



2025

17 - 23 Maret 2025

Kamsib Indonesia on Paper Edisi 7

**Tetap Aman
Bersama Kamsib**

Kamsib Indonesia on Paper adalah majalah yang membahas berbagai aspek keamanan siber, mulai dari ancaman terbaru, teknik perlindungan, hingga tren teknologi yang memengaruhi lanskap keamanan digital.

Edisi 7

17 – 23 Maret 2025

Mari bantu orang tua kita agar tetap aman di dunia digital!

Kamsib Indonesia on Paper

Penipuan Online yang Menargetkan Orang Tua

Penulis: **Anton Lepari**

Penipuan *online* semakin marak, dan orang tua sering menjadi target utama. Kurangnya pemahaman tentang teknologi serta kepercayaan yang tinggi terhadap informasi yang diterima membuat mereka lebih rentan terhadap berbagai jenis kejahatan siber.

Berikut beberapa modus penipuan *online* yang sering menargetkan orang tua serta cara menghindarinya:

1. Penipuan Undian dan Hadiah Palsu
2. Penipuan Berkedok Keluarga dalam Bahaya
3. *Phishing* dan Pencurian Data
4. Penipuan Investasi dan Skema Ponzi
5. Penipuan Jual Beli *Online*
6. Penipuan Layanan Teknologi (*Tech Support Scam*)

Orang tua adalah salah satu target utama penipuan *online* karena kurangnya pemahaman tentang ancaman siber. Dengan mengenali berbagai modus kejahatan digital dan menerapkan langkah-langkah pencegahan, mereka bisa terhindar dari kerugian finansial maupun pencurian identitas.

1. Penipuan Undian dan Hadiah Palsu

Modusnya adalah orang tua menerima pesan atau telepon yang mengklaim mereka memenangkan hadiah besar (misalnya mobil, uang tunai, atau barang elektronik). Namun, untuk mengklaim hadiah, mereka diminta membayar pajak atau biaya administrasi.

Cara menghindari:

- Jangan percaya jika tidak merasa ikut undian.
- Periksa sumber informasi dan konfirmasi langsung ke pihak penyelenggara resmi.
- Jangan pernah mengirimkan uang atau data pribadi ke pihak yang tidak dikenal.

2. Penipuan Berkedok Keluarga dalam Bahaya

Modusnya adalah penipu berpura-pura menjadi anggota keluarga (anak, cucu, atau keponakan) yang sedang dalam kondisi darurat, seperti kecelakaan atau ditahan polisi. Mereka meminta bantuan keuangan dengan alasan mendesak.

Cara Menghindari:

- Jangan panik dan segera hubungi anggota keluarga yang bersangkutan untuk memastikan kebenarannya.
- Jika penelepon mengaku dari polisi atau rumah sakit, minta bukti atau hubungi langsung institusi terkait.
- Jangan pernah memberikan informasi pribadi atau mentransfer uang sebelum melakukan verifikasi.

3. *Phishing* dan Pencurian Data

Modusnya adalah orang tua menerima email atau pesan teks yang mengaku dari bank, *e-wallet*, atau layanan pemerintah yang meminta mereka memasukkan data pribadi seperti nomor kartu kredit, PIN, atau kode OTP.

Cara Menghindari:

- Jangan pernah mengklik tautan dari sumber yang tidak dikenal.
- Pastikan alamat email atau situs web resmi sebelum memberikan informasi apa pun.
- Aktifkan verifikasi dua langkah (2FA) untuk akun penting seperti perbankan *online*.

4. Penipuan Investasi dan Skema Ponzi

Modusnya adalah orang tua ditawarkan investasi dengan keuntungan tinggi dalam waktu singkat, sering kali melalui media sosial atau grup WhatsApp. Setelah mereka menyeter uang, penipu menghilang tanpa jejak.

Cara Menghindari:

- Jangan mudah tergiur dengan iming-iming keuntungan besar tanpa risiko.
- Cek legalitas perusahaan investasi di situs resmi OJK atau lembaga terkait.
- Diskusikan dengan keluarga atau penasihat keuangan sebelum berinvestasi.

5. Penipuan Jual Beli *Online*

Modusnya adalah orang tua melihat iklan barang murah di media sosial atau *marketplace*. Setelah mentransfer uang, barang tidak pernah dikirim atau ternyata berbeda dari yang dijanjikan.

Cara Menghindari:

- Selalu beli dari toko resmi atau seller dengan reputasi baik.
- Gunakan metode pembayaran yang aman, seperti rekening bersama (*escrow*) atau COD (bayar di tempat).
- Jangan tergoda oleh harga yang terlalu murah dibanding pasaran.

6. Penipuan Layanan Teknologi (*Tech Support Scam*)

Modusnya adalah penipu mengaku sebagai teknisi dari perusahaan teknologi besar (misalnya Microsoft atau *internet provider*) dan mengklaim bahwa komputer atau ponsel korban terkena virus. Mereka meminta korban menginstal *software* tertentu yang justru mencuri data pribadi.

Cara Menghindari:

- Perusahaan besar tidak akan menghubungi pengguna secara langsung tanpa laporan sebelumnya.

- Jangan izinkan orang asing mengakses perangkat dari jarak jauh.
- Jika ada masalah, hubungi langsung layanan pelanggan resmi dari perangkat yang dimiliki.

Cara Melindungi Orang Tua dari Penipuan *Online*

Melindungi orang tua dari penipuan *online* bukan hanya soal teknologi, tapi juga soal edukasi dan kesadaran. Orang tua sering kali menjadi sasaran empuk karena sifat mereka yang mudah percaya dan kurangnya pemahaman terhadap trik digital masa kini. Oleh karena itu, penting bagi keluarga untuk mengedukasi mereka agar selalu skeptis terhadap tawaran yang terlalu bagus untuk menjadi kenyataan. Mereka perlu dikenalkan pada berbagai modus penipuan, seperti pesan teks, email mencurigakan, atau panggilan telepon yang mengaku dari pihak bank atau keluarga dalam kondisi darurat. Dengan memahami pola dan tanda-tanda penipuan, orang tua akan lebih waspada dan tidak mudah terjebak.

Selain edukasi, perlindungan teknis juga harus diperkuat. Pasanglah aplikasi keamanan di perangkat mereka untuk mencegah *malware*, dan pastikan akun bank serta *e-wallet* yang mereka gunakan sudah dilengkapi dengan fitur keamanan tambahan seperti OTP dan autentikasi dua faktor. Dorong mereka untuk selalu berdiskusi dengan keluarga sebelum memutuskan sesuatu, terutama yang berkaitan dengan uang atau data pribadi. Ingatkan bahwa di era digital ini, berhati-hati dan bertanya lebih dulu jauh lebih aman daripada menyesal di kemudian hari. Dengan kombinasi edukasi dan perlindungan teknis, kita dapat membantu orang tua tetap aman dari ancaman penipuan *online*.

Sumber

- Abdolrazzagh-Nezhad, Majid & Langarib, Nafise. (2025). *Phishing Detection Techniques: A review*. Data Science: Journal of Computing and Applied Informatics. 9. 32-46. 10.32734/jocai.v9.i1-19904.
- Crgol, Alex & Vrhovec, Simon. (2024). *Recognition of genuine and phishing emails may not be associated with response to phishing attacks*. JUCS - Journal of Universal Computer Science. 30. 1265-1283. 10.3897/jucs.132113.
- Alzboon, Mowafaq & Al-Batah, Mohammad & Alqaraleh, Muhyeeddin & Alzboon, Faisal & Alzboon, Lujin. (2025). *Phishing Website Detection Using Machine Learning*. Gamification and Augmented Reality. 3. 81. 10.56294/gr202581.
- Labhade-Kumar, Neelam. (2024). *OTP-Based Authentication System*. 13. 229-233.

Dengan menerapkan keamanan akun, menjaga privasi, menghindari penipuan, dan mengatasi cyberbullying, kita bisa menikmati media sosial tanpa risiko berlebihan.

Tetap Aman di Media Sosial

Penulis: **Anton Lepari**

Media sosial telah menjadi bagian dari kehidupan sehari-hari, memungkinkan kita untuk berbagi momen, berkomunikasi, dan mendapatkan informasi dengan cepat. Namun, di balik kenyamanan ini, ada berbagai risiko keamanan yang mengintai, seperti pencurian data, peretasan akun, penipuan *online*, hingga *cyberbullying*. Tanpa langkah perlindungan yang tepat, informasi

pribadi yang kita bagikan bisa disalahgunakan oleh pihak yang tidak bertanggung jawab.

1. Mengamankan Akun dari Peretasan

Akun media sosial adalah gerbang utama yang menyimpan banyak informasi pribadi. Untuk menghindari peretasan:

- Gunakan kata sandi yang kuat – Kombinasikan huruf besar, kecil, angka, dan simbol unik.
- Aktifkan autentikasi dua faktor (2FA) – Ini akan memberikan lapisan keamanan tambahan jika ada yang mencoba masuk ke akun Anda.
- Hindari menggunakan *password* yang sama di berbagai *platform* – Jika satu akun diretas, akun lainnya tetap aman.

2. Menjaga Privasi dari Mata-Mata Digital

Banyak pengguna tidak menyadari bahwa setiap unggahan dapat menjadi jejak digital yang permanen. Agar privasi tetap terjaga:

- Atur privasi akun – Batasi siapa saja yang bisa melihat postingan, informasi pribadi, dan daftar teman.
- Jangan sembarangan membagikan lokasi secara *real-time* – Penjahat siber bisa memanfaatkannya untuk melacak keberadaan Anda.
- Hindari berbagi informasi sensitif – Seperti alamat rumah, nomor telepon, atau detail keuangan.

3. Waspada terhadap Penipuan dan Phishing

Penipuan di media sosial semakin canggih, mulai dari akun palsu yang mengaku sebagai teman hingga tautan berbahaya yang dikirim melalui pesan. Untuk menghindari jebakan ini:

- Jangan klik tautan mencurigakan – Periksa sumbernya sebelum mengklik.
- Verifikasi akun sebelum berinteraksi – Jangan langsung percaya pada akun yang menawarkan hadiah atau promosi mencurigakan.
- Laporkan dan blokir akun mencurigakan – Jika menemukan aktivitas yang mencurigakan, segera laporkan ke *platform* media sosial tersebut.

4. Hindari Cyberbullying dan Pelecehan Digital

Cyberbullying dan pelecehan di dunia digital bisa berdampak buruk pada kesehatan mental. Untuk melindungi diri:

- Gunakan fitur blokir dan laporkan – Jangan ragu untuk menghindari interaksi negatif.
- Jangan membalas provokasi – Kadang, diam adalah cara terbaik untuk menghindari konflik lebih lanjut.
- Dukung lingkungan digital yang positif – Berinteraksilah dengan bijak dan hormati orang lain.

Media sosial adalah alat yang luar biasa jika digunakan dengan bijak, tetapi juga bisa menjadi ancaman jika kita lengah. Dengan menerapkan keamanan akun, menjaga privasi, menghindari penipuan, dan mengatasi *cyberbullying*, kita bisa menikmati media sosial tanpa risiko berlebihan. Ingat, keamanan digital adalah tanggung jawab bersama.

Sumber

- Mubaroq, Fariz & Huda, Nurul & Weliangan, Hally & Psikologi, Fakultas & Kunci, Kata & Resiliensi, & Remaja, Dan & Cyberbullying,. (2024).

Satu langkah kecil dalam menjaga keamanan bisa mencegah kerugian besar di masa depan.

Gambaran Resiliensi pada Remaja Korban Cyberbullying. 3. 73-85. 10.35760/arjwa.2024.v3i2.10430.

- Llorent, Vicente J & Seade-Mejía, Carolina & Vélez Calvo, Ximena & Nasaescu, Elena. (2024). The Impact of Lockdown in Cyberbullying in Primary Education: Transitions of Cyberbullying and Bullying. *The Journal of school health*. 94. 10.1111/josh.13505.

Lindungi Uang dan Data Anda dari Kejahatan Siber

Penulis: **Anton Lepari**

Transaksi *online* semakin menjadi bagian dari kehidupan sehari-hari. Dari belanja *online*, pembayaran tagihan, hingga investasi, semua bisa dilakukan dalam hitungan detik. Namun, di balik kemudahan ini, ancaman kejahatan siber seperti *phishing*, *skimming*, dan *malware* terus mengintai. Oleh karena itu, memahami cara melindungi diri saat bertransaksi digital menjadi hal yang sangat penting.

1. Gunakan Metode Pembayaran yang Aman

Dalam dunia digital, memilih metode pembayaran yang tepat sangat penting untuk menghindari risiko kejahatan siber. Berikut beberapa langkah yang bisa Anda lakukan agar transaksi tetap aman:

- Pilih *platform* terpercaya – Gunakan layanan pembayaran digital yang sudah memiliki reputasi baik.
- Aktifkan autentikasi ganda (2FA) – Tambahan keamanan ini membuat akun Anda lebih sulit diretas.
- Periksa kebijakan keamanan platform – Pastikan layanan yang digunakan memiliki enkripsi data.

2. Hindari Jebakan Penipuan Online

Kejahatan siber seperti *phishing*, *scam*, dan *malware* sering kali menasar pengguna yang tidak waspada. Berikut beberapa cara untuk menghindari jebakan penipuan *online*:

- Jangan klik tautan mencurigakan – *Phishing* sering kali berbentuk email atau pesan yang terlihat resmi.
- Pastikan situs menggunakan HTTPS – Situs tanpa enkripsi dapat membahayakan data Anda.
- Waspada terhadap telepon atau pesan palsu – Bank dan *e-wallet* tidak akan meminta data pribadi melalui pesan atau telepon.

3. Jaga Keamanan Data dan Perangkat Anda

Keamanan transaksi digital tidak hanya bergantung pada layanan yang digunakan, tetapi juga pada bagaimana Anda melindungi perangkat dan data pribadi.

- Gunakan kata sandi yang kuat dan unik – Hindari menggunakan tanggal lahir atau kata yang mudah ditebak.
- Perbarui aplikasi secara rutin – Pembaruan sering kali berisi perbaikan keamanan yang penting.

- Gunakan jaringan yang aman – Hindari bertransaksi menggunakan WiFi publik.

4. Laporkan Aktivitas Mencurigakan

Jika Anda menemukan transaksi atau aktivitas yang tidak dikenali, segera ambil tindakan untuk mencegah kerugian lebih lanjut.

- Segera laporkan transaksi yang tidak dikenal – Jika ada aktivitas mencurigakan, hubungi penyedia layanan Anda.
- Gunakan notifikasi transaksi – Dengan notifikasi, Anda bisa segera mengetahui jika ada transaksi yang tidak sah.
- Diskusikan dengan orang terpercaya – Jika ragu terhadap suatu transaksi, minta pendapat orang yang lebih paham.

Peran Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI)

Untuk melindungi konsumen dan menjaga integritas sektor keuangan dari ancaman penipuan (*scam*), Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI) telah menetapkan berbagai peraturan yang mengatur strategi anti-penipuan dan perlindungan konsumen. Berikut adalah beberapa peraturan penting yang berkaitan dengan penanggulangan penipuan dalam sektor perbankan:

1. Peraturan Otoritas Jasa Keuangan (OJK)

- POJK Nomor 12 Tahun 2024 tentang Penerapan Strategi Anti *Fraud* bagi Lembaga Jasa Keuangan
Peraturan ini mewajibkan lembaga jasa keuangan untuk menerapkan strategi anti-penipuan yang efektif, termasuk pencegahan, deteksi, investigasi, pelaporan, dan pemantauan. Tujuannya adalah meminimalisasi kejadian penipuan yang dapat merugikan industri jasa keuangan maupun konsumen.
- POJK Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan
Peraturan ini menggantikan POJK sebelumnya dan bertujuan untuk memperkuat perlindungan konsumen serta masyarakat dalam sektor jasa keuangan. POJK ini menyesuaikan dengan perkembangan industri yang semakin kompleks dan dinamis, memastikan bahwa konsumen mendapatkan perlakuan yang adil dan transparan.

2. Peraturan Bank Indonesia (BI)

- Peraturan Bank Indonesia Nomor 3 Tahun 2023 tentang Pelindungan Konsumen Bank Indonesia (Peraturan Bank Indonesia Nomor 22/20/PBI/2020 tentang Perlindungan Konsumen Bank Indonesia)
Peraturan ini menetapkan prinsip-prinsip perlindungan konsumen dalam layanan sistem pembayaran dan pengelolaan uang rupiah. Prinsip-prinsip tersebut meliputi kesetaraan dan perlakuan yang adil, keterbukaan informasi, serta keamanan dan keandalan layanan. Peraturan ini juga menekankan pentingnya keamanan sistem informasi dan ketahanan siber dalam operasional perbankan, yang merupakan aspek krusial dalam mencegah dan menangani berbagai bentuk penipuan digital.

3. Tindak Pidana Penipuan dalam Hukum Pidana Indonesia

Selain peraturan khusus dari OJK dan BI, tindakan penipuan juga diatur dalam Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP), yang menyatakan bahwa siapa saja yang dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu, martabat palsu, tipu muslihat, atau rangkaian kebohongan, dapat dipidana karena penipuan.

Keamanan dalam transaksi digital adalah tanggung jawab setiap pengguna. Dengan menerapkan langkah-langkah keamanan, seperti memilih metode pembayaran yang terpercaya, mengenali modus penipuan, serta menjaga keamanan data dan perangkat, Anda bisa menikmati kemudahan transaksi digital tanpa rasa khawatir. Satu langkah kecil dalam menjaga keamanan bisa mencegah kerugian besar di masa depan.

Sumber

- Malar, G & Pappa, D & Fathima, M & Sb, Vaidianathan. (2025). *Enhancing Web Application Security: Implementing Two-Factor Authentication (2FA) with TOTP and Flask*.
- Sunay, Miss & Kazi, Kutubuddin. (2018). *Multimodal Biometrics Authentication System using Fusion of Fingerprint and Iris*. 2. 1282-1286.
- Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 12 Tahun 2024 tentang Penerapan Strategi Anti *Fraud* Bagi Lembaga Jasa Keuangan.
- Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan.
- Peraturan Bank Indonesia Nomor 22/20/PBI/2020 tentang Perlindungan Konsumen Bank Indonesia.
- Peraturan Bank Indonesia Nomor 3 Tahun 2023 tentang Pelindungan Konsumen Bank Indonesia.

Internet memberikan banyak manfaat, tetapi juga membawa risiko ancaman siber.

Bagaimana Mencegah Anak-anak dari Ancaman Siber?

Penulis: Anton Lepari

Anak-anak semakin terpapar dunia maya sejak usia dini. Internet memberikan banyak manfaat, tetapi juga membawa risiko ancaman siber, seperti *cyberbullying*, eksploitasi *online*, dan pencurian data pribadi. Oleh karena itu, penting bagi orang tua untuk memahami cara melindungi anak-anak dari bahaya di dunia digital.

1. Ajarkan Kesadaran Keamanan Siber Sejak Dini

Mulailah dengan mendidik anak-anak tentang pentingnya menjaga privasi mereka. Ajarkan mereka untuk tidak membagikan informasi pribadi, seperti alamat rumah, nomor telepon, atau nama sekolah, kepada orang asing di internet.

2. Gunakan Kontrol Orang Tua dan Filter Konten

Manfaatkan fitur *parental control* di perangkat, aplikasi, dan *browser* untuk membatasi akses ke konten yang tidak sesuai. Pastikan anak-anak hanya mengakses *platform* yang aman dan sesuai dengan usia mereka.

3. Awasi Aktivitas Online Anak

Buat aturan tentang batas waktu penggunaan *gadget* dan selalu pantau aktivitas *online* anak. Pastikan mereka memahami bahwa tidak semua orang yang ditemui di internet memiliki niat baik.

4. Ingatkan tentang Bahaya Cyberbullying

Cyberbullying dapat berdampak buruk pada kesehatan mental anak. Beri tahu mereka bahwa jika mereka mengalami atau menyaksikan *cyberbullying*, mereka harus segera memberi tahu orang tua atau guru.

5. Gunakan Password yang Kuat dan Aman

Ajarkan anak-anak untuk membuat kata sandi yang kuat dan tidak membagikannya kepada siapa pun, kecuali kepada orang tua mereka. Gunakan fitur autentikasi dua faktor (2FA) untuk meningkatkan keamanan akun mereka.

6. Beri Contoh yang Baik dalam Penggunaan Teknologi

Anak-anak cenderung meniru kebiasaan orang tua. Gunakan internet dengan bijak dan tunjukkan bagaimana cara berinteraksi secara aman di dunia maya.

Mencegah anak-anak dari ancaman siber bukan hanya tentang membatasi akses mereka ke internet, tetapi juga mengedukasi mereka tentang cara menggunakannya dengan aman. Dengan komunikasi yang baik, pengawasan, dan edukasi, orang tua dapat membantu anak-anak menjelajahi dunia digital dengan lebih aman dan bijaksana.

Gunakan Fitur Parental Control

Parental control adalah fitur yang memungkinkan orang tua untuk mengawasi dan mengatur penggunaan perangkat serta akses konten digital oleh anak-anak mereka. Google menyediakan alat seperti Google Family Link untuk membantu orang tua menetapkan aturan digital dan memastikan keamanan anak saat *online*.

Google Family Link memungkinkan orang tua untuk:

- Menetapkan batas waktu layar: Orang tua dapat mengatur batas harian penggunaan perangkat, menjadwalkan waktu tidur perangkat, dan mengunci perangkat dari jarak jauh untuk membantu anak menemukan keseimbangan yang sehat dalam penggunaan teknologi.
- Mengelola aplikasi: Menyetujui atau menolak unduhan aplikasi dari Google Play Store, menetapkan batas waktu penggunaan untuk aplikasi tertentu, dan memblokir aplikasi yang tidak sesuai.
- Memantau aktivitas aplikasi: Melihat laporan aktivitas aplikasi untuk memahami aplikasi mana yang paling sering digunakan anak, sehingga dapat membuat keputusan yang tepat mengenai akses aplikasi.
- Mengatur filter konten: Mengelola akses anak ke situs web melalui Chrome, memfilter hasil pencarian eksplisit dengan SafeSearch, dan

memilih pengalaman YouTube yang sesuai untuk anak, seperti YouTube Kids atau pengalaman yang diawasi di YouTube.

Selain itu, kontrol orang tua di Google Play memungkinkan orang tua untuk membatasi konten yang dapat diunduh atau dibeli berdasarkan tingkat kedewasaan. Untuk mengatur kontrol ini:

1. Buka aplikasi **Google Play**.
2. Ketuk ikon profil di kanan atas.
3. Pilih **Setelan > Keluarga > Kontrol orang tua**.
4. Aktifkan kontrol orang tua dan buat PIN yang tidak diketahui anak.
5. Pilih jenis konten yang ingin dibatasi dan tetapkan tingkat pembatasannya.

Dengan fitur-fitur ini, orang tua dapat lebih efektif dalam membimbing anak-anak mereka dalam penggunaan teknologi yang aman dan sesuai usia.

Sumber

- Pratiwi, Romi. (2025). *Privasi dan Personalisasi Dilema Teknologi Intuitif Dalam Komunikasi Bisnis*.
- Zahrah, Nurul & Suhasman, Suhasman & Akbar, Muh. (2025). *Pengaruh Second Account Instagram Terhadap Pengungkapan Diri dan Manajemen Privasi Generasi Z*. Al-Kalam : Jurnal Komunikasi, Bisnis Dan Manajemen. 12. 85. 10.31602/al-kalam.v12i1.17547.
- Google. *Set Parental Controls with Family Link*. Tautan: <https://safety.google/families/parental-supervision/>. Diakses Maret 2025.
- Google. *How to set up parental controls on Google Play*. Tautan: <https://support.google.com/googleplay/answer/1075738>. Diakses Maret 2025.

Kamsib ID adalah sebuah platform edukasi yang berfokus pada keamanan informasi dan siber dalam bahasa Indonesia. Kehadiran Kamsib dipicu oleh lonjakan pesat penggunaan internet yang tidak diimbangi dengan kesadaran akan pentingnya keamanan di dunia maya. Fenomena ini juga menjadi salah satu pemicu dari banyaknya kasus penipuan, kebocoran data, dan insiden dalam sistem elektronik, baik yang dimiliki oleh pemerintah maupun swasta.

Kamsib Indonesia on Paper adalah majalah yang membahas berbagai aspek keamanan siber, mulai dari ancaman terbaru, teknik perlindungan, hingga tren teknologi yang memengaruhi lanskap keamanan digital. Diterbitkan secara berkala, majalah ini menyajikan artikel mendalam, studi kasus, serta wawancara dengan para ahli untuk memberikan wawasan bagi profesional keamanan siber, peneliti, dan penggemar dunia siber. Dengan pendekatan yang informatif dan analitis, Kamsib Indonesia on Paper bertujuan menjadi referensi utama bagi siapa saja yang ingin memahami dan menghadapi tantangan di dunia siber yang terus berkembang. [at]kamsib_id

Kamsib Indonesia

Jakarta, Indonesia
 hubungi@kamsib.id