Jurnal Teknologi dan Informasi (JATI)
Volume 14 Nomor 2 Edisi September 2024
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v14i2

Kesadaran Keamanan Siber pada Kalangan Mahasiswa Universitas di Kota Batam

Cybersecurity Awareness among University Students in Batam City

Tony Tan[1]*, **Hendi Sama**[2], **Tony Wibowo**[3], **Gautama Wijaya**[4], **Osei Enoch Aboagye**[5]
Program Studi Sistem Informasi, Universitas Internasional Batam, Indonesia[12345]
tony@uib.ac.id[1], hendi@uib.ac.id[2], tony.wibowo@uib.ac.id[3], gautama.wijaya@uib.ac.id[4], 2031172.osei@uib.edu[5]

Abstrak

Keamanan siber adalah perlindungan sistem perangkat lunak dan perangkat keras komputer. Keamanan siber menetapkan persyaratan yang harus diikuti oleh pengguna komputer untuk mencegah segala jenis serangan siber. Namun, hanya pengguna yang lebih sadar akan keamanan siber yang terlindungi dengan baik. Dengan memastikan kerahasiaan, integritas, dan ketersediaan, kata sandi, sistem operasi, serta konfigurasi privasi dan keamanan platform media sosial harus ditanggapi dengan serius. Penelitian ini bertujuan untuk mengukur tingkat kesadaran keamanan siber mahasiswa di Kota Batam. Penulis menggunakan metode kuantitatif dengan melakukan tes statistik yang berbeda, seperti tes validitas, tes reliabilitas dan ukuran sampel. Survei dilakukan dengan menyebarkan kuesioner kepada mahasiswa untuk diisi secara online. Respon dihitung dalam persentase. Sebanyak 469 mahasiswa dari lima perguruan tinggi yang dipilih secara acak dari Batam, Kepulauan Riau, menanggapi survei tersebut. Setelah menganalisis data, hasilnya menunjukkan bahwa mahasiswa memiliki tingkat kesadaran keamanan siber yang rendah karena 11 mahasiswa tidak menerapkan pembaruan perangkat lunak dan 6 mengabaikan pembaruan perangkat lunak. Selain itu, 75,3% mahasiswa menggunakan kata sandi yang digunakan sebelumnya, 74% menggunakan satu kata sandi yang kuat untuk akun yang berbeda dan 78,5% mengatakan itu menjengkelkan untuk memiliki kata sandi yang panjang dan kuat untuk setiap akun. Terakhir, 73,3% berbagi lokasi saat ini secara publik di media sosial dan 68,7% berbagi informasi pribadi yang sensitif. Oleh karena itu, penulis merekomendasikan universitas untuk memasukkan pendidikan keamanan siber di semua departemen. Juga, ada kebutuhan untuk pelatihan reguler baik dosen maupun mahasiswa tentang keamanan siber.
Kata kunci: Keamanan Browser; Keamanan Kata Sandi; Keamanan Media Sosial.

Abstract

Cybersecurity is the protection of computer software and hardware systems. Cybersecurity lays down the requirements to be followed by computer users to prevent any sort of cyber injury. However, only users who are more aware of cybersecurity are well protected. By ensuring confidentiality, integrity and availability, passwords, operating systems and privacy and security configurations of social media platforms should be taken seriously. This research aims to measure the cybersecurity awareness level of university students in the Batam City. Author used the quantitative method for this research, and conducted different statistical tests, such as validity test, reliability test and sample size. A survey was conducted by distributing questionnaires to students to fill online. A total of 469 students from five universities randomly chosen from Batam, Kepulauan Riau, responded to the survey. Responses were counted in percentages. After analyzing the data, results show that students have low cybersecurity awareness level since 11 students apply no software updates and 6 neglects software updates. Also, 75.3% of students use previously used passwords, 74% use one strong password for different accounts and 78.5% say it is annoying to have long and strong password for each account. Lastly, 73.3% share current location publicly on social media and 68.7% share sensitive personal information. Author therefore recommend universities to include cybersecurity education in all departments. Also, there is the need for regular training of both lecturers and students on cybersecurity.
Keywords: Browser Security; Password Security; Social Media Security.

Naskah diterima 16 Maret 2024; direvisi 7 Agustus 2024; dipublikasi 1 September 2024.

1. Pendahuluan

Menurut DataReportal, terdapat 212,9 juta pengguna internet aktif di Indonesia per Februari 2023. Jumlah ini mewakili 77% dari total populasi Indonesia. Laporan tersebut menyatakan bahwa usia rata-rata Indonesia adalah 29,8 tahun. Juga dinyatakan bahwa 49,5% dari populasi adalah mereka yang berusia antara 13-44 tahun. Hal ini menunjukkan bahwa hampir semua pemuda Indonesia menggunakan perangkat komputer untuk kegiatan sehari-hari mereka yang meliputi studi [1]. Usia rata-rata mahasiswa di berbagai universitas di Indonesia adalah antara 17-22 tahun yang termasuk dalam usia rata-rata Indonesia.

Datareportal mengatakan dalam laporan mereka bahwa penetrasi jaringan di Indonesia adalah 77%. Hal ini menjadikan Indonesia salah satu negara yang paling banyak diretas di ASEAN dalam hal keamanan siber [2]. Sebagian besar industri memiliki insiden yang menunjukkan bahwa mereka sedang dieksploitasi [3][4]. Menurut Kominfo, dinyatakan dalam pidato wisuda Menteri Penerangan RI Universitas Muhammadiyah

Jurnal Teknologi dan Informasi (JATI)
Volume 14 Nomor 2 Edisi September 2024
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v14i2

Malang tahun 2017, 12 institusi diserang oleh Wanacry Ransomware yang termasuk universitas. Indonesia terus mendapatkan serangan [5] dan kerusakan data [6]. Sejarah digital masa lalu ini mengungkapkan betapa pentingnya bagi mahasiswa untuk menyadari masalah keamanan siber. Bagaimana menghindari peretasan, cara memperbaiki, dan cara tetap memperbarui keamanan yang perlu diketahui mahasiswa. Jika mahasiswa dapat menjaga koneksi mereka tetap aman, itu semua tergantung pada tingkat kesadaran tentang *phishing*, *Denial of Service* (DoS), serangan kata sandi, injeksi SQL, interpretasi URL [7], pembajakan sesi, dan malware. Sekali lagi, mahasiswa perlu tahu bagaimana Wi-Fi publik universitas bekerja untuk mencegah serangan apa pun [8].

Di era digital ini, mahasiswa bergantung pada internet untuk studi mereka [9]. Ketergantungan meningkat karena munculnya penyakit Covid-19. *E-learning* adalah salah satu cara universitas mengelola kegiatan akademik di kampus. Ini memungkinkan mahasiswa mengakses bahan belajar dan menyerahkan tugas. Dosen juga menggunakan email dan platform media sosial untuk menyebarkan informasi kepada kolega dan mahasiswa. Karena universitas menggunakan jaringan publik, sangat penting untuk menjaga keamanan siber dan perlindungan data. Perlindungan data paling baik dicapai jika civitas akademika sadar akan standar keamanan. Pendaftaran dilakukan dengan menggunakan informasi pribadi yang sensitif seperti nama, usia, alamat, nomor kartu identitas dan foto. Peretas berusaha memanfaatkan mahasiswa untuk mendapatkan data. Pertanyaan penting seperti "apakah mahasiswa yang merupakan pengguna akhir jaringan universitas sadar bahwa peretas dapat memperoleh akses melalui koneksi mereka?"; "Apakah mahasiswa sadar bahwa mengikuti langkah-langkah keamanan membantu melindungi jaringan universitas?"; dan "Jika mereka menjadi korban, mereka perlu memberi tahu personel IT tentang insiden tersebut?" harus ditanyakan. Mahasiswa membentuk tautan ke jaringan universitas utama dan jika tautan mereka lemah, jaringan kampus menderita di tangan peretas [10].

Kesadaran keamanan siber sangat penting di institusi manapun [11]. Keamanan siber bertujuan untuk melindungi individu dan badan perusahaan dari aktivitas digital terlarang. *Confidentiality*, *Integrity*, dan *Availability* didefinisikan dalam lingkup keamanan siber dengan standar dan protokol yang harus diikuti. Ada pendidikan publik tentang keamanan siber melalui seminar bagi mahasiswa untuk menyadari prinsip-prinsip ini. Pendidikan publik adalah satu-satunya cara untuk membuat orang sadar tentang keamanan sibar.

Penelitian ini bertujuan untuk mengetahui tingkat kesadaran keamanan siber mahasiswa di Kota Batam, Indonesia. Provinsi ini memiliki beberapa universitas yang sebagian besar terkonsentrasi di Kota Batam. Kontribusi utama dari penelitian ini meliputi: (1) Untuk meningkatkan kesadaran keamanan siber mahasiswa; (2) Untuk mengajar mahasiswa tentang bahaya dan tantangan dalam jaringan komputer; dan (3) Untuk menyarankan langkah-langkah keamanan yang efektif dan strategi yang diperlukan agar tetap aman saat menggunakan perangkat komputer.

2. Metode Penelitian

Penelitian ini dimulai dengan proses tinjauan pustaka untuk mengetahui kondisi literatur terkini terkait *cybersecurity awareness* dan indikasi secara *behavioral* pada seseorang yang memiliki tendensi *cybersecurity* yang baik. Dari tinjauan pustaka didapatkan terdapat tiga parameter utama dalam menilai kemampuan seseorang memiliki kesadaran yang baik pada *cybersecurity* pribadi yakni menjaga kerahasiaan (*confidentiality*), kelengkapan (*integrity*) dan ketersediaan akses (*availability*) terutama pada tiga jenis kegiatan di internet yakni keamanaan *password*, keamanan *browser* dan keamanan *platform* media sosial. Berikutnya penulis menyusun instrumen yang sesuai dengan hasil tinjauan pustaka dan menyebarkannya menggunakan internet. Setelah data dikumpulkan, proses analisis data secara kuantitatif dilakukan dengan menggunakan SPSS versi 25 sebagaimana disampaikan pada Gambar 1.

Gambar 1. Alur Metodologi Penelitian

Survei dilakukan untuk mengumpulkan data dari mahasiswa dari berbagai jenis kelamin, usia, demografi, departemen, dan universitas di Kota Batam, Indonesia. Survei dilakukan pada Januari 2024. Kuesioner mencakup pertanyaan tentang aspek-aspek penting dari keamanan siber untuk mengukur tingkat pemahaman dan kesadaran mahasiswa tentang topik tersebut. Pertanyaan termasuk demografis (3 pertanyaan), penggunaan

Jurnal Teknologi dan Informasi (JATI)
Volume 14 Nomor 2 Edisi September 2024
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v14i2

internet (2 pertanyaan), keamanan kata sandi (6 pertanyaan), keamanan browser (4 pertanyaan), dan platform media sosial (5 pertanyaan). Setiap set pertanyaan diberikan untuk mengukur rincian spesifik pengetahuan dan keterampilan mahasiswa tentang keamanan siber. Keamanan internet memiliki pertanyaan yang berusaha untuk mengungkapkan kegiatan mahasiswa dan bagaimana mereka menggunakan internet dalam kaitannya dengan standar keamanan. Pertanyaan keamanan kata sandi berfokus pada bagaimana mahasiswa memahami risiko dan pentingnya menggunakan kata sandi yang lemah atau kuat. Pertanyaan keamanan *browser* menanyakan tentang bagaimana browser digunakan untuk membelok melalui internet yang kompleks. Terakhir, pertanyaan *platform media* sosial menuntut mahasiswa untuk memberikan apa yang mereka ketahui tentang bagaimana *platform media* sosial dapat digunakan dengan aman.

Pada Pengaturan dan Responden Penelitian menggunakan kuesioner. Kuesioner dibuat menggunakan *Google Form* dan dibagikan kepada responden secara *online*. Responden adalah mahasiswa dari Kota Batam, tempat penulis berada. Pertanyaan pertama kali ditulis dalam bahasa Inggris dan kemudian diterjemahkan ke Bahasa Indonesia agar setiap responden mendapatkan pemahaman penuh. Responden diminta untuk memberikan jawaban tulus mereka untuk memberikan hasil yang akurat. Data yang terkumpul diolah dan dianalisis menggunakan SPSS (untuk mengukur validitas dan kualitas variabel).

Pada bagian kriteria inklusi dan pengecualian, partisipasi didistribusikan secara ketat hanya kepada mahasiswa sebagai populasi survei. Seorang mahasiswa sepenuhnya terdaftar di lembaga pendidikan tinggi dan harus berada di Kota Batam.

Kemudian dalam melakukan strategi penelitian dengan memberikan pertanyaan terbaik yang secara efektif dapat mengukur kesadaran keamanan siber mahasiswa dipilih. Dosen pembimbing akademik memeriksa pertanyaan untuk memeriksa silang dan menghilangkan segala jenis kesalahan. Tabel 1, 2 dan 3 berisi semua variabel tentang keamanan kata sandi, keamanan *browser* dan keamanan *platform* media sosial [12].

Tabel 1. Variabel untuk Keamanan Kata Sandi

No	Variabel	Kode Variabel
1	Semua kata sandi saya meliputi: 12 karakter atas dan bawah, angka, dan simbol.	PS1
2	Saya harus mengubah kata sandi saya secara berkala.	PS2
3	Saya dapat menggunakan kata sandi yang digunakan sebelumnya.	PS3
4	Saya menggunakan satu kata sandi yang kuat untuk berbagai situs web dan akun.	PS4
5	Sungguh menjengkelkan memiliki kata sandi yang panjang dan kuat untuk setiap situs web dan akun.	PS5
6	Saya sering membagikan kata sandi saya kepada orang lain.	PS6

Tabel 2. Variabel untuk Keamanan *Browser*

No	Variabel	Kode Variabel
1	*Browser* web harus diperbarui secara berkala.	BS1
2	Saya harus menghindari pemasangan ekstensi dari situs web pihak ketiga.	BS2
3	Saya harus memeriksa pengaturan keamanan dan konfigurasi *browser web* secara berkala.	BS3
4	Saya harus memeriksa riwayat *browser* dan menemukan aktivitas mencurigakan.	BS4

Tabel 3. Variabel untuk Keamanan *Platform Media* Sosial

No	Variabel	Kode Variabel
1	Memposting foto pribadi di media sosial diperbolehkan.	SN1
2	Menerima permintaan pertemanan dari orang asing tidak masalah.	SN2
3	Tidak ada masalah membagikan lokasi saya saat ini secara publik di media sosial.	SN3
4	Tidak ada masalah dalam menambahkan semua informasi pribadi seperti data kelahiran, pekerjaan saat ini, dll.	SN4
5	Saya tahu cara melaporkan ancaman atau aktivitas mencurigakan apa pun di media sosial.	SN5

Kemudian mengenai impressi responden pada kuesioner memiliki lima impressi yang sesuai dengan nomor 1-5. 1 (sangat tidak setuju (S.D)), 2 (tidak setuju (D)), 3 (netral (N)), 4 (setuju (A)) dan 5 (sangat setuju (S.A)) yang dijelaskan dalam deskripsi setiap bagian pada *Google Form* sebelum mahasiswa memilih jawaban mereka berdasarkan tingkat.

3. Hasil dan Pembahasan

Sesi ini menjelaskan hasil survei tentang kesadaran keamanan siber mahasiswa. Tanggapan diwakili dalam tabel yang menunjukkan angka dengan persentase yang sesuai untuk diskusi di sesi berikutnya. Hanya satu penelitian yang mengukur tingkat kesadaran keamanan siber mahasiswa di Kota Batam. Penulis mendorong

Jurnal Teknologi dan Informasi (JATI)
Volume 14 Nomor 2 Edisi September 2024
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v14i2

lebih banyak penelitian tentang topik ini untuk meningkatkan kesadaran di kalangan mahasiswa. Sebagian besar responden tidak mengetahui masalah keamanan siber menurut tanggapan mereka.

3.1 Batasan Penelitian

Studi ini mengungkapkan temuan penting untuk mempromosikan tingkat kesadaran keamanan siber. Namun, penting untuk mengenali keterbatasan yang penulis rencanakan untuk ditingkatkan dalam studi selanjutnya. Variabel tidak mencakup semua aspek keamanan siber dan peserta mengambil dari universitas di kota Batam. Penelitian lain harus dilakukan tentang topik yang sama yang mentargetkan mahasiswa yang berada di luar Batam, dan ukuran sampel juga ditingkatkan.

3.2 Validitas

Aplikasi IBM SPSS digunakan untuk memeriksa validitas dan kualitas variabel setelah memeriksa *outlier* (z-score) untuk membersihkan data untuk hasil yang akurat. 388 tanggapan dari 469 digunakan untuk tes. Sebanyak 81 tanggapan dianggap tidak cukup baik untuk analisis. Hasil penelitian menunjukkan bahwa semua variabel *valid* dan dapat digunakan untuk mengukur tingkat kesadaran keamanan siber mahasiswa. Suatu variabel *valid* jika nilai signifikansinya di bawah 0,05 dan Korelasi Pearson di atas 0,05.

Tabel 4 berisi hasil uji validitas untuk variabel Keamanan Kata Sandi. Semua variabel Keamanan Kata Sandi yaitu; "semua kata sandi saya meliputi: 12 karakter atas dan bawah, angka, dan simbol; saya harus mengubah kata sandi saya secara berkala; saya dapat menggunakan kata sandi yang digunakan sebelumnya; saya menggunakan satu kata sandi yang kuat untuk berbagai situs web dan akun; sungguh menjengkelkan memiliki kata sandi yang panjang dan kuat untuk setiap situs web dan akun; dan saya sering membagikan kata sandi saya kepada orang lain", *valid* karena mencapai nilai signifikansi di bawah 0,05 dan Korelasi Pearson di atas 0,05.

Tabel 4. Hasil Tes Validitas untuk Variabel Keamanan Kata Sandi

Kode Variabel	Korelasi	Signifikan
PS1	.279**	.000
PS2	.484**	.000
PS3	.818**	.000
PS4	.388**	.000
PS5	.734**	.000
PS6	.744**	.000

Tabel 5 berisi hasil validitas untuk variabel Keamanan *Browser*. Keempat variabel Keamanan *Browser* adalah: "browser web harus diperbarui secara berkala; saya harus menghindari pemasangan ekstensi dari situs web pihak ketiga; saya harus memeriksa pengaturan keamanan dan konfigurasi browser web secara berkala; dan saya harus memeriksa riwayat browser dan menemukan aktivitas mencurigakan." Variabel tersebut *valid* karena mencapai nilai signifikansi di bawah 0,05 dan Korelasi Pearson di atas 0,05.

Tabel 5. Hasil Tes Validitas untuk Variabel Keamanan *Browser*

Kode Variabel	Korelasi	Signifikan
BS1	.733**	.000
BS2	.682**	.000
BS3	.266**	.000
BS4	.809**	.000

Tabel 6 berisi hasil validitas untuk variabel Keamanan *Platform* Media Sosial. Variabelnya meliputi "memposting foto pribadi di media sosial diperbolehkan; menerima permintaan pertemanan dari orang asing tidak masalah; tidak ada masalah membagikan lokasi saya saat ini secara publik di media sosial; tidak ada masalah dalam menambahkan semua informasi pribadi seperti data kelahiran, pekerjaan saat ini, dll; dan saya tahu cara melaporkan ancaman atau aktivitas mencurigakan apa pun di media sosial", dimana semuanya *valid* karena mencapai nilai signifikansi di bawah 0,05 dan Korelasi Pearson di atas 0,05.

Tabel 6. Hasil Tes Validitas untuk Variabel Keamanan *Platform* Media Sosial

Kode Variabel	Korelasi	Signifikan
SN1	.836**	.000
SN2	.832**	.000
SN3	.737**	.000
SN4	.943**	.000
SN5	.800**	.000

Jurnal Teknologi dan Informasi (JATI)
Volume 14 Nomor 2 Edisi September 2024
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v14i2

3.3 Reliabilitas

Seperti tes validitas, tes reliabilitas dilakukan dengan menggunakan aplikasi IBM SPSS. Setelah pengujian, semua variabel dapat diandalkan. Variabel yang dapat diandalkan adalah variabel dengan nilai Cronbach Alpha di atas 0,6. Uji reliabilitas juga dilakukan setelah pembersihan data. Tabel 7 menunjukkan hasil uji reliabilitas.

Tabel 7. Hasil Tes Reliabilitas

Kode	Variabel	Alpha Cronbach
1	Keamanan Kata Sandi	.645
2	Keamanan Browser	.641
3	Media Sosial	.864

3.4 Ukuran Sampel

Ukuran sampel adalah bagian dari populasi yang termasuk dalam penelitian [13]. Sangat sulit dan memakan waktu untuk mensurvei populasi besar sehingga sampel diperlukan untuk memperkirakan statistik. Ukuran sampel diperlukan untuk membuktikan seberapa andal variabel dari studi tertentu. Untuk menghitung ukuran sampel, ukuran populasi dan margin kesalahan penerimaan digunakan. Tingkat kepercayaan 95% (0,05) digunakan. Rumus Slovin digunakan untuk menghitung ukuran sampel untuk penelitian ini sebagaimana persamaan 1.

$$n = \frac{N}{(1+Ne^2)} \quad (1)$$

Keterangan:
n = ukuran sampel
N = ukuran populasi
E = margin kesalahan yang dapat diterima
$n = 10.000/(1+10000(,05)^2)$

Jumlah total mahasiswa di Kota Batam dapat diperkirakan sekitar 10,000 sehingga ukuran sampelnya adalah 385 (dibulatkan ke bilangan bulat terdekat).

3.5 Informasi Demografis Responden

Sebanyak 469 mahasiswa mengambil bagian dalam survei. Sebagian besar mahasiswa terkonsentrasi pada Universitas Internasional Batam. Universitas lain termasuk Universitas Putra Batam, Institut Teknologi Batam, Universitas Bina Nusantara dan Sekolah Tinggi Teologi Pantekosta Batam. Tabel 8 merangkum jenis kelamin, usia, universitas, dan perangkat responden yang digunakan sehari-hari.

Seperti yang ditunjukkan pada Tabel 8, sebagian besar peserta adalah laki-laki dan sedikit perempuan. Usia modal berkisar antara 18-25 yang mencakup 96,1% dari jumlah total. Hanya 3,8% yang mewakili usia 26-34 dan 0,4% di atas 34 tahun. Semua mahasiswa memiliki smartphone. Sebanyak 410 mahasiswa menggunakan laptop dan 13 memiliki tablet.

Tabel 8. Informasi Demografis Responden

	Variabel	Jumlah	(%)
Jenis Kelamin	Laki-laki	397	84.6%
	Perempuan	74	15.8%
Usia	18-25	451	96.2%
	26-34	18	3.8%
	Di atas 34	2	0.4%
Universitas	Universitas Internasional Batam	260	55%
	Universitas Bina Nusantara	70	15%
	Universitas Putra Batam	41	9%
	Institut Teknologi Batam	25	5%
	Sekolah Tinggi Teologi Pentekosta Batam	73	16%
Perangkat	*Smartphone*	469	100%
	Laptop	410	87.4%
	Tablet	13	2.8%

3.6 Kesadaran Responden tentang Konsep Keamanan Siber

Triad CIA (*Confidentiality*, *Integrity*, dan *Availability*) menguraikan standar keamanan siber. Penting bagi mereka untuk menjadi lebih sadar akan protokol *Triad* CIA. Setiap perangkat rentan terhadap semacam

Jurnal Teknologi dan Informasi (JATI)
Volume 14 Nomor 2 Edisi September 2024
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v14i2

serangan siber dan pembaruan diperlukan untuk meningkatkan keamanan. Perangkat dengan sistem operasi usang dan perangkat lunak lain lebih rentan terhadap serangan siber [14]. Untuk alasan ini, mahasiswa ditanya tentang bagaimana mereka memperbarui sistem operasi mereka.

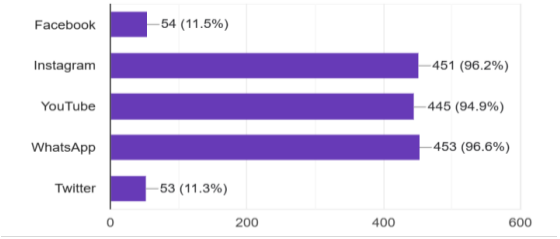
Menurut hasil survei pada Tabel 9, 398 mahasiswa menggunakan pembaruan otomatis (memperbarui secara otomatis oleh sistem tanpa campur tangan pengguna), 76 memperbarui sistem operasi secara manual, 11 menerapkan tidak ada pembaruan dan 6 mengabaikan pembaruan.

Tabel 9. Cara Responden Memperbarui Sistem Operasi

No	Variabel	Jumlah	(%)
1	Pembaruan Otomatis	398	4.9%
2	Pembaruan Manual	76	62%
3	Tidak ada pembaruan	11	2.3%
4	Menolak Pembaruan	6	1.3%

3.7 Media Sosial Responden

Waktu yang dihabiskan oleh mahasiswa menggunakan perangkat yang telah disebutkan tergantung pada apa yang mereka lakukan. Pada era digital ini, sebagian besar mahasiswa menghabiskan lebih banyak waktu di *platform* media sosial. Kebutuhan untuk terhubung dengan mahasiswa lain dan berbagi pengalaman pribadi mendorong lebih banyak mahasiswa untuk tetap menggunakan media sosial setiap saat. Perempuan menghabiskan banyak waktu di *Whatsapp* dibandingkan laki-laki. Gambar 1 menunjukkan bahwa 54, 451, 445, 453 dan 53 mahasiswa masing-masing menggunakan *Facebook*, *Instagram*, *YouTube*, *WhatsApp*, dan *Twitter*. *Platform media* sosial yang paling banyak digunakan oleh mahasiswa adalah *Instagram*, *YouTube*, dan *WhatsApp* sebagaimana disampaikan pada Gambar 2.



Gambar 2. *Platform* Media Sosial Responden

3.8 Pengetahuan Responden tentang Keamanan Kata Sandi

Kata sandi adalah metode otentikasi yang berada di bawah konsep *Confidentiality*. Kata sandi adalah kata keamanan yang unik. Kata sandi yang kuat harus berupa kombinasi huruf (huruf besar dan kecil), angka dan simbol dan harus setidaknya 8-12 karakter [15]. Kata sandi yang lemah mudah dipatahkan atau ditebak [16]. Penulis menemukan pengetahuan responden tentang pengelolaan kata sandi untuk mengukur bagaimana mereka membuat kata sandi untuk menjaga keamanan di berbagai akun.

Tabel 10 menunjukkan bahwa 77% responden 'setuju' kata sandi harus kuat. Juga 74% 'setuju' satu kata sandi yang kuat dapat digunakan diberbagai akun. Hasil dalam Tabel 10 menunjukkan bahwa sejumlah besar mahasiswa tidak terlalu memperhatikan keamanan kata sandi.

Tabel 10. Pengetahuan Responden tentang Keamanan Kata Sandi

Kode	S.D	D	N	A	S.A
PS1	2.6%	4.1%	6.2%	77%	10.2%
PS2	7.9%	7.9%	4.8%	5.8%	3.6%
PS3	3%	3.6%	7%	11.1%	75.3%
PS4	2.1%	3.2%	8.3%	74%	12.4%
PS5	4.3%	3.6%	6.6%	7%	78.5%
PS6	22.4%	3.8%	69.5%	1.7%	2.6%

3.9 Pengetahuan Peserta tentang Keamanan *Browser*

Browser adalah aplikasi yang digunakan untuk mencari informasi di internet. Karena *browser* adalah perangkat lunak yang memiliki kerentanan sehingga perlu adanya pembaruan sistem atau *patch*. Karena penulis menggunakan *browser* untuk mencari informasi, banyak sekali informasi yang menunjukkan aktivitas penulis dikompilasi pada aplikasi *browser*. Seorang peretas dapat membuat tebakan yang tepat hanya dengan melihat apa yang terjadi pada *browser*.

Jurnal Teknologi dan Informasi (JATI)
Volume 14 Nomor 2 Edisi September 2024
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v14i2

Tanggapan dari mahasiswa mengatakan bahwa mereka lebih sadar akan penggunaan *browser*, tetapi mungkin tidak memiliki beberapa keterampilan teknis. Pengaturan keamanan dan konfigurasi *browser* sangat penting, namun 78,5% mahasiswa memilih 'netral', menunjukkan bahwa mereka tidak tahu apakah konfigurasi keamanan diperlukan atau tidak. Tabel 11 menunjukkan respons kesadaran mahasiswa tentang keamanan *browser*.

Tabel 11. Pengetahuan Responden tentang Keamanan *Browser*

Kode	S.D	D	N	A	S.A
BS1	0.4%	4.9%	10.2%	9%	75.5%
BS2	1.1%	4.3%	10.2%	75.7%	8.7%
BS3	1.1%	2.8%	78.5%	9%	8.7%
BS4	0.2%	5.1%	8.1%	8.7%	77.8%

3.10 Pengetahuan Responden tentang *Platform* Media Sosial

Media sosial adalah urutan hari bagi orang-orang dan mahasiswa tidak terkecuali. Mahasiswa membutuhkan media sosial untuk terhubung dengan mahasiswa lain, dosen, dan pemangku kepentingan untuk kesempatan kerja. Berbagai informasi ditemukan di media sosial dan mahasiswa perlu diperbarui. Peretas berusaha mendapatkan informasi dari mahasiswa. Pengaturan privasi dan keamanan pada *platform* media sosial tetap menjadi pusat langkah-langkah keamanan yang harus dilakukan.

Tabel 12 menunjukkan 72,5% mahasiswa 'setuju' bahwa tidak apa-apa untuk menerima permintaan ramah dari orang asing. Sebanyak 68,7% juga 'sangat setuju' bahwa berbagi informasi sensitif pribadi seperti tanggal lahir dan pekerjaan saat ini tidak apa-apa. Hal penting lainnya adalah bahwa 77,6% mahasiswa 'sangat setuju' bahwa mereka tahu cara melaporkan ancaman atau aktivitas mencurigakan di media sosial. Ini mengungkapkan bahwa mereka mungkin telah diserang sebelumnya.

Tabel 12. Pengetahuan Responden tentang Keamanan *Platform* Media Sosial

Kode	S.D	D	N	A	S.A
SN1	0.4%	2.6%	10.7%	11.9%	74.4%
SN2	3.8%	7.9%	12.6%	72.5%	3.2%
SN3	14.1%	6%	74.3%	3.8%	2.8%
SN4	9.6%	8.7%	7.9%	5.1%	68.7%
SN5	1.3%	3%	8.5%	9.6%	77.6%

Hasil penulis telah dibandingkan dengan hasil penelitian sebelumnya tentang tingkat kesadaran keamanan siber mahasiswa. Misalnya salah satu penelitian pada objek mahasiswa di *Northeastern University* di Nigeria mengungkap bahwa mahasiswa memiliki pengetahuan dasar tentang keamanan siber tentang elemen-elemen seperti internet banking, dan pengetahuan moderat tentang *cyber bullying*, perlindungan diri, dan kecanduan internet [17]. Temuan penulis sejalan dengan pernyataan bahwa manajemen kata sandi bermasalah bagi semua sejauh menyangkut keamanan siber [18]. Sementara itu penelitian lainnya menyatakan bahwa sikap mahasiswa dan kontrol perilaku yang dirasakan, secara positif mempengaruhi niat mereka untuk mempraktikkan keamanan siber [19]. Dilain hal, temuan penulis menentang hasil temuan yang mengungkap bahwa tidak ada perbedaan jenis kelamin dan usia pada kesadaran keamanan siber dan mengatakan tidak ada perbedaan dalam tingkat pendidikan pada tingkat kesadaran keamanan siber [20].

Sangat penting untuk menaruh perhatian pengguna pada makna kesadaran keamanan siber. Untuk memecahnya menjadi istilah yang lebih kecil, pengguna bisa mendapatkan 'Keamanan siber' yang merupakan perlindungan perangkat atau pengguna individu dan 'kesadaran' yang berarti sadar akan sesuatu. Kesadaran keamanan siber adalah ketika pengguna 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. Menyadari tentang 'Mengapa sebuah metode digunakan?', 'Metode mana yang harus digunakan?', 'Kapan menggunakan metode seperti itu?' dan 'metode seperti itu harus digunakan untuk apa?' bersatu untuk menentukan tingkat kesadaran keamanan siber seseorang.

Selama bertahun-tahun, telah ditunjukkan bahwa pria lebih tertarik pada pekerjaan keamanan siber dan pada catatan itu, menyatakan pria memiliki lebih banyak jumlah yang lebih sadar akan keamanan siber daripada wanita. Wanita sering menjadi korban ancaman siber. Untuk menganalisis data dari survei penulis, penulis dapat melihat bahwa 397 (84,6%) dari total responden adalah pria dan hanya 74 (15,8%) adalah wanita. Hal ini mengkonfirmasi mengapa mahasiswa di Kota Batam dinyatakan kurang memiliki pengetahuan tentang keamanan siber dan mahasiswa di Kota Batam yang berjenis kelamin pria belum sadar akan keamanan siber. Untuk menjelaskan lebih lanjut, hal ini menarik perhatian penulis pada skenario di mana pria yang dikenal

Jurnal Teknologi dan Informasi (JATI)
Volume 14 Nomor 2 Edisi September 2024
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v14i2

memiliki lebih banyak keterampilan keamanan siber dan memiliki responden penelitian terbanyak adalah mereka yang lebih mempengaruhi hasil temuan penulis. Skenario ini dan kesimpulan penulis didasarkan pada jawaban yang keluar dari survei yang dibahas dalam paragraf berikutnya. Sebagian besar jawaban menunjukkan bahwa mahasiswa tidak memperhatikan keamanan siber dan tidak memiliki keterampilan keamanan siber.

Perangkat komputasi *mobile* yang digunakan responden antara lain *smartphone* (100%), laptop (87,4%), dan tablet (2,8%). Perangkat ini dapat menimbulkan bahaya bagi individu dan perusahaan jika tidak digunakan dengan tepat. Mereka digunakan untuk *Short Message Service* (SMS) dan juga berisi informasi kontak dan *log* panggilan. Perangkat yang baru dibeli dapat memiliki kerentanan asli dalam sistem operasi yang perlu diperbarui. Sekali lagi, mereka bisa salah dikonfigurasi. Kesalahan konfigurasi kemudian menjadi kerentanan [21]. Oleh karena itu, *Personal Identification Number* (PIN) atau *fingerprint* diperlukan untuk mengamankannya. Pengguna harus sadar untuk menghindari menjaga koneksi Wi-Fi diaktifkan sepanjang waktu. Juga, Wi-Fi rumah harus diamankan dan *firewall*, *Intrusion Detection Systems* (IDS), dan *Intrusion Prevetion Systems* (IPS) harus digunakan. Pengguna harus menghindari menjelajah situs yang tidak memiliki enkripsi.

Data dari survei penulis menunjukkan bahwa mahasiswa di Kota Batam tidak menyadari keamanan siber. Mereka ternyata hanya memiliki informasi dasar keamanan siber tetapi tidak memiliki keterampilan tingkat lanjut. Namun, pada penelitian [22] dan [23] mengakui bahwa pendidikan dan pelatihan keamanan siber dapat efektif untuk meningkatkan kesadaran. Dilain hal penelitian [24] mengatakan bahkan dosen perguruan tinggi yang seharusnya mengajar mahasiswa tentang keamanan siber memiliki pengetahuan yang rendah tentang topik tersebut. Kurangnya kesadaran keamanan siber berarti mahasiswa dapat menjadi korban kapan saja dan tidak dapat melakukan apapun untuk memulihkan situasi [25]. Karena tingkat kesadaran dan keterampilan mereka rendah, langkah-langkah yang diambil untuk melindungi diri mereka sendiri juga akan kurang [26]. Melihat Tabel 10 dimana 74,8% mengatakan mereka ‘netral’ bahwa ‘kata sandi harus diubah secara teratur’ mengungkapkan wawasan yang menarik tentang tingkat kesadaran keamanan siber mahasiswa. Ini menyiratkan bahwa mahasiswa tidak mengubah kata sandi mereka secara teratur dan karenanya kesimpulan yand didapatkan bahwa mereka tidak sadar akan keamanan siber. Kata sandi harus diubah secara teratur agar tidak ditebak oleh peretas. Mengubah kata sandi membantu mengusir penyusup dari akun pengguna jika akun tersebut disusupi tanpa sepengetahuan pengguna. Tetapi hasilnya menunjukkan bahwa mahasiswa tidak mengubah kata sandi mereka secara teratur.

Semua sistem operasi menawarkan pembaruan secara teratur untuk menjaga keamanan. *Windows*, yang merupakan sistem operasi yang paling banyak digunakan, misalnya, memungkinkan pembaruan otomatis [27]. Semua sistem operasi memiliki mode pengguna dan mode kernel [28]. Mode pengguna dan kernel memiliki driver yang perlu diperbarui seiring waktu. Menurut hasil temuan, 11 mahasiswa tidak menerapkan pembaruan dan 6 pembaruan terabaikan. Ini berarti mereka tetap menggunakan versi lama dengan kerentanan. Menggunakan sistem operasi lama yang rentan karena mahasiswa tidak menyadari bahaya yang dapat ditimbulkan pada perangkat mereka. Para mahasiswa tidak tahu bagaimana sistem operasi bekerja. Kurangnya keterampilan dan pengetahuan inilah yang penulis anggap naif terhadap masalah keamanan siber. Sebagian besar mahasiswa mungkin berpikir mereka tidak memiliki dokumen penting di perangkat mereka yang dapat mengakibatkan kerugian besar sehingga tidak perlu menjaga keamanan. Jika faktanya, beberapa bahkan mungkin meragukan bahwa peretas tidak dapat menemukan atau mendapatkan akses ke perangkat mereka.

Temuan menarik lainnya adalah persentase mahasiswa yang lebih tinggi menjawab bahwa ‘mereka menggunakan kata sandi yang digunakan sebelumnya’, ‘satu kata sandi yang kuat digunakan di banyak akun yang berbeda’, dan ‘itu menjengkelkan untuk memiliki kata sandi yang panjang dan kuat untuk setiap akun.’ Temuan ini berarti jika satu kata sandi yang kuat disusupi, akun lain juga dapat terpengaruh. Juga, kata sandi yang digunakan sebelumnya yang mungkin telah disusupi atau sudah diketahui dapat menyebabkan intrusi [29]. Tidak heran *Amnesty International* mencatat jumlah mahasiswa yang lebih banyak telah diretas dan diintimidasi karena menyuarakan ketidakadilan sosial di Indonesia. Hal ini sangat mungkin karena mahasiswa ingin menggunakan satu kata sandi dan kata sandi pendek atau lemah untuk mengurangi energi yang digunakan untuk login ke akun mereka. Dalam upaya untuk menggunakan kata sandi yang mudah, sebagian besar mahasiswa menggunakan informasi pribadi yang mudah dimasukkan tetapi juga mudah diperoleh oleh peretas menggunakan rekayasa sosial [30]. Kata sandi adalah metode otentikasi yang penting dan hanya mereka yang tidak mengetahui keamanan siber yang akan menggunakan kata sandi yang lemah, lama, dan kedaluwarsa.

Pada masalah keamanan *browser*, mahasiswa menunjukkan tingkat pengetahuan dan keterampilan yang tinggi kecuali pengaturan dan konfigurasi *browser*. Menurut *'The Global Statistics'*, *Chrome*, *Safari*, dan *Firefox* adalah tiga *browser* teratas yang digunakan di Indonesia [31]. Situs *web* lain *'We Are Social'* menyatakan bahwa mahasiswa menggunakan *browser* chrome untuk mencari 'menerjemahkan' ketika mereka perlu menerjemahkan ke dalam kata-kata ke dalam bahasa Inggris dan itu menjelaskan mengapa *Google*

Jurnal Teknologi dan Informasi (JATI)
Volume 14 Nomor 2 Edisi September 2024
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v14i2

banyak digunakan di Indonesia. Mengambil *Google Chrome* misalnya, lebih banyak yang bisa dilakukan tentang isi otomatis dan kata sandi, privasi dan keamanan, kinerja, penampilan, bahasa, unduhan, dan ekstensi dalam pengaturan [32]. Semua ini adalah pengaturan dan konfigurasi penting yang akan meningkatkan keamanan. Mahasiswa 'netral' tentang pengaturan dimana akun dapat dikelola untuk mengetahui 'berapa banyak perangkat yang saat ini masuk', dan otentikasi dua faktor. Implikasi dari mahasiswa yang tidak mengetahui bagaimana *browser* dapat dikonfigurasi dengan aman adalah bahwa mereka tidak memiliki keterampilan keamanan dan menggunakan *browser* bagaimanapun juga yang tidak memenuhi standar keamanan siber.

Aspek lain dari Keamanan siber adalah penggunaan layanan VPN. Ada banyak layanan VPN gratis yang tersedia saat ini, dan karena pemasaran oleh influencer, VPN dipandang sebagai "pembuka blokir konten" daripada langkah-langkah keamanan tambahan. Layanan VPN terutama digunakan untuk menutupi kehadiran pengguna di internet sehingga pengumpulan data berbahaya dapat dicegah dan sebagian besar layanan VPN tepercaya dibayar untuk menjaga kualitas layanan VPN yang baik. Layanan VPN gratis menawarkan beberapa kemiripan keamanan tetapi ada lebih banyak risiko. Untuk menghasilkan pendapatan, VPN gratis ini sering mengandalkan iklan, tetapi kebanyakan dari mereka mengumpulkan data secara pribadi dan menjualnya kepada penawar tertinggi. Beberapa layanan VPN bahkan merupakan malware langsung. Namun, layanan ini masih dicari karena kemampuannya untuk menyediakan akses ke konten yang biasanya diblokir oleh Internet Indonesia.

DataReportal menyatakan bahwa 60,4% penduduk Indonesia (167 juta orang) menggunakan media sosial. Dengan jumlah orang yang menggunakan media sosial yang sangat besar ini, Indonesia adalah salah satu negara dengan peringkat diantara negara-negara dengan jumlah pengguna media sosial yang tinggi [33]. Sementara itu, penetrasi di Indonesia pada 2023 sebesar 77%. Peretas merasa mudah menemukan data sensitif di media sosial karena orang memposting hampir setiap hari [34]. Orang-orang selalu ingin menunjukkan semisal mobil, rumah mewah, gaun, dan bahkan foto seremonial yang baru mereka beli. Semua ini adalah data yang dapat digunakan oleh peretas untuk mengeksploitasi pengguna media sosial. Hasil penelitian menunjukkan bahwa 74,4% responden memposting foto pribadi, 72,5% menerima permintaan pertemanan dari orang yang tidak dikenal, dan 68,7% juga berbagi informasi sensitif seperti tanggal lahir, status pekerjaan, status perkawinan, dan bahkan sertifikat pendidikan. Sebagian besar mahasiswa membanggakan jumlah pengikut di *platform* media sosial dan tidak peduli untuk mengetahui siapa pengikut itu. Anak muda menjadi target karena mereka menyukai media sosial [35].

Sangat penting untuk tetap mendapatkan informasi terbaru tentang ancaman dan tren keamanan siber terbaru karena lanskap berkembang pesat. Organisasi dan individu sama-sama harus berusaha keras untuk mengadopsi langkah-langkah keamanan proaktif, tetap mendapat informasi tentang ancaman yang muncul, dan mengadopsi pola pikir keamanan siber untuk mengurangi risiko secara efektif. Melindungi data dan informasi seseorang terutama yang sensitif seperti detail pribadi, informasi keuangan, kekayaan intelektual, dan privasi sangat penting untuk melindungi dari ancaman dunia maya. Kepercayaan, reputasi, dan pengaruh menjadi sifat mahal untuk dipertahankan dalam lanskap digital, terutama dengan penggunaan teknologi yang jahat seperti *deep-fake*, *phishing*, dan ancaman lainnya. Kesadaran dan pemahaman terhadap ancaman yang tak terlihat namun berdampak ini harus dikembangkan di semua aspek masyarakat, terutama di lembaga pendidikan dan pendidikan tinggi.

4. Kesimpulan

Menyadari keamanan siber sangat penting bagi semua orang. Penggunaan teknik canggih ancaman siber dan perangkat lunak berbahaya seperti *virus*, *worm* dan *ss* terus meningkat. Semakin banyak orang sadar, semakin mereka bisa menentangnya. Berdasarkan hasil respon yang penulis dapatkan dan nilai semua tes yang dilakukan, dapat disimpulkan bahwa mahasiswa di Kota Batam mempunyai tingkat kesadaran keamanan siber yang rendah karena 11 mahasiswa tidak menerapkan pembaruan perangkat lunak dan 6 mengabaikan pembaruan perangkat lunak. Selain itu, 75,3% mahasiswa menggunakan kata sandi yang digunakan sebelumnya, 74% menggunakan satu kata sandi yang kuat untuk akun yang berbeda dan 78,5% mengatakan itu menjengkelkan untuk memiliki kata sandi yang panjang dan kuat untuk setiap akun. Terakhir, 73,3% berbagi lokasi saat ini secara publik di media sosial dan 68,7% berbagi informasi pribadi yang sensitif. Para mahasiswa hanya memiliki keterampilan dasar dalam keamanan siber. Oleh karena itu disarankan bahwa institusi pendidikan harus memasukkan keamanan siber dalam kurikulum untuk setiap departemen karena semua mahasiswa menggunakan perangkat digital. Juga, beberapa mahasiswa akan menggunakan komputer di sebuah perusahaan suatu hari nanti. Sebagian besar insiden keamanan terjadi di kampus karena mahasiswa berpikir hanya mahasiswa ilmu komputer yang perlu tahu tentang keamanan siber. Ide ini meningkatkan risiko mahasiswa jatuh ke dalam perangkap peretas. Lembaga harus menyelenggarakan lebih banyak seminar tentang keamanan sehingga mahasiswa dapat diperbarui tentang masalah keamanan.

Daftar Pustaka

[1] F. Suwana, A. Pramiyanti, I. D. Mayangsari, R. Nuraeni, and Y. Firdaus, "Digital Media Use of Generation Z During Covid-19 Pandemic," *Jurnal Sosioteknologi*, vol. 19, no. 3, pp. 327–340, 2020, doi: 10.5614/sostek.itbj.2020.19.3.2.

[2] A. Pratamasari, "Cybersecurity and Custom Regulations as Trade Barriers in ASEAN E-Commerce: Case of Indonesian C-Commerce," *Jurnal Global & Strategis*, vol. 14, no. 1, p. 1, 2020, doi: 10.20473/jgs.14.1.2020.1-16.

[3] E. Syarief, "Security Concerns in Digital Transformation of Electronic Land Registration: Legal Protection in Cybersecurity Laws in Indonesia," *International Journal of Cyber Criminology*, vol. 16, no. 2, pp. 32–46, 2022, doi: 10.5281/zenodo.4766565.

[4] I. Ali, "Examining Cyber Security Implementation Through TLS/SSL on Academic Institutional Repository in Indonesia," *Berkala Ilmu Perpustakaan dan Informasi*, vol. 17, no. 2, pp. 238–249, 2021, doi: 10.22146/bip.v17i2.2082.

[5] F. Aferudin and K. Ramli, "The Development of Cybersecurity Information Sharing Framework for National Critical Information Infrastructure in Indonesia," *Budapest International Research and Critics Institute (BIRCI-Journal)*, vol. 5, no. August 2023, pp. 22859–22872, 2022, doi: 10.33258/birci.v5i3.6297.

[6] S. S. Aulianisa and Indirwan, "Critical Review of The Urgency of Strenghthening The Implementation of Cyber Security and Resilience in Indonesia," *Lesrev (Lex Scientia Law Review)*, vol. 4, no. 1, pp. 33–48, 2020, doi: 10.15294/lesrev.v4i1.38197.

[7] F. O. Catak, A. F. Yazi, O. Elezaj, and J. Ahmed, "Deep Learning Based Sequential Model for Malware Analysis Using Windows exe API Calls," *PeerJ Computer Science*, vol. 6, no. 2020, pp. 1–23, 2020, doi: 10.7717/PEERJ-CS.285.

[8] A. Kovacevic, N. Putnik, and O. Toskovic, "Factors Related to Cyber Security Behavior," *IEEE Access*, vol. 8, no. 2020, pp. 125140–125148, 2020, doi: 10.1109/ACCESS.2020.3007867.

[9] M. Salehudin, Z. Zulherman, A. Arifin, and D. Napitupulu, "Extending Indonesia Government Policy for E-Learning and Social Media Usage," *Pegem Journal of Education and Instruction*, vol. 11, no. 2, pp. 14–26, 2021, doi: 10.14527/pegegog.2021.00.

[10] M. Khader, M. Karam, and H. Fares, "Cybersecurity Awareness Framework for Academia," *Information (Switzerland)*, vol. 12, no. 10, pp. 1–20, 2021, doi: 10.3390/info12100417.

[11] B. Dash, M. F. Ansari, P. Sharma, and A. Ali, "Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review," *International Journal of Software Engineering & Applications*, vol. 13, no. 5, pp. 13–21, 2022, doi: 10.5121/ijsea.2022.13502.

[12] T. Alharbi and A. Tassaddiq, "Assessment of Cybersecurity Awareness among Students of Majmaah University," *Big Data and Cognitive Computing*, vol. 5, no. 2, pp. 1–15, 2021, doi: /10.3390/bdcc5020023.

[13] A. M. Adam, "Sample Size Determination in Survey Research," *Journal of Scientific Research and Reports*, vol. 26, no. 5, pp. 90–97, 2020, doi: 10.9734/jsrr/2020/v26i530263.

[14] T. Muhammad, "Integrative Cybersecurity: Merging Zero Trust, Layered Defense, and Global Standards for a Resilient Digital Future," *International Journal of Computer Science and Technology (IJCST)*, vol. 1, no. 4, pp. 99–135, 2017, [Online]. Available: https://www.ijcst.com/

[15] P. Limna, T. Kraiwanit, and S. Siripipattanakul, "The Relationship Between Cyber Security Knowledge, Awareness and Behavioural Choice Protection Among Mobile Banking Users in Thailand," *International Journal of Computing Sciences Research*, vol. 7, no. August 21, pp. 1133–1151, 2023, doi: 10.25147/ijcsr.2017.001.1.123.

[16] E. Löffler, B. Schneider, P. M. Asprion, and T. Zanwar, "CySecEscape 2.0-A Virtual Escape Room to Raise Cybersecurity Awareness," *International Journal of Serious Games*, vol. 8, no. 1, pp. 59–70, 2021, doi: 10.17083/ijsg.v8i1.413.

[17] A. A. Garba, M. M. Siraj, and S. H. Othman, "An Assessment of Cybersecurity Awareness Level Among Northeastern University students in Nigeria," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 1, pp. 572–584, 2022, doi: 10.11591/ijece.v12i1.pp572-584.

[18] L. Bottyán, "Cybersecurity Awareness Among University Students.," *Journal of Applied Technical and Educational Sciences*, vol. 13, no. 3, pp. 1–11, 2023, doi: https://doi.org/10.24368/jates363.

[19] A. Setiawan, S. Wirawan, H. Djajakerta, and H. Haryanto, "Student's Cybersecurity Awareness in Post Covid-19 Pandemic," *Journal of Economics, Finance and Management Studies*, vol. 06, no. 10, pp. 5057–5066, 2023, doi: 10.47191/jefms/v6-i10-38.

[20] K. Matyokurehwa, N. Rudhumbu, C. Gombiro, and C. Mlambo, "Cybersecurity Awareness in Zimbabwean Universities: Perspectives from the Students," *Security and Privacy*, vol. 4, no. 2, pp. 1–

11, 2021, doi: 10.1002/spy2.141.
[21] P. Stockle, B. Grobauer, and A. Pretschner, "Automated Implementation of Windows-related Security-Configuration Guides," *International Conference on Automated Software Engineering*, vol. 20, no. 2020, pp. 598–610, 2020, doi: 10.1145/3324884.3416540.
[22] A. A. Al Shamsi, "Effectiveness of Cyber Security Awareness Program for Young Children: A Case Study in UAE Effectiveness of Cyber Security Awareness Program for Young Children View Project Sentiment Analysis for Arabic Dialects View project Effectiveness of Cyber Security," *International Journal of Information Technology and Language Studies (IJITLS)*, vol. 3, no. 2, pp. 8–29, 2019, doi: 10.13140/RG.2.2.28488.14083.
[23] M. P. Aphane, "Cybersecurity Awareness on Cybercrime Among the Youth in Gauteng Province," *International Journal of Social Science Research and Review*, vol. 6, no. 8, pp. 23–32, 2023, doi: 10.47814/ijssrr.v6i8.1414.
[24] H. İ. Haseski, "Cyber Security Skills of Pre-service Teachers as a Factor in Computer-assisted Education," *International Journal of Research in Education and Science*, vol. 6, no. 3, pp. 484–500, 2020, doi: 10.46328/ijres.v1i1.1006.
[25] M. F. Ansari, "A Quantitative Study of Risk Scores and the Effectiveness of AI-Based Cybersecurity Awareness Training Programs," *International Journal of Smart Sensor and Adhoc Network*, vol. 3, no. 3, pp. 1–8, 2022, doi: 10.47893/ijssan.2022.1212.
[26] S. A. Pitchay, A. S. Suhaimi, N. Hayaati, and M. Alwi, "Enhancing Cyber-attacks Awareness via Mobile Gamification Techniques," *International Journal of Advanced Research in Technology and Innovation*, vol. 4, no. 2, pp. 69–84, 2022, doi: 10.55057/ijarti.2022.4.2.8.
[27] K. Umaima, "Comparative Study Of Linux and Windows," *International Journal of Academic Research*, vol. 2, no. 2, pp. 53–70, 2020, doi: 10.5281/zenodo.3692081.
[28] M. Kulkarni, "Analysis of Process Structure in Windows Operating System," *International Research Journal of Engineering and Technology*, vol. 7, no. 6, pp. 1–5, 2020. [Online]. Available: https://www.irjet.net/archives/V7/i6/IRJET-V7I601.pdf
[29] N. Tosun *et al.*, "A SWOT Analysis to Raise Awareness about Cyber Security and Proper Use of Social Media: Istanbul Sample," *International Journal of Curriculum and Instruction*, vol. 12, pp. 271–294, 2020, [Online]. Available: https://ijci.globets.org/index.php/IJCI/article/view/327
[30] F. Abu-Amara, R. Almansoori, S. Alharbi, M. Alharbi, and A. Alshehhi, "A Novel SETA-based Gamification Framework to Raise Cybersecurity Awareness," *International Journal of Information Technology (Singapore)*, vol. 13, no. 6, pp. 2371–2380, 2021, doi: 10.1007/s41870-021-00760-5.
[31] D. M. Rayman, A. Asmawi, N. Afiza, and M. Ariffin, "WBEC : A Web Browsers Evidence Collection Toolkit for Web Browsers Usage in Windows 10," *International Journal of Technology Management and Information System (IJTMIS)*, vol. 4, no. 1, pp. 1–15, 2022, [Online]. Available: https://myjms.mohe.gov.my/index.php/ijtmis/article/view/17664
[32] B. Hu, E. Gunnell, and Y. Sun, "Smart Tab Predictor: A Chrome Extension to Assist Browser Task Management using Machine Learning and Data Analysis," *International Journal of Information Technology (IJIT)*, vol. 1, no. 6, pp. 227–240, 2021, doi: 10.5121/csit.2021.112318.
[33] L. F. Lina, "Privacy Concerns in Personalized Advertising Effectiveness on Social Media," *Sriwijaya International Journal of Dynamic Economics and Business*, vol. 1, no. 2, p. 147, 2021, doi: 10.29259/sijdeb.v1i2.147-156.
[34] L. Jiang, A. Jayatilaka, M. Nasim, M. Grobler, M. Zahedi, and M. A. Babar, "Systematic Literature Review on Cyber Situational Awareness Visualizations," *IEEE Access*, vol. 10, no. 26, pp. 57525–57554, 2022, doi: 10.1109/ACCESS.2022.3178195.
[35] H. Irfan, K. J. Akhter, and R. Shakeel, "Cybersecurity and Multidisciplinary Students: A Survey," *International Journal of Science and Engineering Research*, vol. 11, no. 4, pp. 1786–1791, 2020, [Online]. Available: https://www.ijser.org/researchpaper/Cybersecurity-and-Multidisciplinary-Students-A-Survey.pdf