Vol. 6, No. 5, September 2026, Hal. 4925-4934
DOI: https://doi.org/10.54082/jamsi.3235

# Edukasi Digital Interaktif untuk Meningkatkan Kewaspadaan Masyarakat terhadap Kejahatan Siber di Desa Rimbo Panjang, Kabupaten Kampar, Riau

**Liant Pratama Ranu Kumbolo*[1], Bayu Fajar Ramadhan[2], Desy Marsella[3], Jul Sari Wanto[4], Edwar Ali[5]**

[1] Program Studi Informatika Medis, Fakultas Teknik dan Informatika, Universitas Sains dan Teknologi Indonesia, Indonesia
[2,3,4,5] Program Studi Teknologi Informasi, Fakultas Teknik dan Informatika, Universitas Sains dan Teknologi Indonesia, Indonesia
*e-mail: ranukoembolo@gmail.com[1], bayufr2005@gmail.com[2], desymarsell19@gmail.com[3], otolilaoli@gmail.com[4], edwarali@usti.ac.id[5]

***Abstrak***

*Hampir seluruh warga di lingkungan permukiman kini menggunakan smartphone dan internet dalam aktivitas sehari-hari, namun belum diimbangi literasi keamanan siber yang memadai, sehingga rentan menjadi korban phishing, file APK palsu, dan penipuan online. Kondisi ini turut ditemukan di RT 002/RW 002, Perumahan Griya Indah Persada 2, Desa Rimbo Panjang, Kabupaten Kampar. Kegiatan pengabdian ini bertujuan meningkatkan kewaspadaan warga terhadap kejahatan siber melalui edukasi digital interaktif berupa ceramah dan diskusi, yang dilaksanakan pada 31 Juli 2026. Kegiatan diikuti oleh 10 warga, dengan 7 di antaranya menyelesaikan instrumen pre-test dan post-test berisi 15 soal pilihan ganda secara lengkap. Hasil menunjukkan rata-rata skor pemahaman meningkat dari 61,90 menjadi 93,33 (+31,43 poin), dengan peningkatan pada seluruh indikator evaluasi, mulai dari pengetahuan dasar kejahatan siber, kemampuan mengenali tanda phishing dan APK berbahaya, hingga kesadaran proteksi data pribadi. Seluruh responden mengalami peningkatan skor, dan dua di antaranya mencapai skor sempurna. Warga menunjukkan antusiasme tinggi selama sesi diskusi dan tanya jawab, khususnya saat membahas cara mengenali file APK mencurigakan yang menyamar sebagai undangan pernikahan digital atau resi paket. Kegiatan ini membuktikan bahwa edukasi digital interaktif berbasis komunitas mampu meningkatkan pemahaman dan kesiapsiagaan warga RT 002/RW 002 Desa Rimbo Panjang dalam menghadapi ancaman kejahatan siber sehari-hari.*

***Kata kunci:*** *edukasi digital, kejahatan siber, kewaspadaan masyarakat, literasi digital, penipuan online*

***Abstract***

*Nearly all residents in the housing area now use smartphones and the internet in daily activities, yet this has not been matched by adequate cybersecurity literacy, leaving them vulnerable to phishing, fake APK files, and online fraud. This condition was also found in RT 002/RW 002, Griya Indah Persada 2 Housing Complex, Rimbo Panjang Village, Kampar Regency. This activity aimed to increase residents' awareness of cybercrime through interactive digital education consisting of lectures and discussion, conducted on 31 July 2026. The activity was attended by 10 residents, with 7 completing the 15-item multiple-choice pre-test and post-test in full. Results showed the average score rose from 61.90 to 93.33 (+31.43 points), with improvement across all evaluation indicators, from basic cybercrime knowledge, the ability to recognise phishing and malicious APK signs, to personal data protection awareness. All respondents improved, with two achieving perfect scores. Residents showed high enthusiasm during the discussion session, particularly when learning to identify suspicious APK files disguised as digital wedding invitations or delivery receipts. This activity demonstrates that community-based interactive digital education can improve the understanding and preparedness of RT 002/RW 002 residents in Rimbo Panjang Village in facing everyday cybercrime threats.*

***Keywords:*** *cybercrime, digital education, digital literacy, online fraud, public awareness*

## 1. PENDAHULUAN

Transformasi digital telah mengubah hampir seluruh aspek kehidupan masyarakat, mulai dari komunikasi, transaksi keuangan, hingga interaksi sosial yang kini banyak berpindah ke ruang siber. Perpindahan dari pola manual ke sistem berbasis daring ini kerap terjadi tanpa disertai kesiapan pengetahuan masyarakat yang memadai, sehingga masyarakat dibawa masuk ke

suasana digital yang sepenuhnya baru tanpa persiapan yang cukup (Sila & Taufik, 2023). Ketidaksiapan inilah yang kemudian dimanfaatkan oleh pihak-pihak tidak bertanggung jawab untuk melancarkan berbagai bentuk kejahatan siber.

Ketergantungan masyarakat pada perangkat seluler untuk transaksi perbankan, belanja daring, hingga komunikasi sehari-hari membuat smartphone menjadi pintu masuk utama berbagai modus kejahatan siber, terutama bagi pengguna yang belum terbiasa memverifikasi keaslian pesan atau tautan yang diterima. Kondisi ini diperparah oleh kecenderungan sebagian pengguna untuk bertindak cepat tanpa memeriksa ulang sumber pesan ketika dihadapkan pada situasi yang terkesan mendesak, seperti ancaman pemblokiran akun atau tawaran hadiah yang harus segera diklaim, sebuah pola manipulasi psikologis yang umum digunakan pelaku kejahatan siber untuk menekan korban agar tidak sempat berpikir kritis.

Ancaman cybercrime di Indonesia tergolong serius dan terus berkembang dari tahun ke tahun (Hapsari & Pambayun, 2023). Di antara berbagai bentuk ancaman siber tersebut, phishing, file aplikasi (APK) palsu, dan penipuan online merupakan tiga modus yang paling banyak ditemukan menyasar masyarakat umum, khususnya pengguna layanan perbankan digital dan aplikasi perpesanan. Phishing bekerja dengan menyamarkan tautan web palsu yang menyerupai halaman resmi bank atau portal bantuan sosial untuk mencuri kredensial pengguna, sedangkan file APK palsu umumnya disamarkan sebagai foto resi paket, undangan pernikahan digital, atau surat tagihan BPJS/pajak yang mendorong korban mengunduh aplikasi berbahaya tanpa disadari (Rizqullah et al., 2025). Setelah terinstal, aplikasi tersebut dapat mencuri kode OTP dan mengambil alih akses layanan perbankan seluler korban hanya dalam hitungan menit, sehingga kecepatan mengenali tanda-tanda kedua modus ini menjadi krusial bagi keselamatan finansial warga.

Berbagai kajian menunjukkan bahwa edukasi keamanan digital berbasis komunitas efektif meningkatkan pengetahuan masyarakat dalam mengenali dan mencegah ancaman siber. Pelatihan kesadaran keamanan siber yang dilaksanakan secara langsung di tingkat sekolah maupun komunitas terbukti mampu meningkatkan pemahaman peserta secara signifikan setelah intervensi edukatif diberikan (Sussolaikah et al., 2023; Agung, 2025). Edukasi yang memadukan ceramah, diskusi studi kasus, dan pelatihan mengenali ciri pesan phishing serta cara melindungi data pribadi juga dilaporkan mampu menumbuhkan kewaspadaan yang lebih tinggi dibandingkan penyuluhan satu arah tanpa sesi praktik (Lubis et al., 2025). Salah satu langkah proteksi teknis yang terbukti signifikan menekan risiko pengambilalihan akun secara ilegal adalah penerapan verifikasi dua langkah atau two-factor authentication (2FA), yang menambah lapisan keamanan di luar kata sandi utama (Aripradono, 2024).

Salah satu bentuk kejahatan siber yang paling banyak dijumpai masyarakat adalah penipuan online. Penipuan ini mencerminkan pergeseran dari pola penipuan konvensional menuju kejahatan berbasis digital yang memanfaatkan media sosial, marketplace, maupun situs web palsu, didorong oleh rendahnya kesadaran keamanan siber masyarakat, mudahnya akses teknologi, serta lemahnya pengawasan terhadap ruang digital. Skema yang banyak ditemukan antara lain penipuan investasi online, phishing, dan penyamaran identitas (Sahara & Kuswandi, 2025). Penipuan digital melalui tautan phishing sendiri sudah diatur sebagai tindak pidana dalam Pasal 378 KUHP serta Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), dan modusnya banyak disebarkan melalui email maupun aplikasi perpesanan seperti WhatsApp dan Telegram (Sahfitri & Rosmalinda, 2024). Kajian mengenai strategi pemolisian juga menegaskan bahwa pelaku kejahatan siber semakin cerdik memanfaatkan media sosial untuk melancarkan serangan phishing dengan menyamar sebagai pihak tepercaya, sementara kesadaran dan pemahaman pengguna terhadap risiko phishing masih rendah (Syah, 2023). Pada level yang lebih mikro, kajian kriminologis terhadap kasus penipuan online di Kota Makassar menemukan bahwa maraknya penipuan tersebut dipengaruhi oleh faktor ekonomi, lingkungan sosial, serta rendahnya literasi digital masyarakat, sehingga merekomendasikan perlunya program literasi digital yang masif sebagai upaya pencegahan (Royyan et al., 2025).

Upaya edukasi berbasis komunitas terbukti menjadi salah satu solusi yang relevan untuk mengatasi persoalan ini. Kegiatan pengabdian masyarakat berupa pemetaan dan penyuluhan kejahatan siber di Kota Baubau menemukan bahwa kasus kejahatan siber yang paling umum di

masyarakat adalah penipuan online, penyebaran hoaks, dan cyberbullying, yang seringkali terjadi tanpa disadari korban sehingga pelaku tidak jera untuk mengulangi perbuatannya (Rantekata et al., 2022). Sementara itu, kegiatan pengabdian mengenai literasi keuangan digital yang dilaksanakan di lingkup RT/RW Kota Surabaya menunjukkan bahwa edukasi partisipatif berbasis komunitas mampu meningkatkan pengetahuan warga sebesar 33,3%, kemampuan mengenali modus dan melaporkan penipuan sebesar 36,0%, serta pemahaman penggunaan dompet digital secara aman sebesar 42,2% (Zulaikha et al., 2026). Pendekatan serupa yang menyasar kelompok keluarga juga menunjukkan bahwa edukasi mengenai perlindungan data pribadi dan pencegahan penipuan online mampu meningkatkan kesiapsiagaan digital warga secara terukur (Putri Silmina et al., 2025). Temuan-temuan ini memperkuat argumen bahwa edukasi langsung di tingkat RT/RW merupakan pendekatan yang efektif untuk membangun benteng pertahanan digital dari lingkup komunitas terkecil.

Pemerintah dan berbagai lembaga terkait sebenarnya telah menekankan pentingnya literasi digital sebagai salah satu kompetensi dasar warga di era digital, namun implementasinya di tingkat komunitas terkecil seperti RT/RW masih terbatas dan sering kali bergantung pada inisiatif pihak eksternal seperti perguruan tinggi melalui program pengabdian kepada masyarakat. Minimnya edukasi keamanan siber yang menjangkau langsung ke tingkat rumah tangga menjadikan warga, khususnya kelompok ibu rumah tangga dan pekerja informal yang aktif menggunakan aplikasi perbankan seluler, sebagai kelompok yang rentan namun jarang menjadi sasaran program edukasi formal.

Kondisi serupa turut teridentifikasi di RT 002/RW 002, Perumahan Griya Indah Persada 2, Desa Rimbo Panjang, Kecamatan Tambang, Kabupaten Kampar, Riau. Berdasarkan hasil observasi dan koordinasi awal tim pelaksana bersama pengurus RT sebelum kegiatan dilaksanakan, sebagian besar warga di wilayah ini merupakan pengguna aktif smartphone dan layanan perbankan digital, namun belum pernah mendapatkan edukasi formal mengenai keamanan siber. Beberapa warga bahkan mengaku pernah menerima pesan mencurigakan berupa file APK yang menyamar sebagai undangan pernikahan digital atau resi paket, namun belum menyadari potensi bahaya di baliknya. Kondisi inilah yang menjadi dasar bagi tim pelaksana untuk melaksanakan kegiatan edukasi digital interaktif secara langsung kepada warga di tingkat RT, alih-alih hanya mengandalkan asumsi umum mengenai rendahnya literasi digital masyarakat perkotaan.

Berdasarkan uraian tersebut, kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan kewaspadaan warga RT 002/RW 002 Desa Rimbo Panjang terhadap kejahatan siber, khususnya phishing, file APK palsu, dan penipuan online, melalui edukasi digital interaktif yang meliputi pengenalan modus-modus penipuan terkini, cara mengenali tanda-tanda pesan atau tautan mencurigakan, serta pemahaman langkah-langkah proteksi data pribadi di ranah digital.

## 2. METODE

Kegiatan pengabdian kepada masyarakat ini menggunakan pendekatan edukasi digital interaktif secara langsung (tatap muka) kepada warga, yang dilengkapi dengan pengukuran tingkat pemahaman peserta sebelum dan sesudah edukasi melalui instrumen pre-test dan post-test.

### 2.1. Lokasi dan Waktu Kegiatan

Kegiatan dilaksanakan pada hari Jumat, 31 Juli 2026, pukul 13.30–15.00 WIB, bertempat di rumah Ketua RT 002, Perumahan Griya Indah Persada 2, Dusun 1, RT 002/RW 002, Desa Rimbo Panjang, Kecamatan Tambang, Kabupaten Kampar, Riau. Lokasi ini dipilih karena merupakan kawasan permukiman berkembang dengan penetrasi penggunaan smartphone dan internet yang cukup tinggi di kalangan warga, namun belum diimbangi dengan literasi keamanan siber yang memadai sebagaimana teridentifikasi pada tahap koordinasi awal dengan pengurus RT.

Vol. 6, No. 5, September 2026, Hal. 4925-4934
DOI: https://doi.org/10.54082/jamsi.3235

### 2.2. Sasaran Kegiatan

Undangan kegiatan disebarkan kepada 15–20 perwakilan warga di lingkungan RT 002. Pada saat pelaksanaan, terdapat 10 orang warga yang hadir mengikuti sesi sosialisasi secara penuh. Dari jumlah tersebut, 7 orang responden mengisi instrumen pre-test dan post-test secara lengkap dan konsisten dari awal hingga akhir kegiatan, 1 orang peserta hanya sempat mengisi post-test karena baru bergabung menjelang sesi evaluasi akhir, sedangkan 2 peserta lainnya tidak menyelesaikan instrumen evaluasi sama sekali karena kendala teknis perangkat dan keterbatasan waktu saat sesi berlangsung. Kondisi keterbatasan perangkat dan waktu tersebut menjadi catatan penting bagi tim pelaksana untuk perbaikan pelaksanaan kegiatan edukasi digital berikutnya, misalnya dengan menyediakan cadangan perangkat pengisian kuesioner atau memperpanjang alokasi waktu sesi evaluasi agar seluruh peserta yang hadir dapat menyelesaikan instrumen secara lengkap.

### 2.3. Metode Pelaksanaan

Metode pelaksanaan kegiatan terbagi menjadi tiga bentuk interaksi utama, yaitu pemaparan materi (ceramah visual) mengenai bentuk-bentuk kejahatan siber, modus penipuan online terkini, serta langkah praktis proteksi data pribadi; diskusi interaktif yang membahas studi kasus nyata mengenai contoh pesan phishing, tautan bodong, dan jebakan file APK yang sering beredar di WhatsApp atau media sosial; serta sesi tanya jawab yang memberi ruang bagi warga untuk berkonsultasi mengenai pengalaman pribadi maupun kendala teknis yang pernah mereka alami. Tahapan pelaksanaan kegiatan secara lebih rinci disajikan pada Tabel 1.

Tabel 1. Tahapan Pelaksanaan Kegiatan Pengabdian kepada Masyarakat

| Tahap | Kegiatan | Uraian |
|---|---|---|
| Persiapan | Koordinasi & perizinan | Koordinasi dan observasi awal dengan Ketua RT setempat, penyusunan materi edukasi dalam bentuk slide presentasi, serta penyusunan instrumen kuesioner pre-test dan post-test. |
| Pelaksanaan | Edukasi & diskusi interaktif | Pembukaan acara, pengisian pre-test oleh peserta, pemaparan materi mengenai jenis-jenis kejahatan siber dan cara pencegahannya, dilanjutkan diskusi interaktif dan tanya jawab, serta pengisian post-test di akhir sesi. |
| Evaluasi | Tabulasi & pelaporan | Tabulasi data jawaban pre-test dan post-test, analisis komparatif peningkatan skor pemahaman peserta per indikator, serta penyusunan laporan kegiatan. |

Materi mengenai verifikasi dua langkah (2FA) dan penggantian kata sandi turut disampaikan sebagai bagian dari edukasi proteksi data pribadi. Namun, karena keterbatasan waktu pelaksanaan kegiatan, sesi praktik langsung pengaktifan 2FA pada perangkat masing-masing peserta tidak sempat dilaksanakan, sehingga penyampaian materi ini bersifat pemaparan dan diskusi.

### 2.4. Media Pembelajaran

Media utama yang digunakan dalam kegiatan ini adalah slide presentasi yang dirancang dengan visualisasi menarik, komunikatif, dan memuat sedikit teks teknis agar mudah dicerna oleh warga. Slide memuat infografis mengenai jenis-jenis penipuan online populer (file APK bodong, modus kurir, undian palsu), panduan visual ciri-ciri pesan phishing atau tautan berbahaya, serta langkah-langkah konkret pengamanan akun seperti pembuatan kata sandi yang kuat dan aktivasi verifikasi dua langkah (2FA).

### 2.5. Alat Ukur dan Evaluasi

Untuk mengukur efektivitas program, digunakan kuesioner pre-test dan post-test yang identik, terdiri atas 15 butir soal pilihan ganda yang mencakup tiga indikator, yaitu pengetahuan

dasar mengenai jenis kejahatan siber dan modus penipuan online (5 butir), kemampuan mengenali tanda-tanda tautan/pesan mencurigakan berupa phishing dan APK (5 butir), serta kesadaran dan keterampilan dalam melakukan proteksi data pribadi (5 butir). Pre-test diberikan sebelum pemaparan materi untuk mengetahui tingkat pemahaman awal peserta, sedangkan post-test diberikan setelah seluruh sesi edukasi dan diskusi selesai untuk mengukur peningkatan pengetahuan peserta. Skor akhir masing-masing peserta dan tiap indikator dihitung dengan rumus: (jumlah jawaban benar/jumlah soal) × 100. Data karakteristik peserta (usia dan pekerjaan) diperoleh melalui tanya jawab langsung saat pelaksanaan kegiatan.

### 2.6. Indikator Keberhasilan Kegiatan

Keberhasilan kegiatan edukasi ditentukan berdasarkan peningkatan skor pemahaman peserta antara pre-test dan post-test, dengan kategori tingkat pengetahuan yang mengacu pada konvensi pengukuran pengetahuan yang umum digunakan pada kegiatan pengabdian masyarakat sejenis, yaitu kategori Baik apabila skor mencapai 76–100%, Cukup apabila skor berada pada rentang 56–75%, dan Kurang apabila skor ≤55% (Hadiyani et al., 2024). Kegiatan dinyatakan berhasil apabila terjadi pergeseran kategori pengetahuan peserta secara mayoritas dari kategori Cukup atau Kurang pada pre-test menuju kategori Baik pada post-test.

## 3. HASIL DAN PEMBAHASAN

### 3.1. Tahap Persiapan dan Pelaksanaan

Pada tahap persiapan, tim pelaksana melakukan koordinasi dan perizinan kepada Ketua RT 002/RW 002 Desa Rimbo Panjang untuk mendapatkan izin pelaksanaan kegiatan sosialisasi, sekaligus melakukan observasi awal mengenai kebiasaan digital warga setempat, dilanjutkan dengan penyiapan slide presentasi materi serta lembar kuesioner pre-test dan post-test.

Kegiatan kemudian dilaksanakan pada Jumat, 31 Juli 2026 pukul 13.30–15.00 WIB, diawali dengan pembukaan acara dan pengisian pre-test oleh peserta untuk mengukur pemahaman awal mereka mengenai kejahatan siber. Selanjutnya, tim menyampaikan materi edukasi secara interaktif, mencakup jenis-jenis modus penipuan online, ciri-ciri pesan atau tautan phishing, serta langkah-langkah pengamanan akun digital. Sesi ini dilanjutkan dengan diskusi interaktif dan tanya jawab mengenai pengalaman warga terkait pesan atau tautan mencurigakan yang pernah mereka terima, sebelum akhirnya peserta mengisi post-test untuk mengukur peningkatan pemahaman setelah edukasi.

Gambar 1. Peserta Mengisi Kuesioner Pre-Test/Post-Test

Vol. 6, No. 5, September 2026, Hal. 4925-4934
DOI: https://doi.org/10.54082/jamsi.3235

Gambar 2. Suasana Peserta Selama Kegiatan Sosialisasi

### 3.2. Karakteristik Responden

Data karakteristik responden diperoleh melalui tanya jawab langsung dengan 7 peserta yang mengisi instrumen evaluasi secara lengkap. Karakteristik responden disajikan pada Tabel 2.

Tabel 2. Karakteristik Responden

| Karakteristik | Kategori | Jumlah (Orang) | Persentase (%) |
|---|---|---|---|
| Jenis Kelamin | Perempuan | 7 | 100 |
| | Laki-laki | 0 | 0 |
| Usia | 20–35 tahun | 3 | 42,9 |
| | 36–50 tahun | 4 | 57,1 |
| Pekerjaan | Ibu Rumah Tangga (IRT) | 3 | 42,9 |
| | Karyawan Swasta/Wiraswasta | 3 | 42,9 |
| | Lainnya | 1 | 14,3 |
| **Total Responden** | | **7** | **100** |

Seluruh responden (100%) berjenis kelamin perempuan, yang sejalan dengan kondisi umum kegiatan sosialisasi di tingkat RT/RW di mana ibu-ibu lebih banyak berperan aktif dan hadir dalam kegiatan komunitas dibandingkan bapak-bapak. Dari sisi usia, mayoritas responden berada pada rentang 36–50 tahun (57,1%), sedangkan sisanya berada pada rentang usia 20–35 tahun (42,9%). Berdasarkan pekerjaan, responden didominasi oleh ibu rumah tangga (42,9%) dan karyawan swasta/wiraswasta (42,9%), dengan sisanya berasal dari kategori pekerjaan lain (14,3%).

### 3.3. Analisis Hasil Pre-Test dan Post-Test

Pengukuran efektivitas kegiatan edukasi dilakukan dengan membandingkan skor pemahaman peserta sebelum (pre-test) dan sesudah (post-test) penyampaian materi. Dari total warga yang hadir, terdapat 7 orang responden yang mengisi instrumen evaluasi secara lengkap dari awal hingga akhir kegiatan, sedangkan 1 orang peserta tambahan (Eli Yani) hanya mengisi instrumen post-test dengan skor 93,33 sehingga dikeluarkan dari sampel analisis komparatif demi menjaga konsistensi data. Hasil rekapitulasi skor ketujuh responden tersebut disajikan pada Tabel 3.

Vol. 6, No. 5, September 2026, Hal. 4925-4934
DOI: https://doi.org/10.54082/jamsi.3235

Tabel 3. Rekapitulasi Skor Pre-Test dan Post-Test Responden (N = 7)

| No | Kode Responden | Skor Pre-Test | Skor Post-Test | Peningkatan (Poin) |
|---|---|---|---|---|
| 1 | R1 | 60,00 | 93,33 | +33,33 |
| 2 | R2 | 73,33 | 100,00 | +26,67 |
| 3 | R3 | 53,33 | 86,67 | +33,33 |
| 4 | R4 | 66,67 | 93,33 | +26,67 |
| 5 | R5 | 80,00 | 100,00 | +20,00 |
| 6 | R6 | 53,33 | 86,67 | +33,33 |
| 7 | R7 | 46,67 | 93,33 | +46,67 |
| | **Rata-Rata** | **61,90** | **93,33** | **+31,43** |

*Catatan: Kode R1–R7 digunakan untuk menjaga privasi responden.*

Sebelum sosialisasi dilaksanakan, rata-rata tingkat pemahaman awal peserta mengenai kejahatan siber tergolong kategori Cukup, yaitu sebesar 61,90. Setelah pemaparan materi dan diskusi, rata-rata skor meningkat menjadi 93,33 dan bergeser ke kategori Baik, atau naik sebesar 31,43 poin (setara dengan peningkatan 50,8% dari nilai awal). Seluruh dari 7 responden mengalami peningkatan skor tanpa satu pun yang mengalami penurunan, dan dua responden bahkan berhasil meraih skor sempurna (100,00) pada post-test. Hasil ini konsisten dengan temuan pada kegiatan pengabdian sejenis di tingkat RT/RW, yang juga melaporkan peningkatan pengetahuan warga setelah edukasi digital berbasis komunitas dilaksanakan (Zulaikha et al., 2026; Putri Silmina et al., 2025), maupun kegiatan edukasi keamanan siber berbasis komunitas lain yang melaporkan peningkatan signifikan setelah intervensi edukatif langsung (Sussolaikah et al., 2023; Agung, 2025; Lubis et al., 2025).

Untuk melihat sebaran peningkatan secara lebih rinci sebagaimana disarankan pada proses telaah naskah, skor peserta turut dianalisis berdasarkan tiga indikator instrumen evaluasi, yaitu pengetahuan dasar mengenai jenis kejahatan siber dan modus penipuan online, kemampuan mengenali tanda-tanda pesan/tautan mencurigakan (phishing dan APK), serta kesadaran dan keterampilan proteksi data pribadi. Hasil analisis per indikator disajikan pada Tabel 4.

Tabel 4. Perubahan Skor Berdasarkan Tiga Indikator Instrumen Evaluasi (N = 7)

| Indikator | Skor Pre-Test (%) | Skor Post-Test (%) | Peningkatan (Poin) |
|---|---|---|---|
| 1. Pengetahuan Dasar Kejahatan Siber | 65,71 | 91,43 | +25,72 |
| 2. Mengenali Tanda Phishing/APK | 54,29 | 88,57 | +34,28 |
| 3. Kesadaran Proteksi Data Pribadi | 65,71 | 100,00 | +34,29 |

Pada indikator pengetahuan dasar, rata-rata skor meningkat dari 65,71 menjadi 91,43 (+25,72 poin). Pada indikator kemampuan mengenali tanda-tanda phishing dan APK mencurigakan, peningkatan tercatat paling besar kedua, yaitu dari 54,29 menjadi 88,57 (+34,28 poin); indikator ini juga memiliki skor pre-test terendah di antara ketiga indikator, mengindikasikan bahwa sebelum edukasi diberikan, warga paling kesulitan mengenali ciri-ciri pesan penipuan dibandingkan aspek pengetahuan umum atau proteksi data. Peningkatan tertinggi justru terjadi pada indikator kesadaran dan keterampilan proteksi data pribadi, yaitu dari 65,71 menjadi 100,00 (+34,29 poin), di mana seluruh responden menjawab benar seluruh

butir soal pada post-test. Pencapaian skor sempurna pada indikator ini kemungkinan besar didorong oleh sifat materi yang disampaikan secara terstruktur dan prosedural, misalnya urutan langkah darurat saat perangkat terindikasi malware serta panduan 'empat rumus aman berinternet', yang relatif lebih mudah diingat peserta dibandingkan keterampilan mengenali pola pesan penipuan yang lebih bervariasi bentuknya (indikator 2).

Perbandingan antara ketiga indikator ini turut memberikan gambaran mengenai prioritas materi edukasi yang paling dibutuhkan warga pada kegiatan serupa di masa mendatang. Rendahnya skor pre-test pada indikator kemampuan mengenali tanda-tanda phishing dan APK dibandingkan dua indikator lainnya mengindikasikan bahwa warga cenderung lebih familiar dengan istilah dan bahaya kejahatan siber secara umum, namun belum terlatih untuk menerapkannya secara praktis ketika dihadapkan pada contoh pesan atau tautan yang menyerupai komunikasi resmi. Hal ini memperkuat pentingnya pendekatan edukasi yang tidak hanya bersifat informatif, tetapi juga menyertakan studi kasus nyata dan simulasi langsung, sebagaimana yang diterapkan pada kegiatan ini.

### 3.4. Temuan dan Dinamika Diskusi

Selain data kuantitatif dari kuesioner, kegiatan edukasi ini turut menghasilkan beberapa temuan kualitatif dari sesi tanya jawab bersama warga. Beberapa peserta mengaku pernah menerima pesan mencurigakan berupa file berekstensi .apk yang menyamar sebagai undangan pernikahan digital atau pemberitahuan resi paket, namun sebagian besar belum mengetahui bahaya laten dari mengklik file tersebut. Temuan ini menjadi salah satu kebutuhan utama edukasi yang paling relevan bagi warga, sekaligus memperkuat hasil kajian yang menunjukkan bahwa file APK palsu berkedok lowongan kerja, resi paket, maupun undangan digital merupakan modus yang tengah marak menyasar korban di berbagai daerah, dengan kerugian yang dapat terjadi hanya dalam hitungan menit setelah file diunduh (Rizqullah et al., 2025). Temuan ini juga memperkuat hasil kajian kriminologis yang menunjukkan bahwa rendahnya literasi digital masyarakat menjadi salah satu faktor utama yang mendorong maraknya penipuan online (Royyan et al., 2025).

Pertanyaan terbanyak yang diajukan peserta berkisar pada cara membedakan pesan resmi perbankan/kurir dengan pesan penipuan, serta langkah darurat yang harus dilakukan jika nomor WhatsApp tiba-tiba diretas atau akun bank terindikasi pembobolan. Peserta juga menunjukkan antusiasme tinggi saat membahas cara mengaktifkan verifikasi dua langkah (2FA) dan pentingnya mengganti kata sandi akun secara berkala untuk mencegah peretasan. Antusiasme ini menegaskan bahwa edukasi langsung dan interaktif di tingkat komunitas terkecil efektif menumbuhkan kesadaran keamanan digital, sejalan dengan temuan kegiatan penyuluhan kejahatan siber di Kota Baubau yang menekankan pentingnya edukasi langsung karena kejahatan siber kerap terjadi tanpa disadari korban (Rantekata et al., 2022), maupun kegiatan pelatihan kesadaran keamanan siber berbasis komunitas lain yang menunjukkan hasil serupa (Sussolaikah et al., 2023).

Meskipun sesi praktik langsung pengaktifan 2FA tidak sempat dilaksanakan pada kegiatan ini karena keterbatasan waktu, tingginya antusiasme peserta terhadap topik tersebut menunjukkan adanya minat nyata warga untuk mempelajari keterampilan proteksi akun lebih lanjut. Hal ini menjadi masukan bagi tim pelaksana untuk menyertakan sesi praktik langsung secara lebih intensif pada kegiatan edukasi digital berikutnya, mengingat prinsip pembelajaran orang dewasa (andragogi) menekankan bahwa pemahaman prosedural cenderung lebih melekat apabila peserta dapat langsung mempraktikkan keterampilan yang dipelajari, bukan hanya menerima informasi secara pasif.

## 4. KESIMPULAN

Kegiatan edukasi digital interaktif yang dilaksanakan di RT 002/RW 002, Perumahan Griya Indah Persada 2, Desa Rimbo Panjang, Kabupaten Kampar, Riau, terbukti efektif meningkatkan kewaspadaan 7 responden yang menyelesaikan instrumen evaluasi secara lengkap

terhadap kejahatan siber, khususnya phishing, file APK palsu, dan penipuan online. Hal ini ditunjukkan oleh peningkatan rata-rata skor pemahaman dari 61,90 (kategori Cukup) pada pre-test menjadi 93,33 (kategori Baik) pada post-test, atau naik sebesar 31,43 poin (50,8%), dengan peningkatan konsisten pada ketiga indikator evaluasi: pengetahuan dasar (+25,72 poin), kemampuan mengenali tanda phishing/APK (+34,28 poin), dan kesadaran proteksi data pribadi (+34,29 poin). Melalui edukasi ini, ketujuh responden menjadi lebih memahami modus-modus penipuan digital seperti phishing dan file APK bodong, mampu mengenali ciri-ciri pesan mencurigakan, serta memahami pentingnya langkah proteksi data pribadi seperti aktivasi verifikasi dua langkah (2FA) dan penggantian kata sandi secara berkala.

Capaian ini merupakan hasil dari kelompok responden yang mengikuti evaluasi secara lengkap, bukan representasi seluruh warga RT 002/RW 002 Desa Rimbo Panjang, mengingat dari 10 warga yang hadir, hanya 7 orang yang menyelesaikan instrumen pre-test dan post-test secara utuh. Sebagai capaian edukasi pada kelompok tersebut, hasil ini menunjukkan manfaat nyata berupa peningkatan pemahaman dan keterampilan proteksi digital yang dapat menjadi bekal bagi warga dalam menghadapi ancaman kejahatan siber sehari-hari, sekaligus menjadi masukan bagi tim pelaksana untuk memperluas jangkauan dan menyempurnakan pelaksanaan kegiatan edukasi digital serupa di masa mendatang.

## UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Sains dan Teknologi Indonesia atas dukungan dalam pelaksanaan kegiatan Kuliah Kerja Nyata ini, serta kepada Ketua RT 002/RW 002 Desa Rimbo Panjang atas izin dan dukungan fasilitas selama kegiatan berlangsung. Terima kasih juga disampaikan kepada seluruh warga RT 002/RW 002 yang telah berpartisipasi dengan antusias dalam kegiatan edukasi ini.

## DAFTAR PUSTAKA

Agung, H. (2025). Efektivitas edukasi cybersecurity dalam meningkatkan pengetahuan siswa tentang ancaman digital pada siswa menengah atas. *Jurnal Ilmu Komputer (JUIK), 5*(2). https://doi.org/10.31314/juik.v5i2.4436

Aripradono, H. W. (2024). Evaluation of two-factor authentication (2FA) TOTP in enhancing security. *E-KOMTEK Journal.* https://jurnal.politeknik-kebumen.ac.id/E-KOMTEK/article/view/2113

Hadiyani, S., Sholeha, A. Z., & Sari, T. P. (2024). Gambaran tingkat pengetahuan para remaja tentang bahaya narkoba di RT/RW Xx/Yy Sudimara Barat Ciledug Tangerang. *Journal of Indonesian Management, 4*(4), 1–8. https://doi.org/10.53697/jim.v4i4.4044

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman cybercrime di Indonesia: Sebuah tinjauan pustaka sistematis. *Jurnal Konstituen, 5*(1). https://doi.org/10.33701/jk.v5i1.3208

Lubis, H., Awaludin, D. T., Sari, D. P., Milasari, L. A., & Sofyan, S. (2025). Edukasi keamanan siber: Pelatihan dasar mengenali phishing dan proteksi data pribadi di dunia digital. *JIPITI: Jurnal Pengabdian kepada Masyarakat, 2*(2), 101–105.

Putri Silmina, E., Sarmin, S., Umar, R., & Herman, H. (2025). Meningkatkan literasi digital: Perlindungan data pribadi dan pencegahan penipuan online di lingkungan PRA Ngadisuryan. *Jurnal Pengabdian UntukMu NegeRI, 9*(2), 322–330. https://doi.org/10.37859/jpumri.v9i2.9860

Rantekata, N. A., Husaini, L. O., Suluhu, F., & Una, W. (2022). Pemetaan dan penyuluhan kejahatan siber di Baubau. *Jurnal Pengabdian Masyarakat Indonesia, 1*(2), 107–118. https://doi.org/10.55606/jpmi.v1i2.5299

Rizqullah, M. R., Nasution, R. S., Lubis, S. A., Parinduri, M. I., & Immanuel, L. (2025). Tindak pidana penyebaran aplikasi malware berbasis APK: Studi terhadap fenomena modus lowongan kerja

Vol. 6, No. 5, September 2026, Hal. 4925-4934
DOI: https://doi.org/10.54082/jamsi.3235

dan paket palsu. *Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora, 4*(3), 858–867. https://doi.org/10.55606/jurrish.v4i2.6033

Royyan, M. Z., Mappaselleng, N. F., & Said, M. F. (2025). Analisis kriminologis terhadap tindak pidana penipuan melalui media online di Kota Makassar. *Legal Dialogica, 1*(1), 1–10. https://jurnal.fh.umi.ac.id/index.php/legal/article/view/1426

Sahara, A., & Kuswandi. (2025). Penipuan online sebagai bentuk kejahatan siber dalam perspektif kriminologi. *Parlementer: Jurnal Studi Hukum dan Administrasi Publik, 2*(4), 92–105. https://doi.org/10.62383/parlementer.v2i4.1425

Sahfitri, A., & Rosmalinda. (2024). Penipuan digital melalui tautan phishing. *Jurnal Dialektika Hukum, 6*(2), 92–107. https://doi.org/10.36859/jdh.v6i2.2881

Sila, G. E., & Taufik, C. M. (2023). Literasi digital untuk melindungi masyarakat dari kejahatan siber. *Komversal: Jurnal Komunikasi Universal, 5*(1), 112–123. https://doi.org/10.38204/komversal.v5i1.1225

Sussolaikah, K., Laksono, R. D., & Andria, A. (2023). Pelatihan media edukasi kesadaran keamanan siber di SDN 01 Pandean Kota Madiun. *Jurnal Pengabdian Masyarakat IPTEK, 3*(2), 131–136. https://doi.org/10.53513/ABDI.V3I2.8749

Syah, R. (2023). Strategi kepolisian dalam pencegahan kejahatan phishing melalui media sosial di ruang siber. *Jurnal Impresi Indonesia, 2*(9), 864–870. https://doi.org/10.58344/jii.v2i9.3594

Zulaikha, Farida, Astutik, S., Maella, N. F. S., & Handayanti, N. (2026). Urgensi literasi keuangan digital sebagai upaya melindungi komunitas urban dari penipuan online. *Journal of Indonesian Society Empowerment, 4*(1), 21–31. https://doi.org/10.61105/jise.v4i1.379