Journal of Information and Information Security (JIFORTY)
Vol. 5, No. 2, Desember 2024, 235-244
e-ISSN : 2722-4058
Available Online at http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Keamanan Cyber dalam Menghadapi Tantangan Ancaman Masa Depan di Universitas Bhayangkara Jakarta Raya

Hafidz Prasetyo [1,*], Iib Ibrahim [1], Jeremia [1], Moh Milhan Hijrah Moelyana [1], Zaidan Muhammad Abid [1]

[1] Informatika; Universitas Bhayangkara Jakarta Raya; Jl. Perjuangan No. 81 Bekasi Utara, (021) 889558822; e-mail: 202310715245@mhs.ubharajaya.ac.id, 202310715267@mhs.ubharajaya.ac.id, 202310715022@mhs.ubharajaya.ac.id, 202310715074@mhsubharajaya.ac.id, 202310715260@mhs.ubharajaya.ac.id

* Korespondensi: e-mail: 202310715245@mhs.ubharajaya.ac.id

Diterima: 2 Jan 25; Review: 4 Jan 25; Disetujui: 11 Jan 25; Diterbitkan: 11 Jan 25

Abstract

The development of information technology has had a major impact on many aspects of life, including higher education. Bhayangkara University faces various challenges related to cybersecurity such as the risk of phishing, malware, ransomware, and data leaks that can disrupt academic and administrative systems. The purpose of this study was to assess how aware and knowledgeable students are about cybersecurity issues, recognize existing threats, and provide strategic suggestions to improve data protection in the campus area. The study involved 40 participants from Informatics majors at Bhayangkara University through a questionnaire. The findings show that the majority of students have a high awareness of the importance of cybersecurity, although there are still shortcomings in the implementation of best practices, such as the use of strong passwords and verification of email authenticity. This study suggests implementing measures such as periodic training, strengthening digital systems, and creating campus policies to comprehensively improve cybersecurity. The results of this study are expected to assist in the development of more effective digital security policies in higher education institutions.
***Keywords**: Cybersecurity, Higher Education, Digital Threats, Data Protection, Universitas Bhayangkara*

Abstrak

Perkembangan teknologi informasi memberikan pengaruh yang besar pada banyak aspek kehidupan, termasuk di dunia pendidikan tinggi. Universitas Bhayangkara menghadapi berbagai tantangan terkait keamanan siber seperti risiko phishing, malware, ransomware, dan kebocoran data yang bisa mengganggu sistem akademik serta administrasi. Tujuan dari penelitian ini adalah untuk menilai seberapa sadar dan paham mahasiswa mengenai masalah keamanan siber, mengenali ancaman yang ada, serta memberikan saran strategis untuk memperbaiki perlindungan data di area kampus. Penelitian ini melibatkan 40 peserta dari jurusan Informatika di Universitas Bhayangkara melalui kuesioner. Temuan menunjukkan bahwa mayoritas mahasiswa memiliki kesadaran yang tinggi mengenai pentingnya keamanan siber, walaupun masih terdapat kekurangan dalam penerapan praktik terbaik, seperti penggunaan kata sandi yang kuat dan verifikasi keaslian email. Penelitian ini menyarankan pengimplementasian langkah-langkah seperti pelatihan berkala, penguatan sistem digital, dan pembuatan kebijakan kampus untuk meningkatkan keamanan siber secara komprehensif. Hasil penelitian ini

diharapkan dapat membantu dalam pengembangan kebijakan keamanan digital yang lebih efektif di institusi pendidikan tinggi.

Kata kunci: Keamanan Siber, Pendidikan Tinggi, Ancaman Digital, Perlindungan Data, Universitas Bhayangkara

1. Pendahuluan

Perkembangan pesat dalam teknologi informasi telah menghasilkan dampak besar pada banyak aspek kehidupan, termasuk bidang pendidikan. Perguruan tinggi sebagai salah satu fondasi utama pendidikan dalam mengandalkan teknologi digital untuk memfasilitasi proses pembelajaran, pengelolaan data, serta komunikasi antara mahasiswa, pengajar, dan staf administratif. Meskipun memiliki banyak keuntungan, perubahan digital ini juga menimbulkan risiko yang serius, yaitu masalah keamanan siber yang tidak bisa diabaikan.

Keamanan Siber merupakan kegiatan untuk menjaga komputer, jaringan, software, sistem penting, dan informasi dari ancaman yang mungkin datang dari dunia digital. Setiap organisasi atau lembaga bertanggung jawab untuk melindungi data agar dapat menjaga kepercayaan dari pelanggan serta memenuhi kewajiban terhadap peraturan yang ada (Aws.amazon, n.d.). Keamanan siber merujuk pada teknologi, prosedur, dan kebijakan yang dirancang untuk menghentikan serangan siber atau mengurangi efeknya. Tujuan dari keamanan siber adalah untuk menjaga sistem komputer, aplikasi, perangkat, data, kekayaan finansial, dan individu dari serangan ransomware dan jenis malware lainnya, penipuan phishing, pencurian informasi, serta ancaman siber lainnya (Lindemulder & Kosinski, 2024).

Keamanan digital menjadi perhatian utama pada zaman sekarang, khususnya untuk lembaga pendidikan seperti Universitas Bhayangkara Jakarta Raya. Ancaman seperti peretasan data, pencurian data pribadi, ransomware, dan malware bisa mengganggu fungsi universitas serta merugikan komunitas akademis. Di samping itu, membangun kesadaran tentang pentingnya keamanan digital di antara mahasiswa, tenaga pengajar, dan staf juga merupakan tantangan yang harus dihadapi.

Universitas Bhayangkara, sebagai lembaga pendidikan yang berfokus pada kemajuan teknologi dan perlindungan informasi, menghadapi tantangan dalam menjamin keamanan dunia maya di tengah meningkatnya risiko. Untuk itu, studi ini bertujuan untuk mengevaluasi seberapa sadar dan pahamnya mahasiswa mengenai keamanan dunia maya, mengidentifikasi kemungkinan ancaman yang ada, serta memberikan saran strategis untuk memperkuat sistem keamanan dunia maya di area universitas.

Penelitian ini bertujuan untuk menggambarkan kondisi terkait keamanan siber di Universitas Bhayangkara Jakarta Raya. Hasil penelitian ini diharapkan dapat memberikan kontribusi nyata dalam upaya meningkatkan keamanan digital di perguruan tinggi dan menjadi acuan untuk pengembangan kebijakan yang lebih efektif dalam menghadapi tantangan keamanan siber di masa depan.

2. Metode Penelitian

2.1 Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan desain deskriptif. Pendekatan ini dipilih karena bertujuan untuk menggambarkan persepsi, pemahaman, dan kesadaran mahasiswa Universitas Bhayangkara terhadap keamanan siber, serta mengevaluasi potensi ancaman yang mereka hadapi. Penelitian deskriptif cocok digunakan untuk memberikan gambaran yang sistematis, faktual, dan akurat mengenai fenomena yang terjadi (Sugiyono, 2010).

2.2 Sampel dan Proses Pengumpulan Data

Populasi penelitian mencakup mahasiswa Universitas Bhayangkara. Sampel diambil menggunakan metode random sampling, dengan jumlah responden sebanyak 40 mahasiswa dari program studi informatika dan beberapa angkatan dari program studi tersebut. Teknik ini dipilih untuk memastikan bahwa data yang diperoleh dapat mewakili populasi secara umum (Neuman, 2014).

Pengumpulan data dilakukan secara daring menggunakan Google Forms. Link kuesioner disebarkan kepada mahasiswa jurusan Informatika Universitas Bhayangkara melalui grup WhatsApp mahasiswa. Pengumpulan data dilakukan selama 1 minggu pada tanggal 11 Desember 2024 sampai 18 Desember.

3. Hasil dan Pembahasan

3.1 Hasil Penelitian

Penelitian ini dilakukan dengan melibatkan 40 responden yang menjawab sejumlah pertanyaan untuk mengidentifikasi tingkat kesadaran dan pemahaman mahasiswa Universitas Bhayangkara tentang keamanan siber, serta persepsi mereka terhadap ancaman keamanan siber di lingkungan universitas. Berikut adalah hasil tabel pada setiap pertanyaan:

a. Tabel Frekuensi Pertanyaan Nomor 1 : *"Apakah Anda tahu apa itu Keamanan Cyber (perlindungan data dari ancaman kejahatan cyber)?"*

Tabel 1. Pengetahuan tentang Keamanan Cyber

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	5.0	5.0	5.0
	2	38	95.0	95.0	100.0
	Total	40	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada Tabel 1 menjelaskan pengetahuan tentang keamanan cyber:

- responden yang menjawab "Tidak" (kode 1) terdapat 2 orang dari total 40 responden, yang setara dengan 5% dari total responden.

- Responden yang menjawab "Ya" (dengan kode 2) sebanyak 38 orang, menunjukkan bahwa mereka tahu tentang keamanan siber setara dengan 95% dari total responden.

b. Tabel Frekuensi Pertanyaan nomor 2 : "*Untuk apa Anda biasanya menggunakan internet di kampus?*"

Tabel 2. Penggunaan Internet di Kampus

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	8	20.0	20.0	20.0
	2	5	12.5	12.5	32.5
	3	10	25.0	25.0	57.5
	4	17	42.5	42.5	100.0
	Total	40	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada Tabel 2 menjelaskan Penggunaan Internet di Kampus:

- responden memilih 1 jawaban (kode 1) sebanyak 8 orang atau 20% dari total responden. Responden tersebut saat menggunakan internet di kampus hanya ada 1 tujuan.
- Responden memilih 2 jawaban (kode 2) sebanyak 5 orang atau 12,5% dari total responden. Responden ini menggunakan internet di kampus untuk 2 tujuan aktivitas di kampus.
- Responden memilih 3 jawaban (kode 3) sebanyak 10 orang atau 25%.
- Responden memilih 4 jawaban (kode 4) sebanyak 17 orang atau 42,5% dari total responden.

c. Tabel Frekuensi Pertanyaan nomor 3 : "*Apakah Anda pernah mendapatkan pembelajaran di kampus terkait Keamanan Cyber?*"

Tabel 3. Pembelajaran Kemanan Siber di Kampus

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	10	25.0	25.0	25.0
	2	30	75.0	75.0	100.0
	Total	40	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada Tabel 3 menjelaskan Pembelajaran Keamanan Siber di Kampus:

- responden yang menjawab "Tidak" (kode 1) terdapat 10 orang yang setara dengan 25% dari total responden.
- Responden yang menjawab "Ya" (kode 2) sebanyak 38 orang, setara dengan 75% dari total responden.

d. Tabel Frekuensi Pertanyaan nomor 4 : "*Menurut Anda, apakah Keamanan Cyber penting untuk mahasiswa di kampus?*"

Tabel 4. Pentingnya Keamanan Siber untuk Mahasiswa

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	4	10.0	10.0	10.0
	3	6	15.0	15.0	25.0
	4	30	75.0	75.0	100.0
	Total	40	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada Tabel 4 menjelaskan pentingnya keamanan siber untuk mahasiswa:

- Terdapat 75% atau 30 orang menyatakan keamanan cyber sangat penting bagi mahasiswa.
- Sebagiannya 15% atau 6 orang menganggap keamanan cyber penting.
- Sementara itu 10% atau 4 orang menyatakan keamanan cyber tidak terlalu penting.

e. Tabel Frekuensi Pertanyaan nomor 5 : "*Berikut ini manakah yang pernah Anda alami saat menggunakan internet?*"

Tabel 5. Pegalaman Menggunakan Internet

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	33	82.5	82.5	82.5
	2	5	12.5	12.5	95.0
	3	2	5.0	5.0	100.0
	Total	40	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada Tabel 5 menjelaskan Pengalaman Menggunakan Internet:

- Terdapat 82.5% atau 33 orang hanya memilikh satu jawaban pengalaman tentang masalah keamanan siber.
- Sementara itu, 12.5% atau 5 orang mengalami 2 jenis masalah tentang keamanan siber.
- Terdapat 5% atau 2 orang yang mengalami 3 masalah tentang keamanan siber pada pengalaman responden.

f. Tabel Frekuensi Pertanyaan nomor 6 : "*Apakah Anda sering menggunakan kata sandi yang berbeda untuk setiap akun Anda?*"

Tabel 6. Menggunakan Password yang Berbeda

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	2.5	2.5	2.5
	2	18	45.0	45.0	47.5
	3	21	52.5	52.5	100.0
	Total	40	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada Tabel 6 menjelaskan Menggunakan Password yang Berbeda:

- Terdapat 52,5% atau 21 orang memiliki kebiasaan yang baik selalu menggunakan kata sandi yang berbeda pada setiap akun.
- Selain itu ada 45% atau 18 orang menunjukkan bahwa mereka kadang-kadang menggunakan kata sandi yang berbeda.
- Sementara hanya 2.5% atau 1 orang saja menggunakan kata sandi yang sama pada setiap akun.

g. Tabel Frekuensi Pertanyaan nomor 7 : "*Jika Anda menggunakan Wi-Fi kampus, apakah Anda merasa aman?*"

Tabel 7. Kemananan Wi-Fi Kampus

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	7	17.5	17.5	17.5
	2	9	22.5	22.5	40.0
	3	20	50.0	50.0	90.0
	4	4	10.0	10.0	100.0
	Total	40	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada Tabel 7 menjelaskan keamanan wi-fi kampus:

- Terdapat 10% atau 4 orang saat menggunakan Wi-Fi kampus merasa sangat aman.
- Sebagian lainnya ada 50% atau 20 orang menyatakan bahwa pada saat menggunakan Wi-Fi kampus merasa aman walaupun tidak maksimal.
- Lalu ada 22.5% atau 9 orang saat menggunakan Wi-Fi kampus merasa tidak aman pada data mereka.
- Terdapat 17.5% atau 7 orang tidak tahu apakah saat menggunakan WI-FI kampus akan merasa aman.

h. Tabel Frekuensi Pertanyaan nomor 8 : "*Apakah Anda pernah memeriksa keaslian tautan atau email sebelum membukanya?*"

Tabel 8. Keaslian Tautan atau Email

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	5.0	5.0	5.0
	2	20	50.0	50.0	55.0
	3	18	45.0	45.0	100.0
	Total	40	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada Tabel 8 menjelaskan keaslian tautan atau email:

- Terdapat 45% atau 18 orang selalu memeriksa keaslian email saat sebelum membuka email tersebut.
- Sementara itu 50% atau 20 orang kadang-kadang memeriksa keaslian email sebelum membuka.
- 5% atau 2 orang lainnya tidak pernah memeriksa keaslian email.

i. Tabel Frekuensi Pertanyaan nomor 9 : "*Menurut Anda, apa saja ancaman cyber yang bisa mengancam data atau keamanan cyber di kampus ini?*"

Tabel 9. Ancaman Siber yang Mengancam Kampus

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	24	60.0	60.0	60.0
	2	10	25.0	25.0	85.0
	3	6	15.0	15.0	100.0
	Total	40	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada Tabel 9 menjelaskan ancaman siber yang mengancam kampus:

- Sebanyak 15% atau 6 orang memilih 3 jawaban pada ancaman siber yang bisa mengancam data atau keamanan siber seperti Phishing, Malware, Ransomware.
- Sementara itu 25% atau 10 orang memilih 2 jawaban yang bisa mengancam data atau keamanan siber di kampus.
- Dan 60% atau 24 orang hanya memilih satu jawaban saja yang bisa mengancam data atau keamanan siber di kampus.

j. Pertanyaan nomor 10 : "*Apakah Anda pernah mendengar kejadian serangan cyber di kampus ini?*"

Tabel10. Kejadian Serangan Siber

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	23	57.5	57.5	57.5
	2	17	42.5	42.5	100.0
	Total	40	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada Tabel 10 menjelaskan kejadian serangan siber:

- Terdapat 42.5% atau 17 orang pernah mendengar kejadian serangan siber di kampus Universitas Bhayangkara.
- Sementara itu xm57.5% atau 23 orang tidak pernah mendengar kejadian serangan siber di kampus tersebut.

3.2 Pembahasan

Berdasarkan hasil analisis yang dilakukan, dapat disimpulkan bahwa informasi data yang diperoleh dari 40 peserta responden menunjukkan variasi kecenderungan yang bervariasi pada setiap masing-masing variabel Pertanyaan 1 hingga Pertanyaan 10. Sebagian besar variabel, seperti Pertanyaan 1, Pertanyaan 3, Pertanyaan 5, Pertanyaan 9, dan Pertanyaan 10, menunjukkan memiliki skor rata-rata yang rendah dan dengan distribusi yang terpusat terkonsentrasi, menunjukkan hasil yang cukup seragam. Di sisi lain relatif homogen. Sebaliknya, variabel seperti Pertanyaan 2, Pertanyaan 4, Pertanyaan 6, dan Pertanyaan 7 menunjukkan distribusi yang lebih seimbang merata dengan skor rata-rata dari moderat hingga tinggi, mencerminkan adanya berbagai pengalaman di antara para responden.

Secara keseluruhan, sebagian besar peserta memberikan penilaian yang lebih rendah pada variabel tertentu, sementara variabel lainnya menunjukkan distribusi yang lebih bervariasi. Temuan ini mengindikasikan perlunya analisis yang lebih mendalam untuk memahami faktor-faktor yang memengaruhi hasil pengujian pada variabel yang memiliki variasi distribusi yang lebih luas responden.

3.2.1 Tingkat Kesadaran Mahasiswa Terhadap Keamanan Siber

Hasil penelitian menunjukkan bahwa mayoritas mahasiswa memiliki tingkat kesadaran yang cukup rendah terhadap keamanan siber. Kesadaran keamanan siber adalah ketika user sadar akan mekanisme perlindungan dan dapat menerapkannya dengan tepat untuk kebutuhan mereka. Oleh karena itu, tidak cukup untuk disebut kesadaran keamanan siber jika prosedur ada tetapi pengguna tidak dapat menggunakan prosedur tersebut (Tan et al., 2024). Penelitian ini juga mencatat bahwa phishing dan malware adalah ancaman utama di lingkungan akademis.

Tingginya jumlah mahasiswa yang pernah mengalami ancaman seperti phishing (45%) dan malware (25%) menunjukkan bahwa ancaman siber sudah menjadi realitas yang perlu diatasi. Phishing merupakan perbuatan yang bertujuan untuk menipu korban dengan cara mencuri akun mereka. Ini dilakukan dengan menyebarkan pesan yang biasanya dikirim melalui email palsu, berisi informasi yang menyesatkan, yang mengarahkan sasaran ke situs palsu. Dengan cara ini, pelaku bisa mendapatkan akses ke akun korban. (Putra Y, 2021) (Intern, 2023). Malware merupakan singkatan dari malicious software, dalam definisi tentang malware disebutkan bahwa malware merupakan program yang sengaja dibuat untuk membahayakan dan merusak sistem operasi atau data pada komputer (Siddiqui et al., 2008) (Intern, 2023).

3.2.3 Pencegahan Keamanan Siber

Berikut ini adalah beberapa hal-hal pencegahan keamanan siber yang bisa diterapkan pada mahasiswa, staf, maupun dari pihak kampus (Diana, 2024):

1 Edukasi dan Kesadaran Keamanan Siber
   - Mengadakan pelatihan rutin kepada mahasiswa dan staf universitas mengenai pentingnya keamanan siber, termasuk cara mengenali phishing, malware, dan ancaman lainnya (Mahendra & Pinatih, 2023).
   - Melakukan edukasi kesadaran melalui seminar, poster, atau media sosial kampus untuk memperkuat pemahaman mengenai risiko dunia maya (Ardiyanti, 2014).

2 Kebijakan Pengelolaan Kata Sandi
   - Mendorong penggunaan kata sandi yang kuat dan unik untuk setiap akun mahasiswa, serta mengganti kata sandi secara berkala.
   - Menerapkan autentikasi dua faktor (2FA) untuk menambahkan lapisan perlindungan tambahan pada akun mahasiswa dan sistem universitas.

3 Penguatan Infrastruktur Keamanan Digital
   - Pastikan sistem keamanan jaringan universitas mampu melindungi data sensitif, seperti data akademik dan administratif. Hal ini selaras dengan konsep perlindungan Rahasia Dagang yang dijelaskan dalam Undang-Undang Nomor 30 Tahun 2000 (Febriharini, 2016).
   - Menerapkan sistem enkripsi untuk melindungi data sensitif dari akses tidak sah dan penyalahgunaan.

4 Monitoring dan Audit Sistem
   - Melakukan audit rutin terhadap sistem teknologi informasi untuk mengidentifikasi celah keamanan.
   - Memasang software deteksi intrusi untuk mendeteksi aktivitas mencurigakan.

5 Pengembangan Kapasitas
   - Mengadakan pelatihan rutin untuk meningkatkan pemahaman staf dan mahasiswa tentang ancaman siber.
   - Mengintegrasikan materi keamanan siber ke dalam kurikulum teknologi informasi.

4. Kesimpulan

Penelitian ini menjelaskan tingkat kesadaran, pemahaman, dan perilaku mahasiswa Universitas Bhayangkara tentang keamanan siber. Seperti yang diharapkan, hasil penelitian menunjukkan bahwa sebagian besar mahasiswa memahami pentingnya keamanan siber dalam kegiatan akademik, sebagaimana disebutkan dalam bab pendahuluan.

Berdasarkan hasil survei, 95% responden sudah mengetahui apa itu keamanan siber, 75% mengatakan keamanan siber sangat penting, sebagian besar responden memverifikasi keaslian email dan menyadari perlunya menggunakan kata sandi yang berbeda. Namun, terdapat sebagian kecil mahasiswa yang belum sepenuhnya memahami atau menerapkan

langkah-langkah keamanan digital secara optimal, antara lain: B. Penggunaan Wi-Fi yang aman di kampus dan memeriksa ancaman dunia maya tertentu.

Perkembangan dalam penelitian ini mencakup peningkatan kesadaran dunia maya melalui program pelatihan yang ditargetkan, kampanye pendidikan tentang praktik keamanan digital, dan penerapan kebijakan kampus berbasis teknologi untuk melindungi data dan sistem dengan lebih baik. Penelitian di masa depan diharapkan dapat menyelidiki lebih lanjut faktor-faktor yang mempengaruhi kesadaran dan perilaku mahasiswa serta mengukur dampak penerapan kebijakan keamanan siber terhadap efektivitas perlindungan data di lingkungan kampus

.

Daftar Pustaka

Ardiyanti, H. (2014). *Cyber-Security Dan Tantangan Pengembangannya Di Indonesia*. 95–110.

Aws.amazon. (n.d.). *Apa itu Keamanan Siber?* Amazon. https://aws.amazon.com/id/what-is/cybersecurity/

Diana. (2024). *Keamanan Siber (Cybersecurity): Tipe, Ancaman, dan Pencegahannya*. Telkom University Jakarta. https://jakarta.telkomuniversity.ac.id/keamanan-siber-cybersecurity/

Febriharini, M. P. (2016). Eksistensi hak atas kekayaan intelektual terhadap hukum siber. *Serat Acitya – Jurnal Ilmiah UNTAG Semarang*, 15–22.

Intern, D. (2023). *Cyber Security: Pengertian, Jenis, dan Ancamannya*. Dicoding.Com. https://www.dicoding.com/blog/cyber-security-pengertian-jenis-dan-ancamannya/

Lindemulder, G., & Kosinski, M. (2024). *What is cyber security?* IBM. https://www.ibm.com/id-id/topics/cybersecurity

Mahendra, Y. C., & Pinatih, N. K. D. S. A. (2023). Strategi Penanganan Keamanan Siber (Cyber Security) Di Indonesia. *Jurnal Review Pendidikan Dan Pengajaran (JRPP)*. http://journal.universitaspahlawan.ac.id/index.php/jrpp/article/view/20659

Neuman, W. L. (2014). Pearson New International Edition Social research methods: Qualitative and Quantitative approaches. In *Pearson*.

Putra Y, V. F. (2021). Modus Operandi Tindak Pidana Phising Menurut UU ITE. *Jurist-Diction*.

Siddiqui, M., Wang, M. C., & Lee, J. (2008). Data mining methods for malware detection using instruction sequences. *Proceedings of the IASTED International Conference on Artificial Intelligence and Applications, AIA 2008*.

Sugiyono, D. (2010). Metode penelitian kuantitatif kualitatif dan R&D. In *Penerbit Alfabeta*.

Tan, T., Sama, H., Wibowo, T., & Wijaya, G. (2024). Kesadaran Keamanan Siber pada Kalangan Mahasiswa Universitas di Kota Batam. *Jurnal Teknologi Dan Informasi*.