JURNAL HASIL PENGABDIAN MASYARAKAT (JURIBMAS)
https://ejurnal.lkpkaryaprima.id/index.php/juribmas
e-ISSN: 2961-7286 | p-ISSN: 2962-3677
Volume 4 No 3 Maret 2026 | Hal : 692-698
DOI: https://doi.org/10.62712/juribmas.v4i3.929

Peningkatan Kesadaran Keamanan Siber *(Cyber Security Awareness)* Melalui Penyuluhan Bagi Siswa Sekolah Menengah Pertama

Dwi Wahyudi[1,*], Radinal Fadli[2]

[1,2]Fakultas Keguruan dan Ilmu Pendidikan, Program Studi Pendidikan Teknologi Informasi, Universitas Lampung, Bandar Lampung, Indonesia

Email: [1]dwiwahyudi@fkip.unila.ac.id, [2]radinalfadli@fkip.unila.ac.id
*Email Corresponding Author: dwiwahyudi@fkip.unila.ac.id

Abstrak

Pesatnya perkembangan teknologi digital meningkatkan risiko ancaman siber bagi kalangan pelajar SMP. Kegiatan pengabdian masyarakat ini bertujuan untuk meningkatkan kesadaran dan niat perilaku keamanan siber siswa melalui penyuluhan interaktif. Metode pelaksanaan meliputi penyampaian materi multimedia, simulasi ancaman, serta evaluasi menggunakan desain pre-test dan post-test pada 40 siswa di SMP Islam Plus At-Tholibin. Instrumen evaluasi mencakup empat skala perilaku: berisiko, konservatif, paparan risiko, dan persepsi risiko. Hasil kegiatan menunjukkan pergeseran pandangan yang signifikan, dengan skor rata-rata meningkat dari 2.15 menjadi 3.72. Analisis N-Gain menghasilkan skor 0,84 yang termasuk dalam kategori "Tinggi". Hal ini membuktikan bahwa pendekatan gamifikasi dan simulasi efektif dalam memberikan pemahaman mendalam untuk mengenali ancaman siber sejak dini. Kegiatan ini diharapkan dapat menjadi model edukasi berkelanjutan untuk membentuk budaya keamanan siber di lingkungan sekolah.

Kata Kunci: Keamanan Siber, Kesadaran Keamanan Siber, Siswa SMP, Pengabdian Masyarakat, N-Gain.

Abstract

The rapid growth of digital technology increases cyber threat risks for junior high school students. This community service activity aimed to enhance students' cyber security awareness and behavioral intentions through interactive counseling. The implementation method included multimedia presentations, threat simulations, and evaluations using pre-test and post-test designs with 40 students at SMP Islam Plus At-Tholibin. The evaluation instrument covered four behavioral scales: risky, conservative, risk exposure, and risk perception behavior. Results showed a significant shift in perspectives, with average scores increasing from 2.15 to 3.72. The N-Gain analysis yielded a score of 0.84, categorized as "High". This proves that gamification and simulation approaches are effective in providing a deep understanding to recognize cyber threats from an early age. This activity is expected to serve as a model for sustainable education to build a cyber security culture within the school environment.

Keywords*: Cyber Security, Cyber Security Awareness, Junior High School Students, Community Service, N-Gain.*

1. PENDAHULUAN

Di era digital saat ini, ancaman serangan siber terus meningkat seiring dengan semakin masifnya transformasi digital di berbagai sektor kehidupan (Hoppe, Gatzert, & Gruner, 2021; Wang, Guo, & Yang, 2022). Teknologi informasi telah menjadi fondasi yang menopang kehidupan individu, bisnis, dan bahkan keamanan nasional, sehingga ancaman serangan siber menjadi perhatian yang sangat serius (Zulkifli, Ismail, Mat Surin, & Okfalisa, 2024). Kejahatan di dunia maya telah meningkat secara signifikan dibandingkan tahun-tahun sebelumnya, dan kesadaran keamanan siber harus menjadi prioritas utama. Berbagai bentuk kejahatan siber seperti *phishing*, penipuan daring *(scam)*, dan peretasan *(hacking)* telah menyebabkan pelanggaran privasi dan sabotase perangkat keras(Alrobaian, Alshahrani, & Almaleh, 2023).

Dalam konteks keamanan siber, faktor manusia secara konsisten diidentifikasi sebagai mata rantai terlemah *(the weakest link)* (Alrobaian et al., 2023; Kont, 2024). Mayoritas serangan siber yang tercatat dapat ditelusuri kembali ke

JURNAL HASIL PENGABDIAN MASYARAKAT (JURIBMAS)
https://ejurnal.lkpkaryaprima.id/index.php/juribmas
e-ISSN: 2961-7286 | p-ISSN: 2962-3677
Volume 4 No 3 Maret 2026 | Hal : 692-698
DOI: https://doi.org/10.62712/juribmas.v4i3.929

kesalahan manusia *(human error*. Meskipun bersifat *intangible* dan bergantung pada pengetahuan serta lingkungan, peningkatan kesadaran keamanan siber pengguna terbukti menjadi salah satu pendekatan perlindungan yang paling efektif (Khader, Karam, & Fares, 2021).

Kalangan pelajar, khususnya siswa Sekolah Menengah Pertama (SMP), merupakan kelompok yang sangat rentan terhadap ancaman siber. Sebagai generasi yang tumbuh bersama teknologi digital, mereka aktif menggunakan internet dan media sosial, namun seringkali belum memiliki pemahaman yang memadai tentang risiko keamanan siber. Aksesibilitas dan arus informasi telah meningkat secara cepat dan efektif. Namun, peningkatan ini juga memunculkan risiko-risiko elektronik baru. Siswa atau peserta didik seringkali melanggar kebijakan keamanan siber karena kurangnya kesadaran mereka tentang lingkungan keamanan siber dan konsekuensi dari kejahatan siber (Alrobaian et al., 2023).

Berdasarkan observasi awal dan diskusi dengan pihak sekolah mitra, yaitu SMP Islam Plus At-Tholibin, Lampung Tengah, teridentifikasi beberapa permasalahan utama terkait keamanan siber di kalangan siswa, antara lain: (1) rendahnya pemahaman siswa tentang berbagai jenis ancaman siber; (2) kurangnya pengetahuan tentang praktik keamanan digital yang baik, seperti manajemen kata sandi, penggunaan *Wi-Fi* publik yang aman, dan identifikasi situs web palsu; (3) belum adanya program edukasi keamanan siber yang terstruktur di sekolah; dan (4) tingginya intensitas penggunaan internet dan media sosial tanpa diimbangi literasi keamanan digital yang memadai.

Permasalahan ini sejalan dengan temuan penelitian sebelumnya yang menunjukkan bahwa beberapa aspek perilaku dalam keamanan siber memerlukan perhatian lebih, seperti penggunaan USB dan media eksternal lainnya, membuka tautan dalam email secara sembarangan, memantau keaslian situs web yang dikunjungi, dan menghapus riwayat penjelajahan sebelum keluar broswer (Kont, 2024). Selain itu, banyak pengguna internet yang tidak memiliki keterampilan teknis yang memadai (Reppoh & da Veiga, 2022), sehingga mereka menjadi sasaran utama bagi pelaku kejahatan siber.

Atas dasar tersebut, kegiatan pengabdian masyarakat ini bertujuan untuk: (1) meningkatkan pengetahuan dan pemahaman siswa SMP tentang konsep dasar keamanan siber; (2) meningkatkan kesadaran siswa terhadap berbagai jenis ancaman siber yang relevan dengan kehidupan sehari-hari mereka; dan (3) mendorong terbentuknya budaya keamanan siber di lingkungan sekolah.

2. METODE PELAKSANAAN

Kegiatan pengabdian masyarakat ini dilaksanakan di SMP Islam Plus At-Tholibin yang berlokasi di Kabupaten Lampung Tengah. Sasaran kegiatan ini adalah siswa sekolah menengah pertama dengan jumlah peserta sebanyak 40 siswa. Pemilihan sampel dilakukan dengan teknik *purposive sampling* untuk memastikan keterwakilan tingkat kelas dan intensitas penggunaan perangkat digital. Kegiatan ini bertujuan untuk meningkatkan sudut pandang dan niat perilaku siswa terhadap keamanan siber melalui pendekatan yang interaktif.

Pelaksanaan kegiatan pengabdian ini dilakukan melalui tiga tahapan utama sebagaimana dapat dilihat pada Gambar 1.

Gambar 1. Diagram alur pengabdian kepada masyarakat

JURNAL HASIL PENGABDIAN MASYARAKAT (JURIBMAS)
https://ejurnal.lkpkaryaprima.id/index.php/juribmas
e-ISSN: 2961-7286 | p-ISSN: 2962-3677
Volume 4 No 3 Maret 2026 | Hal : 692-698
DOI: https://doi.org/10.62712/juribmas.v4i3.929

1. Tahap Persiapan

   Meliputi koordinasi dengan pihak sekolah mitra, penyusunan materi penyuluhan yang relevan dengan usia remaja, serta pengembangan instrumen evaluasi berupa kuesioner dengan skala Likert.

2. Tahap Pelaksanaan

   Terdiri dari rangkaian aktivitas berikut:

   - Pretest: Pengisian kuesioner awal untuk memotret kondisi persepsi risiko keamanan siber siswa sebelum intervensi.
   - Penyampaian Materi: Pemaparan materi menggunakan media multimedia dan video edukatif mengenai konsep dasar keamanan siber dan jenis ancaman siber *(phishing, malware, social engineering, cyberbullying,* dan *malware)*
   - Simulasi: Siswa dilatih mengidentifikasi ancaman siber melalui simulasi interaktif untuk memberikan pengalaman praktis dalam mengenali risiko digital.
   - Diskusi dan Tanya Jawab: Sesi pendalaman untuk membahas pengalaman pribadi siswa terkait keamanan di dunia maya.
   - Posttest: Pengisian kuesioner akhir untuk mengukur pergeseran sudut pandang dan niat perilaku siswa segera setelah penyuluhan.

3. Tahap Evaluasi

   Melakukan analisis data perbandingan antara hasil pretest dan posttest untuk melihat efektivitas kegiatan. Evaluasi dalam kegiatan ini menggunakan instrumen kuesioner yang dirancang berdasarkan empat skala perilaku keamanan siber menurut (Kont, 2024), yaitu: perilaku berisiko (*risky behaviour*), perilaku konservatif (*conservative behaviour*), paparan terhadap pelanggaran (*exposure to offense*), dan persepsi risiko (*risk perception*). Skor yang diperoleh kemudian dianalisis menggunakan teknik N-Gain untuk mengetahui tingkat peningkatan kesadaran siswa secara signifikan. Rumus perhitungan N-Gain yang digunakan adalah sebagai berikut:

$$\text{N-Gain} = \frac{S_{posttest} - S_{pretest}}{S_{maks} - S_{pretest}} \quad (1)$$

Tabel 1. Interpretasi N-Gain

Skor N-Gain	Interpretasi
$g > 0.7$	Tinggi
$0.3 < g \leq 0,.7$	Sedang
$g \leq 0.3$	Rendah

Sumber: (Hake, 1998)

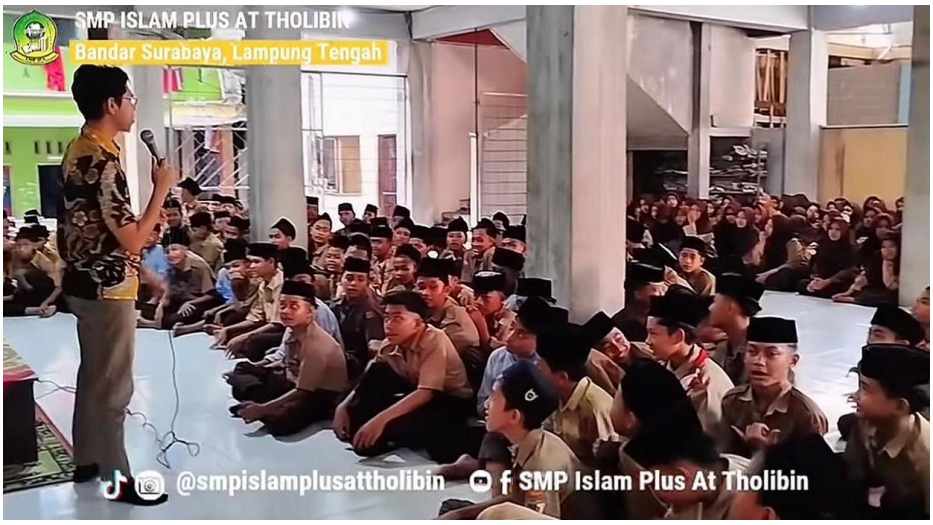
3. HASIL PEMBAHASAN

Pelaksanaan Penyuluhan

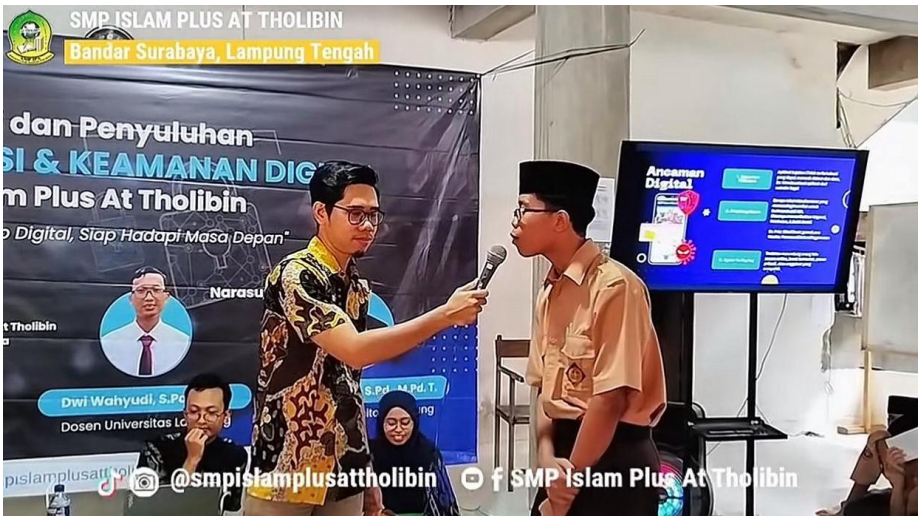
Penyuluhan dilaksanakan dengan pendekatan interaktif yang menggabungkan berbagai metode penyampaian. Materi disajikan secara bertahap, dimulai dari konsep dasar hingga praktik keamanan siber yang lebih spesifik. Sesi pertama memperkenalkan konsep dasar keamanan siber, termasuk definisi, pentingnya keamanan siber dalam kehidupan sehari-hari, dan dampak serangan siber. Siswa diberikan pemahaman bahwa keamanan siber merupakan fenomena global yang mempengaruhi berbagai aspek kehidupan. Sesi kedua membahas berbagai jenis ancaman siber yang relevan dengan kehidupan siswa SMP, meliputi *phishing, social engineering, cyberbullying*, serta *malware* dan virus. Sesi ketiga membekali siswa dengan keterampilan praktis, termasuk manajemen kata sandi, keamanan media sosial, identifikasi situs web palsu, penggunaan *Wi-Fi* publik yang aman. Selanjutnya, sesi keempat melibatkan simulasi interaktif dimana siswa diminta untuk mengidentifikasi ancaman siber dalam skenario yang disimulasikan.

JURNAL HASIL PENGABDIAN MASYARAKAT (JURIBMAS)
https://ejurnal.lkpkaryaprima.id/index.php/juribmas
e-ISSN: 2961-7286 | p-ISSN: 2962-3677
Volume 4 No 3 Maret 2026 | Hal : 692-698
DOI: https://doi.org/10.62712/juribmas.v4i3.929

Pendekatan gamifikasi diterapkan untuk meningkatkan keterlibatan siswa. Simulasi ini mencakup identifikasi email *phishing*, pengenalan situs web palsu, dan latihan pembuatan kata sandi yang kuat.



Gambar 2. Penyampaian materi



Gambar 3. Diskusi dan simulasi

Evaluasi

Hasil pretest menunjukkan bahwa kesadaran awal siswa terhadap kemanan siber berada pada kategori rendah dengan rata-rata skor total 2.15 (skala 1-4) sebagaimana dapat dilihat pada Tabel 2.

Tabel 2. Hasil pretest

Skala Perilaku Keamanan Siber	Skor Pretest	Interpretasi
Perilaku Berisiko (*Risky Behaviour*)	1.82	Rendah
Perilaku Konservatif (*Conservative Behaviour*)	2.10	Cukup
Paparan terhadap Pelanggaran (*Exposure to Offense*)	1.95	Rendah

JURNAL HASIL PENGABDIAN MASYARAKAT (JURIBMAS)
https://ejurnal.lkpkaryaprima.id/index.php/juribmas
e-ISSN: 2961-7286 | p-ISSN: 2962-3677
Volume 4 No 3 Maret 2026 | Hal : 692-698
DOI: https://doi.org/10.62712/juribmas.v4i3.929

Persepsi Risiko (*Risk Perception*)	2.75	Sedang
Rata-rata	**1.15**	**Rendah**

Berdasarkan Tabel 2, skor terendah terdapat pada skala Perilaku Berisiko (1.82). Hal ini menunjukkan bahwa sebelum penyuluhan, siswa memiliki kecenderungan tinggi untuk melakukan tindakan berbahaya secara digital.

Setelah intervensi berupa penyuluhan dan simulasi, dilakukan pengambilan data posttest dan penghitungan N-Gain untuk mengukur pergeseran sudut pandang dan niat perilaku siswa. Data menunjukkan adanya perubahan sudut pandang yang signifikan ke arah yang lebih waspada sebagaimana terlihat pada Tabel 3 dan 4.

Tabel 3. Hasil postest

Skala Perilaku Keamanan Siber	Skor Posttest	Interpretasi
Perilaku Berisiko (*Risky Behaviour*)	3.75	Tinggi
Perilaku Konservatif (*Conservative Behaviour*)	3.60	Tinggi
Paparan terhadap Pelanggaran (*Exposure to Offense*)	3.68	Tinggi
Persepsi Risiko (*Risk Perception*)	3.85	Tinggi
Rata-rata	3.72	Rendah

Tabel 4. Hasil N-Gain

Skala Perilaku Keamanan Siber	Skor N-Gain	Interpretasi
Perilaku Berisiko (*Risky Behaviour*)	0.88	Tinggi
Perilaku Konservatif (*Conservative Behaviour*)	0.79	Tinggi
Paparan terhadap Pelanggaran (*Exposure to Offense*)	0.84	Tinggi
Persepsi Risiko (*Risk Perception*)	0.85	Tinggi
Rata-rata	**0.84**	**Tinggi**

Berdasarkan hasil penghitungan pada Tabel 3 dan 4, Perilaku Berisiko (*Risky Behaviour*) mencatatkan peningkatan tertinggi dengan N-Gain sebesar 0.88. Sebelum penyuluhan, siswa cenderung mengabaikan risiko tindakan seperti mengklik tautan asing atau membagikan kata sandi. Skor posttest yang tinggi menunjukkan bahwa penyuluhan ini berhasil mengubah sudut pandang siswa menjadi lebih waspada. Sementara itu, skala Perilaku Konservatif (*Conservative Behaviour*) mencapai N-Gain 0.79. Peningkatan ini menunjukkan adanya niat yang kuat dari siswa untuk menerapkan langkah proteksi dasar, seperti melakukan *logout* di perangkat umum dan mengelola kata sandi dengan lebih baik. Selanjutnya, skala Paparan terhadap Pelanggaran (*Exposure to Offense*) menghasilkan N-Gain sebesar 0.84, yang mana terlihat adanya pergeseran pandangan siswa mengenai bahaya penggunaan *Wi-Fi* publik dan pembagian informasi pribadi secara berlebihan di media sosial. Kemudian, skala Persepsi Risiko (*Risk Perception*) mencapai skor N-Gain 0.85. Hal ini menandakan bahwa tujuan utama penyuluhan telah tercapai, dimana siswa kini memiliki kesadaran kritis dalam menilai potensi ancaman siber sebelum melakukan tindakan digital. Hasil perhitungan menunjukkan nilai rata-rata N-Gain sebesar 0.84, yang menandakan bahwa kegiatan penyuluhan memiliki tingkat efektivitas pada kategori Tinggi (N-Gain > 0.7) dalam mengubah pola pikir siswa terhadap risiko keamanan siber.

Hasil kegiatan pengabdian masyarakat ini menunjukkan bahwa penyuluhan keamanan siber yang dirancang secara interaktif dan disesuaikan dengan tingkat pemahaman siswa SMP dapat secara efektif meningkatkan kesadaran keamanan siber mereka. Temuan ini konsisten dengan berbagai penelitian sebelumnya yang menunjukkan bahwa peningkatan kesadaran keamanan siber merupakan salah satu pendekatan perlindungan yang paling efektif (Khader et al., 2021) dan bahwa pelatihan keamanan siber memiliki efek nyata terhadap perilaku (Kont, 2024).

JURNAL HASIL PENGABDIAN MASYARAKAT (JURIBMAS)
https://ejurnal.lkpkaryaprima.id/index.php/juribmas
e-ISSN: 2961-7286 | p-ISSN: 2962-3677
Volume 4 No 3 Maret 2026 | Hal : 692-698
DOI: https://doi.org/10.62712/juribmas.v4i3.929

Keberhasilan kegiatan ini dapat dikaitkan dengan beberapa faktor. Pertama, penggunaan pendekatan interaktif dan gamifikasi dalam penyampaian materi terbukti efektif dalam meningkatkan keterlibatan dan motivasi siswa (Chrisdiouf, Linawati, & Loisoklay, 2024; Tchakounté, Wabo, & Atemkeng, 2020). Kedua, materi yang disesuaikan dengan konteks dan pengalaman sehari-hari siswa SMP membuat pembelajaran lebih relevan dan bermakna. Ketiga, kombinasi antara penyampaian teori dan praktik simulasi memberikan pengalaman belajar yang komprehensif (Ariffin et al., 2022).

Namun, perlu dicatat bahwa kegiatan penyuluhan satu kali saja mungkin tidak cukup untuk membentuk perubahan perilaku yang berkelanjutan. Oleh karena itu, diperlukan program edukasi keamanan siber yang berkelanjutan dan terintegrasi dalam kurikulum sekolah (Khader et al., 2021; Zulkifli et al., 2024).

4. KESIMPULAN

Kegiatan pengabdian masyarakat berupa penyuluhan keamanan siber bagi siswa SMP Islam Plus At-Tholibin telah berhasil dilaksanakan dan menunjukkan hasil yang sangat positif. Berdasarkan hasil evaluasi, terdapat pergeseran pandangan dan niat perilaku yang signifikan dalam seluruh dimensi kesadaran keamanan siber siswa. Hal ini dibuktikan dengan peningkatan skor rata-rata dari 2.15 pada tahap pretest menjadi 3.72 pada tahap posttest. Analisis efektivitas menggunakan skor N-Gain menghasilkan nilai sebesar 0.84, yang menempatkan program penyuluhan ini pada kategori Tinggi. Keberhasilan ini mengonfirmasi bahwa pendekatan interaktif yang menggabungkan materi multimedia dengan simulasi ancaman dan gamifikasi sangat efektif dalam mengubah pola pikir siswa sekolah menengah terhadap risiko digital. Namun demikian, perlu disadari bahwa penyuluhan satu kali belum cukup untuk membentuk perubahan perilaku yang bersifat permanen dan berkelanjutan. Oleh karena itu, diperlukan program edukasi keamanan siber yang terintegrasi secara rutin dalam kurikulum sekolah untuk memastikan kewaspadaan digital siswa tetap terjaga. Kolaborasi berkelanjutan antara institusi pendidikan dan akademisi sangat diharapkan agar generasi muda dapat bertransformasi menjadi pengguna teknologi digital yang cerdas, aman, dan bertanggung jawab di masa depan.

5. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada pihak sekolah mitra, SMP Islam Plus At-Tholibin, Lampung Tengah, yang telah memberikan izin, kesempatan, serta dukungan penuh dalam pelaksanaan kegiatan pengabdian masyarakat ini. Apresiasi dan terima kasih juga disampaikan kepada seluruh siswa yang telah berpartisipasi secara aktif, antusias, dan kooperatif selama rangkaian kegiatan penyuluhan berlangsung. Dukungan dari berbagai pihak tersebut telah memungkinkan tercapainya tujuan kegiatan dalam meningkatkan kesadaran keamanan siber di lingkungan sekolah mitra.

6. REFERENSI

Alrobaian, S., Alshahrani, S., & Almaleh, A. (2023). Cybersecurity Awareness Assessment among Trainees of the Technical and Vocational Training Corporation. *Big Data and Cognitive Computing*, *7*(2), 73. https://doi.org/10.3390/bdcc7020073

Ariffin, M. A. M., Darus, M. Y., Haron, H., Kurniawan, A., Muliono, Y., & Pardomuan, C. R. (2022). Deployment of Honeypot and SIEM Tools for Cyber Security Education Model in UITM. *International Journal of Emerging Technologies in Learning*, *17*(20), 149–172. https://doi.org/10.3991/ijet.v17i20.32901

Chrisdiouf, J., Linawati, N., & Loisoklay, W. (2024). Membangun Kebiasaan Keuangan Sehat Sejak Remaja. *Eastasouth Journal of Effective Community Services*, *2*(03), 150–157. https://doi.org/10.58812/ejecs.v2i03.231

Hake, R. R. (1998). Interactive-engagement versus traditional methods: A six-thousand-student survey of mechanics test data for introductory physics courses. *American Journal of Physics*, *66*(1), 64–74.

e-ISSN: 2961-7286 | p-ISSN: 2962-3677
Volume 4 No 3 Maret 2026 | Hal : 692-698
DOI: https://doi.org/10.62712/juribmas.v4i3.929

https://doi.org/10.1119/1.18809

Hoppe, F., Gatzert, N., & Gruner, P. (2021). Cyber risk management in SMEs: insights from industry surveys. *Journal of Risk Finance*, *22*(3–4), 240–260. https://doi.org/10.1108/JRF-02-2020-0024

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information (Switzerland)*, *12*(10), 417. https://doi.org/10.3390/info12100417

Kont, K.-R. (2024). Cybersecurity behaviours of the employees and students at the Estonian Academy of Security Sciences. *Organizational Cybersecurity Journal: Practice, Process and People*, *4*(2), 85–104. https://doi.org/10.1108/ocj-02-2024-0001

Reppoh, V., & da Veiga, A. (2022). Cyber4Dev Security Culture Model for African Countries. *IFIP Advances in Information and Communication Technology*, *658 IFIP*, 173–185. https://doi.org/10.1007/978-3-031-12172-2_13

Tchakounté, F., Wabo, L. K., & Atemkeng, M. (2020). *A Review of Gamification Applied to Phishing*. (March), 1–26. https://doi.org/10.20944/preprints202003.0139.v1

Wang, K., Guo, X., & Yang, D. (2022). Research on the Effectiveness of Cyber Security Awareness in ICS Risk Assessment Frameworks. *Electronics (Switzerland)*, *11*(10), 1659. https://doi.org/10.3390/ELECTRONICS11101659

Zulkifli, Z., Ismail, A., Mat Surin, E. S., & Okfalisa, O. (2024). Cyber Security Awareness Model Based on NIST (National Institute of Standards and Technology) for Secondary School Students in Malaysia. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, 58–68. https://doi.org/10.37934/araset.61.2.5868