JURNAL KOMPREHENSIF
E ISSN: 3031-0970 | Vol. 4 No. 1 2026 | pp. 569-578
Available online at: https://ejournal.edutechjaya.com/index.php/komprehensif

Analisis Kesadaran Mahasiswa Terhadap Ancaman Keamanan Siber di Era Digital

Nur Fadilah Harahap[1], Asrul Habibi Pohan[2], Rydho Kamattuluby Matondang[3] , Ahmad Ibrahim[4]

[1,2,3,4]Universitas Labuhanbatu, Indonesia

Email: nurfadilaharahapfadila@gmail.com[1] , as7883149@gmail.com[2] , lubimtd@gmail.com[3] , ahmadnabila416@gmail.com[4]

ABSTRAK

Perkembangan teknologi digital yang semakin pesat telah meningkatkan penggunaan internet dan perangkat digital di kalangan mahasiswa. Di sisi lain, kondisi ini juga menimbulkan berbagai ancaman keamanan siber, seperti; phishing, malware, pencurian data pribadi, dan penyalahgunaan akun media sosial. Penelitian ini bertujuan untuk menganalisis tingkat kesadaran mahasiswa terhadap ancaman keamanan siber di era digital serta faktor-faktor yang memengaruhi pemahaman mereka mengenai keamanan informasi. Metode penelitian yang digunakan adalah pendekatan deskriptif kuantitatif dengan pengumpulan data melalui penyebaran kuesioner kepada mahasiswa. Hasil analisis menunjukkan bahwa sebagian besar mahasiswa telah mengenal berbagai bentuk ancaman keamanan siber, namun masih terdapat kelemahan dalam penerapan praktik keamanan digital, seperti penggunaan kata sandi yang kuat, autentikasi dua faktor, dan kewaspadaan terhadap tautan atau pesan mencurigakan. Selain itu, tingkat pengetahuan keamanan siber dipengaruhi oleh pengalaman penggunaan teknologi, akses terhadap informasi keamanan digital, dan edukasi yang diterima. Penelitian ini menyimpulkan bahwa kesadaran mahasiswa terhadap keamanan siber berada pada kategori cukup baik, tetapi masih memerlukan peningkatan melalui program edukasi, pelatihan, dan sosialisasi keamanan digital secara berkelanjutan.

Kata Kunci: Kesadaran Mahasiswa, Keamanan Siber, Ancaman Siber, Era Digital, Keamanan Informasi.

ABSTRACT

The rapid development of digital technology has significantly increased the use of the internet and digital devices among university students. However, this advancement has also led to various cybersecurity threats, such as phishing, malware attacks, personal data theft, and social media account misuse. This study aims to analyze students' awareness of cybersecurity threats in the digital era and identify the factors influencing their understanding of information security. The research employs a quantitative descriptive approach, with data collected through questionnaires distributed to university students. The findings indicate that most students are familiar with various forms of cybersecurity threats; however, weaknesses remain in the implementation of digital security practices, such as creating strong passwords, enabling two-factor authentication, and recognizing suspicious links or messages. Furthermore, the level of cybersecurity awareness is influenced by technology usage experience, access to digital security information, and educational exposure. The study concludes that students' cybersecurity awareness is generally at a moderate to good level, but further improvement is needed through continuous educational programs, training, and cybersecurity awareness campaigns. These efforts are expected to enhance students' ability to protect their data and digital activities from various cyber threats.

Keywords: *student awareness, cybersecurity, cyber threats, digital era, information security.*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan yang signifikan dalam berbagai aspek kehidupan, termasuk di bidang pendidikan. Pemanfaatan internet, komputer, dan perangkat seluler telah menjadi bagian penting dalam aktivitas akademik mahasiswa, seperti pembelajaran daring, pencarian informasi, komunikasi, serta penyimpanan dan pertukaran data. Kemajuan teknologi tersebut memberikan berbagai manfaat, namun juga meningkatkan risiko terjadinya ancaman keamanan siber yang dapat membahayakan pengguna dan data yang dimiliki (Stallings, 2018). Keamanan siber (*cybersecurity*) merupakan upaya untuk melindungi sistem informasi, jaringan komputer, perangkat digital, dan data dari berbagai ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan informasi (Whitman & Mattord, 2022). Seiring dengan meningkatnya penggunaan teknologi digital, ancaman keamanan siber juga semakin berkembang dan kompleks. Beberapa bentuk ancaman yang sering terjadi antara lain phishing, malware, ransomware, pencurian identitas, dan kebocoran data pribadi yang dapat menimbulkan kerugian bagi individu maupun organisasi (Von Solms & Van Niekerk, 2013).

Mahasiswa merupakan salah satu kelompok pengguna internet yang memiliki tingkat aktivitas digital yang tinggi. Berbagai kegiatan akademik maupun nonakademik saat ini banyak dilakukan melalui platform digital dan media sosial. Tingginya intensitas penggunaan internet tersebut menyebabkan mahasiswa menjadi kelompok yang rentan terhadap berbagai ancaman siber apabila tidak memiliki pengetahuan dan kesadaran yang memadai mengenai keamanan digital (Hadlington, 2017). Kurangnya kesadaran terhadap keamanan siber dapat menyebabkan pengguna menjadi korban penipuan online, pencurian data pribadi, maupun penyalahgunaan akun digital. Kesadaran keamanan siber (*cybersecurity awareness*) merupakan tingkat pemahaman dan kepedulian individu terhadap ancaman keamanan informasi serta kemampuan untuk menerapkan praktik keamanan yang tepat dalam penggunaan teknologi digital (Parsons et al., 2017). Individu yang memiliki tingkat kesadaran keamanan siber yang baik cenderung lebih berhati-hati dalam menjaga kerahasiaan data, menggunakan kata sandi yang kuat, mengaktifkan autentikasi dua faktor, serta mampu mengenali berbagai bentuk serangan siber yang berpotensi membahayakan keamanan informasi.

Penelitian sebelumnya menunjukkan bahwa tingkat kesadaran keamanan siber dipengaruhi oleh berbagai faktor, seperti tingkat pendidikan, pengalaman penggunaan teknologi, akses terhadap informasi keamanan digital, dan pelatihan yang pernah diikuti (Kruger & Kearney, 2006). Meskipun mahasiswa umumnya telah mengenal teknologi digital dengan baik, masih ditemukan perilaku yang berisiko terhadap keamanan informasi, seperti penggunaan kata sandi yang lemah, kurangnya perlindungan data pribadi, dan rendahnya pemanfaatan fitur keamanan tambahan pada akun digital. Berdasarkan kondisi tersebut, penelitian ini dilakukan untuk menganalisis tingkat kesadaran mahasiswa terhadap ancaman keamanan siber di era

digital. Penelitian ini diharapkan dapat memberikan gambaran mengenai tingkat pemahaman dan perilaku mahasiswa dalam menghadapi ancaman siber serta menjadi dasar bagi perguruan tinggi dalam merancang program edukasi dan literasi keamanan digital yang lebih efektif. Dengan meningkatnya kesadaran keamanan siber, mahasiswa diharapkan mampu memanfaatkan teknologi digital secara aman, bertanggung jawab, dan terhindar dari berbagai ancaman yang dapat merugikan.

METODE PENELITIAN

Penelitian ini menggunakan metode deskriptif kuantitatif untuk menganalisis tingkat kesadaran mahasiswa terhadap ancaman keamanan siber di era digital. Metode ini dipilih karena mampu memberikan gambaran secara sistematis mengenai tingkat pemahaman, pengetahuan, dan perilaku mahasiswa terkait keamanan siber berdasarkan data yang diperoleh dari responden.

Identifikasi Masalah

Berdasarkan latar belakang penelitian mengenai kesadaran mahasiswa terhadap ancaman keamanan siber di era digital, beberapa masalah yang dapat diidentifikasi adalah sebagai berikut:

1. Meningkatnya penggunaan teknologi digital oleh mahasiswa dalam kegiatan akademik maupun non-akademik yang berpotensi meningkatkan risiko terpapar ancaman keamanan siber.
2. Masih rendahnya pemahaman sebagian mahasiswa mengenai ancaman keamanan siber, seperti phishing, malware, ransomware, pencurian identitas, dan kebocoran data pribadi.
3. Kurangnya penerapan praktik keamanan digital yang baik, seperti penggunaan kata sandi yang kuat, pembaruan sistem secara berkala, dan aktivasi autentikasi dua faktor (2FA).
4. Tingginya aktivitas mahasiswa di media sosial dan platform digital, yang dapat meningkatkan risiko penyalahgunaan data pribadi dan serangan siber.
5. Kurangnya edukasi dan pelatihan keamanan siber di lingkungan perguruan tinggi, sehingga mahasiswa belum memiliki pengetahuan yang memadai untuk menghadapi berbagai ancaman digital.
6. Belum diketahui secara pasti tingkat kesadaran mahasiswa terhadap keamanan siber, sehingga diperlukan penelitian untuk mengukur dan menganalisis tingkat kesadaran tersebut.
7. Perbedaan tingkat pengetahuan dan pengalaman penggunaan teknologi di kalangan mahasiswa yang dapat memengaruhi kemampuan mereka dalam mengenali dan mengatasi ancaman keamanan siber.

Identifikasi masalah tersebut menjadi dasar dalam melakukan penelitian untuk mengetahui tingkat kesadaran mahasiswa terhadap ancaman keamanan siber serta merumuskan rekomendasi yang dapat meningkatkan keamanan digital di lingkungan perguruan tinggi.

Studi Literatur

Keamanan siber (*cybersecurity*) merupakan upaya melindungi sistem, jaringan, dan data dari berbagai ancaman digital seperti phishing, malware, ransomware, dan pencurian data. Seiring meningkatnya penggunaan internet dan teknologi digital, ancaman siber juga semakin berkembang dan dapat menimbulkan kerugian bagi pengguna.

Mahasiswa merupakan salah satu kelompok yang aktif menggunakan teknologi digital untuk kegiatan akademik dan komunikasi. Tingginya intensitas penggunaan internet membuat mahasiswa rentan terhadap berbagai ancaman keamanan siber. Oleh karena itu, diperlukan kesadaran keamanan siber yang baik agar mahasiswa mampu melindungi data pribadi dan akun digital mereka.

Kesadaran keamanan siber adalah tingkat pemahaman dan perilaku seseorang dalam mengenali serta mencegah ancaman siber. Tingkat kesadaran ini dipengaruhi oleh pengetahuan, pengalaman penggunaan teknologi, akses informasi, dan edukasi mengenai keamanan digital. Dengan meningkatnya kesadaran keamanan siber, mahasiswa diharapkan dapat menggunakan teknologi secara lebih aman dan bertanggung jawab.

Pengumpulan Data

Pengumpulan data dalam penelitian ini dilakukan menggunakan kuesioner (angket) yang disebarkan kepada mahasiswa melalui Google Form. Kuesioner berisi beberapa pertanyaan mengenai pengetahuan, pemahaman, dan perilaku mahasiswa terhadap ancaman keamanan siber di era digital.

Data yang dikumpulkan meliputi:

- Pengetahuan tentang keamanan siber.
- Pemahaman terhadap ancaman siber seperti phishing dan malware.
- Kebiasaan penggunaan kata sandi yang aman.
- Penggunaan autentikasi dua faktor (2FA).
- Kesadaran dalam menjaga privasi dan data pribadi.

Jawaban responden diukur menggunakan skala Likert 1–5, mulai dari *Sangat Tidak Setuju* hingga *Sangat Setuju*. Data yang diperoleh kemudian diolah dan dianalisis untuk.

Lokasi dan Pengumpulan Data

Penelitian dilakukan di lingkungan UNIVERSITAS LABUHANBATU dengan responden mahasiswa aktif yang menggunakan internet dan perangkat digital dalam kegiatan sehari-hari. Pengumpulan data dilaksanakan pada periode penelitian yang telah ditentukan melalui penyebaran kuesioner secara daring.

Populasi dan Sampel

Populasi dalam penelitian ini adalah seluruh mahasiswa yang aktif menggunakan teknologi digital untuk kegiatan akademik maupun nonakademik. Sampel penelitian dipilih menggunakan teknik purposive sampling, yaitu pemilihan responden berdasarkan kriteria tertentu, seperti:

- Mahasiswa aktif.
- Menggunakan internet setiap hari.
- Memiliki akun media sosial atau platform digital lainnya.
- Bersedia mengisi kuesioner penelitian.

Normalisasi Data

Pengumpulan data dilakukan menggunakan kuesioner (angket) yang disebarkan secara online melalui Google Form. Kuesioner berisi pernyataan yang berkaitan dengan:

1. Pengetahuan tentang keamanan siber.
2. Pemahaman terhadap ancaman siber.
3. Penggunaan kata sandi yang aman.
4. Kesadaran menjaga data pribadi.
5. Penggunaan autentikasi dua faktor (2FA).
6. Kemampuan mengenali phishing dan malware.

Instrumen penelitian menggunakan Skala Likert dengan rentang nilai sebagai berikut:

Skor	Keterangan
5	Sangat Setuju
4	Setuju
3	Netral
2	Tidak Setuju
1	Sangat Tidak Setuju

Intrument Penelitian

Instrumen yang digunakan dalam penelitian ini adalah kuesioner yang disusun berdasarkan indikator kesadaran keamanan siber. Berikut contoh indikator yang digunakan:

No	Indikator
1	Mengetahui berbagai jenis ancaman keamanan siber
2	Memahami risiko penggunaan internet
3	Menggunakan kata sandi yang kuat
4	Menjaga kerahasiaan data pribadi
5	Mengaktifkan autentikasi dua faktor (2FA)

No	Indikator
6	Mampu mengenali email atau tautan phishing
7	Memperbarui aplikasi dan sistem secara berkala

Teknik Analisis Data

Data yang telah terkumpul dianalisis menggunakan analisis statistik deskriptif. Langkah-langkah analisis data meliputi:

1. Mengumpulkan data dari seluruh responden.
2. Mengelompokkan jawaban berdasarkan indikator penelitian.
3. Menghitung skor total dan rata-rata (mean).
4. Menghitung persentase tingkat kesadaran mahasiswa.
5. Menginterpretasikan hasil berdasarkan kategori yang telah ditentukan.

Kategori tingkat kesadaran mahasiswa ditentukan sebagai berikut:

Persentase (%)	Kategori
81–100	Sangat Tinggi
61–80	Tinggi
41–60	Sedang
21–40	Rendah
0–20	Sangat Rendah

Alur Penelitian

Tahapan penelitian yang dilakukan meliputi:

1. Identifikasi masalah mengenai keamanan siber pada mahasiswa.
2. Studi literatur terkait keamanan siber dan kesadaran pengguna.
3. Penyusunan instrumen penelitian.
4. Penyebaran kuesioner kepada responden.
5. Pengumpulan data penelitian.
6. Pengolahan dan analisis data.
7. Penyusunan hasil penelitian.
8. Penarikan kesimpulan dan pemberian rekomendasi.

Dengan metode penelitian ini, diharapkan dapat diperoleh gambaran yang jelas mengenai tingkat kesadaran mahasiswa terhadap ancaman keamanan siber di era digital serta faktor-faktor yang memengaruhinya.

Hasil dan Pembahasan

Hasil Penelitian

Penelitian ini bertujuan untuk menganalisis tingkat kesadaran mahasiswa terhadap ancaman keamanan siber di era digital. Data penelitian diperoleh melalui penyebaran kuesioner kepada mahasiswa yang aktif menggunakan internet dan perangkat digital dalam kegiatan akademik maupun nonakademik. Kuesioner terdiri dari beberapa indikator yang mengukur pengetahuan, pemahaman, dan perilaku mahasiswa terkait keamanan siber.

Berdasarkan hasil pengolahan data, diperoleh rata-rata tingkat kesadaran mahasiswa terhadap ancaman keamanan siber sebesar 76%, yang termasuk dalam kategori tinggi. Hasil ini menunjukkan bahwa sebagian besar mahasiswa telah memahami pentingnya keamanan siber dan memiliki kesadaran yang cukup baik dalam melindungi data serta akun digital yang dimiliki.

Tabel 1. Hasil Tingkat Kesadaran Mahasiswa terhadap Keamanan Siber

No	Indikator	Persentase (%)	Kategori
1	Pengetahuan tentang ancaman siber	82	Sangat Tinggi
2	Pemahaman risiko penggunaan internet	79	Tinggi
3	Penggunaan kata sandi yang aman	76	Tinggi
4	Perlindungan data pribadi	81	Sangat Tinggi
5	Penggunaan autentikasi dua faktor (2FA)	68	Tinggi
6	Kemampuan mengenali phishing	74	Tinggi
7	Pembaruan sistem dan aplikasi	72	Tinggi
Rata-rata	**Kesadaran Keamanan Siber**	**76**	**Tinggi**

Berdasarkan tabel di atas, indikator dengan nilai tertinggi adalah pengetahuan tentang ancaman siber (82%), sedangkan indikator dengan nilai terendah adalah penggunaan autentikasi dua faktor (68%).

Pembahasan

Berdasarkan hasil penelitian, tingkat kesadaran mahasiswa terhadap ancaman keamanan siber di era digital berada pada kategori tinggi dengan rata-rata persentase sebesar 76%. Hasil ini menunjukkan bahwa sebagian besar mahasiswa telah memiliki

pengetahuan dan pemahaman yang cukup baik mengenai keamanan siber serta pentingnya melindungi data dan akun digital dari berbagai ancaman yang ada di internet. Tingginya tingkat kesadaran mahasiswa dapat dipengaruhi oleh semakin luasnya penggunaan teknologi digital dalam kehidupan sehari-hari. Mahasiswa saat ini tidak hanya menggunakan internet untuk mencari informasi dan berkomunikasi, tetapi juga untuk kegiatan akademik seperti pembelajaran daring, pengumpulan tugas, dan akses berbagai layanan pendidikan. Intensitas penggunaan teknologi yang tinggi membuat mahasiswa lebih sering terpapar informasi mengenai keamanan siber dan berbagai bentuk ancaman digital.

Hasil penelitian menunjukkan bahwa indikator pengetahuan tentang ancaman siber memperoleh nilai tertinggi. Hal ini mengindikasikan bahwa sebagian besar mahasiswa telah mengenal berbagai jenis ancaman siber seperti phishing, malware, ransomware, pencurian identitas, dan kebocoran data. Pengetahuan tersebut menjadi dasar yang penting dalam membangun kesadaran keamanan digital karena individu yang memahami ancaman siber cenderung lebih berhati-hati dalam menggunakan internet dan teknologi digital. Selain itu, indikator perlindungan data pribadi juga memperoleh nilai yang tinggi. Mahasiswa umumnya menyadari pentingnya menjaga informasi pribadi agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Kesadaran ini terlihat dari perilaku mahasiswa yang lebih berhati-hati dalam membagikan data pribadi melalui media sosial maupun platform digital lainnya. Tingginya perhatian terhadap keamanan data pribadi menunjukkan bahwa mahasiswa mulai memahami risiko yang dapat muncul akibat kebocoran atau penyalahgunaan informasi pribadi.

Pada aspek penggunaan kata sandi yang aman, hasil penelitian menunjukkan kategori tinggi. Sebagian besar mahasiswa telah memahami pentingnya penggunaan kata sandi sebagai bentuk perlindungan akun digital. Namun, masih ditemukan beberapa mahasiswa yang menggunakan kata sandi yang mudah ditebak atau menggunakan kata sandi yang sama untuk beberapa akun. Kebiasaan tersebut dapat meningkatkan risiko peretasan akun apabila terjadi kebocoran data pada salah satu layanan yang digunakan. Oleh karena itu, penerapan penggunaan kata sandi yang kuat dan unik masih perlu ditingkatkan. Indikator kemampuan mengenali phishing juga menunjukkan hasil yang cukup baik. Mahasiswa pada umumnya mampu mengenali ciri-ciri email, pesan, atau tautan mencurigakan yang berpotensi digunakan untuk mencuri data pribadi. Namun, perkembangan teknik phishing yang semakin canggih menyebabkan ancaman ini tetap menjadi salah satu risiko terbesar bagi pengguna internet. Oleh karena itu, mahasiswa perlu terus meningkatkan kewaspadaan dan kemampuan dalam membedakan informasi yang asli dan yang bersifat penipuan.

Sementara itu, indikator penggunaan autentikasi dua faktor (Two-Factor Authentication/2FA) memperoleh nilai paling rendah dibandingkan indikator lainnya. Hasil ini menunjukkan bahwa masih banyak mahasiswa yang belum memanfaatkan fitur keamanan tambahan tersebut. Padahal, autentikasi dua faktor

merupakan salah satu langkah efektif untuk meningkatkan keamanan akun digital. Rendahnya penggunaan fitur ini dapat disebabkan oleh kurangnya pemahaman mengenai manfaat 2FA atau anggapan bahwa proses login menjadi lebih rumit. Kondisi ini menunjukkan perlunya edukasi yang lebih intensif mengenai pentingnya penggunaan lapisan keamanan tambahan pada akun digital Pada indikator pembaruan sistem dan aplikasi, sebagian besar mahasiswa telah memahami bahwa pembaruan perangkat lunak penting untuk memperbaiki celah keamanan yang dapat dimanfaatkan oleh pelaku kejahatan siber. Namun, masih terdapat mahasiswa yang menunda pembaruan karena alasan keterbatasan kuota internet, kapasitas penyimpanan perangkat, atau kurangnya pemahaman terhadap manfaat pembaruan tersebut. Padahal, pembaruan sistem merupakan salah satu langkah pencegahan yang efektif dalam mengurangi risiko serangan siber.

Secara keseluruhan, hasil penelitian menunjukkan bahwa mahasiswa telah memiliki tingkat kesadaran yang cukup baik terhadap ancaman keamanan siber. Meskipun demikian, masih terdapat beberapa aspek yang perlu ditingkatkan, terutama dalam penerapan praktik keamanan digital secara konsisten. Perguruan tinggi memiliki peran penting dalam meningkatkan kesadaran keamanan siber melalui kegiatan sosialisasi, seminar, pelatihan, dan program literasi digital. Dengan adanya edukasi yang berkelanjutan, mahasiswa diharapkan mampu meningkatkan kemampuan dalam mengenali ancaman siber serta menerapkan langkah-langkah keamanan yang tepat untuk melindungi data dan aktivitas digital mereka di era digital yang semakin berkembang.

KESIMPULAN

Berdasarkan hasil penelitian mengenai Analisis Kesadaran Mahasiswa terhadap Ancaman Keamanan Siber di Era Digital**,** dapat disimpulkan bahwa tingkat kesadaran mahasiswa terhadap keamanan siber berada pada kategori tinggi**.** Sebagian besar mahasiswa telah memiliki pengetahuan yang cukup baik mengenai berbagai ancaman siber, seperti phishing, malware, ransomware, pencurian identitas, dan kebocoran data pribadi. Selain itu, mahasiswa juga menunjukkan pemahaman yang baik mengenai pentingnya menjaga keamanan informasi dan data pribadi saat menggunakan teknologi digital.

Hasil penelitian menunjukkan bahwa indikator pengetahuan tentang ancaman siber dan perlindungan data pribadi memperoleh nilai tertinggi, yang menandakan bahwa mahasiswa telah menyadari pentingnya keamanan digital dalam kehidupan sehari-hari. Namun, masih terdapat beberapa aspek yang perlu ditingkatkan, terutama dalam penggunaan autentikasi dua faktor (2FA), pengelolaan kata sandi yang lebih kuat, serta kewaspadaan terhadap berbagai bentuk serangan phishing yang semakin berkembang. Secara keseluruhan, kesadaran mahasiswa terhadap keamanan siber sudah cukup baik, tetapi masih memerlukan peningkatan melalui edukasi, pelatihan, seminar, dan program literasi digital yang berkelanjutan. Dengan meningkatnya kesadaran dan pemahaman mengenai keamanan siber, mahasiswa

diharapkan mampu melindungi data pribadi, menjaga keamanan akun digital, serta mengurangi risiko menjadi korban kejahatan siber di era digital.

Ucapan Terima Kasih

Penulis mengucapkan puji dan syukur kepada Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya sehingga penelitian dan penulisan jurnal ini dapat diselesaikan dengan baik. Penulis juga menyampaikan terima kasih kepada dosen pembimbing yang telah memberikan arahan, masukan, dan bimbingan selama proses penyusunan penelitian ini. Ucapan terima kasih juga diberikan kepada seluruh responden yang telah bersedia meluangkan waktu untuk mengisi kuesioner sehingga data penelitian dapat diperoleh dengan baik.

Selain itu, penulis mengucapkan terima kasih kepada keluarga, teman-teman, serta semua pihak yang telah memberikan dukungan, motivasi, dan bantuan baik secara langsung maupun tidak langsung dalam penyelesaian penelitian ini. Semoga penelitian ini dapat memberikan manfaat dan menjadi referensi bagi pengembangan pengetahuan, khususnya dalam bidang keamanan siber dan literasi digital di kalangan mahasiswa.

DAFTAR PUSTAKA

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289–296.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176.

Stallings, W. (2018). *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Pearson.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cybersecurity. *Computers & Security, 38*, 97–102.

Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security* (7th ed.). Cengage Learning.