QOLAMUNA
https://jurnal.qolamuna.id/index.php/JQ
e-ISSN : 3063-8925
Vol. 3 No. 1 Mei - Oktober 2026

# KEAMANAN DIGITAL DAN PERLINDUNGAN DIRI DI ERA TEKNOLOGI INFORMASI : TANTANGAN STRATEGI DAN IMPLIKASI PENDIDIKAN

**Siti Nur Azizah**
Pendidikan Agama Islam, Universitas Singaperbangsa Karawang, Indonesia
2510631110152@student.unsika.ac.id

**INFO ARTIKEL**

***Riwayat Artikel:***

Diterima: 15-05-26
Disetujui: 29-05-26

***Kata Kunci:***

*Indonesia:*
*Keamanan siber:*
*literasi digital:*
*UU PDP:*
*ancaman siber.*

***Abstract:*** *This study aims to examine the importance of cybersecurity in the digital era, with a special focus on Indonesia's challenges related to cyber threats, low digital literacy, and evolving regulations. The research uses a qualitative approach with a literature review method, collecting data from journal articles (Kaspersky, NIST, Schneier), government regulations (UU PDP No. 27 Tahun 2022), national survey reports (CSIS), expert opinions (Hafiz Noer, Telkom University), and Islamic perspectives on data privacy. The analysis reveals that Indonesia faces serious vulnerabilities, such as attacks on critical infrastructure like the Temporary National Data Center (PDNS), widespread phishing and ransomware incidents, and limited public awareness of cyber risks. The findings also indicate that existing policies and security protocols are still weakly implemented, especially in the private sector. In conclusion, effective cybersecurity in Indonesia requires a coordinated strategy among government, private stakeholders, and communities. The paper recommends strengthening digital literacy programs, improving enforcement of UU PDP, adopting international security standards, and integrating ethical and religious values into cybersecurity education to enhance national digital resilience.*

***Abstrak:*** Penelitian ini bertujuan untuk mengkaji pentingnya keamanan siber di era digital serta mengeksplorasi tantangan yang dihadapi Indonesia terkait ancaman siber, rendahnya literasi digital, dan perkembangan regulasi. Metode yang digunakan adalah studi pustaka dengan pendekatan kualitatif, mengumpulkan data dari jurnal ilmiah (Kaspersky, NIST, Schneier), peraturan pemerintah (UU PDP No. 27 Tahun 2022), laporan survei nasional (CSIS), pendapat pakar (Hafiz Noer, Telkom University), serta perspektif keagamaan dalam menjaga data pribadi. Hasil penelitian menunjukkan bahwa Indonesia rentan terhadap serangan pada infrastruktur kritis seperti Pusat Data Nasional Sementara (PDNS), serta maraknya phishing, ransomware, dan manipulasi informasi digital seperti deepfake. Selain itu, implementasi regulasi dan praktik keamanan di banyak organisasi masih lemah. Kesimpulannya, ketahanan siber Indonesia membutuhkan kolaborasi antara pemerintah, sektor swasta, dan masyarakat. Dianjurkan peningkatan program literasi digital, penguatan pelaksanaan UU PDP, penerapan standar keamanan internasional, serta integrasi nilai etika dan agama dalam pendidikan keamanan siber.

## PENDAHULUAN

Keamanan siber (cybersecurity) kini jadi isu paling mendesak di era digital. Semakin dalamnya integrasi teknologi ke berbagai sendi kehidupan, ancaman pada infrastruktur digital pun melonjak tajam. Teknologi telah merevolusi transaksi, komunikasi, pekerjaan, serta pengelolaan informasi di sektor finansial, pemerintahan, hingga hiburan. Namun,

kemudahan ini datang dengan risiko serius seperti pencurian data pribadi, sabotase sistem, dan serangan ke infrastruktur vital yang picu kerugian finansial, hilangnya kepercayaan masyarakat, serta kerusakan reputasi.

Secara dunia, serangan siber semakin rumit dan beragam, melibatkan aktor negara, kriminal terorganisir, hingga hacker individu yang manfaatkan celah sistem. Berbagai negara dan lembaga global giat kembangkan strategi penguatan cybersecurity. Indonesia, dengan pertumbuhan digitalnya yang kencang, pun hadapi dilema serupa. Adopsi teknologi luas oleh masyarakat dan lembaga publik-swasta ciptakan peluang sekaligus lubang rentan yang dieksploitasi pihak jahat.

Contoh mencolok adalah pembobolan Pusat Data Nasional Sementara (PDNS), pondasi pengelolaan data pemerintah dan publik. Insiden ini bukti infrastruktur digital negeri masih rapuh dan butuh perlindungan berstandar tinggi. Tantangan lain: literasi siber masyarakat yang rendah. Banyak netizen tak paham bahaya phishing, malware, atau ransomware, sehingga gampang jadi korban. Walau pemerintah telah keluarkan kebijakan dan aturan, pelaksanaannya di lapangan kurang maksimal, terutama di swasta yang belum adopsi standar global.

Keamanan digital adalah upaya lindungi data, gadget, dan identitas online dari serangan seperti hacking, malware, serta pencurian informasi seperti "perisai" penjaga kerahasiaan. Ia krusial jaga stabilitas dunia maya, apalagi data kini berpindah cepat. Perlindungan data tak boleh diremehkan. Banyak orang menganggap cybersecurity urusan korporasi besar atau ahli IT saja. Padahal, siapa pun yang pakai smartphone, laptop, atau akun medsos rentan sama. Risiko hacking, scam online, infeksi malware, dan data curian bisa menyerang pelajar hingga pengusaha. Maka, kesadaran dan pengetahuan keamanan digital wajib dimiliki semua kalangan.

Hadapi situasi ini, Indonesia butuh strategi terpadu dan holistik lawan ancaman siber. Kerja sama pemerintah, swasta, dan mitra internasional esensial kuatkan ketahanan nasional. Lewat kolaborasi terintegrasi, infrastruktur digital bisa lebih aman, sambil tingkatkan kesiapan dan awareness masyarakat terhadap ancaman siber yang terus mutasi.

## METODE PENELITIAN

Studi ini menerapkan pendekatan kualitatif melalui metode studi literatur untuk mengkaji konsep, risiko, serta hambatan keamanan siber di Indonesia. Data diperoleh dari sumber primer dan sekunder, termasuk UU PDP, laporan insiden (PDNS), jurnal akademik, survei, serta pandangan ahli, kemudian diolah secara tematik guna menyusun saran peningkatan ketahanan siber dan literasi.

## HASIL PENELITIAN DAN PEMBAHASAN

### Konsep Keamanan Digital (cybersecurity)

Menurut Kaspersky (2020), keamanan siber merujuk pada tindakan melindungi sistem, jaringan, dan perangkat lunak dari serangan digital yang dirancang untuk mengakses, mengubah, atau menghancurkan data rahasia, memeras dana dari pengguna, atau menginterupsi jalannya bisnis. Serangan siber dapat berasal dari berbagai pihak, seperti individu, sindikat kejahatan terorganisir, hingga negara yang terlibat dalam kegiatan spionase atau perang siber..

NIST (2018) juga mengemukakan bahwa keamanan siber mencakup upaya pengamanan kerahasiaan (confidentiality), keutuhan (integrity), dan ketersediaan (availability) informasi. Seiring dengan kemajuan teknologi, ancaman siber terus berkembang menjadi lebih kompleks dan sulit terdeteksi. Kondisi ini menuntut penerapan strategi keamanan yang lebih komprehensif dan adaptif.

Menurut Schneier (2019), pada era digital saat ini, keamanan tidak hanya terbatas pada perangkat keras dan perangkat lunak. Keamanan juga sangat dipengaruhi oleh perilaku manusia, yang seringkali menjadi elemen paling rentan dalam sistem keamanan siber. Selain upaya pengamanan informasi, peningkatan kesadaran mengenai signifikansi keamanan informasi di seluruh tingkatan organisasi merupakan hal yang krusial. Pelatihan yang teratur dan simulasi serangan phishing dapat mendukung karyawan dalam mengidentifikasi dan menghindari ancaman.

### Jenis-Jenis Ancaman Keamanan Digital

Ancaman keamanan digital menunjukkan kecenderungan yang tidak hanya meningkat, tetapi juga semakin sulit diprediksi. Malware tidak lagi sekadar merusak sistem, melainkan digunakan untuk mengendalikan perangkat dan mengambil data tanpa disadari. Penyebarannya sering terjadi melalui aktivitas yang terlihat biasa, seperti membuka lampiran email atau mengunduh aplikasi dari sumber yang kurang jelas. Pada saat yang sama, phishing tetap bertahan sebagai metode yang efektif karena mampu memanfaatkan kepercayaan pengguna. Pendekatan ini bekerja dengan cara yang sederhana, namun sering berhasil karena pengguna cenderung tidak memverifikasi sumber informasi secara mendalam. Penggunaan isu tertentu, seperti kesehatan pada tahun 2022, memperlihatkan bahwa konteks sosial dapat dimanfaatkan untuk meningkatkan keberhasilan serangan.

Ancaman keamanan digital menunjukkan kecenderungan yang tidak hanya meningkat, tetapi juga semakin sulit diprediksi. Malware tidak lagi sekadar merusak sistem, melainkan digunakan untuk mengendalikan perangkat dan mengambil data tanpa disadari. Penyebarannya sering terjadi melalui aktivitas yang terlihat biasa, seperti membuka lampiran email atau mengunduh aplikasi dari sumber yang kurang jelas. Pada saat yang

sama, phishing tetap bertahan sebagai metode yang efektif karena mampu memanfaatkan kepercayaan pengguna. Pendekatan ini bekerja dengan cara yang sederhana, namun sering berhasil karena pengguna cenderung tidak memverifikasi sumber informasi secara mendalam. Penggunaan isu tertentu, seperti kesehatan pada tahun 2022, memperlihatkan bahwa konteks sosial dapat dimanfaatkan untuk meningkatkan keberhasilan serangan.

Kerentanan juga muncul dari cara komunikasi dilakukan. Man in the Middle memanfaatkan celah pada jaringan yang tidak aman, terutama ketika pengguna tidak menyadari risiko yang ada. SQL Injection menunjukkan bahwa kelemahan kecil dalam validasi input dapat berdampak luas terhadap keamanan data. Di sisi lain, social engineering justru tidak bergantung pada teknologi yang kompleks. Teknik ini lebih mengandalkan pemahaman terhadap perilaku manusia, sehingga sering kali lebih sulit diantisipasi. Hal ini mengindikasikan bahwa aspek manusia masih menjadi titik yang paling mudah dieksploitasi.

Zero day attack memperlihatkan bahwa tidak semua ancaman dapat dicegah sejak awal. Celah yang belum diketahui membuat sistem berada dalam posisi rentan tanpa disadari. Botnet kemudian memperkuat skala serangan dengan memanfaatkan banyak perangkat secara bersamaan. Ancaman juga tidak selalu datang dari luar. Pihak internal yang memiliki akses justru dapat menjadi sumber risiko ketika tidak ada pengawasan yang memadai. Situasi ini menunjukkan bahwa kepercayaan dalam sistem perlu diimbangi dengan kontrol yang jelas.

Kondisi tersebut memperlihatkan adanya jarak antara kemampuan pengguna dan kompleksitas ancaman yang dihadapi. Banyak pengguna masih berfokus pada penggunaan teknologi, tetapi belum memahami risiko yang menyertainya. Dalam konteks ini, literasi digital tidak lagi cukup dipahami sebagai pengetahuan tambahan. Literasi digital perlu ditempatkan sebagai bagian dari kebiasaan dalam berinteraksi dengan teknologi, sehingga keputusan yang diambil tidak hanya didasarkan pada kemudahan, tetapi juga pada pertimbangan keamanan.

**literasi digital sebagai fondasi perlindungan**

Literasi digital mencakup kompetensi dalam menemukan, mengevaluasi, dan mengelola informasi digital secara etis, sebagaimana mencakup pemahaman mengenai perlindungan data pribadi. Hal ini melampaui keterampilan dasar seperti pengkodean, menuju kesadaran akan etiket daring, kemampuan mengidentifikasi upaya phishing, dan pengelolaan privasi. Pakar dari Universitas Gadjah Mada, Hafiz Noer, menekankan bahwa literasi ini merupakan prioritas untuk mendidik masyarakat agar bersikap selektif saat berinteraksi di platform seperti TikTok atau X.Fenomena ini dapat diamati dalam survei nasional yang dilakukan oleh Center for Strategic and International Studies (CSIS) terhadap 1.200 warga Indonesia. Tercatat sebanyak 33,3% dari 11,8% responden yang pernah

menyaksikan konten DeepFake menyatakan keyakinan akan kebenaran konten tersebut. Lebih memprihatinkan lagi, 4,1% responden yang menyaksikan konten DeepFake lainnya mengaku pernah menyebarluaskan konten serupa.

Literasi digital dapat meminimalkan risiko kebocoran data melalui praktik seperti penggunaan kata sandi yang kuat, pembatasan izin aplikasi, serta kehati-hatian terhadap deepfake. Di Indonesia, hal ini selaras dengan RUU PDP dan berbagai program Kominfo untuk meningkatkan kesadaran siber. Penelitian mengungkapkan bahwa individu dengan literasi digital tinggi cenderung lebih taat pada regulasi dan terlindung dari ancaman seperti malware. Menurutnya, pemerintah perlu memandang kebijakan sebagai langkah maju yang progresif, bukan sekadar inisiatif baru. Apa yang telah dilakukan sebelumnya harus dievaluasi untuk mengidentifikasi kekurangan dan merumuskan tindakan selanjutnya. "Kita tidak bisa menyamaratakan kebutuhan serta kondisi literasi digital, sebab setiap platform memiliki pengguna yang beragam. Namun, menurut saya, masih diperlukan banyak upaya," ujar Hafiz.Keamanan Digital Dalam Bingkai Nilai Islam

**Keamana digital dalam bingkai nilai Islam**

Dalam pandangan Islam, perlindungan data pribadi merupakan suatu kewajiban. Meskipun konsep data pribadi baru muncul pada era kontemporer, ajaran Islam senantiasa menekankan pentingnya menjaga kerahasiaan dan menghargai hak-hak individu. Prinsip ini selaras dengan berbagai landasan hukum yang kokoh, mencakup perintah menjaga amanah, larangan memata-matai (tajassus), serta anjuran untuk mempertimbangkan kemaslahatan.

Islam menegaskan perlindungan informasi personal melalui Al-Qur'an dan hadis, termasuk larangan menyebarkan informasi rahasia yang dapat menimbulkan kerugian dan prinsip untuk tidak mengintervensi urusan orang lain tanpa dasar yang sah. Prinsip amanah menuntut setiap individu untuk bertanggung jawab atas data yang dikelola, baik sebagai pemilik maupun sebagai pihak yang dipercayakan, demi mencegah timbulnya dampak negatif (dharar). Sebagaimana firman Allah dalam QS Al-Hujurat ayat 12:

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوا اجْتَنِبُوْا كَثِيْرًا مِّنَ الظَّنِّۖ اِنَّ بَعْضَ الظَّنِّ اِثْمٌ وَّلَا تَجَسَّسُوْا وَلَا يَغْتَبْ بَّعْضُكُمْ بَعْضًاۗ اَيُحِبُّ اَحَدُكُمْ اَنْ يَّأْكُلَ لَحْمَ اَخِيْهِ مَيْتًا فَكَرِهْتُمُوْهُۗ وَاتَّقُوا اللّٰهَۗ اِنَّ اللّٰهَ تَوَّابٌ رَّحِيْمٌ ﴿١٢﴾

*" Wahai orang-orang yang beriman, jauhilah banyak prasangka! Sesungguhnya sebagian prasangka itu dosa. Janganlah mencari-cari kesalahan orang lain dan janganlah ada di antara kamu yang menggunjing sebagian yang lain. Apakah ada di antara kamu yang suka memakan daging saudaranya yang sudah mati? Tentu kamu merasa jijik. Bertakwalah kepada Allah! Sesungguhnya Allah Maha Penerima Tobat lagi Maha Penyayang."*

**Strategi Perlindungan Diri di Dunia Digital**

Perlindungan data pribadi di Indonesia telah diperkuat melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Aturan ini mengatur pengelolaan data sekaligus membatasi potensi penyalahgunaan informasi individu. Namun, pemahaman pengguna terhadap praktik keamanan digital masih belum merata. Kondisi ini menyebabkan perlindungan belum berjalan optimal meskipun regulasi telah tersedia.

Pengamanan akun masih sering bergantung pada kata sandi yang sederhana dan digunakan berulang. Pola tersebut mempermudah akses tidak sah ketika satu akun berhasil ditembus. Penggunaan kombinasi karakter yang lebih beragam dapat meningkatkan ketahanan akun terhadap percobaan peretasan. Di sisi lain, pemanfaatan autentikasi dua faktor belum diterapkan secara konsisten oleh pengguna. Padahal, fitur ini dapat membantu mencegah akses ilegal ketika kata sandi telah diketahui pihak lain. Temuan tersebut juga menunjukkan bahwa langkah dasar dalam menjaga keamanan akun masih sering diabaikan (Ainiyah, 2025).

Paparan terhadap phishing masih sering terjadi karena rendahnya kebiasaan memverifikasi informasi. Pesan yang menyerupai institusi resmi kerap langsung dipercaya tanpa pengecekan lebih lanjut. Tautan dengan tampilan mirip alamat asli juga masih sering diakses tanpa pertimbangan risiko. Kondisi ini menunjukkan bahwa serangan tidak selalu bergantung pada kelemahan sistem, tetapi juga pada respons pengguna. Dalam kajian yang sama, dijelaskan bahwa kelengahan pengguna menjadi faktor utama dalam keberhasilan kejahatan digital berbasis identitas.

Penggunaan jaringan Wi-Fi publik untuk mengakses layanan penting masih sering dilakukan. Aktivitas ini membuka peluang terjadinya penyadapan data pada jaringan yang tidak terlindungi. Upaya pengamanan seperti penggunaan koneksi terenkripsi atau pembatasan akses belum dilakukan secara konsisten. Hal ini menunjukkan adanya celah dalam kebiasaan penggunaan teknologi sehari-hari yang masih belum disadari sepenuhnya oleh pengguna.

Risiko kehilangan data juga meningkat akibat rendahnya praktik pencadangan secara berkala. Data penting sering disimpan tanpa salinan cadangan pada media lain. Ketika terjadi kerusakan perangkat atau serangan siber, pemulihan data menjadi sulit dilakukan. Penyimpanan berbasis awan maupun media eksternal belum dimanfaatkan secara optimal. Kondisi ini memperlihatkan bahwa langkah sederhana seperti pencadangan masih sering dianggap tidak mendesak, padahal perannya cukup besar dalam menjaga keberlanjutan data.

Pemeliharaan sistem juga belum dilakukan secara rutin oleh sebagian pengguna. Pembaruan perangkat lunak sering diabaikan meskipun mengandung perbaikan terhadap

celah keamanan. Penggunaan perangkat lunak tidak resmi turut meningkatkan potensi masuknya program berbahaya. Hal ini menunjukkan bahwa aspek teknis dan perilaku pengguna saling berkaitan dalam menentukan tingkat keamanan.

Kesenjangan antara ketersediaan regulasi dan praktik pengguna menunjukkan perlunya penguatan literasi digital. Kemampuan dalam memahami risiko dan mengambil keputusan menjadi faktor yang menentukan dalam menjaga keamanan data. Tanpa perubahan pada kebiasaan penggunaan, perlindungan yang tersedia tidak akan memberikan hasil yang optimal. Dalam konteks ini, kepatuhan terhadap keamanan digital tidak cukup hanya didorong oleh aturan, tetapi perlu tumbuh dari kesadaran pengguna itu sendiri. Tanpa kesadaran tersebut, regulasi yang ada berpotensi hanya menjadi formalitas tanpa dampak nyata.

## SIMPULAN DAN SARAN

### Simpulan

Keamanan siber telah menjadi pilar utama dalam menjaga kestabilan era digital, baik secara global maupun di Indonesia yang mengalami pertumbuhan digital pesat. Ancaman seperti malware, phishing, ransomware, DDoS, dan serangan zero-day semakin canggih, diperparah oleh rendahnya literasi digital Masyarakat seperti terlihat dari survei CSIS tentang kepercayaan pada deepfake serta kerentanan infrastruktur seperti PDNS. Meskipun ada kemajuan melalui UU PDP No. 27 Tahun 2022 dan prinsip Islam tentang amanah serta larangan tajassus, tantangan implementasi regulasi, kolaborasi lintas sektor, dan kesadaran individu masih menghambat ketahanan siber nasional. Penelitian ini menegaskan bahwa keamanan siber bukan hanya urusan pakar IT, melainkan tanggung jawab bersama untuk melindungi data, identitas, dan infrastruktur dari aktor jahat.

### Saran

Untuk memperkuat ekosistem keamanan siber Indonesia, berikut rekomendasi strategis: Peningkatan Literasi Digital: Pemerintah melalui Kominfo dan Kemdikbud perlu meluncurkan program pelatihan masif berbasis platform (misalnya TikTok dan X), termasuk simulasi phishing dan kampanye anti-deepfake, menargetkan 80% masyarakat dalam 5 tahun.

Penguatan Regulasi dan Implementasi: Evaluasi berkala kebijakan seperti UU PDP dengan sanksi tegas bagi pelanggar; dorong sektor swasta adopsi standar NIST untuk confidentiality, integrity, dan availability. Kolaborasi Multisektor: Bentuk satgas nasional melibatkan pemerintah, swasta, akademisi (seperti Telkom University dan UGM), serta lembaga internasional untuk berbagi intelijen ancaman dan respons insiden seperti PDNS.

Inovasi Teknologi dan Perilaku: Wajibkan update perangkat lunak, autentikasi dua faktor, dan antivirus di institusi publik/swasta; integrasikan pendidikan siber berbasis nilai Islam di kurikulum untuk membangun budaya amanah digital. Pemantauan Insider Threats: Lakukan audit rutin dan pelatihan etika bagi karyawan untuk mencegah ancaman dari dalam.

## DAFTAR REFERENSI


LMS SPADA Indonesia. (n.d.). Cyber Computer Security (Keamanan Sistem Informasi). Diakses pada 13 Mei 2026, dari LMS SPADA Indonesia.

CSIRT Teknokrat. (2025, 28 Juni). Apa itu keamanan digital? Panduan lengkap untuk pemula. Diakses dari csirt.teknokrat.ac.id.

Faris Hadinata. (2024, 31 Agustus). Keamanan siber di era digital: Mengapa penting dan bagaimana menjaganya. Telkom University.

Asosiasi Diskominfo Provinsi Seluruh Indonesia. (2025, September 11). Pentingnya keamanan informasi di era digital. Diakses dari askompsi.or.id.

Budiyanto, D., & Mabruri, M. (2025). Pentingnya keamanan siber dalam era digital: Tinjauan global dan kondisi di Indonesia. Prosiding Seminar Nasional Sains dan Teknologi (SainTek), Universitas Terbuka. Diakses dari https://conference.ut.ac.id/index.php/saintek/article/view/5134/1969.

Redaksi OCBC. (2023, Desember 12). Cyber threat adalah: Pengertian, jenis ancaman, dan cara mengatasinya. OCBC. https://www.ocbc.id/id/article/2023/12/14/cyber-threat-adalah.

Universitas Gadjah Mada. (2025, Januari 18). Soal perlindungan anak di ruang digital, pakar UGM soroti pentingnya evaluasi kebijakan dan literasi digital.https://ugm.ac.id/id/berita/soal-perlindungan-anak-di-ruang digital-pakar-ugm-soroti-pentingnya-evaluasi-kebijakan-dan-literasi-digital/.

Maylaffayza, H. (2025, Maret 26). Big data dan keamanan informasi: Perspektif Al-Qur'an dalam menyikapi pencurian data. Fakultas Adab dan Humaniora UIN Syarif Hidayatullah Jakarta. UIN Jakarta.

Zuhri, M. K. (2025, Juni 30). Perlindungan data pribadi menurut Islam: Antara martabat, maslahat, dan ancaman digital. NU Online. https://nu.or.id/syariah/perlindungan-data-pribadi-menurut-islam-antara-martabat-maslahat-dan-ancaman-digital-u9FPx.

Ainiyah, I. N. (2025, Januari 29). Strategi pencegahan dan perlindungan data pribadi dari doxing di era digital. Universitas Muhammadiyah Sidoarjo. https://hukum.umsida.ac.id/strategi-pencegahan-data-dari-doxing/.

Hadinata, F. (2024, Agustus 31). Keamanan siber di era digital: Mengapa penting dan bagaimana menjaganya. Telkom University. https://bit.telkomuniversity.ac.id/keamanan-siber-di-era-digital-mengapa-penting-dan-bagaimana-menjaganya/

Dinas Komunikasi dan Informatika Kabupaten Kubu Raya. (2025, Oktober 7). Panduan dasar keamanan siber: Langkah sederhana melindungi data dan perangkatmu.