KOMMAS: Jurnal Pengabdian Kepada Masyarakat
Universitas Pamulang
Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

PENINGKATAN LITERASI KEAMANAN SIBER TERHADAP SERANGAN PHISHING DI DUNIA PENERBANGAN MELALUI WORKSHOP EDUKATIF

Indra Aulia[1,6*], Muhammad Azwar Zulmi[2,4,6], Suryo Adhi Wibowo[3,6], Ledya Novamizanti[3,6], Susi Diriyanti Novalina[5], David Chandra[1,6], Muhammad Raia Pratama Putra Wibowo[1,6], Kurnia Ramadani[1,6], Agnes Gabriela Putri Winata[1,6]

[1]Program Studi Teknologi Informasi, Fakultas Informatika, Telkom University, Jakarta, Indonesia
[2]Program Studi Magister Keamanan Siber dan Forensik Digital, Fakultas Informatika, Telkom University
[3]Program Studi Teknik Telekomunikasi, Fakultas Teknik Elektro, Telkom University, Bandung, Indonesia
[4]Standard and Security Division, AirNav Indonesia, Tangerang, Indonesia
[5]Program Studi Pemanduan Lalu Lintas Udara, Politeknik Penerbangan Medan, Medan, Indonesia
[6]Center of Excellence of Artificial Intelligence for Learning and Optimization, Telkom University, Bandung
*E-mail: indraaul@telkomuniversity.ac.id

ABSTRAK

Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan literasi digital sivitas akademika Politeknik Penerbangan Indonesia Curug (PPIC) melalui penyelenggaraan workshop edukatif bertema keamanan siber, khususnya pada isu serangan phishing dan teknik mitigasinya. Pendekatan pembelajaran yang digunakan mengacu pada prinsip andragogi Malcolm Knowles, dengan mengedepankan relevansi materi, partisipasi aktif peserta, serta orientasi pembelajaran pada pemecahan masalah nyata. Kegiatan diikuti oleh 75 peserta yang terdiri dari tenaga pengajar, pegawai, dan taruna, dengan metode evaluasi menggunakan kuesioner skala Likert dan pemetaan ke dalam enam prinsip andragogi. Hasil evaluasi menunjukkan skor tinggi pada dimensi readiness to learn, orientation to learning, dan self-concept, yang mencerminkan kesiapan dan komitmen peserta dalam menerapkan hasil pembelajaran. Kegiatan ini juga relevan secara strategis, mendukung prioritas nasional dalam Program Asta Cita, sejalan dengan visi Telkom University dan peta jalan Center of Excellence Artificial Intelligence for Learning and Optimization (CoE AILO), serta berkontribusi pada pencapaian Sustainable Development Goals (SDGs). Temuan ini menunjukkan bahwa pendekatan andragogi efektif untuk kegiatan literasi digital di lingkungan pendidikan vokasi dan dapat direplikasi untuk penguatan ketahanan digital kelembagaan.

Kata kunci: Andragogi; Keamanan Siber; Phishing; Literasi Digital; Penerbangan.

ABSTRACT

This community service program aimed to enhance the digital literacy of the academic community at the Indonesian Aviation Polytechnic Curug (PPIC) through an educational workshop on cybersecurity, specifically focusing on phishing attacks and effective prevention techniques. The learning approach was grounded in Malcolm Knowles' andragogical principles, emphasizing material relevance, active participant engagement, and problem-solving orientation. The activity was attended by 75 participants, including lecturers, staff, and cadets, and was evaluated using a Likert-scale questionnaire mapped onto six core andragogical dimensions. The evaluation results revealed high scores in readiness to learn, orientation to learning, and self-concept, indicating participants' strong preparedness and commitment to applying the acquired knowledge. Strategically, the program aligns with national priorities outlined in the Asta Cita agenda, supports the vision of Telkom University and the roadmap of the Center of Excellence for Artificial Intelligence for Learning and Optimization (CoE AILO), and contributes to achieving several Sustainable Development Goals (SDGs). These findings suggest that the andragogical approach is effective for digital literacy initiatives within vocational education environments and can be replicated to strengthen institutional digital resilience.

Keywords: Andragogy; Cybersecurity; Phishing; Digital Literacy; Aviation

Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

PENDAHULUAN

Di tengah pesatnya perkembangan era digital, kemajuan teknologi informasi telah membawa beragam kemudahan (Fauzi, Sinatrya, Ramdhani, Ramadhan, & Safari, 2022), terutama dalam industri penerbangan yang mengandalkan sistem komunikasi dan pengelolaan data yang mutakhir (Heiets et al., 2022). Namun, seiring dengan perkembangan tersebut, ancaman keamanan siber semakin meningkat (Möller, 2023), dengan serangan *phishing* menjadi salah satu risiko utamanya. *Phishing* adalah jenis serangan siber dimana pelaku berupaya memperoleh informasi sensitif, seperti kata sandi atau data pribadi, dengan menyamar sebagai pihak tepercaya (Akinyelu & Adewumi, 2014; Jalil, Ahmed, & Khan, 2023; Patil, Pattewar, Pardeshi, Punjabi, & Wagh, 2022; Zhang, Yan, Jiang, & Kim, 2020). Dalam industri penerbangan, ancaman ini memiliki dampak serius karena dapat mengakibatkan akses tanpa izin ke sistem kritis, sehingga mengancam keamanan dan keselamatan operasional (Diriyanti, Pangaribuan, Sukra, & Achaddiah, 2024).

Gambar 1. Pemateri dan Peserta Sasar di Politeknik Penerbangan Indonesia Curug

Berdasarkan laporan Indonesia Anti-Phishing Data Exchange (IDADX) pada kuartal terakhir tahun 2023 (IDADX, 2024), terdapat 8.161 kasus serangan *phishing*, dengan Indonesia menjadi negara dengan penggunaan domain .id tertinggi untuk situs phishing, mencakup 95,7% dari total serangan tersebut. Dengan kata lain, frekuensi dan tingkat kerumitan serangan *phishing* telah meningkat secara signifikan, menciptakan ancaman serius bagi individu maupun organisasi di berbagai negara, khususnya Indonesia (Balasubaramanian, Ganesan, & Rajasekaran, 2025; Purwiantono & Tjahyanto, 2017). Peningkatan ini dipengaruhi oleh beberapa faktor (Stone, 2007), seperti kurangnya pengalaman pengguna, yang meliputi: 1) minimnya pemahaman tentang struktur URL, 2) ketidakpastian dalam mengidentifikasi situs web yang tepercaya, 3) ketidakmampuan untuk melihat alamat web secara lengkap (misalnya, URL yang dialihkan atau tersembunyi dalam kode), 4) kurangnya waktu untuk memverifikasi URL atau kunjungan tidak sengaja ke situs tertentu, dan 5) kesulitan membedakan situs

Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

web resmi dari situs phishing. Dalam banyak kasus, pelaku serangan memanfaatkan kelemahan ini untuk memengaruhi persepsi korban, sehingga mereka lebih mudah menjadi sasaran serangan berbasis rekayasa sosial (*social engineering*) (Jalil et al., 2023).

Berdasarkan permasalahan tersebut, sasaran kegiatan pengabdian masyarakat adalah Tenaga Pengajar, Pegawai, dan Taruna Penerbangan di Politeknik Penerbangan Indonesia Curug (PPIC), yang berlokasi di Jl. Raya PLP Curug, Serdang Wetan, Kec. Legok, Kabupaten Tangerang, Banten 15820 melalui skema kolaborasi dalam negeri dengan Politeknik Penerbangan Medan (Poltekbang) dan AirNav Indonesia. PPIC menghadapi situasi yang tidak kalah pentingnya dengan domain keilmuan penerbangan lainnya yakni dalam upaya meningkatkan pemahaman tentang pencegahan dan penanganan serangan *phishing* guna menghadapi ancaman siber di sektor penerbangan (Lazaro Florido-Benitez, 2024; Lázaro Florido-Benitez, 2024b, 2024a). Untuk itu, sebuah workshop edukatif untuk peningkatan literasi keamanan siber atas serangan *phishing* sangat penting adanya (Vadila & Pratama, 2021). Hal ini tentunya dapat meningkatkan pengetahuan dasar para pemangku kepentingan di dunia penerbangan dalam menghadapi dan mencegah serangan *phishing* yang dapat merugikan keselamatan dan operasional penerbangan.

Pelaksanaan kegiatan ini menggunakan pendekatan andragogi untuk mencapai tujuan dimaksud. Pendekatan ini menekankan pembelajaran pada karakteristik peserta dewasa melalui proses belajar yang diarahkan pada kebutuhan, pengalaman, dan tujuan praktis yang relevan bagi mereka. Menurut Malcolm Knowles, pembelajaran melalui pendekatan ini mengacu kepada enam prinsip utama (Knowles, Holton III, & Swanson, 2014): 1) adanya kebutuhan untuk mengetahui alasan belajar (*need to know*), 2) dorongan untuk belajar secara mandiri (*self-concept*), 3) pemanfaatan pengalaman sebagai sumber belajar (*prior experience*), 4) kesiapan belajar yang muncul dari tuntutan peran sosial (*readiness to learn*), 5) orientasi belajar yang bersifat problem solving (*orientation to learning*), serta 6) motivasi internal yang dominan (*internal motivation*). Melalui pendekatan ini, peserta menjadi mitra aktif dalam proses belajar, bukan hanya sekadar objek yang menerima informasi. Materi disusun secara kontekstual, dikaitkan langsung dengan potensi ancaman *phishing* yang mungkin mereka temui dalam aktivitas akademik dan operasional penerbangan. Penyampaian materi tersebut tidak hanya dilakukan secara satu arah, akan tetapi mendorong partisipasi aktif melalui ruang diskusi dan studi kasus untuk membangun pemahaman peserta sasar. Dengan demikian, pendekatan andragogi memastikan bahwa workshop edukatif kegiatan ini menjadi relevan, bermakna, dan mampu membentuk kesadaran kritis serta keterampilan deteksi phishing yang dapat langsung diterapkan dalam lingkungan profesional peserta sasar dalam upaya menciptakan ekosistem penerbangan yang lebih aman baik seacar langsung maupun tidak langsung.

Workshop edukatif yang dilaksanakan dalam kegiatan pengabdian kepada masyarakat ini bertujuan untuk membangun literasi digital peserta sasar melalui peningkatan pengetahuan yang

Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

mendalam tentang jenis-jenis serangan phishing, teknik pengenalannya, serta langkah-langkah pencegahan yang efektif untuk melindungi diri dan organisasi penerbangan. Hal ini tentunya sejalan dengan prioritas pemerintah dalam Program Asta Cita dalam memantapkan sistem pertahanan negara (Asta Cita 2) melalui penguatan pembangunan Sumber Daya Manusia (SDM), sains dan teknologi Indonesia (Asta Cita 4). Selain itu, kegiatan ini telah sejalan dengan visi dan misi Telkom University dan Peta Jalan Center of Excellence of Artificial Intelligence for Learning and Optimization yang berfokus kepada *Secure Smart Society*. Di lain sisi, kegiatan ini juga menjadi pendukung atas tercapainya *Sustainable Development Goals* (SDG) di sivitas akademika Telkom University dalam hal Pendidikan Berkualitas, Industri, Inovasi dan Infrastruktur, serta Perdamaian, Keadilan dan Kelembagaan yang Tangguh.

METODE

Metode pelaksanaan kegiatan pengabdian kepada masyarakat melalui Workshop Edukatif berbasis Pendekatan Andragogi telah dirancang dan disusun melalui rangka model *Participatory Action Research* (PAR) (Cornish et al., 2023). Rangka model ini adalah suatu rangka model berbasis aksi partisipatif yang menekankan kolaborasi aktif antara tim pelaksana dan peserta sasaran dalam seluruh siklus kegiatan—mulai dari perencanaan, pelaksanaan, hingga refleksi. Dalam kerangka PAR, setiap tahapan kegiatan ini diklasifikasikan ke dalam tiga ruang utama: 1) Ruang Perencanaan Partisipatif, yang mencakup tahap penjajakan kerja sama kolaboratif dengan mitra Politeknik Penerbangan Indonesia Curug (PPIC) dan Poltekbang Medan, serta pemetaan literasi dan kebutuhan peserta melalui pertemuan daring; 2) Ruang Aksi Transformatif, yang direpresentasikan oleh proses penyusunan materi edukatif, koordinasi teknis, serta pelaksanaan workshop interaktif berbasis pendekatan andragogi yang menempatkan peserta sebagai subjek belajar aktif; dan 3) Ruang Refleksi Kolaboratif, yang dijalankan melalui evaluasi berbasis umpan balik peserta dan pelaporan hasil kegiatan untuk keperluan diseminasi pengetahuan dan peningkatan kualitas program berkelanjutan. Pendekatan PAR dipilih karena mampu mengakomodasi keterlibatan nyata peserta dan mitra institusional dalam siklus kegiatan, serta selaras dengan tujuan pemberdayaan literasi keamanan siber yang kontekstual dan aplikatif. Adapun metode kegiatan yang telah dilaksanakan adalah sebagai berikut:

1. Tahap Persiapan: Kolaborasi dan Pemetaan Kebutuhan

   Pada tahap awal, tim pengabdian melakukan penjajakan dan membangun kemitraan strategis dalam skema kolaborasi nasional dengan PPIC dan Poltekbang Medan. Kerja sama ini bertujuan untuk menyinergikan kompetensi teknis, kebutuhan institusi, dan potensi literasi digital peserta sasaran yang berasal dari kalangan penerbangan. Penjajakan dilakukan secara formal melalui pertemuan daring (*online meeting*) yang difasilitasi oleh pihak PPIC. Dalam forum tersebut, tim pengabdian bersama mitra institusi melakukan pemetaan kesiapan kegiatan mencakup aspek teknis

Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

(lokasi, waktu, sarana), serta pemetaan tingkat literasi digital dan keamanan siber peserta sasaran berdasarkan hasil wawancara singkat dengan pihak perwakilan tenaga pendidik dan manajemen kampus. Pemetaan ini sangat krusial untuk menyesuaikan materi dan metode pelaksanaan workshop agar kontekstual dan relevan dengan kebutuhan nyata peserta sasar (Nasution, Aulia, & others, 2019).

2. Tahap Persiapan Lanjutan: Pengembangan Materi dan Koordinasi Eksternal

   Setelah pemetaan dilakukan, tim pengabdian melanjutkan dengan menyusun materi kegiatan secara terstruktur, dengan mempertimbangkan kerangka pendekatan andragogi sebagai basis desain pembelajaran. Materi dirancang untuk bersifat aplikatif dan berbasis pengalaman, menghindari pendekatan monologis yang pasif. Setiap narasumber diberikan alur penyampaian materi yang mendorong partisipasi peserta melalui diskusi terbuka, refleksi pengalaman, dan penyelesaian kasus. Selain itu, dilakukan koordinasi eksternal untuk menyepakati mekanisme teknis workshop, termasuk pemanfaatan ruang pertemuan, perangkat multimedia, dan strategi fasilitasi yang akan diterapkan untuk menciptakan suasana interaktif dan kolaboratif selama pelaksanaan.

3. Tahap Pelaksanaan: Workshop Edukatif Berbasis Andragogi

   Kegiatan inti dilaksanakan pada tanggal 5 Desember 2024 di lingkungan kampus PPIC dengan jumlah peserta sebanyak 75 orang, yang terdiri dari unsur tenaga pengajar, pegawai administratif, dan taruna. Kegiatan dirancang sebagai workshop edukatif interaktif, bukan seminar satu arah, agar sesuai dengan karakteristik pembelajaran orang dewasa. Penerapan pendekatan andragogi menjadi fondasi utama dalam penyampaian seluruh sesi materi. Empat sesi materi disampaikan oleh narasumber yang mewakili bidang keahlian yang saling melengkapi:

   a. Materi 1: Etika Digital dan Keamanan Informasi oleh Indra Aulia menekankan pentingnya kesadaran individu terhadap tanggung jawab digital dalam dunia kerja, serta memperkenalkan prinsip keamanan informasi dasar (Gunawan, Fadhilah, & Sakti, 2024).

Gambar 1 Penyampaian Materi Pertama

Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

b. Materi 2: Teknologi AI dalam Keamanan Siber oleh Suryo Adhi Wibowo memberikan gambaran terkini tentang penggunaan kecerdasan buatan dalam mendeteksi ancaman siber.
c. Materi 3: Serangan Siber Phishing Berbasis *Social Engineering* (Jalil et al., 2023) dalam Dunia Penerbangan oleh M. Azwar Zulmi yang berfokus pada situasi saat ini dan model serangan yang menyasar sektor penerbangan. Materi disampaikan tidak hanya teori dasar tetapi juga teori praktis melalui studi kasus yang relevan dengan organisasi penerbangan.

Gambar 2 Penyampaian Materi Pertama

Setiap sesi materi tidak hanya paparan narasumber, tetapi juga dibuka ruang diskusi dua arah dan pertanyaan langsung yang interaktif untuk menguji pemahaman peserta secara langsung. Pertanyaan langsung yang disampaikan narasumber memiliki relevansi kepada studi kasus dan pemetaan risiko digital serangan *phishing* di sektor penerbangan yang harus dijawab secara spontan dan argumentatif oleh para peserta sasar. Strategi ini memperkuat elemen '*readiness to learn*' dan '*problem-oriented learning*' sebagaimana dijelaskan oleh Malcolm Knowles dalam teori andragoginya. Peserta dilibatkan secara aktif untuk menghubungkan materi dengan pengalaman kerja dan tugas fungsional mereka. Dengan kata lain, peserta diposisikan sebagai subjek belajar yang otonom, dan fasilitator bertindak sebagai mitra dialog, bukan instruktur tunggal.

Gambar 3. Aktif Partisipatif Peserta melalui Pertanyaan Langsung Berbasis Studi Kasus

4. Tahap Evaluasi dan Diseminasi

Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

Setelah pelaksanaan, dilakukan evaluasi kegiatan melalui pengumpulan feedback tertulis dan wawancara singkat dari peserta menggunakan instrumen kuesioner reflektif. Evaluasi mencakup tiga aspek utama: relevansi materi, efektivitas metode, dan kepuasan peserta terhadap kegiatan. Hasil evaluasi dianalisis secara deskriptif dan digunakan sebagai bahan laporan kegiatan yang disusun untuk internal Telkom University serta dokumentasi mitra institusi (PPIC dan Poltekbang Medan). Di tahap akhir, hasil kegiatan ini akan didiseminasikan melalui media publikasi ilmiah dan jaringan mitra nasional sebagai bentuk hilirisasi pengetahuan dan replikasi praktik baik dalam edukasi keamanan siber di institusi pendidikan vokasi lainnya.

Kegiatan pengabdian masyarakat ini mengadopsi pendekatan partisipatif berbasis pelatihan aktif, yang menempatkan siswa sebagai subjek utama dalam proses pembelajaran. Pendekatan ini bertujuan menciptakan suasana belajar yang interaktif, kontekstual, dan aplikatif. Kegiatan dilakukan dalam tiga tahapan utama: persiapan, pelaksanaan inti, dan evaluasi.

HASIL

Kegiatan workshop edukatif diikuti oleh 75 peserta, yang terdiri dari tenaga pengajar, pegawai administratif, dan taruna PPI Curug. Rentang usia peserta cukup bervariasi, dengan dominasi usia antara 18–25 tahun dan >35 tahun, mencerminkan keberagaman latar belakang pengalaman dan fungsi peran di institusi. Variasi usia ini juga memperkuat pentingnya penerapan pendekatan andragogi, di mana peserta dewasa diakomodasi sebagai individu yang memiliki pengalaman belajar terdahulu dan kebutuhan yang kontekstual.

Instrumen evaluasi yang digunakan dalam kegiatan ini berupa kuesioner berbasis skala Likert dengan rentang penilaian 1 sampai 5, yang terdiri atas sepuluh butir pertanyaan. Setiap pertanyaan dirancang untuk mengukur aspek-aspek kunci dalam pembelajaran orang dewasa sesuai prinsip *andragogi* yang dikemukakan oleh Malcolm Knowles. Terdapat 10 instrumen pertanyaan yang secara relevan mengukur konsep pembelajaran berbasis pendekatan andragogi sebagaimana yang disajikan pada Tabel 1.

Tabel 1 Kategorisasi Pertanyaan berdasarkan konsep Andragogi (Knowles et al., 2014)

No	Kategori Andragogi	Pertanyaan	Tujuan
1	*Need to Know*	Seberapa relevan kegiatan ini dengan kebutuhan Anda?	Menggali relevansi langsung materi dengan peran dan kebutuhan peserta
2	*Self-Concept*	Seberapa sering Anda akan menerapkan pengetahuan yang diperoleh dalam aktivitas sehari-hari?	Mengukur sejauh mana peserta merasa bertanggung jawab terhadap tindak lanjut pembelajaran.
3	*Prior Experience*	Sebelum kegiatan ini, seberapa banyak Anda mengetahui tentang phishing website?	Menggali pengalaman awal dan titik tolak peserta sebelum intervensi.

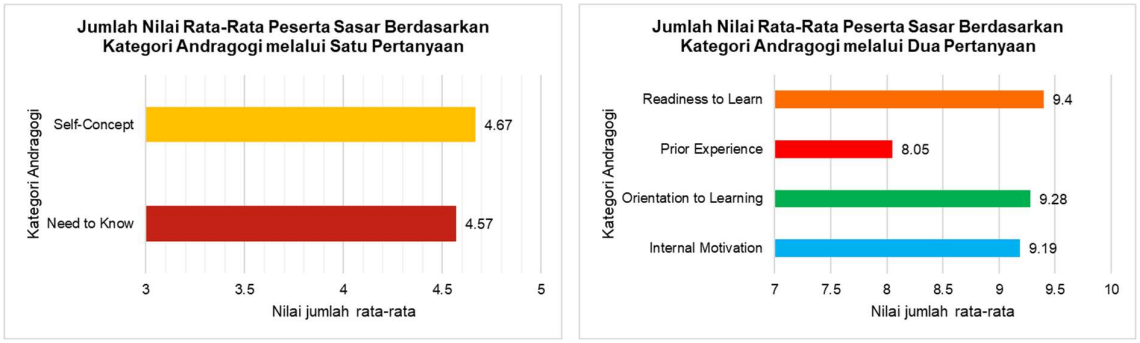
Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

No	Kategori Andragogi	Pertanyaan	Tujuan
		Apakah menurut Anda, simulasi yang dilakukan mencerminkan situasi nyata?	Mengukur hubungan antara materi dan pengalaman kerja peserta sebelumnya.
4	*Readiness to Learn*	Apakah materi yang diberikan mudah diterapkan dalam kehidupan sehari-hari?	Mengukur kesiapan peserta untuk menyerap pembelajaran yang kontekstual.
		Apakah kegiatan ini memotivasi Anda untuk lebih berhati-hati dalam mengakses website?	Indikator kesiapan belajar karena adanya kesadaran atas risiko dunia nyata.
5	*Orientation to Learning*	Setelah kegiatan ini, seberapa yakin Anda dapat mengenali phishing website?	Mengukur keberhasilan materi dalam menumbuhkan keterampilan praktis.
		Apakah Anda memahami konsep phishing setelah kegiatan ini?	Fokus pada pemahaman konkret terhadap masalah nyata yang dihadapi peserta.
		Bagaimana menurut Anda tentang kualitas materi yang disampaikan?	Persepsi kualitas dapat memperkuat atau melemahkan motivasi internal.
6	*Internal Motivation*	Berikan penilaian keseluruhan untuk kegiatan ini?	Menyimpulkan persepsi keseluruhan yang mencerminkan kepuasan dan motivasi berkelanjutan.

Berdasarkan hasil survei yang diberikan, kegiatan ini menunjukkan keberhasilan yang baik dalam menjalankan Workshop Edukatif menggunakan pendekatan Andragogi. Hal ini terlihat dari hasil pengolahan data kemudian direpresentasikan dalam dua kelompok: kategori prinsip andragogi yang direpresentasikan oleh satu pertanyaan (single item), dan kategori prinsip yang direpresentasikan oleh dua pertanyaan (dual item). Temuan ini memberikan gambaran yang lebih dalam tentang bagaimana peserta menyerap dan memaknai kegiatan berdasarkan karakteristik latar belakang peserta sasar.

Pada kategori satu pertanyaan (Gambar 4 (a)), prinsip *Self-Concept* memperoleh skor rata-rata tertinggi sebesar 4,67, menunjukkan bahwa peserta memiliki kesadaran dan tanggung jawab terhadap penerapan pengetahuan yang diperoleh secara mandiri dalam konteks profesional mereka. Diikuti oleh prinsip *Need to Know* dengan skor 4,57, yang menunjukkan bahwa peserta menganggap materi yang disampaikan sangat relevan dengan kebutuhan aktual mereka dalam menghadapi ancaman siber. Kedua hasil ini memperkuat validitas kegiatan sebagai proses belajar yang kontekstual, di mana peserta tidak hanya hadir secara fisik, tetapi juga secara psikologis merasa perlu dan terlibat dalam proses pembelajaran.

Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517



(a) (b)

Gambar 4 Nilai rata-rata untuk setiap kategori andragogi baik melalui satu dan dua pertanyaan

Sementara itu, dalam kategori dua pertanyaan (Gambar 4 (b)), prinsip *Readiness to Learn* mencatatkan skor gabungan tertinggi yaitu 9,4, menunjukkan kesiapan yang tinggi dari peserta untuk menerima materi yang berkaitan dengan keamanan informasi, terutama karena topik yang diangkat menyentuh risiko langsung yang mungkin mereka hadapi. *Orientation to Learning* menempati posisi kedua dengan skor 9,28, yang merefleksikan apresiasi peserta terhadap pendekatan pembelajaran yang berorientasi pada pemecahan masalah nyata, seperti simulasi deteksi phishing yang dihadirkan dalam workshop. Disusul oleh prinsip *Internal Motivation* dengan skor 9,19, yang memperlihatkan bahwa peserta secara intrinsik terdorong untuk memahami dan menerapkan pengetahuan tanpa paksaan eksternal. Adapun prinsip *Prior Experience* mencatat skor terendah yaitu 8,05, yang meskipun masih tergolong baik, menunjukkan bahwa sebagian peserta sebelumnya belum memiliki pengalaman atau pemahaman mendalam mengenai phishing. Hal ini sekaligus mengonfirmasi pentingnya intervensi edukatif ini sebagai bentuk penguatan literasi keamanan siber.

Secara keseluruhan, tingginya skor pada lima dari enam prinsip andragogi mengindikasikan bahwa desain kegiatan yang mengacu pada pembelajaran andragogi telah berhasil menciptakan pengalaman belajar yang tidak hanya informatif tetapi juga transformasional. Peserta tidak hanya memahami materi, melainkan juga menunjukkan kesiapan dan niat untuk mengadopsi perilaku baru yang lebih aman secara digital. Temuan ini memperkuat relevansi pendekatan andragogi dalam pendidikan literasi digital, khususnya dalam konteks pengabdian kepada masyarakat di lingkungan pendidikan vokasi dan penerbangan.

PEMBAHASAN

Hasil kegiatan workshop keamanan siber yang mengusung pendekatan pembelajaran andragogi menunjukkan bahwa peserta, yang terdiri dari dosen, pegawai, dan taruna PPI Curug, memberikan respons yang sangat positif terhadap baik konten materi maupun metode penyampaiannya. Skor tinggi yang diperoleh pada aspek relevansi, kemudahan penerapan, serta motivasi internal peserta menjadi

Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

indikator bahwa kegiatan ini telah memenuhi karakteristik utama pembelajaran andragogi, yaitu kontekstual, reflektif, dan partisipatif. Peserta tidak sekadar menjadi penerima informasi, melainkan juga berperan aktif dalam proses pembelajaran melalui diskusi, simulasi, dan refleksi terhadap pengalaman pribadi yang berkaitan dengan ancaman keamanan siber. Hal ini menunjukkan bahwa pendekatan andragogi sangat efektif diterapkan dalam kegiatan pengabdian kepada masyarakat, khususnya ketika sasarannya adalah individu dewasa dengan peran profesional di sektor pendidikan vokasi dan penerbangan.

Pemetaan hasil evaluasi ke dalam enam prinsip andragogi Knowles semakin memperkuat efektivitas pendekatan ini. Dimensi *Readiness to Learn*, *Orientation to Learning*, dan *Self-Concept* memperoleh skor tertinggi, menandakan bahwa peserta belajar secara aktif ketika materi menyentuh isu nyata, menghargai pendekatan pembelajaran berbasis pemecahan masalah, dan merasa bertanggung jawab atas penerapan hasil belajar dalam lingkungan kerjanya. Sementara itu, skor yang lebih rendah hanya ditemukan pada aspek *Prior Experience*, yang justru menunjukkan bahwa sebagian besar peserta sebelumnya belum memiliki pemahaman memadai mengenai phishing. Temuan ini menggarisbawahi urgensi kegiatan semacam ini sebagai bentuk intervensi literasi digital yang strategis. Dengan menjembatani kesenjangan pengetahuan tersebut, workshop ini tidak hanya mendidik tetapi juga memperkuat pertahanan siber dalam ekosistem pendidikan vokasi yang memiliki peran vital dalam dunia aviasi nasional.

Penerapan andragogi dalam kegiatan ini juga memberikan implikasi metodologis terhadap desain program pengabdian yang lebih adaptif (Arti et al., 2025) terhadap konteks dan karakter peserta. Pendekatan ini terbukti mampu membangun kesadaran kritis, meningkatkan pemahaman, dan mendorong perubahan perilaku digital secara konkret. Oleh karena itu, strategi pembelajaran yang berbasis pada prinsip andragogi dapat menjadi model yang direplikasi untuk kegiatan edukatif serupa di institusi lain, terutama ketika sasaran melibatkan peserta belajar dewasa dengan latar belakang tanggung jawab profesional yang kompleks.

Lebih jauh, kegiatan ini juga sejalan dengan arah strategis nasional dan institusional. Dari sisi kebijakan negara, kegiatan ini mendukung Program Asta Cita, khususnya Asta Cita 2 tentang pemantapan sistem pertahanan negara melalui perlindungan ruang digital, dan Asta Cita 4 yang menekankan penguatan pembangunan sumber daya manusia, sains, dan teknologi. Pada tataran institusi, kegiatan ini sejalan dengan visi Telkom University untuk menjadi universitas berkelas dunia yang berperan aktif dalam transformasi digital, serta mendukung implementasi peta jalan Center of Excellence Artificial Intelligence for Learning and Optimization (CoE AILO) yang berfokus pada pengembangan Secure Smart Society. Selain mendukung misi pendidikan berbasis teknologi, kegiatan ini juga berkontribusi langsung pada pencapaian Sustainable Development Goals (SDGs), terutama pada poin Pendidikan Berkualitas (SDG 4), Inovasi dan Infrastruktur (SDG 9), serta Institusi yang

Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

Tangguh dan Inklusif (SDG 16). Dengan demikian, kegiatan ini tidak hanya berhasil secara teknis dan pedagogis, tetapi juga relevan secara strategis dan berkontribusi nyata tidak hanya terhadap peningkatan literasi individual akan tetapi terhadap pembangunan ketahanan digital nasional dan institusional (Gunawan et al., 2024).

SIMPULAN

Workshop edukatif yang dilaksanakan dalam kegiatan pengabdian kepada masyarakat ini bertujuan untuk membangun literasi digital peserta sasar melalui peningkatan pengetahuan yang mendalam tentang jenis-jenis serangan phishing, teknik pengenalannya, serta langkah-langkah pencegahan yang efektif untuk melindungi diri dan organisasi penerbangan. Berdasarkan evaluasi berbasis pendekatan pembelajaran andragogi, kegiatan ini terbukti mampu meningkatkan kesadaran, pemahaman konseptual, dan kesiapan peserta dalam menghadapi ancaman keamanan siber. Seluruh aspek penilaian menunjukkan respons yang sangat positif, dengan skor tinggi pada indikator relevansi materi, kemudahan penerapan, dan motivasi internal peserta. Pelaksanaan kegiatan ini juga memiliki relevansi strategis dengan prioritas nasional dalam Program Asta Cita, khususnya Asta Cita 2 tentang penguatan sistem pertahanan negara dan Asta Cita 4 terkait pengembangan SDM, sains, dan teknologi. Di tingkat institusi, kegiatan ini sejalan dengan visi dan misi Telkom University serta peta jalan Center of Excellence Artificial Intelligence for Learning and Optimization (CoE AILO) yang berfokus pada penguatan *Secure Smart Society*. Selain itu, kegiatan ini turut berkontribusi terhadap pencapaian Sustainable Development Goals (SDG), terutama dalam aspek Pendidikan Berkualitas (SDG 4), Industri, Inovasi, dan Infrastruktur (SDG 9), serta Perdamaian, Keadilan, dan Kelembagaan yang Tangguh (SDG 16) di lingkungan sivitas akademika.

Diperlukan pelaksanaan workshop edukatif serupa secara berkelanjutan dengan cakupan topik yang lebih luas, seperti keamanan data pribadi, manajemen risiko digital, dan deteksi rekayasa sosial berbasis AI. Selain itu, penting untuk meningkatkan kolaborasi kelembagaan dengan industri yang relevan di bidang keamanan siber dan teknologi informasi, guna memperkuat keterhubungan antara dunia pendidikan dan kebutuhan nyata dunia kerja. Pelibatan lebih banyak pembicara dari kalangan industri juga diharapkan dapat memberikan wawasan aplikatif dan studi kasus aktual. Di samping itu, pelaksanaan kegiatan secara *hybrid* memerlukan dukungan jaringan internet yang stabil dan berkualitas agar pelaksanaan secara *online* dan *onsite* dapat berjalan lancar tanpa hambatan teknis yang mengganggu jalannya interaksi dan proses pembelajaran.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Telkom University dan Politeknik Penerbangan Medan yang telah memberikan dukungan pendanaan kegiatan pengabdian

Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

kepada masyarakat ini, baik dalam bentuk *in cash* maupun *in kind*, melalui *Perjanjian Pelaksanaan Pengabdian kepada Masyarakat Dana Internal Universitas Telkom Skema Kolaborasi Dalam Negeri Periode 2 Tahun 2024*, dengan nomor: 0709/ABD07/PPM-JPM/2024. Dukungan ini menjadi fondasi utama dalam terselenggaranya kegiatan secara optimal dan berdampak.

Ucapan terima kasih juga disampaikan kepada Kelompok Keilmuan Pengolahan Sinyal Informasi, Kelompok Keilmuan Communication and Information Technology Infrastructure, serta Center of Excellence of Artificial Intelligence for Learning and Optimization (CoE AILO) yang telah mendorong dan memfasilitasi terlaksananya kegiatan ini, baik melalui dukungan keilmuan, pendampingan teknis, maupun penguatan jejaring kolaboratif lintas kampus dan institusi.

Selanjutnya, penulis menyampaikan apresiasi yang tinggi kepada Politeknik Penerbangan Curug (PPIC) yang telah bersedia menjadi mitra kegiatan pengabdian kepada masyarakat ini. Kegiatan ini dilaksanakan berdasarkan Surat Persetujuan Masyarakat Sasar tertanggal 23 Agustus 2024 yang ditandatangani oleh Kepala Pusat Penelitian dan Pengabdian kepada Masyarakat PPIC, Dr. Dian Anggraini Purwaningtyas. Tanpa keterlibatan aktif PPIC sebagai mitra nasional bereputasi, kegiatan ini tidak akan berjalan dengan dukungan konteks dan sasaran yang tepat.

Terakhir, penghargaan juga diberikan kepada Telkom University Kampus Utama dan Telkom University Kampus Jakarta atas komitmennya dalam mendukung implementasi kerja sama kelembagaan melalui Memorandum of Understanding Nomor 222/SAM3/KST/2024 dan PJ-POLTEKBANG.MDN 38 Tahun 2024, serta Memorandum of Agreement Nomor 301/SAM4/TUJ/2024 dan PJ-POLTEKBANG.MDN 39 Tahun 2024 yang ditandatangani bersama Politeknik Penerbangan Medan. Kolaborasi ini menjadi wujud nyata sinergi lintas institusi dalam mendukung pengabdian kepada masyarakat berbasis sains, teknologi, dan penguatan sumber daya manusia Indonesia.

MATERI PELENGKAP

Kegiatan ini telah terdokumentasi di berbagai media luaran diantaranya:

1. Berita Nasional di Viva News: Serangan Phising Kian Marak, Mahasiswa Hingga Dosen Dibekali Ini Buat Hadapi Ancaman Siber (Sumiyati, 2024)
2. Berita Nasional di Waspada Online: Bangun Ketahanan Siber SDM Penerbangan, Telkom University Gandeng Poltekbang Medan, PPI Curug dan AirNav Indonesia (Sandy, 2024)
3. Blog Nasional di Kompasiana: Tingkatkan Awareness Keamanan Siber, Telkom University bersinergi dengan Poltekbang Medan dan AirNav Indonesia (Aulia, 2024)
4. Video Kegiatan di Youtube Channel AILO Tel-U Jakarta: Telkom University Perkuat Kolaborasi di Sektor Penerbangan (Sjakha & Kurvanka, 2025)

DAFTAR PUSTAKA

Akinyelu, A. A., & Adewumi, A. O. (2014). Classification of phishing email using random forest and text mining techniques. *Journal of Information Security*, *5*(3), 118–128. https://doi.org/10.4236/jis.2014.53012

Arti, E. S., Amir, E., Endrawijaya, I., Anggraini, D., Wagini, D., Sadiatmi, R., … Muzaki, M. F. (2025). Desain Video Based Learning Pada Mata Kuliah Aeronautical Information Service. *SCIENCE: Jurnal Inovasi Pendidikan Matematika Dan IPA*, *5*(1), 295–303.

Aulia, I. (2024). Tingkatkan Awareness Keamanan Siber, Telkom University bersinergi dengan Poltekbang Medan dan AirNav Indonesia. Retrieved January 1, 2025, from https://www.kompasiana.com/indraauliainar/6768324a34777c1e730b8b94/tingkatkan-awareness-keamanan-siber-telkom-university-bersinergi-dengan-poltekbang-medan-dan-airnav-indonesia

Balasubaramanian, S., Ganesan, P., & Rajasekaran, J. (2025). Weighted ensemble classifier for malicious link detection using natural language processing. *International Journal of Pervasive Computing and Communications*, *21*(1), 26–42.

Cornish, F., Breton, N., Moreno-Tabarez, U., Delgado, J., Rua, M., de-Graft Aikins, A., & Hodgetts, D. (2023). Participatory action research. *Nature Reviews Methods Primers*, *3*(1), 34.

Diriyanti, S., Pangaribuan, L. J., Sukra, R., & Achaddiah, B. N. (2024). Implemementasi Kriptografi Algoritma Hillcipher Dengan Kunci Tandatangan Pengirim Pesan Terhadap Keamanan Message Handling System Di Bandara Kualanamu. *Innovative: Journal Of Social Science Research*, *4*(2), 5953–5965.

Fauzi, E., Sinatrya, M. V., Ramdhani, N. D., Ramadhan, R., & Safari, Z. M. R. (2022). Pengaruh kemajuan teknologi informasi terhadap perkembangan akuntansi. *Jurnal Riset Pendidikan Ekonomi*, *7*(2), 189–197.

Florido-Benitez, Lazaro. (2024). The types of hackers and cyberattacks in the aviation industry. *Journal of Transportation Security*, *17*(1), 13.

Florido-Benitez, Lázaro. (2024a). The Importance of Cybersecurity for Airports in Marketing Activities. In *Airport Marketing Strategies* (pp. 165–183). Emerald Publishing Limited.

Florido-Benitez, Lázaro. (2024b). The types of hackers and cyberattacks in the aviation industry. *Journal of Transportation Security*, *17*(1), 13.

Gunawan, F., Fadhilah, A., & Sakti, E. M. S. (2024). Membangun Benteng Digital Untuk Memperkuat Etika Cyber Security Melawan Ancaman Cyber Crime. *Jurnal Ilmiah Teknik Informatika (TEKINFO)*, *25*(1), 154–167.

Heiets, I., La, J., Zhou, W., Xu, S., Wang, X., & Xu, Y. (2022). Digital transformation of airline industry. *Research in Transportation Economics*, *92*, 101186.

IDADX. (2024). Laporan Kuartal IV 2024.

Jalil, A., Ahmed, M., & Khan, S. (2023). Psychological exploitation in phishing: A study of social engineering tactics. *International Journal of Information Security*, *22*(4), 789–802. https://doi.org/10.1007/s10207-023-00645-3

Knowles, M. S., Holton III, E. F., & Swanson, R. A. (2014). *The adult learner: The definitive classic in adult education and human resource development*. Routledge.

Möller, D. P. F. (2023). Cybersecurity in digital transformation. In *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices* (pp. 1–70). Springer.

Nasution, M. K. M., Aulia, I., & others. (2019). Design of the research problem statement. In *Journal*

of Physics: Conference Series (Vol. 1235, p. 12115).

Patil, D., Pattewar, T., Pardeshi, S., Punjabi, V., & Wagh, R. (2022). Learning to Detect Phishing Web Pages Using Lexical and String Complexity Analysis. *EAI Endorsed Transactions on Scalable Information Systems*, *10*(1), e1. https://doi.org/10.4108/eai.20-4-2022.173950

Purwiantono, F. E., & Tjahyanto, A. (2017). Model Klasifikasi Untuk Deteksi Situs Phising Di Indonesia. *Surabaya: Institut Teknologi Sepuluh Nopember*.

Sandy. (2024). Bangun Ketahanan Siber SDM Penerbangan, Telkom University Gandeng Poltekbang Medan, PPI Curug dan AirNav Indonesia. Retrieved January 5, 2025, from https://waspada.co.id/bangun-ketahanan-siber-sdm-penerbangan-telkom-university-gandeng-poltekbang-medan-ppi-curug-dan-airnav-indonesia/

Sjakha, R. A., & Kurvanka, A. (2025). Telkom University Perkuat Kolaborasi di Sektor Penerbangan. Retrieved January 26, 2025, from https://www.youtube.com/watch?v=wcrXU81GT5M

Stone, A. (2007). Natural-language processing for intrusion detection. *Computer*, *40*(12), 103–105.

Sumiyati. (2024). Serangan Phising Kian Marak, Mahasiswa Hingga Dosen Dibekali Ini Buat Hadapi Ancaman Siber. Retrieved January 5, 2025, from https://www.viva.co.id/edukasi/1783350-serangan-phising-kian-marak-mahasiswa-hingga-dosen-dibekali-ini-buat-hadapi-ancaman-siber#goog_rewarded

Vadila, N., & Pratama, A. R. (2021). Analisis Kesadaran Keamanan Terhadap Ancaman Phishing. *Automata*, *2*(2).

Zhang, D., Yan, Z., Jiang, H., & Kim, T. (2020). A domain-feature enhanced classification model for phishing website detection. *IEEE Access*, *8*, 148123–148135. https://doi.org/10.1109/ACCESS.2020.3016266