

Edukasi Pencegahan Phishing Sebagai Upaya Peningkatan Kesadaran Keamanan Digital

Anzas Ibezato Zalukhu ¹, Metta Dina Gloria ², Adil Priman Hati Hulu ³, Irwan Syahputra ⁴, Ratna Nisti Yuliani Zalukhu ⁵, Dian Khristian Zalukhu ⁶

¹ Sistem Informasi, STMIK Methodist Binjai, Indonesia

^{2,3,5,6} Teknik Informatika, STMIK Methodist Binjai, Indonesia

⁴ Informatika, Fakultas Teknologi dan Ilmu Komputer Informatika, Universitas Satya Terra Bhinneka, Indonesia

Email: ^{1*}anzaszalukhu@stmikmethodistbinjai.ac.id, ²mettagloria2@gmail.com, ³adilprimanhatihulu@gmail.com,

⁴irwan@satyaterabhinneka.ac.id, ⁵ratnanyzalukhu23@gmail.com, ⁶dianzalukhu17@gmail.com

(*: anzaszalukhu@stmikmethodistbinjai.ac.id)

Abstrak

Perkembangan teknologi digital yang pesat telah meningkatkan risiko kejahatan siber, salah satunya *phishing*, yang sering menasar pelajar sebagai pengguna aktif teknologi informasi. *Phishing* merupakan bentuk penipuan digital yang dilakukan dengan menyamar sebagai pihak terpercaya untuk memperoleh informasi sensitif seperti data pribadi dan akun digital. Rendahnya literasi keamanan digital menyebabkan pelajar rentan terhadap serangan tersebut. Oleh karena itu, kegiatan Pengabdian kepada Masyarakat ini bertujuan untuk meningkatkan kesadaran dan pemahaman pelajar terhadap ancaman phishing serta strategi pencegahannya. Kegiatan edukasi dilaksanakan di SMK Negeri 1 Sirapit, Kabupaten Langkat, melalui pendekatan edukatif dan partisipatif yang meliputi ceramah interaktif, diskusi, studi kasus, dan simulasi identifikasi phishing. Materi yang disampaikan mencakup pengenalan keamanan digital, jenis-jenis phishing, dampak phishing, serta langkah-langkah pencegahan dalam aktivitas digital sehari-hari. Hasil kegiatan menunjukkan adanya peningkatan pemahaman pelajar mengenai ciri-ciri phishing dan pentingnya menjaga keamanan data pribadi. Selain itu, pelajar menunjukkan perubahan sikap yang lebih waspada dan bertanggung jawab dalam menggunakan teknologi digital. Dengan demikian, kegiatan edukasi ini terbukti efektif dalam meningkatkan literasi keamanan digital pelajar serta mendukung pembentukan perilaku digital yang aman dan bijak.

Kata Kunci: *Phishing*, Keamanan Digital, Literasi Digital, Pelajar, Pengabdian Kepada Masyarakat.

Abstract

The rapid development of digital technology has increased the risk of cybercrime, one of which is phishing, which frequently targets students as active users of information technology. Phishing is a form of digital fraud carried out by impersonating trusted entities to obtain sensitive information such as personal data and digital accounts. Limited digital security literacy makes students vulnerable to such attacks. Therefore, this Community Service activity aims to enhance students' awareness and understanding of phishing threats and their prevention strategies. The educational activity was conducted at SMK Negeri 1 Sirapit, Langkat Regency, using an educational and participatory approach that included interactive lectures, discussions, case studies, and phishing identification simulations. The materials covered digital security awareness, types of phishing, the impacts of phishing attacks, and preventive measures in daily digital activities. The results indicate an improvement in students' understanding of phishing characteristics and the importance of protecting personal data. Furthermore, students demonstrated a more cautious and responsible attitude toward the use of digital technology. Thus, this educational activity proved effective in improving students' digital security literacy and supporting the development of safe and responsible digital behavior.

Keywords: Phishing, Digital security, Digital literacy, Students, Community Service

1. PENDAHULUAN

Seiring dengan meningkatnya aktivitas digital, ancaman kejahatan siber juga mengalami peningkatan, salah satunya adalah *phishing*. *Phishing* merupakan bentuk serangan siber yang dilakukan dengan cara memanipulasi pengguna agar secara tidak sadar memberikan informasi sensitif, seperti nama pengguna, kata sandi, data akun, maupun informasi pribadi lainnya, kepada pihak yang tidak berwenang. Serangan ini umumnya dilakukan dengan menyamar sebagai institusi atau pihak yang terpercaya melalui media email, pesan singkat, media sosial, maupun situs web palsu yang menyerupai tampilan situs resmi. Teknik phishing sering memanfaatkan faktor psikologis korban, seperti rasa takut, urgensi, atau iming-iming keuntungan tertentu [1].

Pelajar merupakan salah satu kelompok pengguna teknologi digital yang memiliki tingkat kerentanan cukup tinggi terhadap serangan phishing. Faktor usia, keterbatasan literasi keamanan digital, serta tingginya frekuensi penggunaan perangkat digital dan media sosial menjadi penyebab utama rendahnya kewaspadaan terhadap ancaman kejahatan siber. Dampak yang ditimbulkan akibat serangan phishing tidak hanya berupa pencurian data pribadi dan penyalahgunaan akun digital, tetapi juga

berpotensi menimbulkan kerugian finansial serta gangguan psikologis bagi korban. Selain itu, rendahnya kesadaran keamanan digital dapat berdampak negatif terhadap pembentukan perilaku digital yang aman dan bertanggung jawab.

Berdasarkan kondisi tersebut, diperlukan suatu upaya edukatif yang sistematis dan berkelanjutan untuk meningkatkan kesadaran serta pemahaman pelajar terhadap pentingnya keamanan digital. Oleh karena itu, tim dosen STMIK Methodist Binjai dan Dosen Universitas Satya Terra Bhinneka melaksanakan kegiatan Pengabdian kepada Masyarakat berupa edukasi pencegahan *phishing* yang bertujuan untuk membekali pelajar dengan pengetahuan dan keterampilan dasar dalam mengenali, mencegah, serta mengantisipasi ancaman phishing, sehingga mampu memanfaatkan teknologi digital secara aman, bijak, dan bertanggung jawab.

2. TINJAUAN PUSTAKA

Teknologi informasi dan komunikasi (TIK) merupakan seperangkat teknologi yang digunakan untuk mengolah, menyimpan, dan menyampaikan informasi secara digital. Dalam bidang pendidikan, TIK berperan penting dalam mendukung proses pembelajaran, mulai dari penyediaan sumber belajar digital, komunikasi antara pendidik dan peserta didik, hingga pengelolaan administrasi Pendidikan. Pemanfaatan TIK memungkinkan pelajar untuk mengakses informasi secara cepat dan luas, serta meningkatkan efektivitas dan fleksibilitas pembelajaran [2]. Namun, perkembangan dan pemanfaatan TIK yang pesat juga menimbulkan berbagai tantangan, salah satunya adalah meningkatnya risiko keamanan digital. Pelajar sebagai pengguna aktif teknologi digital perlu memiliki pemahaman yang memadai agar mampu memanfaatkan teknologi secara aman, bijak, dan bertanggung jawab [3].

2.1 Keamanan Digital

Keamanan digital merupakan upaya perlindungan terhadap sistem informasi, jaringan, perangkat, dan data dari ancaman penyalahgunaan, peretasan, maupun kejahatan siber. Keamanan digital mencakup perlindungan data pribadi, keamanan akun digital, serta keamanan dalam berinteraksi di dunia maya. Dalam konteks pendidikan, keamanan digital menjadi aspek penting karena pelajar sering menggunakan perangkat digital untuk mengakses berbagai layanan daring [4].

Kurangnya pemahaman tentang keamanan digital dapat menyebabkan pengguna menjadi rentan terhadap berbagai bentuk kejahatan siber [5]. Oleh karena itu, peningkatan kesadaran dan literasi keamanan digital menjadi kebutuhan penting, khususnya bagi pelajar yang berada pada fase aktif menggunakan teknologi informasi [6], [7].

2.2 Phishing

Phishing merupakan salah satu bentuk kejahatan siber yang bertujuan untuk memperoleh informasi sensitif milik korban dengan cara menipu dan menyamar sebagai pihak yang terpercaya. Informasi yang menjadi target phishing meliputi nama pengguna, kata sandi, data akun, nomor identitas, hingga informasi keuangan. Phishing umumnya dilakukan melalui media email, pesan singkat (SMS atau aplikasi pesan instan), media sosial, serta situs web palsu yang memiliki tampilan menyerupai situs resmi [8].

Teknik *phishing* sering memanfaatkan rekayasa sosial (*social engineering*), yaitu manipulasi psikologis korban dengan menciptakan rasa urgensi, ketakutan, atau iming-iming hadiah tertentu. Tanpa kewaspadaan dan pemahaman yang memadai, pelajar dapat dengan mudah menjadi korban phishing, yang berakibat pada penyalahgunaan data pribadi dan kerugian lainnya [9].

2.3 Jenis-Jenis Phishing

Phishing dapat diklasifikasikan ke dalam beberapa jenis berdasarkan media dan teknik yang digunakan, antara lain [10]:

1. Email *Phishing*, yaitu phishing yang dilakukan melalui email palsu yang menyerupai institusi resmi.
2. *Smishing*, yaitu phishing yang dilakukan melalui pesan singkat atau aplikasi pesan instan.
3. Social Media *Phishing*, yaitu phishing yang memanfaatkan platform media sosial untuk menipu korban.
4. Website *Phishing*, yaitu penggunaan situs web palsu yang menyerupai tampilan situs resmi untuk mencuri data pengguna.

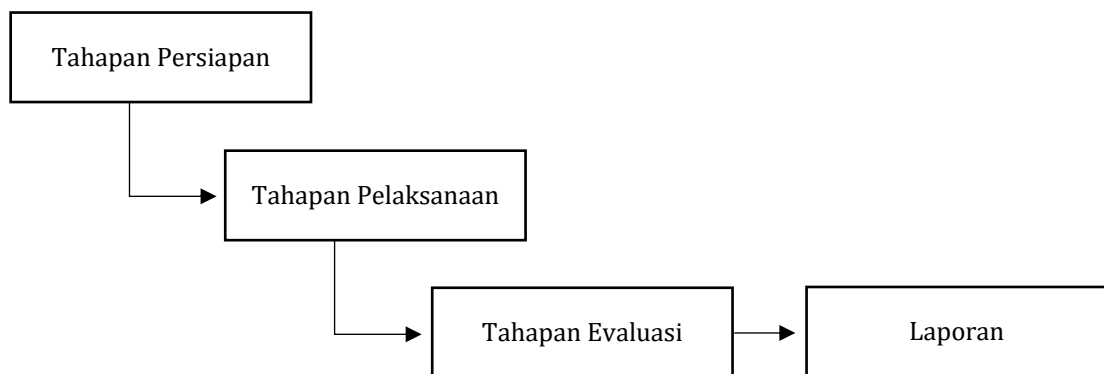
2.4 Literasi Keamanan Digital

Literasi keamanan digital merupakan kemampuan individu dalam memahami risiko penggunaan teknologi digital serta menerapkan langkah-langkah perlindungan terhadap data dan identitas digital. Literasi ini meliputi kemampuan mengenali ancaman digital, menjaga kerahasiaan data pribadi, serta bersikap kritis terhadap informasi yang diterima secara daring.

Bagi pelajar, literasi keamanan digital berperan penting dalam membentuk perilaku digital yang aman dan bertanggung jawab. Tingkat literasi keamanan digital yang baik akan membantu pelajar dalam menghindari kejahatan siber, termasuk phishing, serta mempersiapkan mereka menghadapi lingkungan kerja dan sosial yang semakin bergantung pada teknologi digital.

3. METODE PELAKSANAAN

3.1 Tahapan Pelaksanaan Kegiatan



Gambar 1. Tahapan Pelaksanaan

Pelaksanaan kegiatan Pengabdian kepada Masyarakat dilakukan melalui beberapa tahapan sebagai berikut:

1. Tahap Persiapan, meliputi koordinasi dengan pihak sekolah, penyusunan materi, dan persiapan sarana pendukung kegiatan.
2. Tahap Pelaksanaan, yaitu penyampaian materi edukasi pencegahan phishing kepada pelajar.
3. Tahap Evaluasi, dilakukan untuk mengetahui tingkat pemahaman dan respons pelajar terhadap materi yang telah disampaikan.
4. Tahapan laporan, yaitu tahap ini dilakukan penyusunan laporan kegiatan secara sistematis yang memuat latar belakang, tujuan, metode pelaksanaan, hasil kegiatan, pembahasan, dokumentasi, serta kesimpulan. Laporan disusun berdasarkan seluruh rangkaian kegiatan yang telah dilaksanakan pada Senin, 15 Desember 2025, sebagai bentuk pertanggungjawaban akademik kepada institusi terkait sekaligus sebagai bahan evaluasi dan referensi untuk pengembangan serta pelaksanaan kegiatan Pengabdian kepada Masyarakat yang sejenis di masa mendatang.

3.2 Bentuk dan Kegiatan Pendekatan

Kegiatan Pengabdian kepada Masyarakat ini dilaksanakan dalam bentuk edukasi dan sosialisasi keamanan digital, dengan fokus pada pencegahan *phishing*. Pendekatan yang digunakan adalah pendekatan edukatif dan partisipatif, di mana pelajar tidak hanya menerima materi secara teoritis, tetapi juga dilibatkan secara aktif melalui diskusi, studi kasus, dan simulasi sederhana terkait serangan phishing. Pendekatan ini dipilih agar materi yang disampaikan dapat dipahami secara komprehensif dan mudah diaplikasikan dalam kehidupan sehari-hari.

3.3 Sasaran Kegiatan

Sasaran kegiatan Pengabdian kepada Masyarakat ini adalah pelajar tingkat sekolah menengah atau sederajat yang aktif menggunakan perangkat digital, internet, dan media sosial dalam aktivitas belajar maupun kehidupan sehari-hari. Pelajar dipilih sebagai sasaran utama karena memiliki tingkat interaksi

digital yang tinggi, namun masih membutuhkan penguatan pemahaman terkait keamanan digital dan perlindungan data pribadi.

3.4 Lokasi dan Waktu Pelaksanaan

Kegiatan Pengabdian kepada Masyarakat ini dilaksanakan di SMK Negeri 1 Sirapit yang berlokasi di Kecamatan Sirapit, Kabupaten Langkat, Provinsi Sumatera Utara, dengan pertimbangan bahwa sekolah tersebut memiliki peserta didik yang aktif dalam pemanfaatan teknologi informasi dan komunikasi, baik untuk mendukung proses pembelajaran maupun aktivitas digital lainnya. Pelaksanaan kegiatan berlangsung pada hari Senin, 15 Desember 2025, mulai pukul 10.00 WIB hingga selesai, bertempat di SMK Negeri 1 Sirapit yang beralamat di Tanjung Keriah, Kecamatan Sirapit, Kabupaten Langkat, Provinsi Sumatera Utara 20762.

3.5 Materi Kegiatan

Materi edukasi yang disampaikan dalam kegiatan ini meliputi:

1. Pengenalan keamanan digital dan pentingnya perlindungan data pribadi.
2. Pengertian *phishing* dan jenis-jenisnya.
3. Dampak dan risiko serangan *phishing*.
4. Strategi pencegahan *phishing* dalam aktivitas digital.
5. Studi kasus dan simulasi identifikasi *phishing*
6. Kegiatan dilaksanakan secara tatap muka dengan dukungan fasilitas sekolah serta koordinasi bersama pihak sekolah.

3.6 Metode Penyampaian

Metode penyampaian materi menggunakan ceramah interaktif, diskusi dan tanya jawab, studi kasus, serta simulasi sederhana. Metode ini bertujuan untuk meningkatkan keterlibatan pelajar dan memperkuat pemahaman terhadap materi yang disampaikan.

4. HASIL DAN PEMBAHASAN

4.1 Penjelasan Kegiatan

Kegiatan Pengabdian kepada Masyarakat dengan judul Edukasi Pencegahan *Phishing* sebagai Upaya Peningkatan Kesadaran Keamanan Digital Pelajar telah dilaksanakan di SMK Negeri 1 Sirapit, Kabupaten Langkat. Kegiatan ini bertujuan untuk memberikan edukasi kepada pelajar mengenai ancaman *phishing* serta langkah-langkah pencegahannya dalam penggunaan teknologi digital. Pelaksanaan kegiatan dilakukan secara tatap muka dan melibatkan pelajar yang aktif menggunakan perangkat digital dalam kegiatan pembelajaran maupun aktivitas sehari-hari. Selama kegiatan berlangsung, pelajar menunjukkan respons yang positif dan antusias, baik dalam mengikuti pemaparan materi maupun saat sesi diskusi dan tanya jawab.

4.2 Jadwal Pelaksanaan Kegiatan

Kegiatan Pengabdian kepada Masyarakat dilaksanakan sesuai dengan jadwal yang telah disusun dan disepakati bersama pihak sekolah. Adapun rincian jadwal pelaksanaan kegiatan adalah sebagai berikut:

Tabel 1. Susunan Kegiatan

No.	Waktu	Kegiatan
1	08.00 - 08.30 WIB	Registrasi Peserta dan Pembukaan Kegiatan
2	08.30 - 09.15 WIB	Penyampaian Materi Pengenalan Keamanan Digital
3	09.15 - 10.00 WIB	Penyampaian Materi <i>Phising</i> dan Jenis-Jenisnya
4	10.00 - 10.30 WIB	Diskusi dan Tanya Jawab
5	10.30 - 11.15 WIB	Studi Kasus Dan Identifikasi <i>Phising</i>
6	11.15 - 11.30 WIB	Evaluasi Kegiatan dan Penutupan

4.3 Hasil Kegiatan

Hasil yang diperoleh dari pelaksanaan kegiatan Pengabdian kepada Masyarakat ini dapat diuraikan sebagai berikut:

1. **Peningkatan Pemahaman Pelajar**
Setelah mengikuti kegiatan edukasi, pelajar menunjukkan peningkatan pemahaman mengenai pengertian phishing, bentuk-bentuk *phishing*, serta cara kerja serangan phishing yang sering terjadi melalui pesan singkat, email, dan media sosial.
2. **Meningkatnya Kesadaran Keamanan Digital**
Pelajar mulai menyadari pentingnya menjaga keamanan data pribadi dan akun digital. Hal ini terlihat dari respons pelajar yang lebih berhati-hati terhadap pesan atau tautan yang mencurigakan serta meningkatnya kesadaran untuk tidak sembarangan membagikan informasi pribadi.
3. **Kemampuan Mengenali Ancaman *Phishing***
Melalui penyampaian contoh kasus, pelajar mampu mengidentifikasi ciri-ciri pesan phishing, seperti penggunaan tautan palsu, permintaan data pribadi, dan penyamaran identitas pihak tertentu. Kemampuan ini menjadi indikator awal keberhasilan kegiatan edukasi yang dilaksanakan.

4.4 Pembahasan

Pelaksanaan kegiatan edukasi pencegahan phishing memberikan dampak positif terhadap peningkatan literasi keamanan digital pelajar. Sebelum kegiatan berlangsung, sebagian besar pelajar belum memahami secara mendalam mengenai ancaman phishing dan potensi risiko yang ditimbulkannya. Setelah mengikuti kegiatan, pelajar memiliki pemahaman yang lebih baik mengenai jenis-jenis *phishing* serta langkah-langkah pencegahannya. Hasil kegiatan ini sejalan dengan tujuan Pengabdian kepada Masyarakat, yaitu meningkatkan kesadaran dan pemahaman pelajar terhadap keamanan digital. Edukasi yang disampaikan secara langsung dan disertai contoh kasus nyata terbukti efektif dalam membantu pelajar memahami ancaman *phishing* yang sering ditemui dalam aktivitas digital sehari-hari.

4.5 Dokumentasi Kegiatan



Gambar 2. Pelaksanaan Kegiatan

keterlibatan aktif pelajar selama kegiatan menunjukkan bahwa pendekatan edukatif dan diskusi interaktif yang digunakan mampu meningkatkan minat dan pemahaman peserta. Dengan demikian, kegiatan ini tidak hanya memberikan pengetahuan teoritis, tetapi juga mendorong perubahan sikap pelajar dalam menggunakan teknologi digital secara lebih aman dan bertanggung jawab.

5. KESIMPULAN

Berdasarkan pelaksanaan kegiatan Pengabdian kepada Masyarakat yang telah dilakukan di SMK Negeri 1 Sirapit, dapat disimpulkan bahwa kegiatan edukasi pencegahan *phishing* memberikan dampak positif terhadap peningkatan pengetahuan dan kesadaran keamanan digital pelajar. Pelajar memperoleh pemahaman mengenai pengertian *phishing*, jenis-jenis phishing, serta dampak yang ditimbulkan oleh serangan phishing dalam aktivitas digital sehari-hari. Selain itu, kegiatan ini mampu meningkatkan kesadaran pelajar terhadap pentingnya menjaga keamanan data pribadi dan akun digital. Melalui penyampaian materi, diskusi, dan studi kasus, pelajar menjadi lebih berhati-hati dalam menerima pesan,

mengakses tautan, serta membagikan informasi pribadi. Dengan demikian, kegiatan Pengabdian kepada Masyarakat ini telah mencapai tujuan yang telah ditetapkan dan memberikan kontribusi nyata dalam meningkatkan literasi keamanan digital pelajar.

Daftar Pustaka

- [1] A. Fajar Zulfahri, N. Mia Aristi, A. Syafaadi Rizki, K. Anwar Hafizd, J. Komputer dan Bisnis, and P. Negeri Tanah Laut, "Pengenalan Teknologi Informasi Pada Siswa MTsN 4 Tanah Laut," *Jurnal Masyarakat Indonesia (Jumas)*, vol. 4, no. 01, pp. 58–63, 2025, doi: 10.54209/jumas.v4i01.157.
- [2] H. I. Sumakul, S. V. Tendean, and A. L. Lonto, "Pemanfaatan Teknologi Informasi dan Komunikasi sebagai Media Pembelajaran," *Tumoutou Social Science Journal*, vol. 1, no. 1, pp. 21–30, Jan. 2024, doi: 10.61476/xy1xwh12.
- [3] J. P. Aljabbar, M. Z. Aulya, M. Gilang, I. Swandanang, and D. Pratama, "Analisis Perencanaan Infrastruktur Teknologi Informasi dalam Mendukung Transformasi Digital," *Saturnus: Jurnal Teknologi dan Sistem Informasi*, vol. 4, no. 1, pp. 55–63, Jan. 2026, doi: 10.61132/saturnus.v4i1.1385.
- [4] S. Ambar, S. Syahbana, R. Susilana, and L. E. Ikanubun, "Efektivitas Curipod dalam Meningkatkan Literasi Keamanan Digital Siswa Sekolah Dasar," *Jurnal Basicedu*, vol. 9, no. 6, pp. 1759–1768, Nov. 2025, doi: 10.31004/basicedu.v9i6.10821.
- [5] T. S. Alasi, S. Nasution, R. Yap, I. J. Tarigan, and R. Alamsyah, "MITIGASI KOMPRESIF SERANGAN DDOS PADA SERVER WEB BERBASIS LINUX MENGGUNAKAN ADVANCED POLICY FIREWALL (APF) DAN TEKNIK PEMBLOKIRAN IP BERLAPIS," *Jurnal TIMES*, vol. 14, no. 1, pp. 93–98, 2025.
- [6] M. Naufal Ramadhan, J. A. Jend Yani, K. Naga, K. Kota Kisaran Timur, and S. Utara, "Pemanfaatan Literasi Digital Berbasis Teknologi Informasi untuk Kesadaran Keamanan Data dan Pencegahan Kejahatan Siber," *Neptunus: Jurnal Ilmu Komputer Dan Teknologi Informasi*, vol. 3, no. 1, pp. 151–159, Jan. 2025, doi: 10.61132/neptunus.v3i1.689.
- [7] T. S. Alasi, "Ilmu komputer," 2024, *Media Publikasi Idpress*.
- [8] S. Rustam and S. Rustam, "ANALISA CLUSTERING PHISING DENGAN K-MEANS DALAM MENINGKATKAN KEAMANAN KOMPUTER," *ILKOM Jurnal Ilmiah*, vol. 10, no. 2, pp. 175–181, Aug. 2018, doi: 10.33096/ilkom.v10i2.309.175-181.
- [9] R. Syah, S. Tinggi, and I. Kepolisian, "STRATEGI KEPOLISIAN DALAM PENCEGAHAN KEJAHATAN PHISING MELALUI MEDIA SOSIAL DI RUANG SIBER," *Jurnal Impresi Indonesia*, vol. 2, no. 9, pp. 864–870, Sep. 2023, doi: 10.58344/jii.v2i9.3594.
- [10] A. Trianurahmah *et al.*, "Analisis Ancaman Phising Melalui Aplikasi WhatsApp: Studi Kasus Manajemen Sekuriti Waspada Maraknya Kejahatan Phising Dengan Modus Berbasis Link," *Orbit: Jurnal Ilmu Multidisiplin Nusantara*, vol. 1, no. 2, pp. 60–74, Jan. 2024, doi: 10.63217/orbit.v1i2.81.