KENDURI: Jurnal Pengabdian Dan Pemberdayaan Masyarakat

Vol. 6 No. 2 Hal. 234-245
https://siducat.org/index.php/kenduri
e_ISSN: 2776-9186

Peningkatan Kesadaran Keamanan Data Digital dan Jaringan Wi-Fi Publik bagi Pelajar dari Tiga Sekolah Mitra dan Masyarakat Umum melalui Webinar dan Workshop

Luqman Ali Dinul Ramadhan[1*], Agung Firmansyah[2], Muhammad Kamal Ibrahim[3], Muhammad Bilal Taqwa[4], Muhammad Azril Naufal Shadiq[5], Muhammad Jihan Maulana Zuhri[6], Popy Meilina[7], Rita Dewi Risanty[8], Yana Adharani[9], Sitti Nurbaya Ambo[10], Hendra[11], Rully Mujiastuti[12]

[1-10]Universitas Muhammadiyah Jakarta

e-mail korespondensi*: 23040700050@student.umj.ac.id

History Article

Received: 28 July 2026
Revised: 15 August 2026
Accepted: 18 August 2026

Keyword

Data Security; Network Security; Webinar; Workshop; Digital Literacy

Abstract

This community service activity, part of the KKN Dissemination of Internships and Certified Independent Studies Batch 10 program, aimed at improving data and network security awareness among students from three partner schools, SMA Dewan Dakwah Bekasi, MTsN 24 East Jakarta, and SMK Pendidikan Cikini Jakarta, together with the general public. The team applied four stages: a needs analysis of the partner schools, preparation of materials and event administration, a one-day online webinar and workshop held via Zoom on 27 June 2026, and an evaluation using pre-test, post-test, and feedback instruments covering network threats, the HTTP/HTTPS distinction, Wireshark-based traffic analysis, and two-factor authentication. Of 98 registrants, 56 participants completed both the pre-test and post-test, while 56 participants completed the feedback form. The average score rose from 82.68 to 93.45, a gain of 10.77 points, and most respondents rated the material's relevance and delivery highly. These results indicate that combining conceptual explanation with hands-on demonstration improved participants' understanding of public Wi-Fi network security risks.

To cite this article: Ramadhan, L. A. D. et al. (2026). *Peningkatan Kesadaran Keamanan Data Digital dan Jaringan Wi-Fi Publik bagi Pelajar dari Tiga Sekolah Mitra dan Masyarakat Umum melalui Webinar dan Workshop*. **Kenduri: Jurnal Pengabdian dan Pemberdayaan Masyarakat.** 6(2) 2026, Hal: 234-245. https://doi.org/10.62159/kenduri.v6i.xxx

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong meningkatnya penggunaan internet dalam berbagai aktivitas masyarakat, mulai dari komunikasi, pendidikan, hingga layanan publik (Doloi, 2025). Kondisi tersebut membentuk ekosistem digital yang semakin luas sehingga pertukaran informasi dapat dilakukan secara lebih cepat dan efisien (Dabbous et al., 2023). Seiring dengan meningkatnya pemanfaatan teknologi digital, pengguna internet juga dituntut memiliki kompetensi dalam menggunakan teknologi secara aman agar aktivitas pertukaran informasi tidak menimbulkan risiko terhadap keamanan data pribadi (Tempestini et al., 2023). Dengan demikian, peningkatan literasi keamanan digital menjadi salah satu aspek yang tidak dapat dipisahkan dari pemanfaatan teknologi informasi di masyarakat (Kurniasih, 2023).

Meskipun internet memberikan berbagai kemudahan, penggunaan jaringan publik masih menyimpan berbagai kerentanan terhadap keamanan informasi. Jaringan Wi-Fi publik berpotensi dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan pencurian data, akses tidak sah, maupun penyadapan lalu lintas jaringan (Ananta & Hasa, 2025). Risiko tersebut semakin besar ketika komunikasi masih menggunakan protokol Hypertext Transfer Protocol (HTTP) yang tidak menerapkan mekanisme enkripsi sehingga informasi sensitif, seperti username dan password, dapat terekspos selama proses transmisi data (Manguling & Parenreng, 2023). Oleh karena itu, kemampuan pengguna dalam memahami karakteristik jaringan dan mengenali bentuk-bentuk ancaman keamanan menjadi bagian penting dalam upaya melindungi data pribadi (Kingsley David Onyewuchi Ofoegbu et al., 2024).

Salah satu media yang dapat digunakan untuk memperkenalkan kerentanan komunikasi jaringan kepada masyarakat adalah Wireshark. Aplikasi ini telah dimanfaatkan sebagai media pembelajaran keamanan siber karena mampu menampilkan lalu lintas paket data secara langsung sehingga membantu pengguna memahami proses komunikasi dalam jaringan (Allison, 2022). Selain berfungsi sebagai network protocol analyzer untuk menangkap dan menganalisis paket data (Wu & Jiao, 2023), Wireshark juga dapat digunakan untuk memperlihatkan bagaimana informasi yang dikirim melalui protokol HTTP dapat diamati ketika tidak menggunakan enkripsi (Ananta & Hasa, 2025). Penggunaan media pembelajaran yang bersifat demonstratif tersebut dinilai mampu meningkatkan kesadaran pengguna terhadap pentingnya menjaga keamanan data selama beraktivitas di internet (Ortiz-Garcés et al., 2024). Pendekatan edukasi berbasis demonstrasi dipilih karena memberikan pengalaman belajar yang lebih mudah dipahami dibandingkan penyampaian materi secara konseptual semata (Drushlyak et al., 2025).

Meskipun informasi mengenai keamanan digital semakin mudah diperoleh, masih diperlukan upaya edukasi untuk meningkatkan pemahaman masyarakat mengenai keamanan data dan jaringan (Saleh et al., 2025). Identifikasi kebutuhan program dilakukan melalui hasil pre-test yang diberikan kepada peserta sebelum penyampaian materi webinar dan workshop. Pre-test diikuti oleh peserta yang telah mendaftar melalui tautan pendaftaran yang disebarkan kepada mitra sasaran, yaitu SMA Dewan Da'wah, SMK Perguruan Cikini Jakarta, dan MTsN 24 Jakarta Timur, serta masyarakat umum. Instrumen pre-test memuat pertanyaan mengenai pengetahuan dasar peserta terkait keamanan data pribadi, penggunaan jaringan publik, ancaman keamanan siber, serta penggunaan website yang aman. Hasil pre-test menunjukkan nilai rata-rata awal peserta sebesar 82,68%, yang kemudian digunakan sebagai gambaran kondisi pengetahuan awal peserta sekaligus dasar dalam penyusunan materi webinar dan workshop. Materi selanjutnya diarahkan pada pembahasan keamanan web dan jaringan, HTTP dan HTTPS, SSL/TLS, ancaman pada jaringan publik, serta perlindungan data digital.

Permasalahan tersebut diperkuat oleh masih tingginya risiko serangan pada jaringan publik. Pengguna internet awam masih rentan terhadap berbagai bentuk manipulasi, seperti serangan Evil Twin dan fake captive portal, yang dapat mengecoh pengguna untuk menyerahkan data kredensial demi memperoleh akses internet (Nanayakkara et al., 2024). Kebocoran data tersebut berpotensi menimbulkan penyalahgunaan identitas digital, termasuk untuk pengajuan kredit fiktif pada layanan pinjaman daring ilegal (Fernando, 2024). Oleh karena itu, diperlukan kegiatan edukasi yang tidak hanya memperkenalkan konsep keamanan jaringan, tetapi juga membantu masyarakat memahami bentuk ancaman yang dapat ditemui dalam penggunaan internet sehari-hari sehingga mampu menerapkan langkah-langkah perlindungan secara mandiri (Rahmawati et al., 2024).

Berdasarkan kondisi tersebut, Tim 4 Kuliah Kerja Nyata (KKN) menyelenggarakan kegiatan pengabdian kepada masyarakat melalui webinar dan workshop bertajuk Tingkatkan Kesadaran Keamanan Data & Jaringan. Kegiatan ini dirancang sebagai upaya untuk meningkatkan literasi keamanan digital masyarakat melalui pendekatan edukatif yang disusun berdasarkan kebutuhan mitra hasil observasi lapangan. Artikel ini bertujuan memaparkan pelaksanaan kegiatan pengabdian tersebut serta mengevaluasi upaya peningkatan pemahaman peserta mengenai keamanan data dan jaringan sebagai salah satu bentuk penguatan literasi keamanan digital di masyarakat.

METODE

Pelaksanaan kegiatan ini disusun melalui empat tahap berurutan: analisis kebutuhan mitra, persiapan, pelaksanaan webinar dan workshop, serta evaluasi.

A. Analisis Kebutuhan Mitra

Tim melakukan koordinasi dan observasi awal terhadap tiga mitra sekolah untuk memetakan persoalan yang dihadapi. Hasilnya menunjukkan rendahnya literasi menjaga data pribadi, minimnya

pengenalan terhadap ancaman siber seperti phishing dan malware, belum dikenalnya aplikasi analisis jaringan seperti Wireshark, serta rendahnya penerapan autentikasi dua faktor. Temuan ini menjadi dasar penentuan tema dan cakupan materi kegiatan.

Gambar 1 Koordinasi dan Penyampaian Informasi Kegiatan Kepada Pihak Mitra

Pada tahap ini, tim menyampaikan informasi mengenai tujuan kegiatan, tema webinar, jadwal pelaksanaan, mekanisme pendaftaran, serta manfaat yang akan diperoleh peserta. Melalui kerja sama tersebut, masing-masing mitra membantu menyebarluaskan poster dan informasi kegiatan kepada guru, peserta didik, serta warga sekolah sehingga jumlah peserta yang mengikuti kegiatan dapat menjangkau berbagai kalangan. Kolaborasi ini juga menjadi bentuk sinergi antara perguruan tinggi dengan institusi pendidikan dalam meningkatkan literasi keamanan data dan jaringan.

B. Persiapan

Tahap persiapan diawali dengan konsultasi bersama dosen pembimbing lapangan untuk menentukan tema dan sasaran kegiatan, dilanjutkan koordinasi internal tim melalui pertemuan daring dan grup WhatsApp untuk membagi tugas. Tim juga menjalin komunikasi dengan ketiga mitra untuk menyebarluaskan informasi pendaftaran, menyusun materi webinar dan skenario demonstrasi workshop, menyiapkan instrumen pre-test, post-test, dan formulir feedback, serta menyusun rundown acara. Tahap ini ditutup dengan gladi bersih untuk menguji koneksi internet, perangkat, dan kesiapan platform Zoom Meeting beserta skenario demonstrasi Wireshark dan Have I Been Pwned.

Gambar 2 bimbingan bersama dosen pembimbing

Masukan yang diberikan selama proses bimbingan menjadi dasar bagi tim dalam menyempurnakan konsep kegiatan. Setelah melalui beberapa penyesuaian, disepakati bahwa program kerja yang akan dilaksanakan berupa Webinar dan Workshop "Tingkatkan Kesadaran Keamanan Data & Jaringan" yang berfokus pada edukasi mengenai keamanan web, keamanan jaringan, serta perlindungan data digital. Selain menjadi acuan dalam penyusunan materi, hasil bimbingan tersebut juga digunakan sebagai pedoman dalam menyusun metode pelaksanaan, instrumen evaluasi, serta kebutuhan teknis selama kegiatan berlangsung.

C. Pelaksanaan Webinar dan Workshop

Kegiatan dilaksanakan secara daring pada Sabtu, 27 Juni 2026, pukul 09.30–12.30 WIB melalui Zoom Meeting Conference. Sesi webinar diisi pemaparan konseptual mengenai ancaman jaringan, protokol HTTP/HTTPS, peran SSL/TLS, serta langkah mitigasi dasar. Sesi workshop dilanjutkan dengan dua demonstrasi praktik: perbandingan lalu lintas HTTP dan HTTPS menggunakan Wireshark, serta pengecekan riwayat kebocoran data melalui Have I Been Pwned yang diikuti edukasi mengaktifkan verifikasi dua langkah.

Pada sesi webinar, materi webinar disampaikan oleh Agung Firmansyah selaku pemateri. Materi diawali dengan pembahasan mengenai berbagai ancaman keamanan siber yang sering ditemui dalam penggunaan jaringan publik, seperti *malware*, *phishing*, *Distributed Denial of Service* (*DDoS*), dan *sniffing*. Selanjutnya, peserta diberikan pemahaman mengenai proses pertukaran data pada jaringan komputer, perbedaan antara protokol HTTP dan HTTPS, serta peran SSL/TLS dalam menjaga kerahasiaan, integritas, dan autentikasi data selama proses komunikasi berlangsung.

Gambar 3 Penyampaian materi webinar oleh Agung Firmansyah

Selain membahas konsep dasar keamanan jaringan, pemateri juga menjelaskan berbagai teknik serangan yang dapat terjadi pada jaringan publik, seperti *Man-in-the-Middle* (*MitM*) dan *Evil Twin*, beserta langkah-langkah pencegahan yang dapat dilakukan oleh pengguna. Beberapa upaya perlindungan yang disampaikan antara lain menggunakan website berprotokol HTTPS, mengaktifkan autentikasi dua faktor (*Two-Factor Authentication*), memanfaatkan jaringan pribadi atau *Virtual Private Network* (VPN) saat mengakses jaringan publik, serta melakukan pembaruan sistem secara berkala. Penyampaian materi dilakukan secara interaktif dengan disertai ilustrasi, studi kasus, dan contoh penerapan dalam kehidupan sehari-hari sehingga peserta lebih mudah memahami materi yang disampaikan.

Setelah penyampaian materi selesai, moderator membuka sesi diskusi dan tanya jawab. Pada sesi ini, peserta diberikan kesempatan untuk mengajukan pertanyaan mengenai materi yang telah disampaikan, khususnya terkait keamanan data saat menggunakan jaringan Wi-Fi publik, penerapan HTTPS, penggunaan VPN, serta langkah-langkah yang dapat dilakukan apabila terjadi kebocoran data pribadi. Antusiasme peserta terlihat dari banyaknya pertanyaan yang diajukan selama sesi berlangsung. Seluruh pertanyaan dijawab secara langsung oleh pemateri sehingga peserta memperoleh pemahaman yang lebih mendalam mengenai materi yang telah dipelajari.

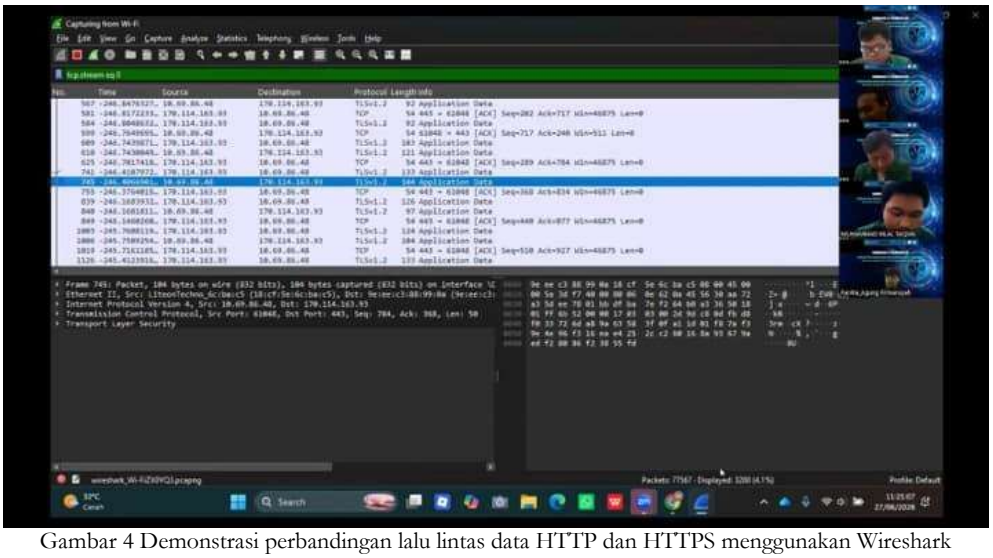
Setelah sesi webinar dan diskusi selesai dilaksanakan, kegiatan dilanjutkan dengan sesi workshop yang dipandu oleh Muhammad Bilal Taqwa selaku pemateri. Berbeda dengan sesi webinar yang berfokus pada penyampaian konsep dan teori, sesi workshop dirancang agar peserta dapat memahami materi melalui

demonstrasi secara langsung mengenai proses pertukaran data pada jaringan komputer serta penerapan langkah-langkah sederhana untuk menjaga keamanan data pribadi ketika menggunakan internet.

Workshop diawali dengan pengenalan aplikasi Wireshark sebagai salah satu perangkat lunak yang digunakan untuk melakukan analisis lalu lintas jaringan (*network traffic analyzer*). Pada sesi ini, pemateri menjelaskan fungsi Wireshark dalam proses pemantauan paket data yang melintas pada suatu jaringan serta pemanfaatannya sebagai media pembelajaran untuk meningkatkan pemahaman mengenai keamanan jaringan komputer. Sebelum demonstrasi dilakukan, pemateri juga menegaskan bahwa penggunaan Wireshark pada kegiatan ini hanya bertujuan sebagai sarana edukasi untuk menunjukkan pentingnya penggunaan protokol komunikasi yang aman dan bukan untuk mengajarkan aktivitas penyadapan data.

Selanjutnya, pemateri mendemonstrasikan proses analisis lalu lintas jaringan dengan membandingkan komunikasi yang menggunakan protokol HTTP dan HTTPS. Pada simulasi pertama, peserta diperlihatkan bagaimana data yang dikirim melalui website yang masih menggunakan protokol HTTP dapat terbaca dalam bentuk *plain text* ketika diamati menggunakan Wireshark. Melalui demonstrasi tersebut, peserta dapat melihat bahwa informasi seperti *username* dan data lainnya masih dapat diidentifikasi karena tidak melalui proses enkripsi.

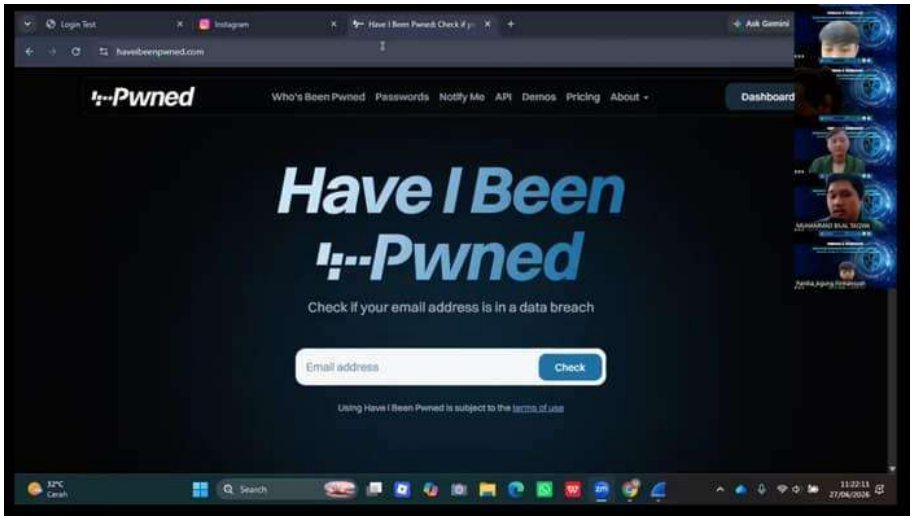
Sebagai perbandingan, pemateri kemudian memperlihatkan proses komunikasi menggunakan website yang telah menerapkan protokol HTTPS. Hasil analisis menunjukkan bahwa paket data yang dikirim telah mengalami proses enkripsi sehingga isi informasi yang dikirimkan tidak dapat dibaca secara langsung. Demonstrasi ini memberikan gambaran kepada peserta mengenai pentingnya penggunaan HTTPS dalam menjaga kerahasiaan data selama proses transmisi melalui jaringan.



Gambar 4 Demonstrasi perbandingan lalu lintas data HTTP dan HTTPS menggunakan Wireshark

Setelah demonstrasi menggunakan Wireshark selesai, workshop dilanjutkan dengan praktik pengecekan kebocoran data menggunakan layanan Have I Been Pwned. Pemateri memperkenalkan fungsi layanan tersebut sebagai media untuk mengetahui apakah suatu alamat email pernah menjadi bagian dari insiden kebocoran data yang dipublikasikan. Selanjutnya, peserta diajak untuk melakukan pengecekan secara mandiri menggunakan alamat email masing-masing dengan mengikuti langkah-langkah yang dicontohkan oleh pemateri.

Melalui praktik tersebut, peserta memperoleh pengalaman secara langsung mengenai cara memeriksa status keamanan akun yang dimiliki. Bagi peserta yang menemukan alamat emailnya pernah terlibat dalam insiden kebocoran data, pemateri memberikan penjelasan mengenai langkah-langkah yang perlu dilakukan, seperti mengganti kata sandi, menggunakan kata sandi yang berbeda pada setiap akun, serta mengaktifkan autentikasi dua faktor (*Two-Factor Authentication*) sebagai upaya meningkatkan keamanan akun.



Gambar 5 Praktik pengecekan kebocoran data menggunakan Have I Been Pwned

Setelah seluruh demonstrasi selesai dilaksanakan, moderator membuka sesi diskusi dan tanya jawab. Peserta memanfaatkan kesempatan tersebut untuk mengajukan berbagai pertanyaan terkait penggunaan Wireshark, keamanan jaringan publik, hasil pengecekan kebocoran data, serta penerapan langkah-langkah perlindungan akun dalam kehidupan sehari-hari. Diskusi berlangsung secara interaktif dan menunjukkan tingginya antusiasme peserta terhadap materi yang telah dipraktikkan selama workshop.

D. Evaluasi

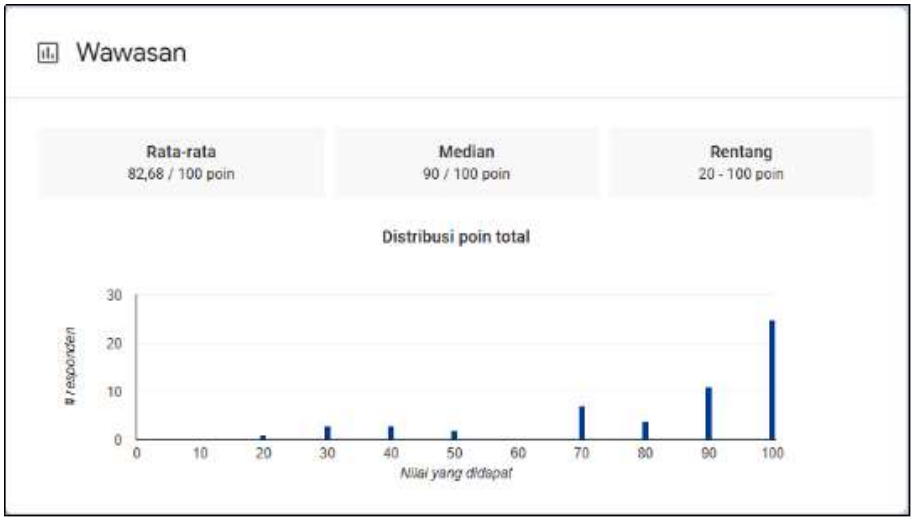
Efektivitas kegiatan diukur melalui tiga instrumen: pre-test yang diisi peserta sebelum materi disampaikan, post-test yang diisi setelah seluruh sesi selesai, dan formulir feedback mengenai kualitas materi, penyampaian pemateri, serta pelaksanaan kegiatan secara umum. Hasil dari ketiga instrumen ini dijadikan dasar penilaian pada bagian selanjutnya.

HASIL DAN PEMBAHASAN

Tahap evaluasi merupakan komponen krusial dalam pelaksanaan program Kuliah Kerja Nyata (KKN) ini guna mengukur tingkat keberhasilan kegiatan secara objektif dan komprehensif. Proses evaluasi dilakukan dengan menganalisis data primer yang diperoleh dari tiga instrumen utama, yaitu pre-test, post-test, dan formulir feedback (umpan balik) yang diisi oleh peserta pada penghujung acara. Hasil dari evaluasi ini menjadi tolok ukur sejauh mana program diseminasi mampu meningkatkan literasi keamanan data dan jaringan masyarakat.

1. Hasil Pre-Test

Sebelum penyampaian materi webinar dimulai, peserta yang mengikuti diminta untuk mengisi *pre-test* melalui Google Form yang telah disediakan oleh panitia. Pelaksanaan *pre-test* bertujuan untuk mengukur tingkat pemahaman awal peserta terhadap materi yang akan disampaikan selama webinar dan workshop. Pertanyaan yang diberikan mencakup konsep dasar keamanan web dan jaringan, ancaman keamanan siber, perbedaan protokol HTTP dan HTTPS, fungsi SSL/TLS, serta langkah-langkah sederhana dalam menjaga keamanan data pribadi ketika menggunakan internet



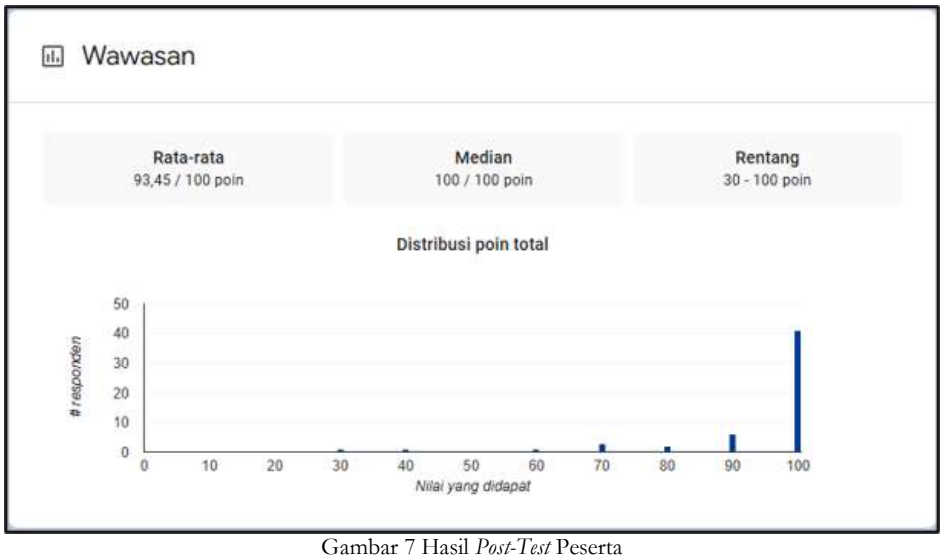
Gambar 6 Hasil *Pre-Test* Peserta

Berdasarkan hasil *pre-test*, diperoleh nilai rata-rata peserta sebesar 82,68 dari skala 100 dengan nilai median 90, sedangkan rentang nilai peserta berada pada kisaran 20 hingga 100. Hasil tersebut menunjukkan bahwa sebagian besar peserta telah memiliki pemahaman dasar mengenai keamanan web dan jaringan. Namun demikian, masih terdapat beberapa peserta yang memperoleh nilai relatif rendah sehingga menunjukkan adanya perbedaan tingkat pemahaman di antara peserta sebelum mengikuti kegiatan.

Distribusi nilai juga memperlihatkan bahwa sebagian besar peserta memperoleh nilai pada rentang 90 hingga 100, sedangkan sebagian kecil peserta masih berada pada rentang nilai di bawah 70. Kondisi tersebut menjadi dasar bagi pemateri untuk menyampaikan materi secara sistematis, dimulai dari konsep-konsep dasar hingga penerapan keamanan web dan jaringan dalam kehidupan sehari-hari sehingga seluruh peserta dapat mengikuti materi dengan baik, terlepas dari perbedaan tingkat pengetahuan awal yang dimiliki.

2. Hasil Post-Test

Setelah seluruh rangkaian webinar dan workshop selesai dilaksanakan, peserta kembali diminta mengisi *post-test* menggunakan instrumen yang sama dengan *pre-test*. Pelaksanaan *post-test* bertujuan untuk mengukur peningkatan pemahaman peserta setelah memperoleh materi webinar, mengikuti demonstrasi penggunaan Wireshark, serta praktik pengecekan kebocoran data menggunakan layanan *Have I Been Pwned*.



Gambar 7 Hasil *Post-Test* Peserta

Hasil *post-test* menunjukkan adanya peningkatan pemahaman peserta terhadap materi yang telah disampaikan. Nilai rata-rata peserta meningkat menjadi 93,45 dari skala 100 dengan nilai median 100, sedangkan rentang nilai berada pada kisaran 30 hingga 100. Dibandingkan dengan hasil *pre-test*, nilai rata-rata peserta mengalami peningkatan sebesar 10,77 poin, yang menunjukkan bahwa materi webinar dan workshop mampu meningkatkan pemahaman peserta mengenai keamanan web dan jaringan.

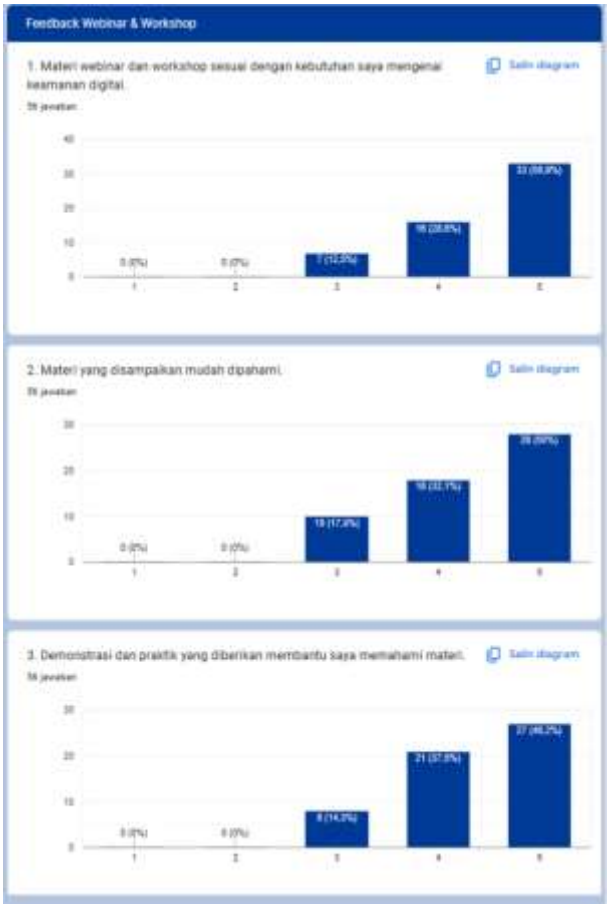
Selain peningkatan nilai rata-rata, distribusi hasil *post-test* juga memperlihatkan bahwa mayoritas peserta memperoleh nilai 100, sementara hanya sebagian kecil peserta yang memperoleh nilai di bawah 90. Hasil tersebut menunjukkan bahwa penyampaian materi secara bertahap yang dipadukan dengan demonstrasi praktik memberikan dampak positif terhadap pemahaman peserta, khususnya mengenai penggunaan protokol HTTPS, fungsi SSL/TLS, ancaman keamanan jaringan publik, serta pentingnya menjaga keamanan data pribadi ketika menggunakan internet.

Secara keseluruhan, hasil *pre-test* dan *post-test* menunjukkan bahwa pelaksanaan webinar dan workshop berhasil meningkatkan pengetahuan peserta mengenai keamanan web dan jaringan. Peningkatan tersebut menjadi salah satu indikator bahwa tujuan kegiatan untuk meningkatkan literasi keamanan data digital telah tercapai dengan baik.

3. Hasil Feedback

Sebagai bagian dari proses monitoring dan evaluasi, panitia menyebarkan formulir *feedback* kepada seluruh peserta setelah rangkaian webinar dan workshop selesai dilaksanakan. Pengisian *feedback* bertujuan untuk mengetahui tingkat kepuasan peserta terhadap pelaksanaan kegiatan, kualitas materi yang disampaikan, serta performa pemateri selama kegiatan berlangsung. Selain itu, hasil *feedback* juga menjadi bahan evaluasi bagi tim penyelenggara dalam merancang kegiatan serupa pada masa mendatang agar dapat memberikan pengalaman belajar yang lebih baik.

A. Feedback terhadap Pelaksanaan Webinar dan Workshop



Gambar 8 Hasil feedback peserta terhadap pelaksanaan webinar dan workshop

Berdasarkan hasil *feedback* yang diberikan oleh 56 peserta, diperoleh tanggapan yang sangat positif terhadap pelaksanaan webinar dan workshop. Pada aspek kesesuaian materi dengan kebutuhan peserta, sebanyak 58,9% peserta memberikan penilaian 5 (sangat setuju) dan 28,6% memberikan penilaian 4 (setuju). Hasil tersebut menunjukkan bahwa materi yang disampaikan dinilai relevan dengan kebutuhan peserta dalam meningkatkan pemahaman mengenai keamanan web dan jaringan.

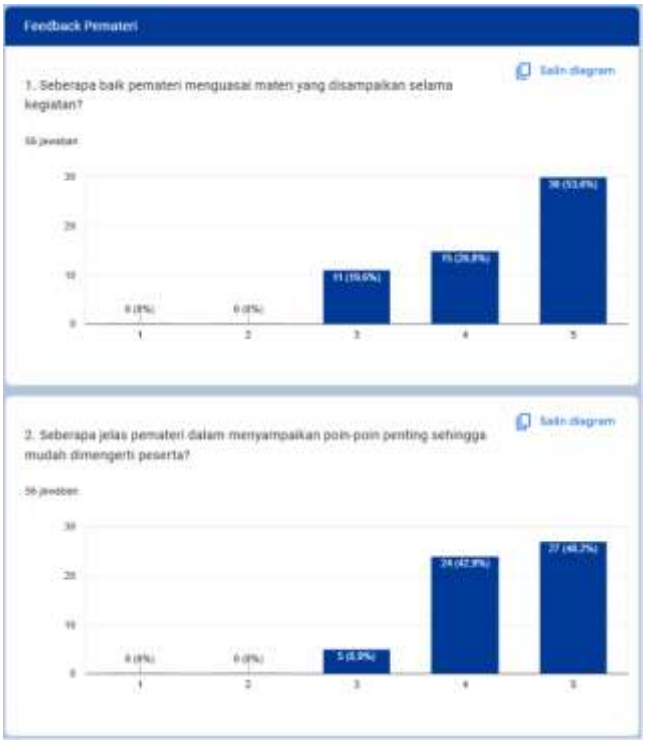
Pada aspek kemudahan memahami materi, sebanyak 50% peserta memberikan nilai 5 dan 32,1% memberikan nilai 4. Hal ini menunjukkan bahwa penyampaian materi dapat dipahami dengan baik oleh

sebagian besar peserta, meskipun latar belakang peserta berasal dari berbagai kalangan, seperti pelajar, mahasiswa, dan masyarakat umum.

Sementara itu, pada aspek demonstrasi dan praktik, sebanyak 48,2% peserta memberikan nilai 5, sedangkan 37,5% memberikan nilai 4. Hasil tersebut menunjukkan bahwa demonstrasi menggunakan Wireshark serta praktik pengecekan kebocoran data melalui layanan *Have I Been Pwned* mampu membantu peserta memahami materi yang telah disampaikan selama sesi webinar.

Dari sisi pelaksanaan kegiatan, sebanyak 58,9% peserta menilai bahwa webinar dan workshop telah berjalan dengan sangat baik dan terorganisasi, sedangkan 28,6% lainnya memberikan penilaian baik. Selain itu, sebanyak 64,3% peserta menyatakan sangat tertarik untuk mengikuti kegiatan serupa pada masa mendatang, sementara 25% peserta memberikan penilaian baik terhadap ketertarikan tersebut. Hasil ini menunjukkan bahwa kegiatan yang diselenggarakan mendapatkan respons positif dan dinilai bermanfaat oleh mayoritas peserta.

B. Feedback terhadap Pemateri



Gambar 9 Hasil feedback peserta terhadap pemateri

Selain mengevaluasi pelaksanaan kegiatan, peserta juga memberikan penilaian terhadap kualitas penyampaian materi oleh pemateri. Berdasarkan hasil *feedback*, sebanyak 53,6% peserta memberikan nilai 5 terhadap penguasaan materi oleh pemateri, sedangkan 26,8% memberikan nilai 4. Hal ini menunjukkan bahwa pemateri dinilai mampu menguasai materi dengan baik serta menyampaikan informasi secara jelas kepada peserta.

Pada aspek kejelasan penyampaian materi, sebanyak 48,2% peserta memberikan nilai 5 dan 42,9% memberikan nilai 4. Selain itu, sebanyak 55,4% peserta memberikan penilaian 5 terhadap kemampuan pemateri dalam menanggapi pertanyaan peserta selama sesi diskusi, sedangkan 30,4% memberikan penilaian 4. Hasil tersebut menunjukkan bahwa sesi diskusi berlangsung secara interaktif dan pemateri mampu memberikan penjelasan yang sesuai dengan pertanyaan yang diajukan peserta.

Adapun pada aspek pengelolaan waktu presentasi, mayoritas peserta memberikan penilaian baik hingga sangat baik, meskipun masih terdapat sebagian kecil peserta yang memberikan penilaian rendah. Hal tersebut menjadi salah satu masukan bagi tim penyelenggara agar pengaturan waktu pada kegiatan serupa dapat lebih dioptimalkan. Sementara itu, pada aspek semangat dan energi pemateri selama membimbing peserta, sebanyak 57,1% peserta memberikan nilai 5 dan 30,4% memberikan nilai 4, yang menunjukkan bahwa pemateri mampu menciptakan suasana pembelajaran yang aktif, komunikatif, dan mendorong partisipasi peserta selama kegiatan berlangsung.

Secara keseluruhan, hasil *feedback* menunjukkan bahwa pelaksanaan webinar dan workshop memperoleh respons yang sangat baik dari peserta. Mayoritas peserta memberikan penilaian baik hingga sangat baik terhadap kualitas materi, penyelenggaraan kegiatan, serta penyampaian materi oleh pemateri. Hasil evaluasi ini menunjukkan bahwa tujuan kegiatan dalam meningkatkan kesadaran mengenai keamanan data dan jaringan telah tercapai, sekaligus menjadi dasar bagi tim penyelenggara untuk terus meningkatkan kualitas pelaksanaan kegiatan serupa di masa yang akan datang.

4. Hasil Evaluasi

Evaluasi kegiatan dilakukan untuk menilai keberhasilan pelaksanaan Webinar dan Workshop "Tingkatkan Kesadaran Keamanan Data & Jaringan" berdasarkan seluruh rangkaian kegiatan yang telah dilaksanakan. Proses evaluasi mengacu pada hasil *pre-test*, *post-test*, formulir *feedback* peserta, serta hasil observasi yang dilakukan oleh panitia selama kegiatan berlangsung. Evaluasi ini bertujuan untuk mengetahui sejauh mana tujuan kegiatan telah tercapai sekaligus mengidentifikasi aspek-aspek yang masih dapat ditingkatkan pada pelaksanaan kegiatan serupa di masa mendatang

Berdasarkan hasil evaluasi, kegiatan webinar dan workshop secara umum telah berjalan dengan baik sesuai dengan *rundown* yang telah disusun. Seluruh rangkaian acara, mulai dari pembukaan, penyampaian materi webinar, sesi diskusi, pelaksanaan workshop, hingga penutupan dapat terlaksana sesuai dengan jadwal yang telah direncanakan. Koordinasi yang baik antar anggota panitia serta kesiapan teknis sebelum kegiatan berlangsung turut mendukung kelancaran pelaksanaan kegiatan sehingga tidak ditemukan kendala yang menghambat jalannya acara secara signifikan.

Dari sisi capaian pembelajaran, kegiatan ini menunjukkan hasil yang positif. Hal tersebut ditunjukkan melalui peningkatan nilai rata-rata peserta dari 82,68 pada saat *pre-test* menjadi 93,45 pada saat *post-test*. Peningkatan sebesar 10,77 poin tersebut menunjukkan bahwa materi yang disampaikan selama webinar dan workshop mampu meningkatkan pemahaman peserta mengenai keamanan web dan jaringan, khususnya terkait perbedaan protokol HTTP dan HTTPS, fungsi SSL/TLS, ancaman keamanan pada jaringan publik, serta langkah-langkah sederhana dalam menjaga keamanan data pribadi saat menggunakan internet.

Selain peningkatan hasil pembelajaran, tanggapan peserta melalui formulir *feedback* juga menunjukkan respons yang sangat positif terhadap pelaksanaan kegiatan. Mayoritas peserta memberikan penilaian baik hingga sangat baik terhadap kualitas materi, metode penyampaian, demonstrasi praktik, maupun kinerja pemateri. Tingginya minat peserta untuk mengikuti kegiatan serupa pada masa mendatang menunjukkan bahwa tema keamanan data digital merupakan topik yang relevan dan dibutuhkan oleh masyarakat, khususnya di kalangan pelajar dan mahasiswa.

Meskipun kegiatan telah berjalan dengan baik, terdapat beberapa hal yang menjadi bahan evaluasi dan porsi keterbatasan bagi tim penyelenggara. Keterbatasan utama dalam pelaksanaan ini meliputi evaluasi yang hanya bersifat jangka pendek dan ketiadaan kelompok pembanding untuk mengukur efektivitas intervensi secara terukur. Selain itu, terdapat bias *self-selection* dari 98 pendaftar awal serta tingginya heterogenitas peserta, yang mengharuskan penyesuaian tempo penyampaian materi. *Baseline* pengetahuan awal peserta juga tergolong tinggi, dan evaluasi capaian masih memiliki ketergantungan pada metrik kepuasan pelaporan mandiri (*self-report satisfaction*). Ke depannya, pengelolaan waktu pada sesi diskusi dan tanya jawab juga perlu dioptimalkan agar seluruh pertanyaan peserta dapat terakomodasi dengan lebih baik.

Berdasarkan hasil evaluasi tersebut, tim merekomendasikan agar kegiatan serupa dapat kembali diselenggarakan dengan cakupan peserta yang lebih luas serta durasi workshop yang lebih panjang sehingga peserta memiliki kesempatan praktik secara langsung. Materi juga dapat dikembangkan dengan menambahkan simulasi pengenalan *password manager*, autentikasi dua faktor (2FA), dan praktik mengenali *phishing*. Mengingat perubahan kebiasaan peserta tidak diukur pasca-kegiatan, direkomendasikan agar program selanjutnya mencakup evaluasi tindak lanjut dalam rentang waktu 2 hingga 8 minggu setelah pelatihan. Evaluasi lanjutan ini diperlukan untuk memvalidasi perubahan perilaku secara nyata, seperti metrik aktivasi 2FA, adopsi *password manager*, atau perubahan praktik saat menggunakan Wi-Fi publik.

Secara keseluruhan, pelaksanaan Webinar dan Workshop "Tingkatkan Kesadaran Keamanan Data & Jaringan" telah berhasil meningkatkan pengetahuan dan pemahaman kognitif peserta mengenai pentingnya menjaga keamanan data pribadi saat menggunakan internet. Mengingat instrumen evaluasi yang digunakan terutama berfokus pada tes kognitif dan tingkat kepuasan, klaim capaian kegiatan ini dibatasi pada peningkatan pengetahuan, sedangkan pengukuran tingkat kesadaran (*awareness*) yang sebenarnya memerlukan instrumen penilaian intensi dan perilaku yang lebih spesifik. Keberhasilan kegiatan ini didukung oleh perencanaan matang, kerja sama tim, dukungan dosen pembimbing dan mitra, serta

partisipasi aktif peserta. Hasil evaluasi ini diharapkan menjadi acuan penyelenggaraan program edukasi keamanan digital yang lebih terukur di masa mendatang.

KESIMPULAN

Kegiatan Webinar dan Workshop "Tingkatkan Kesadaran Keamanan Data & Jaringan" telah dilaksanakan sebagai upaya meningkatkan literasi mengenai keamanan web, keamanan jaringan, dan perlindungan data digital. Melalui materi konsep keamanan dasar, perbedaan HTTP dan HTTPS, peran SSL/TLS, serta demonstrasi menggunakan Wireshark dan Have I Been Pwned, hasil pendataan menunjukkan bahwa skor pengetahuan peserta mengalami peningkatan secara deskriptif. Meskipun peserta memperoleh pemahaman kognitif yang lebih baik mengenai pelindungan data di jaringan publik, dampak langsung kegiatan ini terhadap kesadaran dan perubahan perilaku keamanan siber peserta masih memerlukan pengukuran lanjutan untuk dapat disimpulkan secara utuh.

Keberhasilan kegiatan juga terlihat dari hasil evaluasi yang menunjukkan adanya peningkatan nilai rata-rata peserta dari 82,68 pada pre-test menjadi 93,45 pada post-test. Selain itu, hasil feedback menunjukkan bahwa mayoritas peserta memberikan penilaian baik hingga sangat baik terhadap materi, metode penyampaian, pelaksanaan kegiatan, serta kualitas pemateri. Temuan tersebut menunjukkan bahwa pendekatan yang menggabungkan penyampaian teori dengan demonstrasi dan praktik langsung mampu membantu peserta memahami materi secara lebih efektif.

Melalui kegiatan ini diharapkan peserta tidak hanya memperoleh pengetahuan mengenai keamanan data digital, tetapi juga mampu menerapkan kebiasaan berinternet yang lebih aman dalam kehidupan sehari-hari. Kegiatan serupa diharapkan dapat terus dikembangkan dengan jangkauan peserta yang lebih luas serta materi yang mengikuti perkembangan ancaman siber, sehingga dapat memberikan kontribusi yang berkelanjutan dalam meningkatkan kesadaran masyarakat terhadap pentingnya keamanan informasi di era digital.

REFERENSI

Allison, J. (2022). Network Packet Analysis as a Unit of Assessment: Identifying Emotet. Proceedings of the 22nd Koli Calling International Conference on Computing Education Research, 1–2. https://doi.org/10.1145/3564721.3565952

Ananta, R., & Hasa, M. F. (2025). Implementation of Wireshark to Monitor Security on Indihome Wi-Fi.

Buchan, M., Bhawra, J., & Katapally, T. (2024). Navigating the digital world: Development of an evidence-based digital literacy program and assessment tool for youth. Smart Learning Environments, 11. https://doi.org/10.1186/s40561-024-00293-x

Dabbous, A., Barakat, K., & Kraus, S. (2023). The impact of digitalization on entrepreneurial activity and sustainable competitiveness: A panel data analysis. Technology in Society. https://doi.org/10.1016/j.techsoc.2023.102224

Doloi, H. (2025). Digital Inclusion for Rural Growth: Internet Usage and Smart Villages Development. Asia-Pacific Journal of Rural Development, 35, 40–57. https://doi.org/10.1177/10185291251343357

Drushlyak, M., Semenog, O., Ponomarenko, N., Vovk, M., Budianskyi, D., & Semenikhina, O. (2025). Development of youth information and media literacy: Analysis of non-formal educational activities. Eastern Journal of European Studies. https://doi.org/10.47743/ejes-2025-0109

Kingsley David Onyewuchi Ofoegbu, Olajide Soji Osundare, Chidiebere Somadina Ike, Ololade Gilbert Fakeyede, & Adebimpe Bolatito Ige. (2024). Proactive cyber threat mitigation: Integrating data-driven insights with user-centric security protocols. Computer Science & IT Research Journal, 5(8), 2083–2106. https://doi.org/10.51594/csitrj.v5i8.1493

Kurniasih, N. (2023). Digital Literacy: Education for Safe Internet Usage. Engagement: Jurnal Pengabdian Kepada Masyarakat. https://doi.org/10.29062/engagement.v7i1.1534

Luis Fernando, F., & Luhur Prakoso, A. (2024). PERLINDUNGAN HUKUM TERHADAP PENYALAHGUNAAN DATA PRIBADI NASABAH PINJAMAN ONLINE. https://doi.org/10.36418/syntax-literate.v9i2.14770

Manguling, I. S. W., & Parenreng, J. M. (2023). Security System Analysis Using the HTTP Protocol Against Packet Sniffing Attacks. Internet of Things and Artificial Intelligence Journal, 3(4), 325–340. https://doi.org/10.31763/iota.v3i4.612

Nanayakkara, J. D. A. S. K., Bandara, M. R. P. M., Mawjood, M. S., Perera, R. A. P. M., Yapa, K., & Siriwardana, D. (2024). Enhanced Detection of Evil Twin Attacks in Public Wi-Fi Networks Using Machine Learning Algorithms. 1–6. https://doi.org/10.1109/icitr64794.2024.10857762

Ortiz-Garcés, I., Govea, J., Sánchez-Viteri, S., & Villegas-Ch., W. (2024). CyberEduPlatform: An educational tool to improve cybersecurity through anomaly detection with Artificial Intelligence. PeerJ Computer Science, 10, e2041. https://doi.org/10.7717/peerj-cs.2041

Rahmawati, E., Huda, M., & Aldhi, I. F. (2024). PERSONAL DATA MISUSE IN FINTECH LENDING PROVIDERS FROM PERSPECTIVE INDONESIAN CYBERLAW. Airlangga Development Journal. https://doi.org/10.20473/adj.v8i1.56398

Saleh, O. A. S., Saputra, R. A. M., Maulana, R., Haryanda, M., Mujiastuti, R., Sutrisno, M., Hasbi, M., Adharani, Y., & Rosanti, N. (2025). Introduction to Digital Forensics: Educational Initiatives Through Webinars And

Workshops on Recovering Lost Files in the Windows Operating System. Society : Jurnal Pengabdian Masyarakat. https://doi.org/10.55824/jpm.v4i5.629

Tempestini, G., Rovira, E., Pyke, A., & Di Nocera, F. (2023). The Cybersecurity Awareness Inventory (CAIN): Early Phases of Development of a Tool for Assessing Cybersecurity Knowledge Based on the ISO/IEC 27032. Journal of Cybersecurity and Privacy, 3(1), 61–75. https://doi.org/10.3390/jcp3010005

Wu, Y., & Jiao, T. (2023). A Survey on Packet Capture: Tool Introduction and Security Vulnerability Description. Applied and Computational Engineering, 8(1), 233–240. https://doi.org/10.54254/2755-2721/8/20230149