Vol. 2 No. 1 Edisi Januari 2026 E.ISSN. 3089-8579

Jurnal Pengabdian Indonesia (JPI)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/jpi/index
Email: admin@jurnalcenter.com

IMPLEMENTASI SOPHOS INTERCEPT X SEBAGAI APLIKASI KEAMANAN PERANGKAT DIGITAL PADA KOMUNITAS POS PAUD PANDANWANGI BANDUNG

Aldi Akbar[1*], Budi Rustandi Kartawinata[2]

[1*]Telkom University, Email: aldiakb@telkomuniversity.ac.id
[2]Telkom University, Email: budikartawinata@telkomuniversity.ac.id

*email koresponden: aldiakb@telkomuniversity.ac.id

DOI: https://doi.org/10.62567/jpi.v2i1.1949

Abstract

The widespread ownership of digital devices, especially smartphones, among individuals has made it easier to access information and conduct transactions. However, not many people realize the importance of smartphone security. Therefore, this community service activity was held not only as an educational event but also as a practical tutorial on installing digital device security applications using Sophos Intercept X. This research is a qualitative study that uses a normative approach, group discussions, and simulations in the Pos PAUD Pandanwangi Bandung. The study found that many participants still need understanding and practical guidance on the use of anti-malware applications on their digital devices. Through this activity, the level of anti-malware security literacy among participants has improved.
Keywords: *Sophos Intercept X, Digital Device Security, PAUD Pandanwangi*

Abstrak

Maraknya kepemilikan perangkat digital khususnya smartphone di tiap individu memudahkan dalam kebutuhan akan informasi dan bertranksaksi. Namun tidak banyak yang menyadari pentingnya keamanan pada smartphone mereka. Untuk itu maka kegiatan pengabdian masyarakat ini diadakan bukan hanya berupa edukasi namun sekaligus tutorial praktis menginstal aplikasi keamanan perangkat digital menggunakan Sophos Intercept X. Penelitian ini adalah penelitian kualitatif yang menggunakan pendekatan normatif, grup diskusi, dan simulasi di komunitas Pos PAUD Pandanwangi Kota Bandung. Studi ini menemukan bahwa masih banyak peserta yang membutuhkan pemahaman dan panduan praktis tentang penggunaan aplikasi anti malware di perangkat digital mereka. Melalui kegiatan ini maka level literasi keamanan anti malware di kalangan peserta menjadi lebih baik dari sebelumnya.
Kata Kunci: Sophos Intercept X, Keamanan Perangkat Digital, Pos PAUD Pandanwangi.

1. PENDAHULUAN

Dalam beberapa tahun terakhir, ancaman keamanan digital semakin berkembang pesat, terutama dalam bentuk serangan spam, phishing, dan malware. Menurut Henry (2018) dalam Data Breach Investigations Report, lebih dari 35% pelanggaran data diawali melalui serangan berbasis email, termasuk spam yang mengandung tautan berbahaya. Spam tidak hanya mengganggu pengguna tetapi juga menjadi vektor utama penyebaran ransomware dan penipuan siber (Symantec, 2019). Masyarakat awam sering kali menjadi target utama karena

Jurnal Pengabdian Indonesia (JPI)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/jpi/index
Email: admin@jurnalcenter.com

kurangnya kesadaran akan keamanan digital dan ketidaktahuan dalam mengidentifikasi ancaman tersebut (Kaspersky, 2021).

Perkembangan teknologi digital di Indonesia yang pesat diiringi dengan peningkatan ancaman keamanan siber, terutama serangan spam, phishing, dan malware. Menurut laporan Siber & Negara (2022) Indonesia mengalami lonjakan serangan siber sebesar 87% pada tahun 2022, dengan spam dan email phishing sebagai vektor utama. Lebih dari 60% pengguna internet di Indonesia pernah menerima spam, namun hanya 30% yang mampu mengidentifikasi ancaman tersebut dengan benar (Wibowo & Yulianingsih, 2025). Hal ini menunjukkan rendahnya literasi keamanan digital di kalangan masyarakat awam, sehingga diperlukan solusi anti-spam yang tidak hanya efektif tetapi juga mudah digunakan.

Beberapa aplikasi anti-spam yang banyak digunakan antara lain SpamTitan, Barracuda Sentinel, dan Sophos Intercept X (Mclaughlin & Elliott, 2023). Pengguna Indonesia cenderung memilih aplikasi keamanan dengan antarmuka sederhana dan fitur otomatis, mengingat kompleksitas konfigurasi menjadi hambatan utama. Aplikasi antispan dengan pendekatan berbasis machine learning dan AI, terbukti mampu memblokir 98% spam tanpa memerlukan intervensi pengguna (Salman et al., 2024; Suarti, 2024). Solusi keamanan yang mengintegrasikan proteksi otomatis dan notifikasi intuitif lebih disukai oleh pengguna non-teknis di Indonesia (Santoso, 2023).

Selain itu, rendahnya kesadaran keamanan siber di Indonesia juga dipengaruhi oleh kurangnya edukasi formal mengenai keamanan digital (Ananta et al., 2024). Oleh karena itu, aplikasi seperti Sophos Intercept X, yang mampu beroperasi secara mandiri dengan pembaruan ancaman real-time, menjadi solusi yang sesuai untuk konteks Indonesia. Berdasarkan latar belakang ini, penelitian ini akan menganalisis efektivitas Sophos Intercept X sebagai aplikasi anti-spam yang mudah digunakan bagi masyarakat awam, dengan mempertimbangkan temuan-temuan terbaru dalam literatur keamanan siber.

Dalam upaya mengatasi permasalahan ini, kegiatan pengabdian kepada masyarakat melalui penyuluhan menjadi salah satu solusi yang efektif. Kegiatan ini bertujuan untuk meningkatkan kemampuan pengelolaan keamanan perangkat digital bagi pihak-pihak yang ada di lingkungan TK/PAUD Pandangwangi, serta memberikan informasi tentang cara mengurangi kesenjangan literasi keamanan data di lingkungan keluarga. Di samping itu, kegiatan ini pun bersinergi dengan road map Kelompok Keahlian di Fakultas Ekonomi dan Bisnis Telkom University yaitu turut mendukung dalam membentuk ekosistem Smart City and Urban Development. Alasan utama dipilihnya Pos PAUD Pandanwangi karena merupakan tempat berkumpulnya banyak keluarga dengan anak-anak prasekolah, tempat interaksi antar stakeholder dalam belajar, upgrade skill dan update pengetahuan terkait isu-isu terbaru. Pos PAUD Pandanwangi adalah lembaga pendidikan anak usia dini yang didirikan sejak tahun 2011 dengan Nomor Kepala Sekolah Nasional (NPSN) 69759716 dengan naungan Yayasan Pandanwangi Jaya dan berlokasi di Jl. Kencana Wangi No. 3 Kelurahan Cijawura. Kecamatan Buahbatu, Kota Bandung. Izin operasional dikeluarkan oleh Dinas Penanaman Modal dan

Jurnal Pengabdian Indonesia (JPI)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/jpi/index
Email: admin@jurnalcenter.com

Pelayanan Terpadu Satu Pintu Kota Bandung dengan nomor izin: 0084/IPSPNFI/IX/2022/DPMPTDP.

Potensi pemberdayaan masyarakat sasaran yang ingin dicapai antara lain: (1) Peningkatan kesadaran orang tua dalam melindungi privasi dan keamanan keluarga; (2) Penguatan peran guru dan tenaga kependidikan berupa interaksi yang intensif dengan anak-anak dan orang tua dalam menyebarkan informasi mengenai privasi dan keamanan digital; (3) Keterlibatan komunitas lokal seperti RT/RW, karang taruna, atau organisasi kemasyarakatan guna mendukung upaya edukasi mengenai privasi dan keamanan keluarga di era digital.

2. METODE PENGABDIAN

Kegiatan sosial ini berupa layanan konsultasi dan edukasi kepada kelompok sasaran yang dibagi dalam dua tahap. Kelompok sasaran terdiri dari guru/pendidik dan orang tua siswa di Pos PAUD Pandanwangi. Langkah pertama adalah perencanaan berupa koordinasi antara penyelenggara dengan masyarakat sasaran, diawali dengan materi administrasi seperti formulir rujukan dan surat kesediaan dari masyarakat sasaran yang memuat peran, tanggung jawab, aturan dan fungsi. Pada fase ini juga menentukan tanggal pelaksanaan, jumlah peserta dan teknik pelaksanaan lainnya. Tahap kedua yaitu pelaksanaan berupa penyuluhan yang disampaikan secara luring (luar jaringan) yang bertempat di aula sekolah tersebut. Waktu yang disepakati adalah Selasa, 23 Desember 2025 pukul 13.00 – 17.00 WIB.

Adapun teknis pelaksanaan antara lain: (1) Opening atau sambutan; (2) Penyampaian materi penyuluhan sekaligus pelatihan praktis aplikasi Sophos Intercept X; (3) Tanya jawab; (4) Closing atau penutup berupa rangkuman kegiatan.

Kegiatan ini menggunakan pendekatan kualitatif dan memanfaatkan buku-buku dan jurnal-jurnal terbaru dan relevan tentang materi keamanan perangkat digital. Tujuan dari penelitian ini adalah untuk mengedukasi pentingnya memberi perhatian lebih pada keamanan perangkat digital sekaligus memberikan pelatihan teknis berupa instalasi aplikasi keamanan pada perangkat digital yang dimiliki masyarakat sasar. Serangkaian proses kegiatan di atas dan ditunjang oleh sumber data seperti buku, jurnal, artikel ilmiah, dan laporan penelitian sebelumnya tentang keamanan siber maka muara dari proses ini adalah untuk menghasilkan artikel yang mendalam dan terorganisir. Dengan demikian, pembaca akan memiliki gambaran tentang bagaimana tingkat pemahaman akan keamanan perangkat digital serta sejauh mana penggunaan aplikasi keamanan yang disematkan pada perangkat digital khususnya pada unit terkecil di lingkungan masyarakat.

3. HASIL DAN PEMBAHASAN

a. Perangkat Digital adalah Aset

Mengetahui aset yang dimiliki adalah langkah pertama untuk mewujudkan keamanan yang lebih baik. Perlu diketahui, banyak serangan siber dan pelanggaran data disebabkan oleh laptop dan perangkat lain yang hilang atau dicuri, akses tidak sah ke akun, dan kerentanan perangkat lunak yang tidak di-pacthing dengan baik (Bharathi et al., 2025; Shafik, 2025). Dengan mengetahui komputer, perangkat, dan perangkat lunak (aset) yang dimiliki akan lebih

Jurnal Pengabdian Indonesia (JPI)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/jpi/index
Email: admin@jurnalcenter.com

memahami potensi risiko yang mungkin ada, yang memungkinkan untuk membuat keputusan secara sadar dan mengambil langkah-langkah mitigasi: (i) Mengetahui jumlah laptop dan perangkat seluler yang dimiliki, siapa yang dapat mengaksesnya, serta perangkat lunak dan aplikasi apa yang ada di dalamnya (Saylor & Saylor, 2025); (ii) Berapa lama komputer digunakan dan kapan terakhir memperbarui kemanannya (Halfacree, 2025); (iii) Memiliki sistem otomasi perangkat yang terhubung ke internet. Aset ini dapat menjadi celah masuk bagi peretas untuk mencuri atau merusak data sensitif yang dimiliki (Beretas, 2024).

Identifkasi semua aplikasi termasuk aplikasi bisnis, akun online tempat alamat surat elektronik bisnis, dan aplikasi lain yang diakses baik secara lokal maupun jarak jauh melalui perangkat yang dimiliki (Gilsenan, 2025). Penting untuk mepertimbangkan dan mencatat semua aplikasi dan akun yang sudah lama tidak digunakan karena kemungkinan besar tidak sempat memperbarui perangkat lunaknya (Vitali & Giuliani, 2024). Jika dirasa tidak bermanfaat maka cukup dengan menghapus atau menutup akun tersebut. Akun online lama mungkin menyimpan beberapa informasi pribadi dan jika organisasi tempat akun tersebut diserang maka data yang tersimpan mungkin dapat terpengaruh (Garfinkel, 2024).

b. Mencegah Phishing dan Malware

Malware adalah perangkat lunak yang dirancang untuk menyebabkan kerusakan pada dan/atau akses tidak sah ke perangkat atau jaringan (Babak et al., 2025). Surat elektronik phishing mengelabui pengguna agar percaya bahwa mereka berurusan dengan entitas yang dapat dipercaya sehingga penyerang dapat memperoleh akses tidak sah ke konten pribadi yang rahasia dan sensitif, atau uang (Al Qwaid, 2025; Ali & Mohd Zaharon, 2024). Diperkirakan sekitar lebih dari 90% serangan siber bermula dari surat elektronik phishing (Tanti, 2024). Jika mengklik tautan atau membuka lampiran dalam surat elektronik phishing kemungkinan akan memicu sejumlah aktivitas yang telah disiapkan oleh penyerang (Gallo et al., 2024), misalnya mencuri data, membuat rute rahasia (dikenal sebagai backdoor) ke komputer untuk kemudian mengaksesnya nanti (Feng & Tramèr, 2024), menginstal jenis malware yang digunakan untuk mengakses data lalu meminta uang tebusan (dikenal sebagai ransomware), atau membuat untuk mengunduh jenis malware lain yang memungkinkan penyerang untuk melihat apa yang diketik, seperti kata sandi atau nomor rekening, dikenal sebagai perangkat mata-mata (Jabid et al., 2024; Triantafyllou, 2024).

Penggunaan antivirus real time sangat penting karena pemeriksaan virus dilakukan secara real-time, dapat menghilangkan virus sebelum menimbulkan kerusakan, dan diperbarui jika perlindungan virus baru dikembangkan. Vishwakarma & Dhakad (2024), pemblokir iklan, beberapa iklan online atau pesan yang muncul saat menjelajahi situs web berguna, namun beberapa lainnya mungkin berisi kode berbahaya dan dapat menginfeksi perangkat digital jika mengkliknya. Pemblokir iklan dapat digunakan untuk mencegah iklan muncul di halaman web, menawarkan perlindungan tambahan saat menjelajah.

Shahid et al (2024), pengawal digital (anti virus, anti malware) ibarat satpam atau bodyguard untuk semua perangkat digital yang dimiliki. Tugas pengawal digital ini antara lain mengunci pintu dari virus, menahan iklan-iklan nakal dan website penipu agar tidak masuk,

Jurnal Pengabdian Indonesia (JPI)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/jpi/index
Email: admin@jurnalcenter.com

menutup mata para mata-mata digital, mengamankan gudang data kita yang berisi foto-foto keluarga dan info penting lainnya.

Manfaat yang didapat dari pengawal digital ini dari sisi orang tua/ keluarga yaitu hati lebih tenang, aktivitas online (belanja, banking) lebih aman, gadget bebas lemot, perangkat digital jadi zona aman untuk semua. Bagi anak-anak, memberikan rasa lebih aman saat menggunakan gadget untuk belajar & bermain, terhindar dari klik yang salah (Akbar et al., 2025).

Aplikasi anti malware sendiri banyak jenisnya seperti AVG, Kasperksy, AVAST, AVIRA, Bitdefender, Sophos Intercept X, dll. Dalam penyuluhan ini dipilih aplikasi Sophos Intercept X karena alasan kepraktisan, kemudahan, kehandalan, serta bebas lisensi alias gratis.

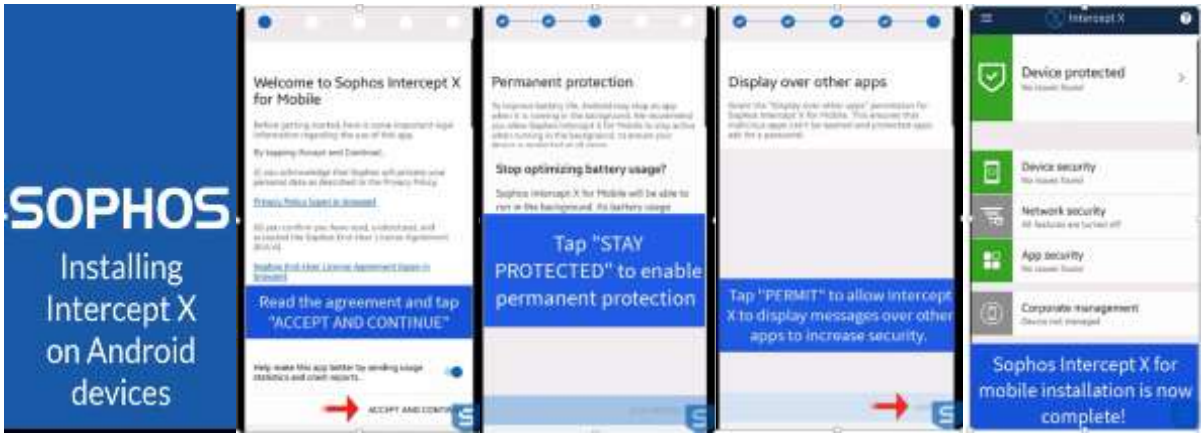
c. Sophos Intercept X

Aplikasi ini ibarat memberikan vaksin untuk melindungi dari penyakit, dan memasang pagar untuk keamanan rumah, intinya 'vaksin & pagar' untuk perangkat digital kita. Jadi, bayangkan Sophos Intercept X ini seperti vaksin untuk HP/laptop kita, atau seperti pagar dan satpam untuk rumah digital kita. Fungsinya satu: melindungi."

Gambar 1. Logo Sophos Intercept X (sumber: www. sophos.com)

Dalam kegiatan ini peserta diminta untuk mengunduh aplikasi yang dimaksud agar perangkat digital mereka khususnya smartphone dapat lebih terlindungi. Proses instalasi sendiri melalui lima tahapan utama yang mana tiap tahapannya meminta otorisasi keamanan perangkat agar nantinya aplikasi tersebut dapat lebih optimal dalam menjaga keamanan smartphone tersebut.

Jurnal Pengabdian Indonesia (JPI)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/jpi/index
Email: admin@jurnalcenter.com



Gambar 2. Proses Instalasi Sophos Intercept X (sumber: www. sophos.com)

Mayoritas peserta antusias dalam mengikuti proses instalasi ini dan mereka kini semakin menyadari pentingnya aplikasi keamanan digital di perangkat mereka. Karena ternyata hampir seluruhnya tidak atau belum memiliki aplikasi keamanan digital dan oleh karenanya kegiatan ini sangat membantu dalam hal edukasi terkait isu-isu keamanan dan keselamatan dunia siber. Dari angket tingkat kepuasan yang disebar 83% menyatakan sangat puas dan sisanya (17%) cukup puas.

Gambar 3. Tingkat kepuasan peserta akan kegiatan pengabdian masyarakat

Salah satu peserta, Ibu Gita, menanyakan terkait jika menggunakan wifi di ruang publik bagaimana level keamanannya dan apakah berpotensi mencuri data di smarthpone kita. Pemateri memberikan pemahaman bahwasannya untuk menggunakan wifi yang disediakan secara gratis di ruang publik, hendaknya hanya sekedar mencari informasi dan menjelajah hal-hal yang bersifat hiburan atau pengetahuan (Abdulkader, 2025). Hindari sebisa mungkin bertransaksi (belanja online, mobile banking) dan atau akses ke situs yang membutuhkan informasi pribadi dan bersifat sensitif (password, PIN). Karena para pelaku kejahatan dunia maya lebih menekankan pada kebiasaan pengguna atau user dari perangkat digital yang mereka miliki (Le, 2025; Puspitaningrum & Insani, 2024).

Jurnal Pengabdian Indonesia (JPI)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/jpi/index
Email: admin@jurnalcenter.com

Gambar 4. Antusiasme peserta akan kegiatan pengabdian masyarakat

Peserta lain, Bapak Gesa, menanyakan langkah-langkah pencegahan apa yang sebaiknya dilakukan sebagai user untuk meminimalisir bobolnya keamanan data di perangkat digital kita. Salah satu langkah yang bisa dilakukan adalah secara berkala melakukan penggantian password atau PIN. Hindari menggunakan password atau PIN yang mudah ditebak seperti tanggal, hari, bulan, dan tahun kelahiran (Korkes et al., 2024; Sadik & Ruoti, 2025). Juga sebisa mungkin jangan membuat password yang sama untuk berbagai akun yang dimiliki karena begitu satu akun berhasil diretas maka akun yang lain berpeluang tinggi untuk mudah juga diretas (Kissell, 2024). Kegiatan berjalan sangat interaktif saling bertukar pengalaman baik pemateri dengan peserta maupun antar sesama peserta. Harapan peserta adalah kegiatan serupa bisa kiranya dilakukan kembali secara berkala dengan topik-topik terkini seperti literasi keuangan digital, penggunaan artificial intelligence (AI) dalam memberdayakan UMKM di lingkungan mereka, dan lain-lain. Tentunya ini menjadi masukan bagi tim pelaksana kegiatan pengabdian masyarakat Prodi Administrasi Bisnis, Fakultas Ekonomi dan Bisnis, Telkom University untuk selanjutnya diagendakan di kemudian hari. Kegiatan ditutup dengan kesimpulan dan saran serta foto bersama dengan tim pemateri dan seluruh peserta.

Gambar 5. Sesi foto akhir kegiatan pengabdian masyarakat

Jurnal Pengabdian Indonesia (JPI)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/jpi/index
Email: admin@jurnalcenter.com

4. KESIMPULAN

Keamanan di perangkat digital mutlak diperlukan agar pengguna merasa lebih aman dalam menggunakan perangkatnya untuk berbagai keperluan bukan hanya mencari informasi dan hiburan namun utamanya adalah saat melakukan transaksi online seperti mobile banking maupun belanja online. Terbukti dalam kegiatan pengabdian masyarakat yang diadakan hampir seluruh peserta belum memiliki aplikasi keamanan digital yang terpasang di perangkat smartphone mereka. Melalui edukasi penyuluhan dan pelatihan maka level literasi keamanan akan pentingnya aplikasi anti malware di kalangan peserta menjadi lebih baik dari sebelumnya. Dan mereka akan menularkan hal baik ini di lingkungan keluarga masing-masing dan masyarakat sekitar khususnya yang belum sempat hadir dalam kegiatan yang diadakan.

5. DAFTAR PUSTAKA

Abdulkader, M. (2025). *Navigating privacy and usability: A user-centric study of public WiFi networks*.

Akbar, A., Kuswanto, A., & Kartawinata, B. R. (2025). MAINTAINING FAMILY PRIVACY AND SECURITY IN THE DIGITAL AGE. *Jurnal Pengabdian Indonesia (JPI)*, *1*(2), 119–125.

Al Qwaid, M. (2025). Cybersecurity Threats: Ransomware, Phishing, and Social Engineering. In *Complexities and Challenges for Securing Digital Assets and Infrastructure* (pp. 399–434). IGI Global Scientific Publishing.

Ali, M. M., & Mohd Zaharon, N. F. (2024). Phishing—A cyber fraud: The types, implications and governance. *International Journal of Educational Reform*, *33*(1), 101–121.

Ananta, K. D., Ambodo, T., & Tohawi, A. (2024). Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia. *Islamic Law: Jurnal Siyasah*, *9*(2), 113–118.

Babak, V., Babak, S., Eremenko, V., Kuts, Y., & Zaporozhets, A. (2025). Protection of Measurement Information from Unauthorized Access. In *Information-Measuring Systems: Theory and Application* (pp. 409–458). Springer.

Beretas, C. (2024). Information systems security, detection and recovery from cyber attacks. *Universal Library of Engineering Technology*, *1*(1).

Bharathi, M., Sandhyakumari, G., Madhurima, V., Tabassum, S., Kumar, N. A., & Neelima, K. (2025). Protecting Your Digital Life From Cyber Threats and Vulnerabilities. In *Convergence of Cybersecurity and Cloud Computing* (pp. 457–472). IGI Global Scientific Publishing.

Feng, S., & Tramèr, F. (2024). Privacy backdoors: Stealing data with corrupted pretrained models. *ArXiv Preprint ArXiv:2404.00473*.

Gallo, L., Gentile, D., Ruggiero, S., Botta, A., & Ventre, G. (2024). The human factor in phishing: Collecting and analyzing user behavior when reading emails. *Computers & Security*, *139*, 103671.

Garfinkel, S. (2024). *Complete Delete: In Practice, Clicking'Delete'Rarely Deletes. Should it?*

Gilsenan, C. (2025). *Exploring the Security and Privacy Impacts of Using 2FA Apps*.

Jurnal Pengabdian Indonesia (JPI)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/jpi/index
Email: admin@jurnalcenter.com

Halfacree, G. (2025). *The official Raspberry Pi Beginner's Guide: How to use your new computer*. Raspberry Pi Press.

Henry, V. (2018). *Verizon 2018 data breach investigations report (DBIR)*.

Jabid, T., Masum, S., Shams, R. A., Chowdhury, A., Islam, M. M., Ferdaus, M. H., Ali, M. S., & Islam, M. (2024). A brief history of ransomware. In *Ransomware Evolution* (pp. 3–17). CRC Press.

Kaspersky, I. C. S. (2021). Threat landscape for industrial automation systems. *Statistics for H*, *1*, 2021.

Kissell, J. (2024). *Take Control of 1password*. alt concepts.

Korkes, E., Munyendo, C. W., Isaac, A., Hennemann, V., & Aviv, A. J. (2024). " I'm going to try her birthday": Investigating How Friends Guess Each Other's Smartphone Unlock PINs in the Lab. *Proceedings of the 2024 European Symposium on Usable Security*, 220–234.

Le, K. (2025). *Are We Safe in the Digital World? Why We Still Fall Victim to Cybercrime*.

Mclaughlin, K. L., & Elliott, E. S. A. (2023). UNLEASHING THE POWER OF MOBILE THREAT HUNTING TOOLKITS: WHY THEY ARE CRUCIAL IN TODAY'S CYBERSECURITY LANDSCAPE. *EDPACS*, *68*(3), 1–6.

Puspitaningrum, N., & Insani, K. T. K. C. (2024). KESADARAN AKAN KEAMANAN DIGITAL. *TRANSFORMASI PEMBELAJARAN Anak Usia Dini Di Zaman Digital*, 116.

Sadik, J., & Ruoti, S. (2025). A large-scale survey of password entry practices on non-desktop devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *9*(3), 1–30.

Salman, M., Ikram, M., & Kaafar, M. A. (2024). Investigating evasive techniques in SMS spam filtering: A comparative analysis of machine learning models. *IEEE Access*, *12*, 24306–24324.

Santoso, J. T. (2023). Teknologi Keamanan Siber (Cyber Security). *Penerbit Yayasan Prima Agus Teknik*, 1–173.

Saylor, M. J., & Saylor, M. (2025). *The mobile wave: How mobile intelligence will change everything*. Hachette+ ORM.

Shafik, W. (2025). Data Loss Software Reason and Hardware Reason. In *Data Recovery Techniques for Computer Forensics* (pp. 27–61). Bentham Science Publishers.

Shahid, S. Z., Bangash, M. A., Hussain, M. R., & Arshad, S. (2024). CyberCure-Malware Defense System. *2024 4th International Conference on Innovations in Computer Science (ICONICS)*, 1–7.

Siber, B., & Negara, S. (2022). Laporan tahunan keamanan siber di Indonesia. *Jakarta: BSSN*.

Suarti, I. (2024). *Deteksi situs Phishing berbasis Neural Network*. Universitas Islam Negeri Maulana Malik Ibrahim.

Symantec, C. (2019). Internet security threat report: Volume 24. *Symantee Enterprise Security*.

Tanti, R. (2024). Study of Phishing Attack and their Prevention Techniques. *International Journal of Scientific Research in Engineering and Management*, *8*(10), 1–8.

Jurnal Pengabdian Indonesia (JPI)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/jpi/index
Email: admin@jurnalcenter.com

Triantafyllou, G. P. (2024). *Malware analysis*. Πανεπιστήμιο Πειραιώς.

Vishwakarma, R., & Dhakad, R. (2024). Online advertising and fraud click in online advertisement: A survey. *International Journal of Computer Applications*, *186*(1), 975–8887.

Vitali, S., & Giuliani, M. (2024). Emerging digital technologies and auditing firms: Opportunities and challenges. *International Journal of Accounting Information Systems*, *53*, 100676.

Wibowo, A., & Yulianingsih, S. (2025). Hukum Teknologi Informasi. *Penerbit Yayasan Prima Agus Teknik*.