi sensitif, terutama di sektor perbankan.

2.4. Metode Penelitian yang Mendukung

Penelitian ini menggunakan pendekatan **tinjauan literatur** untuk menganalisis pengaruh kesadaran pengguna terhadap keberhasilan serangan phishing dalam jaringan perbankan. Proses penelitian melibatkan pengumpulan, evaluasi, dan sintesis data dari literatur yang relevan.

a. Pengumpulan Data: Artikel jurnal, laporan industri, buku, dan sumber terpercaya lainnya yang diterbitkan dalam 10 tahun terakhir digunakan sebagai bahan utama. Literatur diperoleh melalui pencarian di basis data akademik seperti IEEE Xplore, ScienceDirect, Sinta Kemdikbud, dan Google Scholar dengan kata kunci seperti:
   - "bank network phishing"
   - "Phishing"
   - "keamanan jaringan"
   - "keamanan informasi"
   - "cybersecurity"
   - "bank network"
b. Kriteria Seleksi: Literatur yang relevan diseleksi berdasarkan kriteria inklusi dan eksklusi. Kriteria inklusi meliputi artikel yang membahas pengaruh kesadaran pengguna terhadap keberhasilan serangan phishing, keamanan jaringan perbankan, dan strategi mitigasi. Kriteria eksklusi mencakup artikel yang tidak mencakup data empiris atau diterbitkan lebih dari 10 tahun yang lalu.
c. Fokus Analisis: Analisis dilakukan untuk mengidentifikasi pola umum, mengevaluasi strategi mitigasi, dan memahami faktor-faktor utama yang memengaruhi keberhasilan phishing, termasuk literasi digital pengguna, kompleksitas serangan, dan kebijakan keamanan perbankan.

2.5. Objek Penelitian

Penelitian ini berfokus pada beberapa objek utama:

a. Pengguna Jaringan Perbankan: Terutama pengguna yang berinteraksi dengan layanan perbankan online dan aplikasi mobile, yang rentan terhadap serangan phishing.
b. Keamanan Jaringan Perbankan: Meneliti teknologi dan kebijakan yang diterapkan oleh lembaga perbankan untuk mencegah phishing dan serangan siber lainnya.
c. Strategi Mitigasi: Menganalisis efektivitas berbagai strategi mitigasi yang diterapkan di sektor perbankan, seperti autentikasi dua faktor, perangkat lunak anti-phishing, dan pelatihan keamanan siber.

2.6. Faktor-Faktor yang Mempengaruhi Keberhasilan Serangan Phishing

Berbagai faktor dapat memengaruhi keberhasilan serangan phishing, yang diidentifikasi dalam tinjauan pustaka ini, antara lain:

a. Literasi Digital Pengguna: Pengguna yang kurang paham tentang ancaman siber lebih mudah terjebak dalam serangan phishing.
b. Kompleksitas Serangan: Semakin kompleks dan meyakinkan suatu serangan phishing, semakin besar kemungkinan korban tertipu.
c. Kebijakan Keamanan di Sektor Perbankan: Tingkat keamanan yang diterapkan oleh lembaga perbankan juga berperan besar dalam mencegah serangan phishing.

2.7. Kesenjangan Penelitian dan Arah Penelitian Selanjutnya

Dalam tinjauan pustaka ini, beberapa kesenjangan dalam penelitian yang ada telah diidentifikasi, khususnya terkait dengan:

a. Efektivitas Program Pelatihan: Meskipun banyak penelitian yang menunjukkan bahwa pelatihan pengguna dapat mengurangi risiko phishing, masih ada kekurangan data yang lebih terperinci tentang program pelatihan yang paling efektif.
b. Kebijakan Keamanan Perbankan: Perlu lebih banyak studi yang menganalisis kebijakan keamanan dalam sektor perbankan yang berfokus pada mitigasi phishing secara sistematik.

Penelitian ini bertujuan untuk mengisi kesenjangan tersebut melalui analisis literatur yang mendalam dan memberikan rekomendasi strategis untuk meningkatkan kesadaran pengguna dan efektivitas kebijakan keamanan di sektor perbankan.

3. METODE PENELITIAN

3.1. Pendahuluan

Penelitian ini menggunakan metode tinjauan literatur (*literature review*) untuk menganalisis pengaruh kesadaran pengguna terhadap keberhasilan serangan *phishing* dalam jaringan perbankan. Metode ini mencakup pengumpulan, evaluasi, dan sintesis data dari berbagai sumber literatur yang relevan. Tujuannya adalah untuk mengidentifikasi pola, strategi mitigasi, dan faktor-faktor yang memengaruhi keberhasilan serangan *phishing*.

3.2. Pengumpulan Data

Data yang digunakan dalam penelitian ini berasal dari artikel jurnal, laporan industri, buku, dan sumber terpercaya lainnya yang diterbitkan dalam 10 tahun terakhir. Literatur diperoleh melalui penelusuran pada basis data akademik seperti *IEEE Xplore*, *ScienceDirect*, *Sinta Kemdikbud*, dan *Google Scholar*. Kata kunci yang digunakan dalam pencarian literatur meliputi:

a. *"bank network phishing"*
b. *"Phishing"*
c. *"keamanan jaringan"*
d. *"keamanan informasi"*
e. *"cybersecurity"*
f. *"bank network"*

3.3. Kriteria Seleksi

Kriteria inklusi:

a. Artikel yang relevan dengan pengaruh kesadaran pengguna terhadap keberhasilan serangan *phishing* dalam jaringan perbankan.
b. Sumber yang terverifikasi dan terindeks pada basis data akademik.
c. Studi yang membahas keamanan siber dalam konteks perbankan.

Kriteria eksklusi:

a. Artikel yang tidak mencakup data empiris atau temuan yang relevan.
b. Literatur yang diterbitkan lebih dari 10 tahun yang lalu.

3.4. Analisis Literatur

Setiap literatur yang terpilih dianalisis secara kritis dengan tujuan:

a. Mengidentifikasi pola umum tentang hubungan antara tingkat kesadaran pengguna dan keberhasilan serangan *phishing*.
b. Mengevaluasi strategi mitigasi yang efektif, seperti pelatihan keamanan siber dan simulasi serangan *phishing*.
c. Mengkaji faktor-faktor utama yang memengaruhi keberhasilan serangan *phishing*, termasuk literasi digital, kompleksitas serangan, dan kebijakan keamanan perbankan.

3.5. Sintesis Temuan

Hasil analisis literatur kemudian disintesis untuk memberikan gambaran komprehensif mengenai pengaruh kesadaran pengguna terhadap keberhasilan serangan *phishing* di jaringan perbankan. Proses sintesis ini meliputi:

a. Perbandingan hasil antar penelitian.
b. Identifikasi kesenjangan penelitian.
c. Rekomendasi strategis untuk meningkatkan kesadaran pengguna sebagai langkah mitigasi.

3.6. Kesimpulan

Pendekatan tinjauan literatur ini diharapkan dapat memberikan wawasan yang relevan bagi sektor perbankan dalam mengurangi risiko keberhasilan serangan *phishing*. Peningkatan kesadaran pengguna menjadi salah satu langkah utama dalam upaya mitigasi tersebut.

4. HASIL DAN PEMBAHASAN

4.1. Hasil Tinjauan Literatur

Hasil tinjauan literatur ini menyoroti pentingnya kesadaran pengguna dan sistem keamanan yang memadai dalam mengurangi risiko serangan phishing pada layanan perbankan online. Phishing sering terjadi akibat rendahnya kesadaran pengguna terhadap

ancaman siber serta lemahnya keamanan situs web perbankan. Hal ini diperparah oleh penggunaan teknik rekayasa sosial yang mampu mengelabui pengguna untuk memberikan informasi pribadi seperti kata sandi dan data finansial mereka [7].

Dalam konteks keamanan jaringan, serangan phishing umumnya menggunakan manipulasi tautan dan rekayasa sosial, yang membuat pengguna sulit membedakan antara situs web asli dan palsu. Penurunan kesadaran terhadap keamanan informasi, seperti yang terjadi pada pengguna aplikasi WhatsApp, dapat memperburuk penyebaran link phishing. Sebuah penelitian menunjukkan bahwa sebagian besar pengguna WhatsApp tidak sepenuhnya menyadari pentingnya keamanan informasi, dengan 37% responden menyebarkan informasi tanpa menyaringnya terlebih dahulu [8]. Selain itu, pengguna yang kurang sadar akan potensi ancaman phishing, baik di kalangan remaja maupun perempuan, sangat rentan terhadap serangan tersebut [9]. Simulasi di sebuah perusahaan juga mengungkapkan bahwa meskipun banyak karyawan yang mampu mendeteksi phishing, sebagian masih terjebak dalam serangan, dengan 8% di antaranya memberikan informasi pribadi saat menerima email phishing[10]. Rendahnya pengetahuan dan literasi digital pengguna menjadi celah utama yang dimanfaatkan oleh penyerang. Edukasi pengguna, sebagaimana disarankan oleh penelitian ini, dapat menjadi salah satu langkah mitigasi yang efektif, selain penerapan teknologi seperti perangkat lunak anti-phishing dan sistem autentikasi dua faktor (*OTP*) [11].

4.2. Pengumpulan dan Seleksi Literatur

Penelitian ini menggunakan sumber-sumber literatur terpercaya yang diperoleh dari basis data akademik seperti IEEE Xplore, ScienceDirect, dan Sinta. Literatur yang relevan dipilih berdasarkan kriteria inklusi dan eksklusi. Kriteria inklusi meliputi studi yang membahas pengaruh kesadaran pengguna terhadap keberhasilan serangan *phishing*, keamanan jaringan perbankan, dan strategi mitigasi. Sementara itu, kriteria eksklusi mencakup artikel yang tidak memuat data empiris atau diterbitkan sebelum 10 tahun terakhir. Pendekatan ini memastikan hanya data yang relevan dan mutakhir yang digunakan.

4.3. Pengaruh Kesadaran Pengguna terhadap Keberhasilan Serangan Phishing

Studi kasus di Bank Syariah Indonesia (BSI) menyoroti bagaimana ancaman *phishing* sering kali berasal dari faktor eksternal, seperti email dan tautan palsu. Namun, dampaknya diperbesar oleh rendahnya kesadaran nasabah. Untuk mengatasi hal ini, BSI telah menerapkan kebijakan keamanan (*IT*) yang komprehensif melalui manajemen risiko berlapis. Kebijakan ini melibatkan identifikasi, pengukuran, pemantauan, dan pengendalian risiko untuk mencegah potensi serangan *phishing*. Meskipun pendekatan ini terbukti efektif, penelitian juga menunjukkan bahwa faktor manusia tetap menjadi elemen paling rentan, sehingga diperlukan program literasi digital bagi pengguna .[12]

4.4. Strategi Mitigasi Teknis dan Edukasi

Penelitian oleh Ramadhanti dan Sugiyono (2023) menambahkan bahwa tanggung jawab bank dalam menangani tindakan *phishing* memerlukan penguatan regulasi dan perlindungan hukum bagi nasabah. Dalam studi kasus Bank BRI, mereka menemukan bahwa meskipun bank telah menerapkan prinsip kehati-hatian dan kerahasiaan data nasabah, ancaman *phishing* yang berasal dari luar sistem bank, seperti undangan dalam format aplikasi palsu (*APK*) melalui WhatsApp, menyoroti pentingnya edukasi tambahan kepada nasabah [13].

Berbagai metode *phishing*, seperti *spoofing*, *email phishing*, dan situs web palsu, dirancang untuk menipu korban. Langkah-langkah pencegahan yang diidentifikasi meliputi:

a. Edukasi pengguna.
b. Penguatan sistem keamanan teknis, seperti penggunaan *OTP*.
c. Penerapan perangkat lunak *anti-phishing* [14].

4.5. Sintesis Temuan

Hasil sintesis literatur mengungkapkan bahwa tingkat kesadaran pengguna merupakan faktor krusial dalam mengurangi keberhasilan serangan *phishing*. Strategi mitigasi yang melibatkan sinergi antara teknologi, edukasi, dan kebijakan perbankan telah terbukti efektif. Selain itu, studi menyoroti pentingnya perbandingan hasil antar penelitian untuk mengidentifikasi kesenjangan penelitian, seperti kurangnya evaluasi terhadap efektivitas program edukasi digital jangka panjang.

4.6. Perlindungan Hukum terhadap Korban Phishing

Penelitian oleh Hasanudin dan Babussalam (2023) lebih berfokus pada aspek hukum dalam menghadapi kejahatan *phishing*. Mereka menyoroti pentingnya upaya hukum yang dapat diambil oleh korban *phishing*, termasuk melaporkan kasus kepada pihak berwenang atau mengajukan gugatan perdata. Meskipun regulasi yang ada, seperti UU ITE, telah mengatur kejahatan *phishing*, perlindungan hukum bagi korban perlu diperkuat untuk memastikan penanganan yang lebih efektif terhadap kejahatan siber ini [14].

4.7. Kesimpulan

Secara keseluruhan, temuan dari berbagai studi ini menegaskan bahwa upaya pencegahan *phishing* memerlukan pendekatan holistik yang mencakup:

a. Penguatan sistem keamanan teknis, seperti penggunaan perangkat lunak *anti-phishing* dan *OTP*.
b. Peningkatan literasi digital pengguna melalui program edukasi.

c. Penegakan regulasi dan perlindungan hukum yang lebih kuat bagi korban.

Sinergi antara langkah teknis, regulasi, dan edukasi pengguna tidak hanya mampu mengurangi keberhasilan serangan *phishing*, tetapi juga membangun ekosistem keamanan digital yang lebih tangguh di sektor perbankan, baik pada bank konvensional maupun syariah.

5. KESIMPULAN DAN SARAN

Penelitian ini menyoroti peran penting kesadaran pengguna dalam mengurangi risiko serangan phishing pada sektor perbankan. Berdasarkan hasil tinjauan literatur, rendahnya kesadaran pengguna terhadap ancaman siber dan literasi digital yang terbatas menjadi faktor utama yang meningkatkan kerentanannya terhadap serangan phishing. Teknik rekayasa sosial yang digunakan oleh penyerang, seperti manipulasi tautan dan email palsu, sering kali menyebabkan pengungkapan informasi pribadi dan data finansial.

Dalam hal mitigasi, pendekatan yang efektif mencakup edukasi pengguna melalui program literasi digital, penggunaan perangkat lunak anti-phishing, dan penerapan autentikasi dua faktor (OTP). Selain itu, sinergi antara teknologi, edukasi, dan regulasi perbankan yang lebih kuat dapat menciptakan ekosistem keamanan digital yang lebih tangguh. Meskipun teknologi keamanan dan kebijakan telah diterapkan, faktor manusia tetap menjadi elemen yang paling rentan, yang menandakan perlunya peningkatan kesadaran dan edukasi yang lebih intensif bagi pengguna. Perlindungan hukum terhadap korban phishing juga perlu diperkuat agar penanganan kejahatan siber lebih efektif.

Penelitian selanjutnya diharapkan dapat memperdalam analisis mengenai dampak program literasi digital terhadap peningkatan kesadaran pengguna dalam mencegah serangan phishing. Penelitian ini juga dapat mengkaji lebih lanjut efektivitas teknologi keamanan seperti perangkat lunak anti-phishing dan autentikasi dua faktor (OTP) dalam berbagai jenis transaksi perbankan. Selain itu, perlu eksplorasi lebih lanjut mengenai efektivitas program edukasi digital jangka panjang dalam meningkatkan pengetahuan dan respons pengguna terhadap potensi ancaman siber.

DAFTAR PUSTAKA

[1] I. Radiansyah, C. Rusdjan, and Y. Priyadi, "Analisis Ancaman Phishing Dalam Layanan Online Banking," *J. Innov. Bus. Econ.*, vol. 7, no. 1, p. 1, 2016, doi: 10.22219/jibe.vol7.no1.1-14.

[2] M. Syani, R. M. Tresna, E. A. Firdaus, and F. F. Nugraha, "Penerapan Network Access Control Autentikasi Internal Network Security Protokol 802.1 X," *Nuansa Inform.*, vol. 16, no. 2, pp. 77–86, 2022, doi: 10.25134/nuansa.v16i2.5800.

[3] ULFA LADAYYA, Deni Prayitno, Mamay Syani, Rizki Hikmawan, and Nuur Wachid Abdulmajid, "Kesadaran Keamanan Informasi atas Phising, Smishing, dan Vishing pada Warga Kota Cimahi," *Nuansa Inform.*, vol. 18, no. 2, pp. 109–119, 2024, doi: 10.25134/ilkom.v18i2.201.

[4] A. H. Satria Nusantara, I. Kahirul Umam, and M. Lubis, "Jaminan Informasi dan Keamanan yang Lebih Baik: Studi Kasus BPJS Kesehatan," *Nuansa Inform.*, vol. 18, no. 2, pp. 120–127, 2024, doi: 10.25134/ilkom.v18i2.202.

[5] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," *Comput. Secur.*, vol. 106, p. 102267, 2021, doi: 10.1016/j.cose.2021.102267.

[6] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and Information Security Awareness," *Comput. Human Behav.*, vol. 69, pp. 151–156, 2017, doi: 10.1016/j.chb.2016.11.065.

[7] E. J. Pranata and L. Ependi, "Phising Terhadap Website Bank Bca," *J. Trends*, vol. 01, no. 01, pp. 34–40, 2023, [Online]. Available: https://ejurnal.ibisa.ac.id/index.php/jsd/article/view/293

[8] Y. Arie Budi Suprio and M. Najib, "Analisa Dampak Kesadaran Keamanan Informasi Pengguna Aplikasi Whatsapp Terhadap Penyebaran Link Web Phising," *Semin. Nas. Corisindo*, pp. 318–322, 2022, [Online]. Available: https://corisindo.stikom-bali.ac.id/penelitian/index.php/semnas/article/view/65

[9] N. Vadila and A. R. Pratama, "Analisis Kesadaran Keamanan Terhadap Ancaman Phishing," *Automata*, vol. 2, no. 2, pp. 1–4, 2021.

[10] B. Wibowo and T. Hidayat, "Strategi Efektif dalam Meningkatkan Kesadaran Keamanan Siber terhadap Ancaman Phishing di Lingkungan Perusahaan PT. XYZ," *J. Pengabdi. Masy. Sultan Indones.*, vol. 2, no. 1, pp. 1–9, 2024, doi: 10.58291/abdisultan.v2i1.294.

[11] A. Muftiadi, T. P. M. Agustina, and M. Evi, "Studi kasus keamanan jaringan komputer: analisis ancaman phising terhadap layanan online banking," *Hexatech J. Ilm. Tek.*, vol. 1, no. 2, pp. 60–65, 2022, doi: 10.55904/hexatech.v1i2.346.

[12] D. F. Rohmah, "Implementasi Manajamen Risiko Dalam Menghadapi Ancaman Phising Pada Bank Syariah Indonesia KC Jakata Pondok Indah," pp. 1–163, 2023.

[13] R. A. T. P. Putri and H. Sugiyono, "Tanggung Jawab Bank Terhadap Tindakan Phising Dalam Sistem Penggunaan E-Banking (Studi : Kasus Phising Pada Pt . Bank Rakyat Indonesia (PERSERO) TBK)," *J. Interpret. Huk.*, vol. 4, no. 3, pp. 682–690, 2023.

[14] Akhmad Fery Hasanudin and A Basuki Babussalam, "Perlindungan Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo M-Banking," *J. Gagasan Huk.*, vol. 6, no. 01, pp. 16–29, 2024, doi: 10.31849/jgh.v6i01.18827.