

**PENGARUH KESADARAN KEAMANAN SIBER,
PENGUNAAN GADGET, DAN ANCAMAN
DIGITAL TERHADAP KEAMANAN
SIBER**
(Survei Pada Pelaku Umkm Bidang Kuliner Yang Terdigitalisasi Di
Kecamatan Alang-Alang Lebar Kota Palembang)

Skripsi



**Nama : Muhammad Zulfikri
NIM : 222022043**

**FAKULTAS EKONOMI DAN BISNIS
UNIVERSITAS MUHAMMADIYAH PALEMBANG
2026**

Skripsi

**PENGARUH KESADARAN KEAMANAN SIBER,
PENGUNAAN GADGET, DAN ANCAMAN
DIGITAL TERHADAP KEAMANAN
SIBER**

**(Survei Pada Pelaku Umkm Bidang Kuliner Yang Terdigitalisasi Di
Kecamatan Alang-Alang Lebar Kota Palembang)**

**Untuk Memenuhi Salah Satu Persyaratan
Memperoleh Gelar Sarjana Akuntansi**



**Nama : Muhammad Zulfikri
NIM : 222022043**

**FAKULTAS EKONOMI DAN BISNIS
UNIVERSITAS MUHAMMADIYAH PALEMBANG
2026**

PERNYATAAN BEBAS PLAGIAT

Saya yang bertanda tangan dibawah ini:

Nama : Muhammad Zulfikri
NIM : 222022043
Fakultas : Ekonomi dan Bisnis
Program Studi : Akuntansi
Konsentrasi : Audit
Mata Kuliah : Sistem Informasi Akuntansi
Judul Skripsi : Pengaruh Kesadaran Keamanan Siber, Penggunaan Gadget, dan Ancaman Digital Terhadap Keamanan Siber (Survei Pada Pelaku Umkm Bidang Kuliner Yang Terdigitalisasi di Kecamatan Alang-Alang Lebar Kota Palembang)

Dengan ini saya menyatakan:

1. Karya tulis ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik serjana strata satu baik di Universitas Muhammadiyah Palembang maupun di perguruan tinggi lainnya.
2. Karya tulisan ini murni gagasan, rumusan, dan penelitian saya sendiri tanpa bantuan pihak lain kecuali arahan pembimbing.
3. Dalam karya tulis ini terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar Pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila dikemudian hari terdapat penyimpangan dan tidak benaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang diperoleh karena karya ini serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi ini.

Palembang, Mei 2026



Muhammad Zulfikri

Fakultas Ekonomi Dan Bisnis
Universitas Muhammadiyah
Palembang

TANDA PENGESAHAN SKRIPSI

Judul : Pengaruh Kesadaran Keamanan Siber, Penggunaan Gadget, dan Ancaman Digital Terhadap Keamanan Siber (Survei Pada Pelaku UMKM Bidang Kuliner Yang Terdigitalisasi di Kecamatan Alang-Alang Lebar Kota Palembang).

Nama : Muhammad Zulfikri
Nim : 222022043
Fakultas : Ekonomi dan Bisnis
Program Studi : Akuntansi
Konsentrasi : Audit
Mata Kuliah : Sistem Informasi Akuntansi

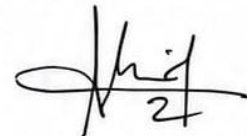
Diterima dan Disahkan
Pada, Mei 2026

Pembimbing I,



Dr. Hj. Yuhanis Ladewi, S.E., M.Si., Ak., CA., CATr., CIAS
NIDN/NBM : 0226016901/765380

Pembimbing II,



Anggrelia Afrida, S.E., M.Si.
NIDN/NBM: 0218048403/1187168

Mengetahui,
Dekan
Ketua Program Studi Akuntansi



Aprianto, S.E., M.Si.

NIDN/NBM: 02160087201/ 859190

MOTTO DAN PERSEMBAHAN

Motto:

“Dan bahwa manusia hanya memperoleh apa yang telah diusahakannya, dan sesungguhnya usahanya itu kelak akan diperlihatkan (kepadanya), kemudian akan diberi balasan kepadanya dengan balasan yang paling sempurna.”

(QS. An-Najm: 39–41)

Skripsi ini saya persembahkan kepada:

- ❖ **Orang Tuaku**
- ❖ **Adik-adikku**
- ❖ **Keluarga, dan**
- ❖ **Almamater**

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

PRAKATA

Assalamualaikum Warahmatullahi Wabarakatuh

Allahamdulillahi rabbil'alaamiin, segala puji bagi Allah SWT yang telah melimpahkan rahmat, ridho dan karunia-Nya. Sholawat dan salam selalu tercurahkan kepada junjungan Nabi Muhammad SAW sehingga penulis dapat menyelesaikan skripsi dengan judul **“Pengaruh Kesadaran Keamanan Siber, Penggunaan Gadget, dan Ancaman Digital terhadap Keamanan Siber”** telah selesai sesuai dengan waktu yang telah direncanakan. Skripsi ini disusun untuk memenuhi syarat memperoleh gelar Sarjana Akuntansi pada Program Strata Satu Fakultas Ekonomi dan Bisnis Universitas Muhammadiyah Palembang.

Penulis menyadari bahwa proses penulisan skripsi ini masih banyak mengalami kendala, namun berkat bantuan, bimbingan, dan kerjasama dari berbagai pihak serta berkah dan karunia dari Allah SWT sehingga kendala-kendala tersebut dapat diatasi sebagaimana mestinya. Penulis menyampaikan ribuan terimakasih dan penghargaan setinggi-tingginya, khususnya kepada kedua orangtua, Ayahanda Yulisman, Ibunda Emi dan keluarga besar penulis yang selalu mendoakan dan memberikan dukungan dan kesuksesan penulis. Penulis juga mengucapkan terima kasih kepada dosen pembimbing I Ibu Dr. Yuhanis Ladewi, S.E., M.Si., Ak., CA., CATr., CIAS dan dosen pembimbing II Ibu Anggrelia Afrida, S.E., M.Si. yang telah sabar, tekun, tulus serta dengan ikhlas meluangkan waktu, tenaga, pikiran serta memberikan bimbingan dan motivasi yang membangun semangat penulis selama menyusun skripsi. Selain itu, disampaikan juga ucapan

terima kasih kepada pihak-pihak yang telah mengizinkan dan membantu penulis menyelesaikan studi di Fakultas Ekonomi dan Bisnis Universitas Muhammadiyah Palembang, kepada yang terhormat:

1. Bapak Prof. Dr. H. Abid Djazuli, S.E., M.M selaku Rektor Universitas Muhammadiyah Palembang.
2. Bapak Dr. Yudha Mahrom DS, S.E., M.Si selaku Dekan Fakultas Ekonomi dan Bisnis Universitas Muhammadiyah Palembang.
3. Bapak Aprianto, S.E., M.Si dan Ibu Fenty Astrina, S.E., M.Si selaku Ketua dan Sekretaris Program Studi Akuntansi Fakultas Ekonomi dan Bisnis Universitas Muhammadiyah Palembang.
4. Bapak Muhammad Fahmi, S.E., M.Si.,ACPA selaku Dosen Pembimbing Akademik penulis di Program Studi Akuntansi Fakultas Ekonomi dan Bisnis Universitas Muhammadiyah Palembang.
5. Seluruh bapak dan ibu Dosen yang telah membekali ilmu sehingga pengetahuan penulis semakin bertambah, serta staff dan karyawan Fakultas Ekonomi dan Bisnis Universitas Muhammadiyah Palembang.
6. Bapak dan ibu yang telah memberikan izin untuk melakukan penelitian di Dinas Koperasi dan UKM Kota Palembang.
7. Ketiga adik-adikku ”Vitria, Salsa, dan Gilang” atas dukungan, kebersamaan, serta semangat yang selalu diberikan dalam setiap langkah perjalanan ini.
8. Sahabat seperjuangan dengan NIM 005,044,007 dan teman- teman yang tidak bisa disebutkan satu persatu, serta semua pihak yang terlibat dalam penulisan skripsi ini yang tidak bisa penulis sebutkan semuanya.

Semoga Allah SWT membalas kebaikan kalian semua atas terselesainya penulisan skripsi ini. Penulis menyadari dengan segala keterbatasan yang ada dalam penyusunan skripsi ini terdapat bannyak kekurangan dan kesalahan. Oleh karena itu, kritik dan saran yang bersifat membangun sangat diharapkan sehingga laporan ini bisa terselesaikan dan berjalan dengan baik serta lebih bermanfaat. Semoga skripsi ini dapat berguna dan memberikan manfaat untuk pembacanya.

Palembang, Maret 2026
Penulis

Muhammad Zulfikri

DAFTAR ISI

HALAMAN SAMPUL	
HALAMAN JUDUL	ii
PERNYATAAN BEBAS PLAGIAT	iii
HALAMAN PENGESAHAN SKRIPSI	iv
MOTTO DAN PERSEMBAHAN	v
PRAKATA	vi
DAFTAR ISI	ix
DAFTAR TABEL	xi
DAFTAR GAMBAR	xiii
ABSTRAK	xiv
ABSTRACT	xv
BAB I PENDAHULUAN	
A. Latar Belakang Masalah.....	1
B. Rumusan Masalah	10
C. Tujuan Penelitian.....	10
D. Manfaat Penelitian.....	11
BAB II KAJIAN PUSTAKA, KERANGKA PEMIKIRAN DAN HIPOTESIS.	
A. Kajian Pustaka.....	12
1. Kesadaran Keamanan Siber.....	12
a. Pengertian Kesadaran Keamanan Siber.....	12
b. Pengukuran Kesadaran Keamanan Siber.....	13
2. Penggunaan Gadget.....	15
a. Pengertian Penggunaan Gadget	15
b. Pengukuran Penggunaan Gadget	17
3. Ancaman Digital.....	18
a. Pengertian Ancaman Digital	18
b. Pengukuran Ancaman Digital	19
4. Keamanan Siber.....	22

a. Pengertian Keamanan Siber.....	22
b. Pengukuran Keamanan Siber.....	23
B. Kerangka Pemikiran.....	27
1. Pengaruh Kesadaran Keamanan Siber Terhadap Keamanan Siber	26
2. Pengaruh Penggunaan Gadget Terhadap Keamanan Siber.....	28
3. Pengaruh Ancaman Digital Terhadap Keamanan Siber	30
C. Hipotesis.....	35
BAB III METODOLOGI PENELITIAN	36
A. Jenis Penelitian.....	36
B. Lokasi Penelitian.....	37
C. Operasionalisasi Variabel	37
D. Populasi dan Sampel	38
1. Populasi	38
2. Sampel.....	39
E. Jenis Data	41
F. Teknik Pengumpulan Data	42
G. Pengujian Data	44
1. Uji Validitas	44
2. Uji Reliabilitas.....	44
H. Analisis Data dan Teknik Analisis.....	45
1. Teknik Analisis Data Secara Statistik Deskriptif.....	45
2. Teknik Analisis Secara Analisis Statistik Inferensial	45
BAB IV HASIL PENELITIAN DAN PEMBAHASAN	50
A. Hasil Penelitian	50
1. Tingkat Pengembalian Kuesioner	50
2. Profil Responden.....	51
3. Hasil Pengujian Data.....	51
a. Uji Validitas	52
b. Uji Reliabilitas	55
4. Teknik Analisis	56
a. Analisis Statistik Deskriptif.....	56

b. Analisis Statistik Inferensial	63
B. Pembahasan Penelitian	
1. Pengaruh kesadaran keamanan siber terhadap keamanan siber.....	70
2. Pengaruh penggunaan gadget akuntansi terhadap keamanan siber ..	73
3. Pengaruh ancaman digital terhadap keamanan siber	75
BAB V KESIMPULAN DAN SARAN	
A. Kesimpulan.....	79
B. Saran	80
DAFTAR PUSTAKA.....	81

DAFTAR TABEL

Tabel I.1 Survei Pendahuluan	7
Tabel III.1 Lokasi Penelitian	37
Tabel III.2 Operasional Variabel	37
Tabel III.3 Daftar UMKM dan Jumlah Responden.....	39
Tabel IV.1 Tingkat Pengembalian Kuesioner	52
Tabel IV.2 Profil Responden	53
Tabel IV.3 Hasil Uji Validitas Kesadaran Keamanan Siber	54
Tabel IV.4 Hasil Uji Validitas Penggunaan Gadget.....	55
Tabel IV.5 Hasil Uji Validitas Ancaman Digital	56
Tabel IV.6 Hasil Uji Validitas Keamanan Siber	56
Tabel IV.7 Hasil Uji Reliabilitas	57
Tabel IV.8 Kriteria Statistik Deskriptif Per Variabel.....	59
Tabel IV.9 Hasil Deskriptif Per Variabel	59
Tabel IV.10 Kriteria Statistik Deskriptif Per Indikator	60
Tabel IV.11 Hasil Deskriptif Indikator Pengetahuan.....	60
Tabel IV.12 Hasil Deskriptif Indikator Sikap.....	61
Tabel IV.13 Hasil Deskriptif Indikator Perilaku.....	61
Tabel IV.14 Hasil Deskriptif Indikator Kegunaan Yang Dirasakan	62
Tabel IV.15 Hasil Deskriptif Indikator Kemudahan Penggunaa	62
Tabel IV.16 Hasil Deskriptif Indikator <i>Malware</i>	63
Tabel IV.17 Hasil Deskriptif Indikator <i>Phishing</i>	63
Tabel IV. 18 Hasil Deskriptif Indikator <i>Ransomware</i>	64
Tabel IV.19 Deskriptif Indikator Serangan Denial Of Service (DoS/DdoS).....	64
Tabel IV.20 Hasil Deskriptif Indikator Man In The Middle.....	64
Tabel IV.21 Hasil Deskriptif Indikator Kerahasiaan	65
Tabel IV.22 Deskriptif Indikator Keasliah	65
Tabel IV.23 Hasil Deskriptif Indikator Ketersediaan	66
Tabel IV.24 Hasil Uji Normalitas	83
Tabel IV.25 Hasil Uji Multikolineritas	84

Tabel IV.26 Hasil Uji Heterokedatisitas Metode Uji Glejser	85
Tabel IV.27 Hasil Uji Regresi Linier Berganda	88
Tabel IV.28 Koefien Determinasi.....	89
Tabel IV.29 Hasil Uji Hipotesis (Uji T)	89

DAFTAR GAMBAR

Gambar II.1 Kerangka Pemikiran	34
Gambar Model Hasil Penelitian IV.1	67

DAFTAR LAMPIRAN

- Lampiran 1 : Kuesioner Penelitian
- Lampiran 2 : Hasil Kuesioner
- Lampiran 3 : Tabel R
- Lampiran 4 : Tabel T
- Lampiran 5 : Hasil Output SPSS
- Lampiran 6 : Fotokopi Sertifikat *Workshop* Audit Forensik
- Lampiran 7 : Fotokopi Sertifikat Pengantar Aplikasi Komputer
- Lampiran 8 : Fotokopi *Certified Fundamental Internal Audit*
- Lampiran 9 : Fotokopi *Certified Senior Activity Based Costing* (CSABC)
- Lampiran 10 : Fotokopi *Certified Professional Fraud Investigator* (CPFI)
- Lampiran 11 : Fotokopi Sertifikat Membaca Dan Menghafal Al-Quran
- Lampiran 12 : Fotokopi Sertifikat Computer Akuntansi
- Lampiran 13 : Fotokopi Sertifikat Aplikasi Manajemen Sitasi Dan SPSS
- Lampiran 14 : Fotokopi Aktivitas Bimbingan Skripsi
- Lampiran 15 : Fotokopi Surat Keterangan Riset Dari Tempat Penelitian
- Lampiran 16 : Surat Ketereangan BPP
- Lampiran 17 : Lembar Persetujuan Perbaiki Skripsi
- Lampiran 18 : Fotokopi Plagiarisme
- Lampiran 19 : Bio Data

ABSTRAK

Muhammad Zulfikri / 222022043 / Pengaruh Kesadaran Keamanan Siber, Penggunaan Gadget, dan Ancaman Digital Terhadap Keamanan Siber (Survei Pada Pelaku UMKM Bidang Kuliner Yang Terdigitalisasi di Kecamatan Alang-Alang Lebar Kota Palembang).

Penelitian ini bertujuan untuk mengetahui dan menganalisis secara parsial pengaruh kesadaran keamanan siber, penggunaan gadget, dan ancaman digital terhadap keamanan siber pada pelaku UMKM bidang kuliner yang terdigitalisasi di Kecamatan Alang-Alang Lebar Kota Palembang. Penelitian ini menggunakan penelitian asosiatif dan deskriptif. Populasi dalam penelitian ini terdiri dari 117 UMKM bidang kuliner yang terdigitalisasi di 4 kelurahan kecamatan alang-alang lebar kota Palembang, dengan teknik pengambilan sampel menggunakan metode sampel jenuh. Data yang digunakan adalah data primer dan data sekunder. Teknik pengumpulan data menggunakan kuesioner dan wawancara. Pengujian data menggunakan uji validitas, dan uji reliabilitas. Teknik analisis yang digunakan statistik deskriptif dan statistik inferensial (uji normalitas, uji multikolinieritas, dan uji heteroskedastisitas) dan analisis regresi linier berganda, uji koefisien determinasi (R^2) serta uji hipotesis (t). Teknik analisis pada penelitian ini menggunakan aplikasi SPSS versi 25. Hasil penelitian berdasarkan kuesioner yang kembali dan diolah sebanyak 87 menunjukkan bahwa semua variabel valid dan reliabel. Dari hasil analisis statistik deskriptif per variabel dan per indikator menunjukkan nilai dominannya tinggi. Pada hasil analisis statistik inferensial menunjukkan nilai residual normal, tidak terjadi multikolinieritas, dan heteroskedastisitas. Hasil uji regresi linear berganda menunjukkan bahwa kesadaran keamanan siber, penggunaan gadget dan ancaman digital mengalami peningkatan maka keamanan siber akan meningkat. Hasil uji t menunjukkan bahwa secara parsial kesadaran keamanan siber, penggunaan gadget, dan ancaman digital berpengaruh signifikan terhadap keamanan siber.

Kata Kunci: Kesadaran Keamanan Siber, Penggunaan Gadget, Ancaman Digital, Keamanan Siber, UMKM.

ABSTRACT

Muhammad Zulfikri / 222022043 / *The Influence of Cyber Security Awareness, Gadget Use, and Digital Threats on Cyber Security (Survey of Digitalized Culinary MSMEs in Alang-Alang Lebar District, Palembang City).*

This study aims to determine and partially analyze the influence of cybersecurity awareness, gadget use, and digital threats on cybersecurity among digitalized culinary MSMEs in Alang-Alang Lebar District, Palembang City. This study uses associative and descriptive research. The population in this study consists of 117 digitalized culinary MSMEs in 4 sub-districts of Alang-Alang Lebar District, Palembang City, with a sampling technique using the saturated sampling method. The data used are primary data and secondary data. Data collection techniques use questionnaires and interviews. Data testing uses validity tests and reliability tests. The analysis techniques used are descriptive statistics and inferential statistics (normality tests, multicollinearity tests, and heteroscedasticity tests) and multiple linear regression analysis, coefficient of determination (R²) tests and hypothesis (t) tests. The analysis technique in this study uses the SPSS version 25 application. The results of the study based on 87 returned and processed questionnaires show that all variables are valid and reliable. The descriptive statistical analysis results for each variable and indicator show a high dominant value. The inferential statistical analysis results show normal residual values, no multicollinearity, and no heteroscedasticity. The results of the multiple linear regression test indicate that as cybersecurity awareness, gadget use, and digital threats increase, cybersecurity will also increase. The t-test results indicate that partially, cybersecurity awareness, gadget use, and digital threats have a significant effect on cyber security.

keywords: *Cybersecurity Awareness, Gadget Usage, Digital Threats, Cybersecurity UMKM.*

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan teknologi digital merupakan peluang sekaligus tantangan yang mendorong terjadinya perubahan dalam berbagai aspek kehidupan. Perubahan tersebut terjadi mulai dari lingkup yang paling kecil, yaitu individu, hingga lingkup yang lebih luas seperti negara bahkan dunia. Kemajuan yang pesat di bidang teknologi dan informasi juga memberikan pengaruh yang signifikan terhadap berbagai komponen kehidupan, seperti ekonomi, politik, sosial, dan keamanan. Pada dasarnya, sifat ancaman dan keamanan bersifat dinamis. Hal ini menunjukkan bahwa isu mengenai ancaman dan keamanan tidak pernah sepenuhnya selesai untuk diperbincangkan, didiskusikan, maupun diperbarui seiring dengan perkembangan zaman (Rizky, 2022).

Pemanfaatan teknologi digital memungkinkan pelaku usaha untuk tetap terhubung dengan konsumen, menjangkau pasar yang lebih luas, serta meningkatkan pendapatan. Namun demikian, proses adaptasi digital juga memiliki berbagai risiko, di antaranya risiko siber seperti penipuan daring, peretasan, pemalsuan identitas, serta kebocoran data konsumen. Kejahatan siber tersebut dapat menimbulkan kerugian baik secara material maupun nonmaterial bagi pelaku usaha. Oleh karena itu, perhatian terhadap aspek keamanan siber tidak hanya penting bagi perusahaan besar yang beroperasi pada skala nasional maupun global, tetapi juga menjadi hal yang penting bagi pelaku usaha. Selain itu, kurangnya pemahaman mengenai keamanan siber juga dianggap sebagai

salah satu faktor utama yang menyebabkan masih banyak pelaku usaha rentan terhadap berbagai bentuk kejahatan di ruang siber. (Putri, Susilo, & Pramurindra, 2025)

Keamanan siber meliputi serangkaian praktik, teknologi, dan proses yang dirancang untuk melindungi sistem komputer, jaringan, perangkat, dan data dari ancaman yang dapat menyebabkan kerusakan, pencurian, atau akses tidak sah (Gunawan, 2025). Keamanan siber (*cyber security*) dapat diartikan sebagai tindakan untuk melindungi sistem informasi dan komunikasi dari serangan siber. (Istiningsih, et al., 2024). Untuk melihat seberapa kuat keamanan siber dapat diterapkan, beberapa aspek menjadi acuan pengukuran. Aspek tersebut antara lain kerahasiaan informasi, integritas atau keaslian data, dan ketersediaan sistem saat dibutuhkan. Ketiga aspek tersebut menggambarkan seberapa aman sebuah sistem dan bagaimana data dijaga dari potensi gangguan.

Keamanan siber dalam pemanfaatan teknologi tidak dapat berjalan secara optimal tanpa adanya kesadaran dari para penggunanya. Meskipun teknologi memberikan berbagai manfaat, khususnya bagi pelaku usaha, penggunaannya juga membawa berbagai risiko yang dapat mengancam keberlangsungan usaha. Risiko tersebut dapat berasal dari berbagai ancaman, seperti serangan dari *attacker*, *aktivitas spammer*, serta bentuk kejahatan siber lainnya yang terus mengalami peningkatan. Kejahatan siber (*cyber crime*) dapat menimbulkan dampak yang serius, di antaranya kerugian *finansial*, terganggunya sistem komputer, serta kerusakan atau penyalahgunaan informasi penting yang dapat mengancam integritas (*integrity*) dan kerahasiaan (*confidentiality*) jaringan.

Oleh karena itu, pemanfaatan teknologi perlu disertai dengan kesadaran terhadap kejahatan siber (*cyber crime awareness*), salah satunya melalui peningkatan perhatian terhadap keamanan siber dengan melakukan pengelolaan terhadap berbagai risiko ancaman digital. (Winarto & Bisma, 2021)

Menurut teori *protection motivation theory (PMT)*, keputusan seseorang untuk berperilaku aman secara digital dipengaruhi oleh persepsi risiko pengguna. Kesadaran keamanan siber pada karyawan yang memahami risiko dan sikap waspada memberikan kontribusi langsung terhadap perilaku keamanan siber dalam suatu organisasi (Yusnanto, 2025). Penggunaan gadget dapat meningkatkan risiko keamanan dan privasi data. Pengguna yang tidak memahami dalam penggunaan tersebut maka akan beresiko, dan jika pengguna yang memahami maka akan minim risiko yang timbul (Christofora K, 2023). Pengelolaan akses keamanan siber oleh karyawan yang baik, dengan menerapkan prinsip kewenangan dan pemantauan akses, dapat mengurangi potensi ancaman digital (J. Prayoga, et al., 2025).

Salah satu faktor yang mempengaruhi keamanan siber adalah kesadaran keamanan siber. Kesadaran keamanan siber mencerminkan kemampuan seseorang untuk memahami ancaman digital dan menerapkan perilaku yang aman dalam aktivitas sehari-hari. Kesadaran ini mencakup pemahaman mengenai risiko seperti *phishing* dan *malware* (Deni, 2024). Kesadaran juga meliputi tindakan pencegahan yang dilakukan pengguna saat berinteraksi dengan perangkat dan internet (Mawarni, et al., 2024).

Selanjutnya, penggunaan *gadget* juga menjadi faktor yang berhubungan dengan keamanan digital. Penggunaan *gadget* adalah pemanfaatan perangkat atau alat dengan tujuan dan fungsi praktis yang dirancang lebih canggih dibandingkan teknologi sebelumnya (Dewanti, 2024). Penggunaan *gadget* dapat diartikan aktivitas atau kegiatan seseorang dalam menggunakan teknologi gadget seperti *smarthpone*, kamera, dan laptop (Chusna, 2023).

Selain faktor internal yang berasal dari perilaku dan pemanfaatan perangkat, keamanan siber UMKM juga dipengaruhi oleh faktor eksternal berupa ancaman digital. Ancaman digital merupakan suatu aktivitas tindak kriminal yang dilakukan menggunakan internet maupun bentuk komunikasi digital lainnya (Wibowo, Wangsajaya, & Surahmat, 2023). Dengan kondisi teknologi yang semakin maju, ancaman tersebut semakin beragam dan perlu mendapatkan perhatian serius dari pelaku UMKM. Ancaman digital adalah peretas yang ingin mencuri informasi, tetapi juga dari perangkat lunak berbahaya seperti *malware*, *ransomware*, dan *spyware* yang dapat merusak sistem atau memata-matai aktivitas pengguna (Oktaarina, Hariyawan, Rasmana, & Briantoro, 2025).

Adapun fenomena yang berkaitan dengan kesadaran keamanan siber yang dikemukakan oleh (Rusli, 2025) Meskipun serangan siber menjadi lebih canggih dengan memanfaatkan *AI*, UMKM masih belum siap menghadapi ancaman ini. Kelemahan terbesar dari serangan siber masih berasal dari sisi manusia. Karena karyawan mengabaikan peringatan keamanan, 13% serangan *social engineering* berhasil. Senada yang dikemukakan oleh (Kaspersky, 2025) menemukan bahwa

hampir 8.500 bisnis kecil dan menengah menghadapi serangan perangkat lunak berbahaya yang disamarkan sebagai aplikasi produktivitas yang populer, seperti ChatGPT dan layanan *AI*. Perusahaan UMKM disarankan untuk melatih karyawan mereka untuk mengidentifikasi serangan *phishing* dan tautan mencurigakan. Seirama yang dikemukakan oleh (Supriyadi, 2024) menyebutkan bahwa sekitar 4,63 juta produsen UMKM, beberapa di antaranya telah mengalami serangan siber. Lebih dari 11.900 file berbahaya menyerang pelaku UMKM di Indonesia pada semester pertama. Dia menyatakan bahwa serangan siber meningkat 83% dari tahun sebelumnya. Kursus keamanan digital ini sangat penting karena merupakan langkah strategis dalam membangun ketahanan ekonomi berbasis komunitas.

Terdapat peristiwa yang berkaitan dengan penggunaan gadget yang dikemukakan oleh (Iskandar R. , 2024) Para pelaku usaha mikro kecil menengah (UMKM) di kabupaten Cianjur mulai menggunakan sistem marketing digital, tetapi banyak dari mereka belum memahami teori digital *marketing*. Senada yang dikemukakan oleh (Abdurrahman, 2025) Menteri usaha mikro, kecil, dan menengah (UMKM) menolak tuduhan bahwa penurunan pendapatan pedagang di pasar tradisional disebabkan oleh penurunan daya beli masyarakat. Dia menegaskan bahwa penurunan pendapatan lebih banyak disebabkan oleh keterlambatan UMKM untuk menyesuaikan diri dengan pertumbuhan digitalisasi dan keuangan digital. Seirama yang dikemukakan oleh (Iskandar M. , 2025) Kemenko PM, 35% UMKM belum memanfaatkan teknologi dengan optimal. Data dari 2024 menunjukkan bahwa sekitar 35% UMKM di Indonesia

belum memanfaatkan teknologi digital untuk operasional bisnis mereka. Namun, UMKM yang telah mengintegrasikan *e-commerce* dan media sosial mencatat peningkatan penjualan yang signifikan.

Masalah yang berkaitan dengan ancaman digital yang dikemukakan oleh (Pamungkas, 2025) deputi bidang keamanan siber dan sandi perekonomian, badan siber dan sandi negara (BSSN), ancaman siber saat ini juga menyerang banyak bisnis kecil dan menengah (UMKM), dengan kecerdasan buatan (*AI*) yang dapat mengganggu dan membahayakan keamanan data. Senada yang dikemukakan oleh (Kasperski, 2025) mengatakan bahwa ketika perangkat lunak berbahaya disamarkan sebagai alat produktivitas daring yang populer, hampir 8.500 bisnis mikro, kecil, dan menengah (UMKM) akan menghadapi serangan siber pada tahun 2025. Seirama yang dikemukakan oleh (Wisniewski, 2024) Laporan tahunan *Sophos Threat Report 2024* mendetail kejahatan siber di jalur utama dan ancaman terbesar yang dihadapi oleh bisnis kecil (UKM). Menurut laporan ini, *keyloggers*, *spyware*, dan *stealers* adalah *malware* yang digunakan oleh penyerang untuk mencuri data dan kredensial pada tahun 2023.

Ditemukan juga fenomena yang berkaitan dengan Keamanan Siber yang dikemukakan oleh (Setiawan, 2025) Sejak beberapa hari terakhir, data masyarakat Lotim penerima bantuan modal usaha mikro kecil dan menengah (UMKM) menjadi viral di berbagai platform media sosial. Data yang bocor mencakup puluhan ribu orang dari Lombok Timur yang memiliki Nomor Induk Kependudukan (NIK). Senada dikemukakan oleh (Kaspersky, 2023) Sekitar 22% kebocoran data di sektor UMKM disebabkan oleh tindakan karyawan, yang

dapat menyebabkan pelanggaran keamanan yang serius dan membahayakan keamanan industri. Menurut survei Kaspersky 2022 tentang ekonomi keamanan *IT*. Seirama yang dikemukakan oleh (Karayan, 2025) Data pelanggan telah dicuri oleh kelompok *hacker* yang tampan, menurut Google. Perusahaan mengetahui bahwa peretas dapat menghubungi korban untuk meminta tebusan. Dalam pernyataan pers yang dirilis Selasa (5/8) malam, Google menyebut peretas membobol *Salesforce*, platform untuk menyimpan informasi kontak bisnis kecil dan menengah.

Tabel I.1
Survei Pendahuluan

Nama Usaha	Hasil Survei
Dimsum Mentai Desty, dan puty cake online shop	<p>Berdasarkan hasil survei pada Dimsum Mentai Desty di Kecamatan Alang-Alang Lebar Kota Palembang, Melisa (dimsum mentai desty), Ningsih (puty cake online shop) mengatakan penggunaan <i>gadget</i> dalam aktivitas usaha berguna dan mudah dalam mendukung komunikasi, transaksi, dan promosi usaha. Namun, belum diseimbangkan dengan kesadaran keamanan siber yang memadai. Ditemukan bahwa:</p> <ul style="list-style-type: none"> - Pelaku UMKM belum memahami berbagai ancaman digital seperti <i>phishing</i> dan <i>malware</i>. - Pelaku UMKM belum menerapkan praktik autentikasi keamanan 2 faktor, Mulai dari aplikasi dana, instagram, whatsapp, facebook dan juga umkm belum meyakini menggunakan autentikasi 2 faktor meningkatkan perlindungan akun. <p>Kondisi ini menyebabkan pelaku UMKM maupun karyawan belum mampu berperan sebagai lini pertahanan pertama dalam menjaga kerahasiaan dan keakuratan data usaha, serta belum meyakini fasilitas penggunaan teknologi (<i>perceived Usefulness</i>) sehingga berpotensi menurunkan tingkat keamanan siber.</p>
Es Teh Clasicc 77	<p>Berdasarkan hasil survei pada UMKM Es Teh Classic 77 di kecamatan alang-alang lebar kota palembang, bahwa Amel mengatakan pelaku usaha telah menggunakan <i>gadget</i> dalam kegiatan usaha, terutama untuk pembayaran digital seperti aplikasi <i>qris</i> dana. Dan perluasan pemasaran melalui <i>shoppeefood</i>. Namun, penggunaan <i>gadget</i> tersebut:</p> <ul style="list-style-type: none"> - belum menerapkan praktik keamanan seperti email pemulihan, dan <i>login</i> autentikasi dua (2) faktor <p>pelaku usaha lebih memfokuskan pada kemudahan dan kelancaran transaksi. Selain itu, belum ditemukan penerapan khusus terkait kesadaran keamanan siber dalam penggunaan <i>gadget</i>, meskipun aktivitas digital berpotensi menghadapi ancaman digital yang dapat mempengaruhi keamanan data usaha.</p>

Sumber: Penulis 2025

Penelitian kesadaran keamanan siber yang dilakukan oleh (Rahmawati, 2023), (Zwilling, Klien, Lesjak, & Wiechetek, 2022) Hasil penelitian menunjukkan bahwa kesadaran keamanan siber berpengaruh signifikan terhadap perilaku keamanan informasi. Namun berbeda dengan hasil penelitian (Sari, Hariyadi, Sahtyawan, & Kusumaningtyas, 2023) yang menyatakan bahwa Kesadaran keamanan siber tidak berpengaruh signifikan terhadap keamanan siber, karena sampel menunjukkan bahwa sampel berada di level kesadaran buruk.

Selanjutnya penelitian penggunaan *gadget* yang dilakukan oleh (Kamil, 2020) dengan Hasil analisis untuk model ini menunjukkan bahwa Keamanan berpengaruh positif dan signifikan terhadap Sistem Penggunaan *Technology (Fintech)*. Temuan tersebut berbeda dengan penelitian (Shah & Agrawal, 2020) yang mengungkapkan bahwa *The results of the study show that smartphone users do not have a significant influence on cyber security, because respondents did not exhibit good cybersecurity behaviour.* (Hasil penelitian menunjukkan bahwa pengguna ponsel pintar tidak memiliki pengaruh signifikan terhadap keamanan siber, karena responden tidak menunjukkan perilaku keamanan siber yang baik).

Penelitian ancaman digital yang dilakukan oleh (Kehista, 2023) (Kumar, 2023) dengan hasil penelitian menunjukkan bahwa ancaman keamanan berpengaruh terhadap keamanan data pribadi pengguna *e-commerce*. Hal tersebut tidak sejalan dengan penelitian yang dilakukan oleh (Djatsa, 2020) *The results of the study indicate that digital threats do not have a significant direct effect on cybersecurity behaviors.* (Hasil penelitian tersebut menunjukkan bahwa

ancaman digital tidak memiliki pengaruh yang signifikan terhadap perilaku keamanan siber secara langsung).

Berdasarkan uraian latar belakang diatas maka peneliti akan membahas faktor yang mempengaruhi Keamanan Siber dengan mengangkat judul **“Pengaruh Kesadaran Keamanan Siber, Penggunaan Gadget, dan Ancaman Digital Terhadap Keamanan Siber Survei Pada Pelaku UMKM Bidang Kuliner Yang Terdigitalisasi di Kecamatan Alang-Alang Lebar Kota Palembang”**

B. Rumusan Masalah

Berdasarkan latar belakang masalah diatas, maka dapat dirumuskan permasalahan sebagai berikut:

1. Bagaimana pengaruh kesadaran keamanan siber terhadap keamanan siber pada UMKM bidang kuliner yang terdigitalisasi di kecamatan alang-alang lebar kota palembang?
2. Bagaimana pengaruh penggunaan gadget terhadap keamanan siber pada UMKM bidang kuliner yang terdigitalisasi di kecamatan alang-alang lebar kota palembang?
3. Bagaimana pengaruh ancaman digital terhadap keamanan siber pada UMKM bidang kuliner yang terdigitalisasi di kecamatan alang-alang lebar kota palembang?

C. Tujuan Penelitian

Berdasarkan perumusan masalah diatas, maka tujuan penelitian sebagai berikut:

1. Untuk mengetahui dan menganalisis pengaruh kesadaran keamanan siber terhadap keamanan siber survei pada pelaku UMKM bidang kuliner yang terdigitalisasi di kecamatan alang-alang lebar kota palembang.
2. Untuk Mengetahui dan menganalisis pengaruh penggunaan gadget terhadap keamanan siber pada UMKM bidang kuliner yang terdigitalisasi di kecamatan alang-alang lebar kota palembang.
3. Untuk mengetahui dan menganalisis pengaruh ancaman digital terhadap keamanan siber pada UMKM bidang kuliner yang terdigitalisasi di kecamatan alang-alang lebar kota palembang.

D. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat dan wawasan untuk pihak-pihak sebagai berikut:

1. Bagi Penulis

Dapat menambah wawasan pengetahuan secara empiris mengenai pentingnya Pengaruh Kesadaran Keamanan Siber, Penggunaan Gadget, dan Ancaman Digital Terhadap Keamanan Siber Survei Pada Pelaku UMKM di Kecamatan Alang-Alang Lebar Kota Palembang.

2. Bagi UMKM Bidang Kuliner Yang Terdigitalisasi Di Kecamatan Alang-alang Lebar Kota Palembang

Penelitian ini diharapkan dapat memberikan masukan mengenai

pentingnya Pengaruh Kesadaran Keamanan Siber, Penggunaan Gadget, dan Ancaman Digital Terhadap Keamanan Siber Survei Pada Pelaku UMKM Di Kecamatan Alang-Alang Lebar Kota Palembang.

3. Bagi Almamater

Hasil penelitian ini diharapkan menjadi referensi tambahan, menambah ilmu pengetahuan, serta menjadi acuan kajian bagi penulis dimasa yang akan datang khususnya penelitian yang memiliki topik yang sama, serta memberikan manfaat bagi semua pihak.

DAFTAR PUSTAKA

- Abdurrahman, M. (2025, Mei 27). *Menteri Maman Sebut UMKM Lambat Memanfaatkan Teknologi*. Retrieved from Tempo: https://www.tempo.co/ekonomi/menteri-maman-sebut-umkm-lambat-memanfaatkan-teknologi-1563699#google_vignette
- Agrawal, R. (2025). *Mastering Cyber Security* (1nd ed.). India: The Readers Paradise. ISBN 978-93-5977-282-0
- Assegaff, S., Rasywir, E., Pratama, Y., Kurniabudi, Rohaini, E., Sharipuddin, . . . Akbar, N. (2024). *Penerapan Teknologi Informasi dalam Era Revolusi Industri di Indonesia* (1nd ed.). Makassar: Tohar Media. ISBN 978-623-8421-46-6
- Christofora K. (2023). *Melek Teknologi Mengeksplorasi Aplikasi dan Gadget Terbaru* (1nd ed.). Yogyakarta: Cahaya Harapan. ISBN 978-623-84925-5-4
- Chusna, N. (2023). Analisis Intensitas Penggunaan Gadget terhadap Rendahnya. *Journal of Islamic Education Studies*, 8(1), 2540-8070.
- Cozma, L. S., & Radu, A. F. (2025). *Challenges to Security Policies in a Digital Environment. A Study with a View to the Situation in Romania and Bulgaria* (1nd ed.). Cyprus: Daniela Georgiana Golea. ISBN 978-992-5644-85-8
- Deni, A. (2024). *Manajemen Risiko Pada Era Digital* (1nd ed.). Batam: Rey Media Grafika. ISBN 978-623-8609
- Dewanti, L. (2024). *Edukasi Di Era Digital: Peran Teknologi, Kesehatan Mental, Motivasi Dalam Mencapai Prestasi* (1nd ed.). Yogyakarta: Deepublish Digital. ISBN 978-634-200-233-0
- Djatsa, F. (2020). Threat Perceptions, Avoidance Motivation and Security Behaviors Correlations. *Journal of Information Security vol 11 no 1 2020 yang berjudul Threat Perceptions, Avoidance Motivation and Security Behaviors Correlations*, 11(1).
- Fahriza, F. (2023, November 15). *UMKM Rentan Kena Kejahatan Siber, Pelaku Usaha Masih Abai Perkembangan Teknologi*. Retrieved from Radar Jogja: <https://radarjogja.jawapos.com/jogja/amp/653286288/umkm-rentan-kena-kejahatan-siber-pelaku-usaha-masih-abai-perkembangan-teknologi>
- Gunawan, A. (2025). *Keamanan Siber* (1nd ed.). Malang: Literasi Nusantara Abadi Grup. ISBN 978-634-234-165-0
- Hassandi, I. (2025). *Manajemen Risiko Dalam Bisnis* (1nd ed.). Yogyakarta: KBM Indonesia. ISBN 978-634-2023-86-0

- Hertina, D., Sulasmi, Taufik, M. Z., Sutarto, Aziza, N., Suharyanto, . . . Lukito, D. (2024). *Buku Ajar Metode Penelitian Bisnis* (1nd ed.). Jambi: Sonpedia Publishing Indonesia. ISBN 978-623-8483-88-4
- Iskandar, M. (2025, Mei 23). *Kemenko PM Jangkau 35% UMKM yang Belum Optimal Gunakan Teknologi*. Retrieved from MetroTV : <https://www.metrotvnews.com/read/NgxCDpxo-kemenko-pm-jangkau-35-umkm-yang-belum-optimal-gunakan-teknologi>
- Iskandar, Putra, D. D., Yasin, A. I., & Khairan. (2025). *Cyber Smart Campus Cakap Digital dan Aman Siber* (1nd ed.). Jambi: Sonpedia Publishing Indonesia. ISBN 978-623-514-435-1
- Iskandar, R. (2024, Juni 18). *Walau Tidak Gagap Teknologi Gadget, Masih Banyak Pelaku UMKM Belum Paham Teknik Digital Marketing*. Retrieved from Warkotalive: <https://wartakota.tribunnews.com/2023/06/18/walau-tidak-gagap-teknologi-gadget-masih-banyak-pelaku-umkm-belum-paham-teknik-digital-marketing>
- Istiningsih, Darsana, I., Payon, A. S., Nugroho, S. D., Kristiadi, A., Mulyani, F., . . . Sadikin, M. R. (2024). *Pemimpin di Era Digital: Menghadapi Tantangan dan Peluang Teknologi* (1nd ed.). Bali: Infes Media. ISBN 978-634-7033-20-8
- J. Prayoga, Saragih, A. F., Aulia, P., Isnawan, F., Mahesa, I., Yana, D. S., . . . Hafiz. (2025). *Mitigasi Bencana* (1nd ed.). Medan: Serasi Media. ISBN 62-60811795839
- Kamil, I. (2020). Cashless Society: Pengaruh Kemampuan Financial, Kemudahan Dan Keamanan Terhadap Perilaku Sistem Penggunaan Financial Technology. *Jurnal Akuntansi Dan Keuangan Islam* (8)1.
- Karayan, M. (2025, Agustus 7). *Google Akui Data UMKM Dicuri, Waspada Hacker Minta Tebusan ke Korban*. Retrieved from Dkata Data: <https://katadata.co.id/amp/digital/teknologi/68941d3e0f2eb/google-akui-data-umkm-dicuri-waspada-hacker-minta-tebusan-ke-korban>
- Kasmir. (2022). *Pengantar Metodologi Penelitian (Untuk Ilmu Manajemen, AkuntasI dan Bisnis)*. PT. Rajagrafindo Persada. ISBN 978-623-3724-64-7
- Kasperski. (2025, Juli 7). *Ancaman Siber Peniru ChatGPT Melonjak 115% di Awal 2025, UMKM Makin Jadi Sasaran*. Retrieved from Media Indonesia: https://mediaindonesia.com/teknologi/789164/ancaman-siber-peniru-chatgpt-melonjak-115-di-awal-2025-umkm-makin-jadi-sasaran#google_vignette

- Kaspersky. (2025, Juli 1). *Tsunami Malware 2025! Ribuan UMKM Dijebak Aplikasi Palsu ChatGPT dan Zoom*. Retrieved from Inilah.com: <https://www.inilah.com/tsunami-malware-2025-ribuan-umkm-dijebak-aplikasi-palsu-chatgpt-dan-zoom>
- Kaspersky. (2023, Juni 25). *Aduh, Kebocoran Data Sektor UMKM Disebabkan Karyawan*. Retrieved from It Works: <https://www.itworks.id/60049/aduh-kebocoran-data-sektor-umkm-disebabkan-karyawan.html>
- Kehista, A. P. (2023). Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Keamanan. *Jurnal Ilmu Manajemen Terapan (JIMT)*, 6, 1..
- Kumar, I. (2023). Emerging threats in cybersecurity: A review article. *International Journal of Applied and Natural Sciences*, 1, 1.
- Maagøe, V. (2022). *Mobile Device Efficiency (2022)*. Paris: Report prepared for IEA 4E EDNA.
- Mahardika, F., & Ripai, R. (2025). *Keamanan Siber dan Forensik Digital* (1nd ed.). Yogyakarta: Penamudah Media. 978-634-7269-30-0
- Malamuthu, B. K. (2025). *Digital Forensics and Incident Response: Investigating and Mitigating Cyber Attacks* (1nd ed.). India: RK Publications. ISBN 978-934-9701-89-2
- Marsiela, A. (2022). *Panduan Keamanan Digital* (1nd ed.). Jakarta: Aliansi Jurnalis Independen. ISBN 978-979-3530-53-6
- Mawarni, I., Wantouw, F., Raymond, Ningsih, E., Pandey, R. D., Reken, F., . . . Candra, M. (2024). *Manajemen Risiko* (1nd ed.). Padang: Gita Lentera. ISBN 978-623-8548-47-7
- Oktaarina, E. S., Hariyawan, M. Y., Rasmana, S. T., & Briantoro, H. (2025). *Dari Pengguna Menjadi Pencipta Teknologi Inspirasi Bagi Generasi Muda Menyongsong Era Digital* (1nd ed.). Yogyakarta: Deepublish Digital. ISBN 978-634-20089-8-0
- Pamungkas, S. A. (2025, Juli 18). *Ancaman Siber Sasar UMKM, BSSN Ingatkan Pelaku Usaha Jaga Keamanan Data*. Retrieved from Sindo News: <https://ekbis.sindonews.com/newsread/1594689/34/ancaman-siber-sasar-umkm-bssn-ingatkan-pelaku-usaha-jaga-keamanan-data-1752844072>
- Putri, P. K., Susilo, I. F., & Pramurindra, R. (2025). Cyber Crime Awareness Pada Digitalisasi Akuntansi UMKM Kota Tasikmalaya. *Jurnal Nasional UMP*.

- Quayyum, F., S., Cruzes, D., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child Computer Interaction*, 30.
- Rahmawati. (2023). Analisis Pengaruh Kesadaran Keamanan Siber terhadap Perilaku Keamanan Informasi pada Pegawai Pemerintah Daerah. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 7(3), 421-430.
- Raisah, R. (2025, April 11). *Ancaman Siber Mengintai UMKM: Pentingnya Perlindungan Data Digital*. Retrieved from Datacomm: <https://www.datacomm.co.id/release/ancaman-siber-mengintai-umkm-pentingnya-perlindungan-data-digital/>
- Richter, O. Z., & Jung, I. (2023). *Handbook of Open, Distance and Digital Education* (1nd ed.). Singapore: Springer Published. ISBN 978-981-19208-0-6
- Rizky, M. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan . *POLITEIA: Jurnal Ilmu Politik*, 54-62.
- Romney, M., & Steinbart, P. (2021). *Sistem Informasi Akuntansi* (13nd ed.). Jakarta: Salemba Empat. ISBN 978-979-061-528-1
- Rubab, U. E., Gul, H., Rahman, F., Aslam, S., Khan, M., & Bakht, M. (2025). Awareness Of Cybersecurity Measures And Students Academic Performances. *Testing, Psychometrics, Methodology In Applied Psychology*, 32(S7), 1972-6325.
- Rusli, A. (2025, September 11). *UMKM Indonesia Butuh Perlindungan Ekstra Akibat Meningkatnya Serangan Siber*. Retrieved from Koran Jakarta: <https://koran-jakarta.com/2025-09-11/umkm-indonesia-butuh-perlindungan-ekstra-akibat-meningkatnya-serangan-siber>
- Saenong, M. T. (2025). *Digitalisasi Pelayanan Kesehatan* (1nd ed.). Purbalingga: Eureka Media Aksara. ISBN 978-634-2484-38-8
- Santos, O. (2024). *Developing Cybersecurity Programs and Policies* (1nd ed.). Amerika: Perason It Certification. ISBN 978-0134-8585-48
- Sari, I. D., Hariyadi, D., Sahtyawan, R., & Kusumaningtyas, N. I. (2023). Analisis Tingkat Security Awareness-Personal Threat Terhadap Ancaman Phishing Dengan Metode Technology Threat Avoidance Theory (TTAT). *TEKNOMATIKA: Jurnal Informatika dan Komputer*, 49-55.
- Sarraya, S., Kusumoningtyas, A. A., Fajrina, R. M., Astuti, S. R., Siregar, L. V., Sirait, R. M., . . . Khairiah, U. (2025). *Hukum Telematika: Regulasi*,

- Perlindungan Data, dan Keamanan Siber* (1nd ed.). Agam: Yayasan Tri Edukasi Ilmiah. ISBN 978-634-7178-74-9
- Setiawan, M. (2025, Desember 1). *Data UMKM Bocor; LPKP Kritik Pemerintah, Abai dan Berbahaya*. Retrieved from Ampenan News: <https://www.ampenannews.com/2025/12/data-umkm-bocor-lpkk-kritik-pemerintah-abai-dan-berbahaya.html>
- Shah, P., & Agrawal, A. (2020). Cybersecurity behaviour of smartphone users in India: an empirical analysis. *Information & Computer Security*.
- Supriyadi. (2024, Juli 31). *UMKM juga Kena Serangan Siber*. Retrieved from KORAN Pikiran Rakyat: <https://koran.pikiran-rakyat.com/ekonomi/amp/pr-3039537040/umkm-juga-kena-serangan-siber>
- Susanto, A., Aini, Q., & Fitriyani, A. (2025). *Evaluasi Anteseden Kesuksesan E-Commerce Berbasis Komunitas* (1nd ed.). Bandung: Widina Media Utama. ISBN 978-623-500-737-3
- Tripathi, S. L., Agrawal, D., Pal, A., & Perwej, Y. (2023). *Emerging Trends In Iot And Computing Technologies* (1nd ed.). Amerika: CRS Press. ISBN 978-104-01556-9-1
- Wardianti, D., Djupri, D. R., Yatnikasari, A., & Rostariana, N. (2024). Hubungan Pengawasan Orang Tua dalam Penggunaan Gadget dengan Tingkat Perkembangan pada Anak Usia Prasekolah di Wilayah RW 001 Kelurahan Pondok Betung Kecamatan Pondok Aren Kota Tangerang Selatan. *Nursing Applied Journal*, 2(4), 2.
- Whitman, M. (2025). *Principles of Information* (1nd ed.). Amerika: Cengage. ISBN 978-0357-5064-43-1
- Wibowo, A., Wangsajaya, Y., & Surahmat, A. (2023). *Pemolisian Digital Dengan Artificial Intelligence* (1nd ed.). Depok: Rajagrafindo Persada. ISBN 978-623-37928-0-2
- Winarto, S. R., & Bisma, R. (2021). Studi Literatur: Analisis Persepsi UMKM di Indonesia Terhadap Cyber Security Menggunakan Model Protection. *Journal of Informatics and Computer Science*.
- Wiseman, M. (2024). *Menggenggam Gadget dengan Bijak: Memahami Bahaya Media Sosial bagi Anak-anak dan Cara Melindungi Mereka* (1nd ed.). Yogyakarta: Cahaya Harapan.
- Wisniewski, C. (2024, Juli 12). *Tahun 2024 Serangan Siber Terhadap UKM Makin Marak, Peretas Incar Data dan Kredensial*. Retrieved from Tribun: <https://m.tribunnews.com/techno/2024/07/12/tahun-2024-serangan-siber-terhadap-ukm-makin-marak-peretas-incar-data-dan-kredensial>

- Yanti, R., Suryani, I., & Putri, I. (2024). *Buku Ajar Statistik dan Probabilitas Dasar*. Medan: Serasi Media Teknologi. ISBN 978-623-10-0021-7
- Yudatama, U., Gustee, K., Komalasari, R., Purabaya, R. H., Solihin, H. H., Herjuna, S. A., . . . Akbar, Z. (2022). *Audit Sistem Informasi Teori, Framework dan Studi Kasus Menggunakan Framework* (1nd ed.). Bandung: Indie Press. ISBN 978-623-88145-0-3
- Yuhanis, L., & Welly. (2024). *Metodologi Penelitian Akuntansi*. Palembang: NoerFikri Offset. ISBN 978-602-447-894-0
- Yusnanto, T. (2025). *Strategi Melindungi Data Di Era siber* (1nd ed.). Yogyakarta: Tren Digital Publishing. ISBN 978-623-04-4494-0
- Zudiah, H. A. (2024). Analisis Faktor-Faktor Yang Mempengaruhi Intention To Use Pada Aplikasi Tokopedia Menggunakan Technology Acceptance Model (Tam) Termodifikasi. *Jurnal Sistem Informasi*, 52.
- Zudiah, H. R. (2024). Analisis Faktor-Faktor Yang Mempengaruhi Intention To Use Pada Aplikasi Tokopedia Menggunakan Technology Acceptance Model (Tam) Termodifikasi. *Jurnal Sistem Informasi*, 5(1), 52.
- Zwilling, M., Klien, G., Lesjak, D., & Wiechetek, L. (2022). Cyber Security Awareness, Knowledge and Behavior; A Comparative Study. *Journal of Computer Information Systems*, 62(1), 82-97.