

EFEKTIVITAS PROGRAM EDUKASI KEAMANAN SIBER TERHADAP PENINGKATAN KESADARAN MALWARE PADA MAHASISWA PROGRAM STUDI SISTEM INFORMASI

Nur Riska Zulvi Oktaviani¹, Chairunissa Azahro², Zola Bazani³

Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri
Sulthan Thaha Saifuddin Jambi

Email : nurrriska2003@gmail.com, nisaazahro736@gmail.com, zolabazani9@gmail.com

ABSTRAK

Penelitian ini bertujuan menganalisis efektivitas program edukasi keamanan siber terhadap peningkatan kesadaran malware pada mahasiswa Program Studi Sistem Informasi. Penelitian menggunakan pendekatan kuantitatif dengan desain quasi-eksperimental model one-group pretest-posttest. Program edukasi disampaikan secara terstruktur dan aplikatif melalui pemaparan materi, diskusi interaktif, studi kasus, simulasi, serta praktik keamanan digital dasar. Data dikumpulkan menggunakan kuesioner skala Likert yang mengukur aspek pengetahuan, sikap terhadap risiko keamanan siber, dan pemahaman tindakan pencegahan malware, kemudian dianalisis menggunakan uji paired sample t-test. Hasil penelitian menunjukkan peningkatan signifikan pada seluruh aspek kesadaran malware setelah intervensi edukasi. Temuan ini menegaskan bahwa edukasi keamanan siber yang terstruktur dan berbasis pengalaman efektif dalam meningkatkan kesadaran keamanan digital mahasiswa.

Kata Kunci : Keamanan Siber, Kesadaran Malware, Edukasi Keamanan Siber, Mahasiswa Sistem Informasi, Literasi Digital.

ABSTRACT

This study aims to examine the effectiveness of a cybersecurity education program in improving malware awareness among Information Systems students. A quantitative approach with a quasi-experimental one-group pretest-posttest design was employed. The program was delivered in a structured and practice-oriented manner through lectures, interactive discussions, case studies, simulations, and hands-on digital security practices. Data were collected using Likert-scale questionnaires measuring knowledge, attitudes toward cybersecurity risks, and understanding of malware prevention actions, and were analyzed using paired sample t-tests. The results indicate a statistically significant improvement across all dimensions of malware awareness following the educational intervention. These findings demonstrate that structured and experiential cybersecurity education is effective in strengthening students' digital security awareness and supports the integration of cybersecurity education within higher education curricula.

Keywords: cybersecurity, malware awareness, cybersecurity education, Information Systems students, digital literacy.

Article History

Received: Desember 2025

Reviewed: Desember 2025

Published: Desember 2025

Plagiarism Checker No
234.KK.443

Prefix DOI :

10.9765/Krepa.V218.3784

Plagiarism Checker No 234

Prefix DOI : Prefix DOI :

10.8734/Krepa.v1i2.365

Copyright : Author

Publish by : Krepa



This work is licensed under
a [Creative Commons
Attribution-NonCommercial
4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/)

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi digital yang masif dalam berbagai aspek kehidupan, termasuk pendidikan tinggi. Internet, perangkat mobile, dan aplikasi digital kini menjadi bagian integral dari aktivitas akademik mahasiswa, mulai dari pembelajaran daring, pengelolaan data akademik, hingga interaksi sosial berbasis platform digital. Kondisi ini menjadikan mahasiswa sebagai pengguna aktif ekosistem digital yang secara intensif memproduksi, mengelola, dan menyimpan data pribadi serta data akademik dalam jumlah besar. Di sisi lain, peningkatan ketergantungan terhadap teknologi digital juga berbanding lurus dengan meningkatnya risiko keamanan siber yang mengancam pengguna. (Qolbi & Kabetta, 2024)

Ancaman keamanan siber di Indonesia menunjukkan tren yang semakin mengkhawatirkan, khususnya dalam bentuk malware, phishing, kebocoran data, dan serangan ransomware. Laporan berbagai lembaga keamanan siber nasional menunjukkan bahwa insiden serangan siber terus mengalami peningkatan seiring dengan tingginya aktivitas digital masyarakat. Malware, sebagai salah satu bentuk ancaman utama, sering disebarkan melalui aplikasi tidak resmi, tautan berbahaya, lampiran email, maupun perangkat lunak hasil modifikasi. Serangan ini tidak hanya berpotensi merusak sistem perangkat, tetapi juga membuka akses ilegal terhadap data pribadi dan informasi sensitif pengguna (Zifa Nafilah et al., 2024).

Di tengah tingginya intensitas ancaman tersebut, tingkat literasi dan kesadaran keamanan siber di kalangan pengguna internet, termasuk mahasiswa, masih tergolong rendah. Berbagai survei nasional menunjukkan bahwa pilar keamanan digital secara konsisten menjadi aspek terlemah dalam indeks literasi digital dibandingkan dengan pilar lainnya. Kondisi ini mencerminkan adanya kesenjangan antara tingginya penggunaan teknologi digital dengan pemahaman praktis mengenai risiko keamanan siber, khususnya terkait bahaya malware dan cara pencegahannya. Rendahnya kesadaran ini menjadikan mahasiswa kelompok yang rentan terhadap eksploitasi digital, baik secara teknis maupun sosial. (Zalmadani et al., 2025)

Mahasiswa Program Studi Sistem Informasi memiliki posisi yang unik dalam konteks keamanan siber. Di satu sisi, mereka dibekali pengetahuan teknis terkait sistem, aplikasi, dan pengelolaan data. Namun, di sisi lain, penguasaan teknis tersebut tidak selalu diikuti oleh kesadaran perilaku keamanan digital yang memadai dalam praktik sehari-hari. Interaksi intensif mahasiswa Sistem Informasi dengan perangkat lunak, sumber daya daring, dan aplikasi pihak ketiga meningkatkan potensi paparan malware apabila tidak disertai pemahaman risiko dan kebiasaan digital yang aman. Hal ini menunjukkan bahwa pengetahuan teknis semata belum cukup tanpa dukungan kesadaran keamanan siber yang kuat.

Dari perspektif kebijakan, pemerintah Indonesia telah memperkuat landasan hukum melalui Undang-Undang Perlindungan Data Pribadi serta regulasi terkait penyelenggaraan sistem elektronik. Namun, efektivitas regulasi tersebut sangat bergantung pada tingkat pemahaman dan kesadaran pengguna dalam menerapkan prinsip keamanan digital. Tanpa edukasi yang berkelanjutan dan kontekstual, regulasi berpotensi belum memberikan perlindungan optimal terhadap ancaman malware yang terus berkembang. Oleh karena itu, intervensi edukatif yang terstruktur menjadi elemen penting dalam menjembatani kesenjangan antara kebijakan, teknologi, dan perilaku pengguna. (Hafidzul Haq et al., 2025)

Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk menganalisis efektivitas program edukasi keamanan siber terhadap peningkatan kesadaran malware pada mahasiswa Sistem Informasi. Fokus penelitian diarahkan pada pengukuran perubahan pengetahuan, sikap, dan pemahaman mahasiswa setelah mengikuti program edukasi yang dirancang secara sistematis dan aplikatif. Hasil penelitian ini diharapkan dapat memberikan kontribusi ilmiah dalam pengembangan model edukasi keamanan siber di lingkungan perguruan tinggi, sekaligus

menjadi dasar rekomendasi praktis untuk meningkatkan kesadaran dan ketahanan mahasiswa terhadap ancaman malware di era digital.

METODE PENELITIAN

1. Desain dan Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan desain quasi-eksperimental, khususnya model one-group pretest-posttest design, untuk mengukur efektivitas program edukasi keamanan siber terhadap peningkatan kesadaran malware pada mahasiswa Program Studi Sistem Informasi. Pendekatan kuantitatif dipilih karena memungkinkan pengukuran perubahan tingkat kesadaran malware secara objektif melalui data numerik yang diperoleh sebelum dan sesudah intervensi edukatif.

Desain one-group pretest-posttest digunakan untuk membandingkan kondisi responden sebelum dan setelah mengikuti program edukasi keamanan siber. Perbedaan skor pretest dan posttest dipandang sebagai indikator dampak intervensi, sehingga efektivitas program dapat dianalisis secara sistematis dan terukur. Desain ini banyak digunakan dalam penelitian pendidikan dan keamanan siber untuk mengevaluasi pengaruh intervensi edukatif dalam konteks akademik yang terkontrol (Habie et al., 2024).

2. Program Edukasi Keamanan Siber

Program edukasi keamanan siber dirancang sebagai intervensi pembelajaran yang terstruktur, kontekstual, dan aplikatif, dengan fokus utama pada peningkatan kesadaran malware. Materi edukasi mencakup pengertian malware, jenis-jenis malware, mekanisme penyebaran, potensi dampak terhadap sistem dan data pribadi, serta langkah-langkah pencegahan dasar yang relevan dengan aktivitas digital mahasiswa.

Perancangan program mempertimbangkan karakteristik mahasiswa Sistem Informasi yang memiliki latar belakang teknis, namun masih memerlukan penguatan pada aspek perilaku dan kesadaran keamanan digital. Oleh karena itu, program mengintegrasikan pemahaman konseptual dengan penerapan praktis agar peserta tidak hanya memahami risiko malware secara teoretis, tetapi juga mampu menerapkan praktik keamanan siber dalam penggunaan teknologi sehari-hari (Luthfi Prasetyo et al., 2024).

3. Metode Penyampaian Edukasi

Penyampaian program edukasi dilakukan secara bertahap, dari konseptual hingga aplikatif, melalui metode berikut:

a) Pemaparan Materi dan Diskusi Interaktif (30-40 menit)

Materi disampaikan melalui presentasi terstruktur yang membahas konsep dasar malware, jenis-jenis malware, pola penyebaran, serta dampaknya terhadap perangkat dan data pribadi. Diskusi interaktif digunakan untuk mendorong partisipasi aktif mahasiswa, memberikan ruang refleksi terhadap pengalaman digital mereka, serta memperkuat pemahaman konseptual melalui tanya jawab terbuka.

b) Studi Kasus dan Simulasi Sederhana (20-30 menit)

Mahasiswa diberikan ilustrasi kasus nyata terkait serangan malware, seperti infeksi melalui aplikasi tidak resmi, tautan phishing, dan file berbahaya. Simulasi sederhana dilakukan untuk menunjukkan alur masuknya malware ke sistem serta tindakan pencegahan yang dapat dilakukan. Metode ini membantu mahasiswa mengaitkan teori dengan situasi nyata yang sering dihadapi dalam lingkungan digital.

c) Praktik Tindakan Keamanan Digital Dasar (15-20 menit)

Pada tahap ini, mahasiswa diarahkan untuk mempraktikkan langkah-langkah dasar keamanan siber, seperti pengelolaan kata sandi yang kuat, pengaturan privasi perangkat dan aplikasi, verifikasi sumber aplikasi, serta identifikasi file atau aplikasi yang

berpotensi berbahaya. Praktik langsung ini bertujuan membentuk kebiasaan digital yang lebih aman dan bertanggung jawab.

4. Subjek, Lokasi, dan Waktu Penelitian

Subjek penelitian adalah mahasiswa Program Studi Sistem Informasi pada salah satu perguruan tinggi di Indonesia, yang dipilih berdasarkan kriteria aktif menggunakan perangkat digital dan sistem informasi akademik. Pemilihan mahasiswa Sistem Informasi didasarkan pada tingginya intensitas interaksi mereka dengan teknologi digital, sehingga memiliki potensi risiko paparan malware yang lebih besar dibandingkan pengguna umum.

Penelitian dilaksanakan di Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi, yang beralamat di Jl. Jambi-Muara Bulian KM.16 Simpang Sungai Duren. Pelaksanaan kegiatan dilakukan selama 1 hari, yaitu di hari Kamis, 18 September 2025, yang meliputi pelaksanaan pretest, penyampaian program edukasi keamanan siber, serta pelaksanaan posttest.

5. Instrumen Pengumpulan Data

Pengumpulan data dilakukan menggunakan instrumen berikut:

a) Kuesioner Pretest dan Posttest

Kuesioner digunakan untuk mengukur tingkat kesadaran malware mahasiswa sebelum dan setelah mengikuti program edukasi. Instrumen disusun dalam bentuk pernyataan tertutup menggunakan skala Likert lima poin yang mencakup tiga aspek utama, yaitu pengetahuan tentang malware, sikap terhadap risiko keamanan siber, dan pemahaman tindakan pencegahan. Skor total digunakan untuk mengukur perubahan tingkat kesadaran malware secara kuantitatif.

b) Lembar Observasi Partisipasi

Observasi dilakukan selama pelaksanaan edukasi untuk menilai tingkat keterlibatan mahasiswa dalam diskusi, simulasi, dan praktik keamanan digital. Data observasi digunakan sebagai informasi pendukung untuk memperkuat interpretasi hasil kuantitatif (Habie et al., 2024).

6. Materi Pembinaan dan Penyuluhan Kegiatan

Data yang diperoleh dari kuesioner pretest dan posttest dianalisis menggunakan analisis statistik deskriptif dan inferensial. Analisis deskriptif digunakan untuk menggambarkan karakteristik responden serta rata-rata skor kesadaran malware sebelum dan sesudah intervensi edukasi. Selanjutnya, analisis inferensial dilakukan menggunakan uji beda paired sample t-test untuk mengetahui signifikansi perbedaan skor pretest dan posttest. Hasil analisis ini digunakan sebagai dasar dalam menilai efektivitas program edukasi keamanan siber terhadap peningkatan kesadaran malware pada mahasiswa Sistem Informasi (Hafidzul Haq et al., 2025).

HASIL DAN PEMBAHASAN

1. Perubahan Tingkat Kesadaran Malware Mahasiswa

Hasil analisis data menunjukkan adanya peningkatan signifikan tingkat kesadaran malware pada mahasiswa Program Studi Sistem Informasi setelah mengikuti program edukasi keamanan siber. Perbandingan skor pretest dan posttest memperlihatkan bahwa nilai rata-rata kesadaran malware pada tahap posttest lebih tinggi dibandingkan dengan pretest, yang mencerminkan adanya perubahan positif setelah intervensi edukatif diberikan.

Secara teoritis, kesadaran keamanan siber dipahami sebagai konstruk multidimensi yang mencakup pengetahuan, sikap, dan perilaku protektif pengguna terhadap risiko digital (Ribble, 2015). Dalam konteks ini, peningkatan skor posttest menunjukkan bahwa program edukasi tidak hanya meningkatkan aspek kognitif mahasiswa, tetapi juga memengaruhi dimensi afektif dan kecenderungan perilaku mereka terhadap ancaman malware. (Nofri Yudi Arifin et al., 2024)

Hasil uji beda menggunakan paired sample t-test menunjukkan bahwa perbedaan skor tersebut signifikan secara statistik. Hal ini menegaskan bahwa peningkatan kesadaran malware yang terjadi merupakan dampak langsung dari intervensi edukasi keamanan siber, bukan sekadar perubahan alami

atau faktor kebetulan. Dengan demikian, program edukasi berperan sebagai mekanisme efektif dalam menjembatani kesenjangan antara intensitas penggunaan teknologi digital dan pemahaman risiko keamanan siber di kalangan mahasiswa Sistem Informasi (Azzahra & Atqiya, 2024).

2. Program Edukasi Keamanan Siber

Hasil kuesioner menunjukkan adanya peningkatan yang jelas pada aspek pengetahuan mahasiswa terkait malware. Setelah mengikuti program edukasi, mahasiswa memiliki pemahaman yang lebih baik mengenai definisi malware, jenis-jenis malware, mekanisme penyebaran, serta potensi dampaknya terhadap sistem dan data pribadi.

Dalam kerangka teori literasi digital dan keamanan siber, pengetahuan merupakan fondasi awal pembentukan kesadaran risiko digital. Pengguna yang memahami cara kerja ancaman siber akan lebih mampu melakukan evaluasi risiko sebelum mengambil keputusan dalam aktivitas digitalnya. Oleh karena itu, peningkatan pengetahuan mahasiswa dalam penelitian ini menunjukkan bahwa program edukasi berhasil memperkuat literasi keamanan siber pada level konseptual.

Mahasiswa tidak hanya mengenali malware sebagai ancaman teknis, tetapi juga memahami jalur penyebarannya, seperti aplikasi tidak resmi, tautan phishing, dan file unduhan dari sumber yang tidak terpercaya. Temuan ini mendukung pandangan bahwa peningkatan literasi keamanan siber berperan penting dalam membentuk pengguna digital yang lebih kritis dan waspada (Adinda Nova Octavia et al., 2025).

3. Perubahan Sikap Mahasiswa terhadap Risiko Keamanan Siber

Selain peningkatan pengetahuan, penelitian ini juga menemukan adanya perubahan sikap mahasiswa terhadap risiko keamanan siber, khususnya ancaman malware. Setelah mengikuti program edukasi, mahasiswa menunjukkan sikap yang lebih berhati-hati dalam menggunakan perangkat lunak, mengunduh aplikasi, serta mengakses tautan dari sumber yang tidak jelas.

Perubahan sikap ini dapat dijelaskan melalui Protection Motivation Theory (PMT) yang menyatakan bahwa perilaku protektif individu dipengaruhi oleh persepsi ancaman (threat appraisal) dan keyakinan terhadap efektivitas tindakan pencegahan (coping appraisal) (Rogers, 1983). Program edukasi dalam penelitian ini meningkatkan persepsi mahasiswa terhadap tingkat keparahan dan kemungkinan risiko malware, sekaligus memperkuat keyakinan mereka terhadap langkah-langkah pencegahan yang dapat dilakukan.

Dengan demikian, mahasiswa tidak lagi memandang ancaman malware sebagai sesuatu yang abstrak atau jauh dari kehidupan sehari-hari, tetapi sebagai risiko nyata yang dapat berdampak langsung pada aktivitas akademik, keamanan data, dan privasi pribadi (Syaddan, 2024).

4. Peningkatan Pemahaman Tindakan Pencegahan Malware

Hasil penelitian juga menunjukkan peningkatan signifikan pada pemahaman mahasiswa terhadap tindakan pencegahan malware. Setelah mengikuti sesi praktik keamanan digital, mahasiswa lebih memahami dan mengenali langkah-langkah preventif, seperti penggunaan kata sandi yang kuat, pengaturan privasi aplikasi, verifikasi sumber perangkat lunak, serta identifikasi file atau aplikasi yang mencurigakan.

Dalam perspektif teori pembelajaran berbasis pengalaman (experiential learning), pemahaman yang diperoleh melalui praktik langsung cenderung lebih bertahan dan mudah diterapkan dalam situasi nyata dibandingkan pembelajaran teoretis semata (Kolb, 1984). Temuan ini menunjukkan bahwa integrasi praktik keamanan digital dalam program edukasi berkontribusi signifikan dalam membentuk kesiapan mahasiswa menghadapi ancaman malware secara konkret.

Hasil ini sejalan dengan penelitian sebelumnya yang menegaskan bahwa edukasi keamanan siber yang bersifat aplikatif lebih efektif dalam membentuk perilaku keamanan digital yang berkelanjutan (Alunaza, 2024).

5. Peran Metode Edukasi Interaktif dalam Meningkatkan Kesadaran Malware

Efektivitas program edukasi keamanan siber dalam penelitian ini tidak terlepas dari metode penyampaian yang interaktif dan bertahap, mulai dari pemaparan materi, diskusi, studi kasus, hingga praktik langsung. Hasil observasi menunjukkan bahwa mahasiswa terlibat aktif dan mampu mengaitkan materi dengan pengalaman digital mereka sehari-hari.

Pendekatan ini sejalan dengan teori konstruktivisme, yang menekankan bahwa pengetahuan dibangun secara aktif melalui interaksi antara pengalaman, refleksi, dan pemahaman baru. Dengan melibatkan mahasiswa secara aktif, proses pembelajaran menjadi lebih bermakna dan mendorong internalisasi konsep keamanan siber secara lebih mendalam (Adinda Nova Octavia et al., 2025).

6. Implikasi Teoretis dan Praktis

Secara teoretis, temuan penelitian ini memperkuat pandangan bahwa kesadaran keamanan siber merupakan konstruk multidimensi yang membutuhkan pendekatan edukasi holistik. Integrasi teori literasi digital, teori motivasi protektif, dan pembelajaran berbasis pengalaman terbukti relevan dalam menjelaskan perubahan kesadaran malware mahasiswa.

Secara praktis, hasil penelitian ini menunjukkan bahwa program edukasi keamanan siber yang terstruktur dan aplikatif dapat menjadi strategi efektif dalam meningkatkan ketahanan mahasiswa terhadap ancaman malware di lingkungan perguruan tinggi, khususnya pada program studi berbasis teknologi informasi (Ceng Giap et al., 2024).

7. Keterbatasan dan Arah Penelitian Selanjutnya

Meskipun menunjukkan hasil yang positif, penelitian ini memiliki keterbatasan pada desain one-group pretest-posttest yang tidak melibatkan kelompok kontrol. Selain itu, pengukuran dilakukan dalam jangka waktu yang relatif singkat, sehingga keberlanjutan perubahan kesadaran malware belum dapat dievaluasi secara longitudinal.

Penelitian selanjutnya disarankan untuk menggunakan desain eksperimental dengan kelompok kontrol serta pengukuran lanjutan (follow-up test) guna menilai stabilitas perubahan kesadaran dan perilaku keamanan siber mahasiswa dalam jangka panjang (Sindar, 2022).



KESIMPULAN

Penelitian ini menunjukkan bahwa program edukasi keamanan siber yang dirancang secara terstruktur, kontekstual, dan aplikatif terbukti efektif dalam meningkatkan kesadaran malware mahasiswa Program Studi Sistem Informasi. Peningkatan tersebut tercermin secara signifikan pada aspek pengetahuan, sikap terhadap risiko keamanan siber, serta pemahaman tindakan pencegahan malware setelah mahasiswa mengikuti rangkaian edukasi. Temuan ini menegaskan bahwa kesadaran keamanan siber tidak terbentuk secara alami melalui intensitas penggunaan teknologi semata, melainkan memerlukan intervensi edukatif yang sistematis dan berorientasi pada kebutuhan pengguna digital.

Selanjutnya, hasil penelitian memperkuat pandangan bahwa kesadaran malware merupakan konstruk multidimensi yang dipengaruhi oleh integrasi antara pemahaman

konseptual, persepsi risiko, dan pengalaman praktik keamanan digital. Pendekatan edukasi yang mengombinasikan pemaparan materi, diskusi interaktif, studi kasus, serta praktik langsung terbukti mampu mendorong perubahan dari sekadar pemahaman kognitif menuju sikap yang lebih waspada dan kesiapan bertindak secara preventif. Hal ini sejalan dengan kerangka literasi keamanan siber, Protection Motivation Theory, serta teori pembelajaran berbasis pengalaman yang menekankan pentingnya keterlibatan aktif peserta didik dalam membangun kesadaran dan perilaku keamanan digital yang berkelanjutan.

Secara praktis, temuan penelitian ini memberikan implikasi penting bagi perguruan tinggi, khususnya program studi berbasis teknologi informasi, untuk mengintegrasikan edukasi keamanan siber sebagai bagian dari pembinaan mahasiswa secara berkelanjutan. Program edukasi yang terstruktur dan aplikatif dapat menjadi strategi preventif dalam meningkatkan ketahanan mahasiswa terhadap ancaman malware di tengah meningkatnya risiko keamanan siber. Meskipun penelitian ini masih memiliki keterbatasan pada desain tanpa kelompok kontrol dan jangka waktu pengukuran yang relatif singkat, hasil yang diperoleh menunjukkan bahwa edukasi keamanan siber memiliki peran strategis dalam menjembatani kesenjangan antara kebijakan, teknologi, dan perilaku pengguna. Oleh karena itu, penelitian lanjutan dengan desain eksperimental dan pengukuran longitudinal diperlukan untuk memperkuat generalisasi temuan serta mengembangkan model edukasi keamanan siber yang lebih komprehensif.

DAFTAR PUSTAKA

- Adinda Nova Octavia, Achmad Fauzi, Gilang Aditya Kurniawan, Nazwa Febriyana Putri, Rama Dwi Alghifari, Rasim Rasim, Sumarno Manrejo, & Yusrina Mutiara Adienda. (2025). Peran Pemahaman Cyber Security Untuk Keamanan Akun Media Sosial Instagram Mahasiswa. *Orbit : Jurnal Ilmu Multidisiplin Nusantara*, 1(2), 89-99. <https://doi.org/10.63217/Orbit.V1i2.80>
- Alunaza, H. (2024). Edukasi Penggunaan Internet Dalam Diplomasi Dan Upaya Mengatasi Ancaman Keamanan Siber Bagi Mahasiswa Hubungan Internasional Universitas Tanjungpura. *Jurnal Abdi Insani*, 11(2), 1199-1206. <https://doi.org/10.29303/Abdiinsani.V11i2.1505>
- Azzahra, S., & Atqiya, A. (2024). Membangun Kesadaran Mahasiswa Dalam Menghadapi Tantangan Cyber Security Di Era Digital. In *Iuris Studia: Jurnal Kajian Hukum* (Vol. 5, Issue 3). <http://jurnal.bundamedia grup.co.id/index.php/luris>
- Ceng Giap, Y., Prawira Gunawan, M., Witopo, D. E., Kebaowolo, J. A., Salim, J. V., & Cahyadi, D. (2024). *Peningkatan Literasi Digital Melalui Edukasi Keamanan Siber Di Kalangan Siswa Sekolah Menengah*. 1(3). <https://lgakerta.com/jurnal/index.php>
- Habie, K. F., Putro, A. P., Yuliansyah, H., & Riadi, I. (2024). Peningkatan Cyber Security Awareness Melalui Pelatihan Edukatif Kepada Siswa Sekolah Menengah Kejuruan. *Mohuyula : Jurnal Pengabdian Kepada Masyarakat*, 3(2), 46. <https://doi.org/10.31314/Mohuyula.3.2.46-53.2024>
- Hafidzul Haq, S., Achmad Fauzi, Djuni Thamrin, Panji Maulana, Arafanditama Najim Hidayat, Syahid Abdullah Muslih, & Toman Andreas Fernando. (2025). Peran Manajemen Sekuriti Dalam Meningkatkan Kesadaran Keamanan Data Mahasiswa Pada Sistem Informasi Akademik Ubhara Jaya. *Orbit : Jurnal Ilmu Multidisiplin Nusantara*, 1(2), 35-50. <https://doi.org/10.63217/Orbit.V1i2.77>

- Luthfi Prasetyo, R., Nugraha Hernanjaya, A., Shofiyatun, S., Prasetyo, S., Putra, D., Sains, F., & Teknologi, D. (2024). 61 Edukasi Masyarakat Terhadap Kejahatan Dunia Digital Di Dusun Kampung Baru Rt 03 Rw 07 Pabelan, Kartasura, Sukoharjo Community Education On Cybercrime In Kampung Baru Hamlet Rt 03 Rw 07 Pabelan, Kartasura, Sukoharjo Article History. *Jurnal Pengabdian Bersama Masyarakat Indonesia*, 2(3), 61-74. <https://doi.org/10.59031/jpbmi.V2i2.480>
- Nofri Yudi Arifin, Okta Veza, Albertus Laurensius Setyabudhi, & Atman Lucky Fernandes. (2024). Sosialisasi Pentingnya Cyber Security Untuk Menjaga Keamanan Online Studi Fakultas Teknik Informatika Universitas Ibnu Sina. *Karya Nyata : Jurnal Pengabdian Kepada Masyarakat*, 1(3), 46-51. <https://doi.org/10.62951/karyanyata.V1i3.451>
- Qolbi, N., & Kabetta, H. (2024). Platform Edukasi Keamanan Siber Berbasis Web Berdasarkan Kerangka Global Literasi Digital Unesco. *Jurnal Intekna*, 24(2). <http://ejurnal.poliban.ac.id/index.php/intekna/issue/archive>
- Sindar, A. S. A. S. R. D. S. (2022). *Workshop Peran Generasi Milenial Dalam Meningkatkan Skill Bidang Keamanan Informasi Dan Jaringan*.
- Syaddan, S. (2024). Sosialisasi Keamanan Data Di Dunia Siber Untuk Meningkatkan Kewaspadaan Smk 1 Negeri Tarakan Terhadap Ancaman Cybercrime. *Archive: Jurnal Pengabdian Kepada Masyarakat*, 3(2), 289-299. <https://doi.org/10.55506/arch.V3i2.103>
- Zalmadani, H., Fakhri Rahmat Muzakki, M., Zayani, N., & Piala Sakti Pariaman, Stik. (2025). *Cyber Safety For All : Edukasi Keamanan Digital Bagi Peserta Fun Run*. 4(2). <https://doi.org/10.58266/jpmb.V4i2.811>
- Zifa Nafilah, A., Fadmayla Jasmine, N., & Ari Rahmadanti, R. (2024). *Peran Mahasiswa Dalam Meningkatkan Kesadaran Keamanan Siber Di Lingkungan Kampus* (Vol. 1, Issue 10). <https://inovanpublisher.org/fibonacci>