TRIDHARMADIMAS: Jurnal Pengabdian Kepada Masyarakat Jayakarta
http://journal.stmikjayakarta.ac.id/index.php/tridharmadimas
EmaiL: info@stmik.jayakarta.ac.id , tridharmadimas.jayakarta@gmail.com
DOI : 10.52362/tridharmadimas.v5i2.2206
E-ISSN: 2798-8295 **(Online), P-ISSN:** 2798-8554 **(Print)** Vol. 5 No.2, Desember 2025

Memperkenalkan CyberSecurity Kepada Karang Taruna di Kelurahan Tangki Jakarta Barat

Bernadus Gunawan Sudarsono [1*], Alexius Ulan Bani [2], Sharyanto [3], Raditya Galih Whendasromo [4]

[1]Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya, Indonesia
[2,3,4]Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Bung Karno, Jakarta

Email: [1*]bernadus.gs@dsn.ubharajaya.ac.id, [2]alexiusulanbani@ubk.ac.id, [3]syahriyanto@ubk.ac.id, [4]raditya_gw@ubk.ac.id

Abstrak: Perkembangan teknologi informasi yang masif telah membawa transformasi digital yang signifikan di tengah masyarakat, mengubah pola interaksi sosial dan transaksi ekonomi. Namun, kemajuan ini berbanding lurus dengan peningkatan ancaman kejahatan siber (cyber crime). Generasi muda, khususnya anggota Karang Taruna di Kelurahan Tangki, Jakarta Barat, merupakan kelompok "digital natives" yang sangat aktif menggunakan internet, namun sering kali memiliki kesadaran keamanan (security awareness) yang rendah. Kurangnya pemahaman mengenai perlindungan data pribadi menjadikan mereka target yang rentan terhadap serangan siber seperti Phishing, Social Engineering, dan peretasan akun. Kegiatan Pengabdian kepada Masyarakat (PkM) ini bertujuan untuk meningkatkan literasi digital dan memberikan keterampilan teknis praktis mengenai Cybersecurity. Metode pelaksanaan kegiatan menggunakan pendekatan mixed-method yang sistematis, meliputi tahapan observasi awal, penyusunan materi berbasis masalah, pelaksanaan pelatihan partisipatif, dan evaluasi efektivitas. Materi difokuskan pada pengenalan konsep CIA Triad (Confidentiality, Integrity, Availability), identifikasi ancaman siber, dan praktik pengamanan Akun Google melalui fitur 2-Step Verification dan Security Checkup. Hasil kegiatan menunjukkan adanya peningkatan pemahaman peserta secara signifikan mengenai urgensi keamanan data. Peserta mampu mengidentifikasi tautan berbahaya dan secara mandiri mengimplementasikan pengaturan keamanan pada perangkat gawai mereka. Diharapkan kegiatan ini dapat membentuk ekosistem digital yang aman dan produktif di lingkungan pemuda Kelurahan Tangki, serta mendorong mereka menjadi agen perubahan literasi digital bagi komunitas sekitarnya.

Kata Kunci: *Cybersecurity*, Karang Taruna, Keamanan Akun Google, Literasi Digital, *Social Engineering*.

Abstract: *The massive development of information technology has brought significant digital transformation to society. However, this progress is directly proportional to the increase in cyber crime threats. The younger generation, specifically members of the Karang Taruna in Tangki Village, West Jakarta, are "digital natives" who are very active in using the internet but often have low security awareness. The lack of understanding regarding personal data protection makes them vulnerable targets for cyber attacks such as Phishing, Social Engineering, and account hacking. This Community Service (PkM) activity aims to increase digital literacy and provide practical technical skills regarding Cybersecurity. The implementation method uses a mixed-method approach, combining interactive lectures, question-and-answer discussions, and direct practical assistance (simulation). The material focuses on introducing the CIA Triad concept (Confidentiality, Integrity, Availability), identifying cyber threats, and practicing Google Account security through the 2-Step Verification and Security Checkup features. The results of the activity showed a significant increase in participants' understanding of the urgency of data security. Participants were able to identify malicious links and independently implement security settings on their mobile devices. It is hoped that this activity can form a secure and productive digital ecosystem among the youth of Tangki Village.*

TRIDHARMADIMAS: Jurnal Pengabdian Kepada Masyarakat Jayakarta
http://journal.stmikjayakarta.ac.id/index.php/tridharmadimas
EmaiL: info@stmik.jayakarta.ac.id , tridharmadimas.jayakarta@gmail.com
DOI : 10.52362/tridharmadimas.v5i2.2206
E-ISSN: 2798-8295 **(Online), P-ISSN:** 2798-8554 **(Print)** Vol. 5 No.2, Desember 2025

Keywords: *Cybersecurity, Karang Taruna, Google Account Security, Digital Literacy, Social Engineering.*

1. PENDAHULUAN

Memasuki dekade ketiga abad ke-21, dunia sedang mengalami percepatan transformasi digital yang didorong oleh Revolusi Industri 4.0 dan transisi menuju masyarakat cerdas (*Society 5.0*). Di Indonesia, penetrasi internet telah menjangkau berbagai lapisan masyarakat, menjadikan teknologi informasi sebagai tulang punggung aktivitas sehari-hari, mulai dari komunikasi, pendidikan, hingga transaksi finansial. Perangkat seluler (*smartphone*) tidak lagi sekadar alat komunikasi, melainkan menjadi penyimpan data pribadi yang paling krusial. Namun, fenomena adopsi teknologi yang cepat ini sering kali tidak diimbangi dengan literasi digital yang memadai, khususnya terkait aspek keamanan dan privasi data (*data privacy*). Kesenjangan antara penggunaan teknologi dan pemahaman keamanannya menciptakan celah kerentanan (*vulnerability*) yang dimanfaatkan oleh pelaku kejahatan siber.

Ancaman kejahatan siber (*cyber crime*) kini telah berevolusi menjadi industri kriminal yang terorganisir. Serangan siber tidak lagi hanya menyasar infrastruktur kritis negara atau korporasi multinasional, tetapi semakin masif menargetkan individu pengguna akhir (*end-user*). Laporan keamanan siber nasional menunjukkan tren peningkatan kasus pencurian identitas, penipuan daring (*online fraud*), dan pengambilalihan akun (*account takeover*). Modus operandi yang digunakan pun semakin canggih, sering kali menggunakan teknik *Social Engineering* yang memanipulasi psikologis korban. Dalam banyak kasus, peretas tidak perlu memiliki kemampuan teknis yang tinggi untuk membobol sistem, melainkan cukup mengeksploitasi kelalaian manusia (*human error*), seperti penggunaan *password* yang lemah atau ketidaktahuan dalam mengidentifikasi tautan berbahaya (*phishing link*).

Kelurahan Tangki, yang terletak di Jakarta Barat, memiliki demografi penduduk yang dinamis dengan populasi pemuda yang cukup besar. Para pemuda yang tergabung dalam organisasi Karang Taruna di wilayah ini merupakan representasi dari generasi "digital natives". Mereka sangat adaptif terhadap tren teknologi baru, aktif di media sosial, dan terbiasa menggunakan layanan digital. Namun, berdasarkan observasi awal, tingginya intensitas penggunaan internet ini berbanding terbalik dengan kesadaran keamanan siber (*security awareness*). Banyak anggota Karang Taruna yang belum memahami bahwa data pribadi seperti Nomor Induk Kependudukan (NIK), tanggal lahir, nama ibu kandung, dan lokasi *real-time* adalah aset berharga yang harus dilindungi secara ketat.

Salah satu aspek krusial yang sering diabaikan adalah keamanan Akun Google. Bagi mayoritas pengguna perangkat Android di Indonesia, Akun Google berfungsi sebagai identitas digital tunggal (*Single Sign-On*) yang terintegrasi. Akun ini menghubungkan pengguna ke berbagai layanan vital seperti email (Gmail), penyimpanan awan (Google Drive), peta dan lokasi (Google Maps), hingga akses ke perangkat itu sendiri. Jika akun ini diretas, dampaknya sangat katastropik. Pelaku kejahatan dapat mengakses foto pribadi, dokumen penting, hingga melakukan reset pabrik pada perangkat korban dari jarak jauh. Lebih jauh lagi, akun yang diretas sering digunakan untuk melakukan penipuan terhadap daftar kontak korban, sehingga merusak reputasi pemilik akun.

Permasalahan utama yang diidentifikasi di mitra Karang Taruna Kelurahan Tangki meliputi: (1) Kurangnya pemahaman tentang jenis-jenis ancaman siber modern; (2) Kebiasaan manajemen *password* yang buruk (menggunakan tanggal lahir atau satu *password* untuk semua akun); (3) Ketidaktahuan tentang fitur keamanan lanjut seperti Verifikasi 2 Langkah (2FA); dan (4) Ketidakmampuan membedakan situs web asli dan palsu.

Merespons urgensi permasalahan tersebut, kegiatan Pengabdian kepada Masyarakat (PkM) ini dirancang untuk memberikan edukasi komprehensif mengenai *Cybersecurity*. Kegiatan ini tidak hanya bertujuan mentransfer pengetahuan teoritis, tetapi juga memberikan keterampilan teknis praktis (*hands-on*) agar anggota Karang Taruna mampu mengamankan aset digital mereka secara mandiri. Dengan memberdayakan pemuda Karang Taruna, diharapkan mereka dapat menjadi "benteng pertahanan" pertama dalam keluarga dan komunitas mereka melawan ancaman siber, serta menyebarluaskan praktik internet sehat dan aman di lingkungan Kelurahan Tangki.

TRIDHARMADIMAS: Jurnal Pengabdian Kepada Masyarakat Jayakarta
http://journal.stmikjayakarta.ac.id/index.php/tridharmadimas
EmaiL: info@stmik.jayakarta.ac.id , tridharmadimas.jayakarta@gmail.com
DOI : 10.52362/tridharmadimas.v5i2.2206
E-ISSN: 2798-8295 **(Online), P-ISSN:** 2798-8554 **(Print)** Vol. 5 No.2, Desember 2025

2. KERANGKA TEORI

2.1 Konsep Dasar Keamanan Siber dan CIA Triad

Cybersecurity atau keamanan siber didefinisikan sebagai serangkaian proses, teknologi, dan praktik yang dirancang untuk melindungi jaringan, perangkat, program, dan data dari serangan, kerusakan, atau akses yang tidak sah. Dalam literatur keamanan informasi, tujuan utama dari implementasi keamanan siber selalu merujuk pada tiga pilar fundamental yang dikenal sebagai CIA Triad:

1. Confidentiality (Kerahasiaan): Prinsip ini menjamin bahwa informasi hanya dapat diakses oleh pihak yang memiliki otoritas. Dalam konteks data pribadi, ini berarti melindungi NIK, data keuangan, dan kata sandi dari pengintipan atau pencurian. Pelanggaran terhadap kerahasiaan terjadi ketika data sensitif bocor ke publik atau pihak ketiga yang tidak berhak.
2. Integrity (Integritas): Prinsip ini menjamin bahwa data tetap akurat, konsisten, dan lengkap selama siklus hidupnya. Integritas memastikan bahwa informasi tidak dimodifikasi, dirusak, atau diubah oleh pihak yang tidak bertanggung jawab. Contoh pelanggaran integritas adalah ketika *malware* mengubah isi file dokumen atau ketika peretas mengubah nomor rekening tujuan dalam sebuah transaksi.
3. Availability (Ketersediaan): Prinsip ini memastikan bahwa sistem, aplikasi, dan data selalu tersedia dan dapat diakses oleh pengguna yang sah (*authorized users*) kapan pun dibutuhkan. Serangan seperti *Ransomware* yang mengunci data atau serangan *Denial-of-Service* (DoS) adalah contoh ancaman langsung terhadap prinsip ketersediaan ini.

2.2 Klasifikasi Ancaman Keamanan Siber

Lanskap ancaman siber terus berkembang. Masyarakat awam sering kali menjadi korban karena ketidaktahuan mereka terhadap metode serangan yang digunakan oleh peretas. Berikut adalah klasifikasi ancaman yang relevan dengan pengguna individu:

1. *Malware (Malicious Software)*: Merupakan istilah umum untuk perangkat lunak berbahaya. Jenis-jenisnya meliputi:
   - *Virus:* Program yang menempel pada file bersih dan menyebar ke file lain, sering kali merusak fungsi sistem.
   - *Trojan:* Perangkat lunak berbahaya yang menyamar sebagai aplikasi yang sah atau berguna untuk menipu pengguna agar mengunduhnya.
   - *Ransomware:* Jenis malware yang mengenkripsi data korban dan menuntut pembayaran tebusan untuk kunci dekripsinya. Ini adalah ancaman yang sangat merugikan secara finansial.
   - *Spyware:* Perangkat lunak yang beroperasi secara diam-diam untuk memata-matai aktivitas pengguna, mencuri *keystrokes* (ketikan keyboard), dan data pribadi.
2. *Phishing***:** Sebuah teknik *Social Engineering* di mana penyerang mengirimkan komunikasi palsu (biasanya email atau pesan instan) yang tampak berasal dari sumber tepercaya. Tujuannya adalah menipu korban agar mengungkapkan informasi sensitif seperti nomor kartu kredit atau kredensial *login*. Indikator utama *phishing* sering kali terdapat pada kesalahan penulisan URL, tata bahasa yang buruk, dan desakan urgensi yang dibuat-buat.
3. *Social Engineering:* Metode manipulasi yang mengeksploitasi psikologi manusia daripada kerentanan teknis sistem. Pelaku memanfaatkan rasa ingin tahu, rasa takut, atau keinginan menolong korban untuk mendapatkan akses. Inti dari serangan ini adalah menipu manusia, bukan meretas mesin.

2.3 Manajemen Identitas dan Keamanan Akun Digital

Dalam ekosistem digital, Akun Google berperan vital sebagai pusat identitas. Akun ini menyimpan riwayat pencarian, lokasi perjalanan, foto, dan dokumen. Jika akun ini kompromi, dampaknya meliputi pencurian identitas, kerugian finansial, dan hilangnya privasi total.

Pengamanan akun digital modern memerlukan pendekatan berlapis:

1. *Password Hygiene***:** Penggunaan kata sandi yang kuat (kombinasi huruf besar, kecil, angka, simbol) dan unik untuk setiap akun. Hindari penggunaan data mudah ditebak seperti tanggal lahir.
2. *Two-Factor Authentication (2FA)***:** Mekanisme keamanan yang mewajibkan dua bentuk identifikasi: sesuatu yang Anda tahu (kata sandi) dan sesuatu yang Anda miliki (kode

TRIDHARMADIMAS: Jurnal Pengabdian Kepada Masyarakat Jayakarta
http://journal.stmikjayakarta.ac.id/index.php/tridharmadimas
EmaiL: info@stmik.jayakarta.ac.id , tridharmadimas.jayakarta@gmail.com
DOI : 10.52362/tridharmadimas.v5i2.2206
E-ISSN: 2798-8295 **(Online), P-ISSN:** 2798-8554 **(Print)** Vol. 5 No.2, Desember 2025

verifikasi di HP). Ini adalah pertahanan paling efektif melawan pencurian *password*.

3. *Security Checkup***:** Fitur bawaan penyedia layanan untuk meninjau perangkat yang terhubung dan aktivitas login yang mencurigakan.

3. METODE PELAKSANAAN

Untuk memastikan program pengabdian masyarakat ini berjalan efektif dan mencapai tujuan yang diharapkan, digunakan metode pelaksanaan yang terstruktur dan sistematis. Pendekatan yang diadopsi adalah Participatory Action Research (PAR) yang dikombinasikan dengan metode pelatihan teknis. Pendekatan ini dipilih untuk melibatkan peserta secara aktif dalam proses pembelajaran dan pemecahan masalah keamanan yang mereka hadapi.
Tahapan pelaksanaan kegiatan dibagi menjadi tiga fase utama: Persiapan, Pelaksanaan, dan Evaluasi.

3.1 Fase Persiapan dan Analisis Kebutuhan

Sebelum pelaksanaan kegiatan, tim pengabdi melakukan serangkaian persiapan untuk memetakan kebutuhan mitra:

1. Observasi Lapangan: Tim melakukan kunjungan ke Sekretariat Karang Taruna Kelurahan Tangki untuk berdiskusi dengan pengurus. Tujuannya adalah mengetahui tingkat literasi digital anggota dan infrastruktur teknologi yang dimiliki (kepemilikan *smartphone*/laptop).
2. Identifikasi Masalah: Berdasarkan diskusi, ditemukan bahwa banyak anggota pernah mengalami upaya penipuan *online* atau lupa kata sandi akun mereka, namun tidak tahu cara menanganinya.
3. Penyusunan Materi: Materi disusun berdasarkan hasil identifikasi masalah, mencakup pengenalan ancaman siber (*phishing*, *malware*) dan panduan teknis langkah demi langkah (*step-by-step guide*) untuk mengamankan Akun Google. Materi disiapkan dalam bentuk *slide* presentasi visual yang menarik dan mudah dipahami.

3.2 Fase Pelaksanaan Pelatihan

Kegiatan inti dilaksanakan di Aula Kelurahan Tangki dengan durasi total 4 jam efektif. Metode penyampaian materi dibagi menjadi beberapa sesi:

1. Sesi 1: Ceramah Interaktif (Teori Dasar) Penyampaian materi mengenai *Cybersecurity Awareness*. Pada sesi ini, narasumber menggunakan bahasa yang populer dan analogi sehari-hari untuk menjelaskan konsep teknis seperti enkripsi dan *malware*. Peserta diajak berdialog mengenai pengalaman mereka berinternet.
2. Sesi 2: Demonstrasi (Studi Kasus) Narasumber mendemonstrasikan secara *real-time* bagaimana cara mengidentifikasi sebuah *link* berbahaya. Ditampilkan contoh *website* palsu yang menyerupai halaman *login* media sosial dan bank. Peserta diajarkan menggunakan *tools* publik seperti VirusTotal untuk memeriksa keamanan sebuah tautan atau file sebelum membukanya.
3. Sesi 3: Praktik Mandiri (Hands-on Lab) Ini adalah sesi inti di mana peserta diminta mengeluarkan *smartphone* masing-masing. Didampingi oleh tim fasilitator (penulis), peserta dipandu untuk:
    - Membuka pengaturan Akun Google.
    - Melakukan pemeriksaan keamanan (*Security Checkup*).
    - Mengaktifkan fitur Verifikasi 2 Langkah (2FA).
    - Memeriksa daftar perangkat yang terhubung dan menghapus perangkat yang tidak dikenal.

3.3 Fase Evaluasi dan Pendampingan

Evaluasi dilakukan dalam dua bentuk:

1. Evaluasi Formatif: Dilakukan selama sesi tanya jawab untuk mengukur pemahaman peserta secara langsung.
2. Evaluasi Sumatif: Melalui observasi keberhasilan peserta dalam mempraktikkan pengamanan akun. Keberhasilan diukur dari jumlah peserta yang berhasil mengaktifkan 2FA pada akhir sesi.

TRIDHARMADIMAS: Jurnal Pengabdian Kepada Masyarakat Jayakarta
http://journal.stmikjayakarta.ac.id/index.php/tridharmadimas
EmaiL: info@stmik.jayakarta.ac.id , tridharmadimas.jayakarta@gmail.com
DOI : 10.52362/tridharmadimas.v5i2.2206
E-ISSN: 2798-8295 **(Online), P-ISSN:** 2798-8554 **(Print)** Vol. 5 No.2, Desember 2025

4. HASIL DAN PEMBAHASAN

Kegiatan pelatihan ini dihadiri oleh anggota Karang Taruna Kelurahan Tangki dengan antusiasme yang tinggi. Berikut adalah rincian tahapan dan hasil dari kegiatan yang telah dilaksanakan:

Tabel 1. Rangkaian Program Pelatihan Cybersecurity

No.	Komponen Program	Deskripsi Kegiatan	Waktu	Metode
1	Pra-Kegiatan	Analisis kebutuhan mitra dan identifikasi isu keamanan yang sering terjadi di lingkungan warga.	1 Minggu	Observasi
2	Penyusunan Materi	Membuat modul presentasi tentang *Malware*, *Phishing*, dan panduan teknis keamanan Google.	1 Minggu	Studi Pustaka
3	Sesi Edukasi	Pemaparan materi mengenai pentingnya menjaga privasi data dan mengenali *Social Engineering*.	Saat Acara	Ceramah & Visualisasi
4	Workshop Teknis	Simulasi *Security Checkup* dan aktivasi Verifikasi 2 Langkah pada Akun Google peserta.	Saat Acara	Praktik Langsung
5	Evaluasi & Diskusi	Diskusi studi kasus penipuan *online* dan solusi pemulihan akun.	Akhir Sesi	Diskusi Interaktif

4.1 Peningkatan Pemahaman terhadap Lanskap Ancaman Siber

Pada sesi awal pelatihan, dilakukan penilaian cepat (*rapid assessment*) melalui tanya jawab. Hasilnya menunjukkan bahwa sebagian besar peserta tidak menyadari bahwa data sederhana seperti tanggal lahir dan nama ibu kandung adalah data krusial yang sering digunakan untuk verifikasi perbankan.

Melalui pemaparan materi, terjadi peningkatan pemahaman yang signifikan. Peserta kini memahami bahwa ancaman siber tidak selalu berupa peretasan sistem yang rumit, melainkan sering kali berupa *Social Engineering* yang menyerang psikologis. Peserta diperkenalkan pada konsep "Human Firewall", di mana kewaspadaan pengguna adalah lapisan pertahanan terakhir dan terkuat.

Salah satu poin diskusi yang menarik adalah pembahasan mengenai *Phishing*. Peserta ditunjukkan anatomi URL (alamat web). Mereka diajarkan untuk membaca domain dengan teliti. Misalnya, membedakan klikbca.com dengan klikbca-promo.com. Kemampuan deteksi dini ini sangat krusial untuk mencegah insiden kehilangan akun di masa depan.

TRIDHARMADIMAS: Jurnal Pengabdian Kepada Masyarakat Jayakarta
http://journal.stmikjayakarta.ac.id/index.php/tridharmadimas
EmaiL: info@stmik.jayakarta.ac.id , tridharmadimas.jayakarta@gmail.com
DOI : 10.52362/tridharmadimas.v5i2.2206
E-ISSN: 2798-8295 **(Online), P-ISSN:** 2798-8554 **(Print)** Vol. 5 No.2, Desember 2025

Gambar 1 Pemaparan Materi Mengenai Anatomi Serangan *Phishing dan Malware*

4.2 Implementasi Keamanan Akun Google

Sesi praktik (*hands-on*) menjadi indikator keberhasilan utama kegiatan ini. Mengingat Akun Google adalah pusat dari ekosistem digital peserta (pengguna Android), pengamanannya menjadi prioritas mutlak.

Berdasarkan panduan yang diberikan, peserta melakukan langkah-langkah berikut pada perangkat mereka:

1. Audit Perangkat (Device Activity): Peserta diarahkan mengakses menu Kelola Akun Google > Keamanan > Perangkat Anda.
    - *Temuan:* Sekitar 30% peserta menemukan bahwa akun mereka masih terhubung (*login*) di perangkat lama yang sudah dijual atau diberikan kepada orang lain.
    - *Tindakan:* Peserta langsung dibimbing untuk melakukan *logout* paksa (sign out) pada perangkat-perangkat asing tersebut untuk memutus akses.
2. Aktivasi Verifikasi 2 Langkah (2FA): Sebelum pelatihan, hanya sebagian kecil peserta yang mengaktifkan fitur ini karena menganggapnya rumit. Setelah dijelaskan bahwa 2FA adalah "gembok ganda", peserta antusias mengaktifkannya.
    - *Hasil:* Peserta berhasil mendaftarkan nomor telepon mereka sebagai metode verifikasi kedua. Mereka memahami bahwa meskipun *password* mereka dicuri lewat *phishing*, peretas tetap tidak bisa masuk tanpa kode OTP yang dikirim ke HP mereka.
3. Pemeriksaan Aplikasi Pihak Ketiga: Peserta memeriksa aplikasi apa saja yang memiliki izin akses ke data Google mereka (seperti akses ke Google Drive atau Kontak). Peserta menghapus izin akses untuk aplikasi *game* atau kuis *online* yang sudah tidak dimainkan namun masih memiliki akses data

TRIDHARMADIMAS: Jurnal Pengabdian Kepada Masyarakat Jayakarta
http://journal.stmikjayakarta.ac.id/index.php/tridharmadimas
EmaiL: info@stmik.jayakarta.ac.id , tridharmadimas.jayakarta@gmail.com
DOI : 10.52362/tridharmadimas.v5i2.2206
E-ISSN: 2798-8295 **(Online), P-ISSN:** 2798-8554 **(Print)** Vol. 5 No.2, Desember 2025

Gambar 2 Suasana Peserta Melakukan Praktik Security Checkup pada Smartphone

4.3 Diskusi Kasus dan Solusi Masalah

Sesi diskusi membuka wawasan mengenai kerentanan yang sering terjadi di masyarakat. Beberapa peserta menceritakan pengalaman kerabatnya yang terkena penipuan "undangan pernikahan digital" yang ternyata adalah file *malware* (.apk).
Narasumber memberikan solusi preventif:

1. Jangan pernah mengunduh file .apk dari sumber tidak resmi (di luar Play Store).
2. Selalu verifikasi pengirim pesan sebelum mengklik tautan.
3. Jika terlanjur mengklik dan menginstal, segera putuskan koneksi internet dan lakukan *factory reset* jika diperlukan, serta segera ganti *password* akun-akun penting dari perangkat lain yang aman.

Tabel berikut merangkum peningkatan keterampilan peserta sebelum dan sesudah pelatihan:

Tabel 2. Perbandingan Keterampilan Peserta Sebelum dan Sesudah Pelatihan

Indikator Keterampilan	Kondisi Awal (Pre-Training)	Kondisi Akhir (Post-Training)
Pemahaman *Phishing*	Rendah (sering asal klik tautan)	Tinggi (mampu cek URL dan verifikasi pengirim)
Penggunaan *Password*	Lemah (menggunakan tanggal lahir/nama)	Kuat (memahami konsep kombinasi karakter)
Status Verifikasi 2 Langkah	Mayoritas Non-Aktif	Mayoritas Aktif
Manajemen Perangkat Login	Tidak pernah dicek	Mampu melakukan *audit* dan *logout* perangkat asing
Sikap terhadap Keamanan	Pasif / Abai	Proaktif / Waspada

Kegiatan ditutup dengan komitmen bersama anggota Karang Taruna untuk menularkan ilmu ini kepada anggota keluarga di rumah, mengingat orang tua sering menjadi target utama penipuan digital.

5. KESIMPULAN

Berdasarkan pelaksanaan kegiatan Pengabdian kepada Masyarakat dengan topik pengenalan

TRIDHARMADIMAS: Jurnal Pengabdian Kepada Masyarakat Jayakarta
http://journal.stmikjayakarta.ac.id/index.php/tridharmadimas
EmaiL: info@stmik.jayakarta.ac.id , tridharmadimas.jayakarta@gmail.com
DOI : 10.52362/tridharmadimas.v5i2.2206
E-ISSN: 2798-8295 **(Online), P-ISSN:** 2798-8554 **(Print)** Vol. 5 No.2, Desember 2025

Cybersecurity di Kelurahan Tangki, Jakarta Barat, dapat ditarik beberapa kesimpulan penting:

1. Peningkatan Literasi: Pelatihan ini berhasil meningkatkan literasi digital anggota Karang Taruna secara signifikan. Peserta yang sebelumnya awam terhadap istilah teknis keamanan siber kini memahami konsep dasar kerahasiaan (*confidentiality*) dan integritas data.
2. Perubahan Perilaku: Terjadi perubahan perilaku digital ke arah yang lebih aman. Peserta tidak lagi sembarangan dalam mengelola akun. Hal ini dibuktikan dengan keberhasilan peserta dalam melakukan audit keamanan (*security checkup*) dan mengaktifkan Verifikasi 2 Langkah pada akun Google mereka.
3. Kemandirian Teknis: Metode pelatihan yang bersifat praktik langsung (*hands-on*) terbukti efektif. Peserta mampu secara mandiri mengidentifikasi potensi ancaman *phishing* dan *malware* menggunakan langkah-langkah verifikasi yang telah diajarkan.
4. Dampak Berkelanjutan: Anggota Karang Taruna memiliki potensi besar sebagai agen perubahan. Pengetahuan yang mereka dapatkan diharapkan dapat disebarluaskan kepada lingkungan sekitar, menciptakan efek bola salju dalam peningkatan kesadaran keamanan siber di Kelurahan Tangki.

Sebagai rekomendasi untuk kegiatan selanjutnya, diperlukan pelatihan lanjutan dengan topik yang lebih spesifik, seperti keamanan transaksi perbankan digital (*mobile banking*) dan etika bermedia sosial sesuai UU ITE, mengingat dinamika kejahatan siber yang terus berkembang.

DAFTAR PUSTAKA

[1] Aini, N., Hasmin, E., Heriadi, H., Samsie, I., Aisa, S., Rasyid, M. F., ... & Arwansyah, A. (2023). Pelatihan teknologi informasi pada kantor kelurahan Barrang Caddi Kepulauan Sangkarrang. *ABSYARA: Jurnal Pengabdian Pada Masyarakat*, 4(1), 123-130.

[2] Gede, I., Putra, J. E., Pradnyandari, A., Erawan, D., Aditya, W., Juniarta, W., ... & Baskara, W. (2023). Pelatihan Digital Marketing Dalam Upaya Meningkatkan Literasi Digital UMKM Desa Keramas. *BERNAS: Jurnal Pengabdian Kepada Masyarakat*, 4(1), 200-205.

[3] Kementerian Komunikasi dan Informatika. (2021). *Status Literasi Digital di Indonesia*. Jakarta: Kemenkominfo.

[4] Kadek Novayanti Kusuma Dewi, & Luh Putu Mahyuni. (2022). Pelatihan Digital Marketing Kepada UMKM di Banjar Pitik untuk Daya Saing Usaha. *Dinamisia: Jurnal Pengabdian Kepada Masyarakat*, 6(3), 716-724.

[5] Lova, A. N. (2023). Pelatihan Digital Marketing Pada Benih Cabe Unggul Untuk Meningkatkan Perekonomian Desa Siulak Tenang. *Jurnal Pengabdian Harapan Bangsa*, 2(1), 81-86.

[6] Mendrofa, Y. F. J., Lase, D., Waruwu, S., & Mendrofa, S. A. (2023). Analisis kebutuhan pelatihan dan pengembangan perangkat desa se-Kecamatan Alasa Talumuzoi dalam meningkatkan pelayanan publik. *Tuhenori: Jurnal Ilmiah Multidisiplin*, 1(1), 11-21.

[7] Muslihudin, M., Suyono, S., & Renaldo, R. (2022). Pengabdian Kepada Masyarakat Pelatihan Pemanfaatan Website Desa Dan Internet Dasar. *Jurnal PkM Pemberdayaan Masyarakat*, 3(3), 91-98.

[8] Pratama, I. P. A. E. (2020). *Handbook Jaringan Komputer: Teori dan Praktik Berbasiskan Open Source*. Bandung: Informatika.

[9] Setiawan, A., Arifudin, R., Sugiharti, E., Sekartaji, N. A., Nugroho, P. B., & Subarkah, A. (2023). Pelatihan New Media pada Perangkat Desa Wadaslintang Wonosobo dalam Digitalisasi Promosi Wisata. *Abdimasku Jurnal Pengabdian Masyarakat*, 6(3), 719.

[10] Trisudarmo, R., & Puteriawati, D. (2023). Peningkatan Pengelolaan Manajemen Dokumen Dan File Dengan Pemanfaatan Google Drive Pada Aparatur Pemerintah Desa. *Jurnal Abdikaryasakti*, 3(1), 45-86.

[11] Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security*. Cengage Learning.

DOI : 10.52362/tridharmadimas.v5i2.2206
E-ISSN: 2798-8295 **(Online), P-ISSN:** 2798-8554 **(Print)** Vol. 5 No.2, Desember 2025

[12] Wicaksono, D., Rakhmawati, Y., & Suryandari, N. (2021). Pelatihan "Cerdas Ber Internet" Bagi Orang Tua di Desa Burneh Bangkalan. *Jurnal Pengabdian Kepada Masyarakat*, 5(2), 137-143.

[13] Yandy, T. E., Armansyah, Y., & Ariawijaya, M. (2022). Pendampingan Penggunaan Google sebagai Pendukung Digitalisasi Pemerintahan Desa. *Jurnal Pengabdian Mandiri*, 1(3), 355-364.