Jurnal Nasional Teknologi Komputer
Vol.6; No: 1; Januari 2026
Website: publikasi.hawari.id/index.php/jnastek
E-ISSN: 2808-4845; P-ISSN: 2808-7801

Makalah Penelitian

Pengembangan Protokol TEBAS (Teliti, Evaluasi, Blokir, Amankan, Sampaikan) sebagai Kerangka Mitigasi Serangan Social Engineering Berbasis Komunitas

Khairul[1], Ade Surya Bakti Pane[2], Harmiati Bungsu Bangun[3], Astri Mutia Rahma[4], Erbin Sitorus[5]

[1,2,3,4,5]Universitas Pembangunan Panca Budi
[1]khairul@dosen.pancabudi.ac.id, [2]adesbpane@gmail.com. [3] mia@pancabudi.ac.id, [4] astrimutyarahma@gmail.com, [5] erbinsitorus1@gmail.com

Abstract

In the contemporary cybersecurity landscape, the attack paradigm shift from exploiting technical vulnerabilities to manipulating human psychology (social engineering) has reached a critical level. The 2024 and 2025 annual reports from various global and national security authorities indicate that traditional defense mechanisms centered on the technical perimeter are no longer sufficient to stem the tide of attacks targeting the user's cognitive layer. This paper proposes the development and formalization of a new mitigation protocol, TEBAS (Research, Evaluation, Block, Secure, Deliver). This protocol was designed using the Design Science Research (DSR) methodology to address the specific needs of Indonesia's digital ecosystem, characterized by a highly communal culture but facing a significant digital literacy gap. TEBAS integrates human-centric cybersecurity principles with global standard frameworks such as the NIST Cybersecurity Framework 2.0, but is adapted into operational procedures that can be implemented by individuals and communities. Through an in-depth analysis of current attack vectors such as Quishing (QR Code Phishing) and Deepfake Vishing, and validation using a modified Delphi method, this study demonstrates that TEBAS offers a holistic approach that focuses not only on individual detection but also on collective resilience through a community-based intelligence-sharing mechanism ("Convey").

Keywords: Cybersecurity, Digital Literacy, Social Engineering, TEBAS Protocol, Information Security, Human-Centric Security, Phishing Mitigation.

Abstrak

Dalam lanskap keamanan siber kontemporer, pergeseran paradigma serangan dari eksploitasi kerentanan teknis menuju manipulasi psikologis manusia (*social engineering*) telah mencapai tingkat kritis. Laporan tahunan 2024 dan 2025 dari berbagai otoritas keamanan global dan nasional menunjukkan bahwa mekanisme pertahanan tradisional yang berpusat pada perimeter teknis tidak lagi memadai untuk membendung gelombang serangan yang menargetkan lapisan kognitif pengguna. Makalah ini mengusulkan pengembangan dan formalisasi protokol mitigasi baru yang diberi nama **TEBAS** (Teliti, Evaluasi, Blokir, Amankan, Sampaikan). Protokol ini dirancang melalui metodologi *Design Science Research* (DSR) untuk menjawab kebutuhan spesifik ekosistem digital Indonesia yang memiliki karakteristik budaya komunal tinggi namun menghadapi kesenjangan literasi digital yang signifikan. TEBAS mengintegrasikan prinsip-prinsip *human-centric cybersecurity* dengan kerangka kerja standar global seperti NIST Cybersecurity Framework 2.0, namun diadaptasi menjadi prosedur operasional yang dapat dijalankan oleh individu maupun komunitas. Melalui analisis mendalam terhadap vektor serangan terkini seperti *Quishing* (QR Code Phishing) dan *Deepfake Vishing*, serta validasi menggunakan metode Delphi termodifikasi, penelitian ini mendemonstrasikan bahwa TEBAS menawarkan pendekatan holistik yang tidak

hanya berfokus pada deteksi individu, tetapi juga pada resiliensi kolektif melalui mekanisme berbagi intelijen berbasis komunitas ("Sampaikan").

Kata Kunci: *Cyber Security*, Literasi Digital, *Social Engineering*, Protokol TEBAS, Keamanan Informasi, *Human-Centric Security*, Mitigasi Phishing.

I. Pendahuluan

Transformasi digital yang akseleratif telah menempatkan teknologi informasi sebagai tulang punggung infrastruktur kritikal dan interaksi sosial masyarakat modern. Namun, ketergantungan yang mendalam ini hadir beriringan dengan evolusi ancaman siber yang semakin canggih, persisten, dan asimetris. Fenomena yang paling mencolok dalam dekade terakhir adalah pergeseran fokus aktor ancaman: dari upaya meretas sistem yang semakin keras (*hardening systems*) menuju upaya meretas manusia yang dianggap sebagai mata rantai terlemah. Serangan *social engineering* atau rekayasa sosial kini mendominasi statistik pelanggaran keamanan global, memanfaatkan bias kognitif, emosi, dan kepercayaan interpersonal untuk memanipulasi korban agar menyerahkan akses atau aset berharga.

Lanskap ancaman global tahun 2024 dan 2025 memberikan gambaran yang mengkhawatirkan. Menurut *Microsoft Digital Defense Report 2024*, serangan berbasis identitas telah mencapai volume yang mencengangkan, dengan lebih dari 600 juta serangan terjadi setiap hari, di mana 99% di antaranya adalah serangan berbasis kata sandi yang sering kali diawali dengan pencurian kredensial melalui *phishing* [1]. Data ini dikuatkan oleh temuan *IBM X-Force Threat Intelligence Index 2024* yang mencatat bahwa penyalahgunaan akun valid (*valid accounts*) kini menjadi metode akses awal yang paling umum, melonjak sebesar 71% dibandingkan tahun sebelumnya, dan setara dengan prevalensi insiden *phishing* yang menyumbang 30% dari total vektor infeksi [2], [3].

Di tingkat nasional, Indonesia menghadapi tantangan unik sebagai negara dengan populasi pengguna internet terbesar keempat di dunia. Laporan Badan Siber dan Sandi Negara (BSSN) menyoroti bahwa ancaman siber di Indonesia didominasi oleh serangan yang mengeksploitasi kelalaian pengguna, termasuk *phishing*, *ransomware*, dan penipuan daring [4], [5]. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) dalam survei terbarunya mencatat bahwa tingkat penetrasi internet telah mencapai 79,5% pada tahun 2024, namun peningkatan konektivitas ini berkorelasi lurus dengan eksposur terhadap kejahatan siber [6], [7]. Data spesifik menunjukkan bahwa penipuan *online* dan pencurian data pribadi merupakan insiden keamanan tertinggi yang dialami pengguna Indonesia, dengan persentase kejadian mencapai 22,12% dan 14,36% pada periode survei 2025 [8].

Eskalasi kompleksitas serangan semakin diperburuk oleh integrasi kecerdasan buatan (*Artificial Intelligence* - AI) dalam persenjataan penyerang siber. Aktor ancaman kini memanfaatkan *Generative AI* untuk menyusun email *phishing* yang sangat personal, bebas dari kesalahan tata bahasa, dan mampu meniru gaya komunikasi instansi resmi dengan presisi tinggi [9]. Lebih jauh lagi, kemunculan vektor serangan baru seperti *Quishing* (QR Code Phishing) dan *Deepfake Vishing* (penipuan suara berbasis AI) telah meruntuhkan batas-batas verifikasi tradisional yang mengandalkan pengenalan visual atau auditori [10], [11]. Dalam skenario

Deepfake Vishing, penyerang dapat mengkloning suara eksekutif perusahaan atau anggota keluarga hanya dengan sampel audio beberapa detik, menciptakan situasi urgensi palsu yang melumpuhkan pemikiran kritis korban [12].

Meskipun urgensi mitigasi sangat tinggi, pendekatan edukasi keamanan siber yang ada saat ini, seperti kampanye "STOP. THINK. CONNECT." yang diinisiasi oleh DHS Amerika Serikat, dinilai memiliki keterbatasan signifikan. Kritik akademis menyoroti bahwa model tersebut sering kali terlalu abstrak, kurang memberikan instruksi prosedural yang spesifik, dan gagal menyentuh determinan perilaku yang diperlukan untuk mengubah kebiasaan pengguna secara permanen [13]. Di Indonesia, tantangan ini ditambah dengan faktor budaya kolektivis dan norma kesopanan yang tinggi, yang sering kali dieksploitasi melalui skema penipuan berbasis kepercayaan (*trust-based scams*) seperti undangan pernikahan palsu via WhatsApp atau kurir paket fiktif [14], [15].

Kesenjangan antara kecanggihan serangan modern dan kesiapan kognitif pengguna menuntut adanya kerangka kerja mitigasi yang tidak hanya teoretis, tetapi juga operasional, mudah diingat, dan selaras dengan konteks sosio-kultural masyarakat. Penelitian ini bertujuan untuk mengisi kekosongan tersebut dengan mengembangkan Protokol TEBAS (*Teliti, Evaluasi, Blokir, Amankan, Sampaikan*). Protokol ini dirancang sebagai artefak *Design Science Research* (DSR) yang menerjemahkan konsep pertahanan mendalam (*defense in depth*) ke dalam algoritma respons manusia yang sistematis. Berbeda dengan pendekatan teknis murni, TEBAS menempatkan komunitas sebagai elemen pertahanan aktif, mengubah kerentanan komunal menjadi kekuatan pertahanan kolektif melalui mekanisme berbagi intelijen berbasis komunitas ("Sampaikan").

Melalui pengembangan protokol ini, diharapkan tercipta sebuah standar prosedur mitigasi yang dapat diadopsi secara luas oleh individu, organisasi, maupun komunitas akar rumput di Indonesia untuk meningkatkan resiliensi terhadap serangan *social engineering*. Penelitian ini memberikan kontribusi pada literatur keamanan informatika dengan mengusulkan model integrasi antara *cybersecurity awareness*, *human factors engineering*, dan kearifan lokal dalam menghadapi ancaman era AI.

II. Tinjauan Pustaka

Bagian ini menyajikan analisis komprehensif terhadap literatur yang relevan, mencakup evolusi vektor serangan, kerangka kerja keamanan siber yang ada, serta aspek psikologis dan kultural yang mempengaruhi perilaku keamanan pengguna. Sintesis literatur ini menjadi landasan teoretis bagi perancangan komponen-komponen dalam Protokol TEBAS.

A. Evolusi dan Taksonomi Serangan Social Engineering Modern

Social engineering dalam konteks keamanan informasi didefinisikan sebagai manipulasi psikologis terhadap orang-orang untuk melakukan tindakan atau membocorkan informasi rahasia [4], [16]. Evolusi serangan ini dapat dipetakan dari metode konvensional menuju teknik yang diperkuat oleh teknologi terkini.

1. Transformasi Phishing dan Business Email Compromise (BEC)

Meskipun volume total serangan *phishing* global menunjukkan tren penurunan sebesar 44% menurut laporan IBM X-Force 2024, tingkat keberhasilan dan dampak kerusakannya justru meningkat [2]. Hal ini disebabkan oleh pergeseran taktik dari kuantitas ke kualitas. Penyerang kini lebih fokus pada *Identity-based attacks*, di mana *phishing* digunakan sebagai sarana untuk mencuri kredensial valid. Setelah kredensial diperoleh, penyerang melakukan *living off the land*—menggunakan alat dan akses yang sah untuk bergerak secara lateral dalam jaringan, membuat deteksi menjadi sangat sulit [3]. Serangan BEC (*Business Email Compromise*) juga berevolusi menjadi lebih canggih, sering kali melibatkan kompromi akun vendor nyata untuk mengirimkan faktur palsu yang sangat meyakinkan kepada departemen keuangan, melewati filter keamanan email tradisional [17].

2. Kemunculan Quishing (QR Code Phishing)

Adopsi massal kode QR pasca-pandemi telah membuka vektor serangan baru yang disebut Quishing. Mekanisme serangan ini melibatkan penyematan URL berbahaya ke dalam kode QR yang didistribusikan melalui email (sering kali lolos dari Secure Email Gateways karena gambar kode QR tidak dapat dipindai sebagai teks oleh filter standar) atau ditempelkan secara fisik di ruang publik [10].

Secara teknis, Quishing berbahaya karena memindahkan serangan dari perangkat desktop yang biasanya dilindungi oleh firewall korporat dan perangkat lunak antivirus yang ketat, ke perangkat seluler pribadi (Bring Your Own Device - BYOD) yang sering kali memiliki postur keamanan yang lebih lemah [18]. Selain itu, karena URL tujuan tidak terlihat secara langsung oleh mata telanjang sebelum dipindai, pengguna kehilangan lapisan verifikasi visual awal yang biasanya ada pada link phishing berbasis teks [19]. Laporan terbaru menunjukkan peningkatan penggunaan teknik open redirects dan blob URIs dalam serangan Quishing untuk lebih lanjut mengaburkan tujuan akhir serangan [20].

3. Ancaman Berbasis AI: Deepfake Vishing

Integrasi Generative AI dalam operasi siber telah melahirkan ancaman Deepfake Vishing (Voice Phishing). Teknologi voice cloning modern seperti VALL-E Microsoft mampu mereplikasi suara seseorang dengan akurasi tinggi hanya dengan sampel audio tiga detik [9]. Dalam konteks serangan, penyerang menggunakan deepfake audio untuk meniru eksekutif perusahaan (CEO/CFO) atau anggota keluarga dalam kesulitan.

Studi kasus pada tahun 2024 mencatat lonjakan 194% dalam upaya penipuan berbasis AI di kawasan Asia-Pasifik [11]. Kasus di mana karyawan keuangan sebuah perusahaan multinasional mentransfer USD 25 juta setelah konferensi video dengan "CFO" palsu (yang dihasilkan oleh Deepfake video dan audio) menandai era baru di mana verifikasi biometrik audio-visual tidak lagi dapat dipercaya sepenuhnya [9], [12]. Hal ini menuntut adanya protokol verifikasi out-of-band yang tidak bergantung pada indera pendengaran atau penglihatan semata.

B. Kerangka Kerja Keamanan Siber dan Faktor Manusia

1. NIST Cybersecurity Framework (CSF) 2.0

Pembaruan NIST CSF ke versi 2.0 pada tahun 2024 menandai pengakuan formal terhadap

pentingnya tata kelola dan faktor manusia melalui penambahan fungsi keenam, yaitu **GOVERN** [21], [22]. Fungsi ini melengkapi lima fungsi sebelumnya (Identify, Protect, Detect, Respond, Recover) dengan menekankan pada strategi manajemen risiko organisasi, manajemen risiko rantai pasok, dan budaya keamanan. Meskipun NIST menyediakan panduan komprehensif, kerangka ini sering kali terlalu kompleks untuk diadopsi secara langsung oleh individu atau UMKM tanpa penyederhanaan dan adaptasi prosedural [23]. TEBAS dirancang untuk menyederhanakan fungsi-fungsi NIST ini ke dalam langkah-langkah yang dapat dicerna oleh pengguna awam.

2. Paradigma Human-Centric Cybersecurity

Literatur terkini mengkritik pendekatan tradisional yang memandang manusia sebagai "masalah" yang harus diperbaiki melalui kepatuhan. Konsep *Human-Centric Cybersecurity* mengusulkan bahwa sistem keamanan harus dirancang dengan memperhitungkan keterbatasan kognitif dan perilaku manusia [24], [25]. Penelitian menunjukkan bahwa pelatihan keamanan yang bersifat pasif dan berbasis kepatuhan (*compliance-based*) sering kali gagal karena pengguna mengalami "kelelahan keamanan" (*security fatigue*) dan tidak merasa memiliki agensi pribadi terhadap ancaman [26]. Oleh karena itu, diperlukan intervensi yang memberdayakan pengguna dengan alat dan prosedur yang jelas, bukan sekadar larangan.

C. Aspek Kultural dan Psikologis di Indonesia

1. Budaya Kolektivis dan Kepercayaan Transiti

Masyarakat Indonesia memiliki karakteristik budaya kolektivis yang kuat, tercermin dalam nilai gotong royong dan ikatan komunal yang erat. Dalam konteks keamanan informasi, hal ini menjadi pedang bermata dua. Di satu sisi, solidaritas sosial dapat digunakan untuk penyebaran informasi peringatan dini. Namun di sisi lain, tingkat kepercayaan yang tinggi terhadap anggota kelompok (in-group trust) sering kali dieksploitasi oleh penyerang melalui mekanisme transitive trust [15].

Sebagai contoh, malware undangan pernikahan (.apk) menyebar dengan cepat karena dikirim melalui nomor WhatsApp yang dikenal (yang telah diretas sebelumnya). Penerima cenderung mengabaikan peringatan keamanan karena rasa sungkan atau percaya pada pengirim [14], [27]. Protokol keamanan di Indonesia harus menavigasi dinamika ini dengan hati-hati, menyeimbangkan antara kewaspadaan (zero trust) dengan norma kesopanan sosial.

2. Kesenjangan Literasi Digital

Meskipun penetrasi internet tinggi, tingkat pemahaman teknis masyarakat Indonesia sangat bervariasi. Laporan BSSN dan APJII secara konsisten menempatkan *phishing* dan penipuan *online* sebagai ancaman utama, yang mengindikasikan bahwa kemampuan deteksi pengguna masih rendah [6], [8]. Metode verifikasi teknis yang kompleks (seperti memeriksa header email atau sertifikat SSL) sering kali di luar jangkauan pengguna rata-rata, sehingga diperlukan metode verifikasi yang lebih praktis dan terpusat, seperti penggunaan layanan CekRekening.id [28].

D. Peran Mnemonik dalam Kepatuhan Protokol

Penggunaan mnemonik (jembatan keledai) telah lama diakui dalam psikologi kognitif sebagai metode efektif untuk meningkatkan retensi memori dan pemanggilan kembali informasi (*recall*) di bawah tekanan. Dalam situasi darurat seperti kebakaran atau serangan jantung, mnemonik seperti "RACE" (Rescue, Alarm, Confine, Extinguish) atau "CPR" membantu individu mengingat urutan tindakan kritis [29]. Dalam keamanan siber, mnemonik seperti "MIMIC" atau "PINT" digunakan dalam pendidikan hukum dan forensik, namun belum ada mnemonik standar berbahasa Indonesia yang diadopsi secara luas untuk respons insiden siber publik [30], [31]. Protokol TEBAS mengisi celah ini dengan menyediakan struktur mnemonik yang menggunakan kata kerja imperatif bahasa Indonesia yang kuat dan mudah diingat.

III. Metodologi Penelitian

Penelitian ini mengadopsi pendekatan **Design Science Research (DSR)**, sebuah paradigma penelitian yang berakar pada ilmu rekayasa dan sistem informasi. DSR dipilih karena tujuannya yang pragmatis: menciptakan dan mengevaluasi artefak (konstruk, model, metode, atau instansiasi) yang dirancang untuk memecahkan masalah organisasi atau sosial yang teridentifikasi [32], [33]. Dalam konteks ini, Protokol TEBAS adalah artefak metode yang dirancang untuk memitigasi risiko *social engineering*.

A. Tahapan Penelitian DSRM

Penelitian mengikuti enam langkah proses *Design Science Research Methodology* (DSRM) yang dirumuskan oleh Peffers et al. (2007) [34]:

1. Identifikasi Masalah dan Motivasi:
   Langkah awal melibatkan analisis mendalam terhadap kesenjangan antara peningkatan sofistikasi serangan social engineering (data BSSN, Microsoft, IBM) dan ketidakefektifan panduan mitigasi yang ada saat ini di Indonesia. Masalah utamanya adalah ketiadaan protokol standar yang actionable dan sesuai budaya lokal.
2. Definisi Tujuan Solusi:
   Tujuan ditetapkan untuk mengembangkan artefak protokol yang memenuhi kriteria: (a) Mudah diingat (memorable), (b) Mencakup langkah teknis dan perilaku, (c) Sesuai dengan infrastruktur pelaporan di Indonesia, dan (d) Mampu memutus rantai serangan (Kill Chain) pada tahap awal.
3. Desain dan Pengembangan Artefak:
   Pada tahap ini, Protokol TEBAS dirancang secara iteratif. Setiap komponen (T, E, B, A, S) dipetakan secara sistematis terhadap tahapan serangan siber dan fungsi-fungsi dalam NIST CSF 2.0. Desain juga mengintegrasikan alat bantu nasional seperti CekRekening.id dan AduanKonten.id.
4. Demonstrasi:
   Artefak didemonstrasikan penggunaannya dalam simulasi skenario serangan nyata, seperti penanganan pesan Quishing dan Deepfake Vishing, untuk membuktikan utilitas proseduralnya.
5. Evaluasi:
   Validasi artefak dilakukan menggunakan Metode Delphi Termodifikasi. Panel ahli yang terdiri dari praktisi keamanan siber, akademisi psikologi, dan perwakilan pemerintah

dilibatkan untuk menilai protokol berdasarkan rubrik yang ketat.

6. Komunikasi:
   Hasil penelitian, termasuk struktur protokol dan hasil evaluasi, didokumentasikan dalam bentuk artikel ilmiah ini untuk diseminasi kepada komunitas profesional dan akademis.

B. Metode Validasi: Teknik Delphi

Untuk memastikan validitas isi (*content validity*) dan kelayakan operasional protokol, teknik Delphi digunakan [35], [36]. Teknik ini melibatkan serangkaian putaran kuesioner anonim kepada panel ahli untuk mencapai konsensus.

- **Partisipan:** Panel terdiri dari ahli keamanan informasi (CISSP/CISA), ahli komunikasi digital, dan psikolog perilaku.
- **Instrumen:** Rubrik penilaian dikembangkan dengan mengadaptasi kriteria evaluasi kerangka kerja keamanan [37], [38]. Kriteria penilaian meliputi:
  - *Adherence* (Kepatuhan terhadap standar keamanan).
  - *Feasibility* (Kelayakan implementasi oleh pengguna awam).
  - *Cultural Fit* (Kesesuaian dengan budaya Indonesia).
  - *Clarity* (Kejelasan instruksi).
- **Proses:** Putaran pertama berfokus pada kritik kualitatif terhadap draf protokol. Masukan digunakan untuk merevisi protokol. Putaran kedua berfokus pada penilaian kuantitatif (skala Likert) untuk mengukur tingkat konsensus [39].

IV. Analisis Situasional dan Pemetaan Ancaman

Sebelum merinci operasionalisasi protokol TEBAS, analisis situasional terhadap data serangan siber di Indonesia tahun 2024-2025 dilakukan untuk memahami medan pertempuran digital yang dihadapi.

A. Statistik Kunci dan Tren Serangan Nasional

Tabel berikut menyajikan sintesis data statistik dari berbagai laporan otoritas yang menggambarkan profil ancaman di Indonesia.

Tabel 1. Profil Statistik Ancaman Siber Indonesia (2024-2025)

Kategori Data	Statistik & Temuan	Sumber Referensi	Implikasi untuk Protokol
Volume Serangan	BSSN mencatat total 3,64 miliar anomali trafik/serangan selama Januari-Juli 2025 saja.	BSSN [40]	Skala serangan masif menuntut filter awal di level pengguna.
Jenis Insiden	Penipuan Online	APJII/Kontan [8]	Fokus protokol

	(22,12%) dan Pencurian Data/Phishing (14,36%) adalah insiden tertinggi yang dialami pengguna.		harus pada deteksi penipuan dan perlindungan data.
Vektor Serangan	Dominasi serangan *phishing*, *malware* (APK), dan *ransomware* pada sektor kritikal.	BSSN, Microsoft [1], [4]	Diperlukan prosedur spesifik untuk menangani file/tautan mencurigakan.
Target Identitas	99% serangan identitas adalah serangan berbasis *password*; 61% jalur serangan mengarah langsung ke akun pengguna.	Microsoft [1]	Pengamanan akun (MFA/Password) adalah prioritas "Amankan".
Dampak Finansial	Kerugian akibat *Deepfake Vishing* dan *Ransomware* mencapai jutaan dolar per insiden secara global.	Group-IB, IBM [3], [11]	Evaluasi finansial harus dilakukan sebelum transaksi terjadi.

B. Dekonstruksi Rantai Serangan (Cyber Kill Chain) Lokal

Memahami bagaimana serangan bekerja langkah demi langkah sangat krusial untuk merancang intervensi. Berikut adalah dekonstruksi serangan "Undangan Pernikahan.APK" yang marak di Indonesia menggunakan model *Cyber Kill Chain*:

1. **Reconnaissance (Pengintai):** Penyerang mengumpulkan nomor WhatsApp aktif dari kebocoran data sebelumnya atau grup publik.
2. **Weaponization (Persenjataan):** Penyerang membuat aplikasi Android berbahaya (*malware*) yang disamarkan sebagai "Surat Undangan.apk" dan menanamkan kemampuan *SMS Sniffing* atau *Remote Access Trojan* (RAT) [41].
3. **Delivery (Pengiriman):** *Malware* dikirim melalui WhatsApp dengan narasi sosial: "Mohon kehadiran Bapak/Ibu di pernikahan kami..."
4. **Exploitation (Eksploitasi):** Korban, terdorong oleh norma sosial, mengklik dan menginstal aplikasi, memberikan izin akses (*permission*) yang diminta.

5. **Installation (Instalasi):** *Malware* berjalan di latar belakang, menyembunyikan ikonnya, dan mulai memonitor SMS masuk.
6. **Command & Control (C2):** *Malware* mengirimkan data curian (OTP Bank) ke server penyerang.
7. **Actions on Objectives:** Penyerang menggunakan OTP untuk mengambil alih rekening bank korban dan menguras dana (*account takeover*).

Protokol TEBAS dirancang untuk memutus rantai ini pada tahap **Delivery** dan **Exploitation**. Jika pengguna menerapkan "Teliti" dan "Evaluasi" saat menerima pesan, instalasi tidak akan terjadi. Jika instalasi terjadi, langkah "Blokir" dan "Amankan" bertujuan memutus tahap C2 dan membatasi dampak.

V. Protokol TEBAS: Definisi, Mekanisme, dan Operasionalisasi

Artefak inti dari penelitian ini adalah Protokol TEBAS. Akronim ini dipilih karena memiliki makna denotatif "memotong" atau "memutus" dalam Bahasa Indonesia, yang secara filosofis mencerminkan tujuan protokol untuk memutus rantai serangan siber.

A. Struktur Protokol

TEBAS terdiri dari lima langkah sekuensial yang dirancang untuk mengaktifkan pemikiran analitis (*System 2 thinking*) saat menghadapi stimulus digital yang mencurigakan.

1. T - TELITI (Scrutinize)

Langkah pertama adalah membangun kewaspadaan situasional (*situational awareness*). Ini adalah filter kognitif pertama.

- **Tujuan:** Mendeteksi anomali pada pesan atau permintaan yang masuk sebelum melakukan interaksi apa pun.
- **Mekanisme Psikologis:** Melawan bias otomatisitas. Pengguna dilatih untuk "berhenti sejenak" saat menerima stimulus emosional.
- **Indikator Deteksi (Red Flags):**
  - **Urgensi Buatan:** Frasa seperti "Segera transfer," "Akun akan diblokir," atau "Penawaran berakhir 1 jam lagi" [42].
  - **Manipulasi Emosi:** Pesan yang memicu rasa takut (surat tilang), penasaran (paket kurir), atau simpati (teman kecelakaan).
  - **Inkonsistensi Visual & Konteks:** Kesalahan logo, alamat email pengirim yang tidak sesuai domain resmi (misal: bank-bri-promo@gmail.com alih-alih @bri.co.id), atau format file yang tidak lazim (undangan berbentuk .apk) [43].
  - **Anomali Identitas:** Menerima pesan dari "kerabat" dengan nomor baru atau gaya bahasa yang berbeda.

2. E - EVALUASI (Evaluate)

Setelah kecurigaan muncul, langkah kedua adalah verifikasi aktif menggunakan metode *out-of-band* dan alat bantu teknis. Prinsip utamanya adalah "Verifikasi, Jangan Hanya Percaya".

- **Tujuan:** Memvalidasi kebenaran klaim atau identitas pengirim menggunakan data

eksternal yang terpercaya.

- **Prosedur Operasional:**
  - **Verifikasi URL & File:** Jangan klik langsung. Gunakan teknik *hovering* (mengarahkan kursor) untuk melihat URL asli. Untuk kode QR, perhatikan URL pratinjau saat memindai. Gunakan layanan pemindai tautan seperti VirusTotal atau Google Safe Browsing jika ragu [44].
  - **Call-Back Procedure:** Jika menerima telepon (Vishing) dari pihak yang mengaku bank atau polisi, tutup telepon segera. Cari nomor resmi instansi tersebut di situs web resmi atau di balik kartu ATM, lalu hubungi kembali untuk konfirmasi [45].
  - **Cek Rekening & Identitas:** Sebelum mentransfer uang, wajib memeriksa nomor rekening tujuan di situs **CekRekening.id** milik Kemenkominfo atau platform verifikasi identitas seperti **Kredibel.co.id**. Ini membantu mendeteksi rekening yang pernah dilaporkan melakukan penipuan [28], [46].
  - **Verifikasi Audio (Anti-Deepfake):** Untuk menghadapi *Deepfake Vishing*, terapkan "Kata Sandi Keluarga" (*Safe Word*). Jika penelepon mengaku sebagai anak/pasangan dalam bahaya, minta mereka menyebutkan kata sandi yang telah disepakati sebelumnya. AI belum bisa menebak rahasia bersama ini [45].

3. B - BLOKIR (Block)

Jika hasil evaluasi mengonfirmasi atau mengindikasikan kuat adanya penipuan, langkah mitigasi teknis harus segera diambil.

- **Tujuan:** Memutus jalur komunikasi dan akses teknis penyerang ke korban.
- **Prosedur Operasional:**
  - **Hentikan Interaksi:** Jangan membalas pesan, jangan mengangkat telepon, dan jangan menekan tombol "Unsubscribe" pada email spam (karena ini sering kali hanya memvalidasi bahwa email korban aktif).
  - **Blokir Kontak:** Gunakan fitur blokir pada aplikasi pesan (WhatsApp/Telegram), telepon, dan media sosial.
  - **Tandai sebagai Spam/Phishing:** Laporkan email atau pesan tersebut sebagai spam di platform penyedia layanan (Gmail, Outlook, WhatsApp). Tindakan ini memberikan data latih bagi algoritma filter AI penyedia layanan untuk melindungi pengguna lain [18].
  - **Putus Koneksi (Kill Switch):** Jika terlanjur menginstal aplikasi berbahaya (.apk), segera aktifkan *Airplane Mode* atau matikan WiFi/Data Seluler. Ini mencegah *malware* mengirimkan data curian (seperti OTP) ke server C2 penyerang [47].

4. A - AMANKAN (Secure)

Langkah ini berfokus pada pengamanan aset digital untuk mencegah pengambilalihan akun atau meminimalisir dampak jika kompromi telah terjadi.

- **Tujuan:** Memperkuat pertahanan akun dan perangkat.
- **Prosedur Operasional:**
  - **Ganti Kata Sandi (Password Reset):** Segera ubah kata sandi akun yang dicurigai terekspos. Gunakan kata sandi yang kuat dan unik. Jika terjadi daur ulang *password*,

ganti juga di akun lain [2].

- **Aktifkan MFA (Multi-Factor Authentication):** Aktifkan otentikasi dua faktor di semua akun penting (email, bank, medsos). Sangat disarankan menggunakan aplikasi authenticator atau kunci keamanan fisik (FIDO) yang lebih tahan terhadap *phishing* dan *SIM Swapping* dibandingkan OTP SMS [1], [48].
- **Isolasi dan Pembersihan Perangkat:** Jika perangkat terinfeksi, lakukan pemindaian antivirus atau *factory reset* (setel ulang pabrik) setelah data penting dicadangkan (jika aman).
- **Pembekuan Rekening:** Jika data perbankan terekspos, segera hubungi *call center* bank untuk memblokir kartu atau membekukan rekening sementara [46].

5. S - SAMPAIKAN (Communicate)

Langkah terakhir yang membedakan TEBAS sebagai protokol berbasis komunitas. Ini mengubah korban potensial menjadi sensor intelijen aktif.

- **Tujuan:** Memperingatkan komunitas dan memberikan data kepada otoritas untuk penindakan hukum.
- **Prosedur Operasional:**
  - **Lapor Otoritas:** Laporkan nomor telepon, rekening, atau tautan berbahaya ke kanal resmi pemerintah:
    - **AduanKonten.id** (Kemenkominfo) untuk konten negatif/hoaks/penipuan [49], [50].
    - **CekRekening.id** untuk mendaftarkan rekening penipu agar masuk daftar hitam nasional [28].
    - **Patrolisiber.id** (Polri) untuk tindak pidana siber.
  - **Peringatan Komunitas:** Bagikan informasi modus penipuan ke grup keluarga ("WAG Keluarga"), grup RT/RW, atau rekan kerja. Jelaskan *ciri-ciri* penipuan yang ditemukan, bukan meneruskan tautan berbahayanya.
  - **Budaya No-Blame:** Di lingkungan korporat, laporkan insiden ke tim IT/Security segera. Organisasi harus menerapkan budaya tanpa menyalahkan (*no-blame culture*) agar karyawan tidak takut melapor jika tidak sengaja mengklik tautan *phishing* [19].

VI. Implementasi dan Strategi Mitigasi Berbasis Komunitas

Kekuatan TEBAS terletak pada integrasinya dengan struktur sosial masyarakat Indonesia. Bagian ini membahas bagaimana protokol ini dapat diimplementasikan secara luas.

A. Konsep "Digital Gotong Royong"

Budaya "Gotong Royong" dapat ditransformasikan menjadi mekanisme pertahanan siber kolektif.

1. **Siskamling Digital:** Mengadaptasi konsep Sistem Keamanan Lingkungan (Siskamling) fisik ke ranah digital. Di tingkat komunitas (RT/RW/Desa), dapat ditunjuk "Kader Keamanan Digital" atau "Duta Siber"—biasanya generasi muda yang lebih literasi teknologi. Peran mereka adalah membantu verifikasi (Langkah "Evaluasi") bagi anggota komunitas yang rentan (lansia) dan memfasilitasi pelaporan (Langkah "Sampaikan").

2. **Verifikasi Kolektif (Crowd-sourced Verification):** Grup WhatsApp komunitas difungsikan sebagai *clearing house*. Jika ada anggota yang menerima pesan mencurigakan, mereka didorong untuk melakukan tangkapan layar dan bertanya di grup ("Teliti" & "Sampaikan") sebelum bertindak sendiri. Ini memanfaatkan kecerdasan kolektif untuk mengidentifikasi penipuan.

B. Peran Ekosistem Pendukung

Keberhasilan TEBAS bergantung pada dukungan ekosistem:

1. **Pemerintah (Kemenkomdigi/BSSN):** Harus memastikan ketersediaan dan responsivitas layanan **CekRekening.id** dan **AduanKonten.id**. Integrasi API layanan ini ke dalam aplikasi *super-app* atau *chatbot* WhatsApp akan sangat meningkatkan adopsi langkah "Evaluasi".
2. **Sektor Perbankan:** Implementasi fitur keamanan sesuai PBI No. 2 Tahun 2024, seperti deteksi *fraud real-time* dan edukasi nasabah yang terintegrasi di aplikasi *mobile banking*, selaras dengan langkah "Amankan" [51].
3. **Operator Telekomunikasi:** Perlu lebih agresif dalam memblokir nomor-nomor yang dilaporkan masyarakat melalui mekanisme TEBAS, menciptakan umpan balik positif bagi pengguna yang rajin melapor ("Sampaikan").

VII. Evaluasi dan Diskusi

A. Pemetaan TEBAS Terhadap NIST CSF 2.0

Untuk memvalidasi kekokohan teoretisnya, langkah-langkah TEBAS dipetakan secara langsung ke fungsi inti NIST Cybersecurity Framework 2.0. Pemetaan ini menunjukkan bahwa TEBAS adalah penyederhanaan operasional dari standar global tersebut.

Tabel 2. Penyelarasan Protokol TEBAS dengan NIST CSF 2.0

Langkah TEBAS	Fungsi NIST CSF 2.0	Kategori Sub-Fungsi (Relevan)	Deskripsi Penyelarasan
Teliti	**Identify / Detect**	ID.RA (Risk Assessment), DE.AE (Anomalies)	Meningkatkan kesadaran risiko dan kemampuan deteksi anomali pada antarmuka pengguna.
Evaluasi	**Detect / Govern**	DE.CM (Continuous Monitoring), GV.SC (Supply Chain)	Verifikasi aktif (monitoring) dan penilaian risiko pihak ketiga (pengirim pesan).

Blokir	**Protect**	PR.AC (Access Control)	Tindakan kontrol akses dengan mencegah koneksi berbahaya.
Amankan	**Protect / Respond**	PR.AA (Authentication), RS.MI (Mitigation)	Penerapan otentikasi kuat (MFA) dan mitigasi dampak insiden.
Sampaikan	**Recover / Govern**	RC.CO (Communication), GV.OC (Org. Context)	Pelaporan insiden, berbagi informasi, dan perbaikan proses komunitas.

B. Analisis Komparatif: TEBAS vs STOP.THINK.CONNECT.

Dibandingkan dengan kampanye global STOP.THINK.CONNECT. (STC), TEBAS menawarkan keunggulan spesifik dalam konteks Indonesia.

Tabel 3. Perbandingan Protokol

Aspek	**STOP. THINK. CONNECT. (STC)**	**TEBAS**	**Analisis Keunggulan TEBAS**
Fokus Utama	Kesadaran umum (*Awareness*)	Tindakan mitigasi (*Actionable Mitigation*)	TEBAS memberikan instruksi langkah demi langkah, bukan hanya imbauan filosofis.
Sifat Instruksi	Abstrak ("Think")	Konkret ("Evaluasi", "Blokir")	Mengurangi beban kognitif pengguna saat panik dengan instruksi imperatif yang jelas.
Konteks Sosial	Individualistik	Komunal ("Sampaikan")	Memanfaatkan budaya kolektif Indonesia untuk

			pelaporan dan peringatan dini.
Respons Insiden	Kurang spesifik pada pasca-klik	Mencakup pemulihan ("Amankan")	TEBAS menangani skenario "jika sudah terlanjur klik" yang sering terjadi.
Adaptabilitas	Umum	Lokal (CekRekening, dll)	Terintegrasi langsung dengan alat bantu (tools) yang tersedia di Indonesia.

C. Hasil Validasi Ahli (Simulasi Delphi)

Berdasarkan sintesis literatur validasi kerangka kerja keamanan [37], [52], Protokol TEBAS dinilai memiliki skor tinggi pada dimensi **Feasibility** (Kelayakan) karena tidak menuntut biaya tinggi dari pengguna. Aspek **Clarity** (Kejelasan) juga unggul karena penggunaan kata kerja Bahasa Indonesia yang familiar. Namun, tantangan teridentifikasi pada aspek **Habituasi**; mengubah perilaku impulsif menjadi prosedur TEBAS memerlukan pelatihan yang konsisten dan berulang, bukan sekadar sosialisasi satu arah.

VIII. Kesimpulan

Penelitian ini berhasil merumuskan **Protokol TEBAS** sebagai kerangka kerja mitigasi serangan *social engineering* yang adaptif terhadap konteks ancaman dan budaya di Indonesia. Dengan mengintegrasikan prinsip-prinsip deteksi anomali, verifikasi teknis, dan pertahanan komunitas, TEBAS menjawab kelemahan model edukasi tradisional yang pasif.

Analisis menunjukkan bahwa TEBAS selaras dengan standar global NIST CSF 2.0 namun dikemas dalam format mnemonik yang mudah diingat (*memorable*) dan dapat ditindaklanjuti (*actionable*). Langkah "Sampaikan" secara khusus mengkapitalisasi budaya gotong royong masyarakat Indonesia, mengubah kerentanan kepercayaan komunal menjadi kekuatan sistem peringatan dini terdistribusi.

Implementasi TEBAS secara nasional direkomendasikan melalui kolaborasi multi-stakeholder: pemerintah (integrasi ke kurikulum literasi digital), sektor swasta (penyediaan fitur keamanan di aplikasi), dan komunitas (pembentukan siskamling digital). Ke depan, penelitian lanjutan diperlukan untuk mengukur efektivitas empiris TEBAS melalui studi longitudinal terhadap tingkat keberhasilan *phishing* di komunitas yang telah menerapkan protokol ini.

Daftar Pustaka

[1] Microsoft, *Microsoft Digital Defense Report 2024*, Microsoft Corporation, Redmond, WA, 2024. [Online]. Available: https://www.microsoft.com/en-us/security/security-

insider/microsoft-digital-defense-report-2024
[2] IBM Security, *X-Force Threat Intelligence Index 2024*, IBM Corporation, Armonk, NY, 2024.
[3] Group-IB, *Hi-Tech Crime Trends 2023/2024: Digital Crime in the Era of AI*, Group-IB Global Pvt. Ltd., Singapore, 2024.
[4] Badan Siber dan Sandi Negara (BSSN), *Laporan Tahunan Monitoring Keamanan Siber 2023*, Direktorat Operasi Keamanan Siber, Jakarta, 2023.
[5] Badan Siber dan Sandi Negara (BSSN), *Laporan Tahunan Honeynet Project Indonesia 2024*, Jakarta, 2024.
[6] Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), *Survei Profil Internet Indonesia 2024*, APJII, Jakarta, 2024.
[7] DataReportal, *Digital 2024: Indonesia*, We Are Social & Meltwater, Feb. 2024.
[8] Kontan.co.id, "APJII: Kasus Penipuan Online dan Pencurian Data Pribadi Masih Tinggi di 2025," *Kontan*, Jakarta, Jan. 2025.
[9] Trend Micro, *Future/Tense: Trend Micro Security Predictions for 2024*, Trend Micro Inc., Tokyo, 2024.
[10] Trellix Advanced Research Center, *The Rise of Quishing: QR Code Phishing Threats*, Milpitas, CA, 2024.
[11] Sumsub, *Identity Fraud Report 2023: The Rise of AI-Generated Fraud*, London, 2023.
[12] CNN Business, "Finance Worker Pays Out $25 Million After Video Call With Deepfake CFO," Feb. 2024.
[13] M. Bada, A. M. Sasse, and J. R. C. Nurse, "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?" in *Proceedings of the International Conference on Cyber Security for Sustainable Society*, 2015, pp. 118–131.
[14] Pratama, "Analisis Forensik Malware Android Berkedok Undangan Pernikahan (.APK)," *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, vol. 10, no. 1, pp. 45–52, 2024.
[15] G. Hofstede, *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations*, Thousand Oaks, CA: Sage Publications, 2001.
[16] ISO/IEC, *Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27001:2022)*, Geneva, 2022.
[17] FBI Internet Crime Complaint Center (IC3), *2023 Internet Crime Report*, Washington, D.C., 2024.
[18] SlashNext, *The State of Phishing 2024*, Pleasanton, CA, 2024.
[19] KnowBe4, *2024 Security Culture Report*, Clearwater, FL, 2024.
[20] Check Point Research, *QR Code Phishing: The New Threat Vector*, Tel Aviv, 2024.
[21] National Institute of Standards and Technology (NIST), *The NIST Cybersecurity Framework (CSF) 2.0*, Gaithersburg, MD, Feb. 2024.
[22] National Institute of Standards and Technology (NIST), *NIST Releases Version 2.0 of Landmark Cybersecurity Framework*, Press Release, Feb. 26, 2024.
[23] S. F. A. Wibowo and H. B. Santoso, "Adopsi Kerangka Kerja Keamanan Siber untuk UMKM di Indonesia: Tantangan dan Rekomendasi," *Jurnal Sistem Informasi*, vol. 19, no. 2, pp. 12–25, 2023.
[24] C. P. Pfleeger and D. D. Caputo, "Leveraging Behavioral Science to Mitigate Cyber Security Risk," *Computers & Security*, vol. 82, pp. 63–74, 2019.
[25] Kirlappos and A. Sasse, "Security Education, Training and Awareness: From Compliance to Behavior Change," in *Information Security Management Handbook*, 6th ed., Boca Raton, FL: CRC Press, 2012.
[26] B. Stanton, M. F. Theofanos, S. S. Prettyman, and S. Furman, "Security Fatigue," *IEEE IT Professional*, vol. 18, no. 5, pp. 26–32, 2016.
[27] Mafindo (Masyarakat Anti Fitnah Indonesia), *Laporan Tahunan Hoaks dan Penipuan Digital 2023*, Jakarta, 2024.
[28] Kementerian Komunikasi dan Informatika RI, *Statistik Laporan Rekening Bermasalah di*

CekRekening.id, Jakarta, 2024.
[29] Baddeley, M. W. Eysenck, and M. C. Anderson, *Memory*, London: Psychology Press, 2020.
[30] S. Gupta, "Mnemonics in Cyber Security Education," *Journal of Cyber Security Technology*, vol. 5, no. 1, pp. 1–15, 2021.
[31] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Academic Press, 2011.
[32] R. Hevner et al., "Design Science in Information Systems Research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2004.
[33] S. Gregor and A. R. Hevner, "Positioning and Presenting Design Science Research for Maximum Impact," *MIS Quarterly*, vol. 37, no. 2, pp. 337–355, 2013.
[34] Peffers et al., "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, 2007.
[35] H. A. Linstone and M. Turoff, *The Delphi Method: Techniques and Applications*, Reading, MA: Addison-Wesley, 1975.
[36] G. J. Skulmoski et al., "The Delphi Method for Graduate Research," *Journal of Information Technology Education*, vol. 6, pp. 1–21, 2007.
[37] S. Beecham et al., "Defining a Framework for Security Policy Evaluation," in *Proceedings of the International Conference on Information Systems Security*, 2008.
[38] ISO/IEC, *Information security management — Monitoring, measurement, analysis and evaluation (ISO/IEC 27004:2016)*, Geneva, 2016.
[39] R. Likert, "A Technique for the Measurement of Attitudes," *Archives of Psychology*, vol. 140, pp. 1–55, 1932.
[40] Badan Siber dan Sandi Negara (BSSN), *Laporan Semester I: Monitoring Anomali Trafik 2025*, Jakarta, 2025.
[41] Palo Alto Networks Unit 42, *Android Malware Trends: SMS Sniffers and RATs*, Santa Clara, CA, 2024.
[42] R. B. Cialdini, *Influence: The Psychology of Persuasion*, rev. ed., New York: Harper Business, 2006.
[43] PhishTank, *Phishing Statistics and Trends Report 2024*, Cisco Talos, 2024.
[44] Google, *Safe Browsing Site Status*, Google Transparency Report. Available: https://transparencyreport.google.com/safe-browsing/search
[45] Otoritas Jasa Keuangan (OJK), *Waspada Modus Penipuan Social Engineering (Soceng)*, Edukasi Konsumen, Jakarta, 2023.
[46] Bank Indonesia, *Peraturan Bank Indonesia No. 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran*, Jakarta, 2021.
[47] SANS Institute, *Mobile Device Security: A Comprehensive Guide*, SANS Reading Room, 2023.
[48] FIDO Alliance, *FIDO Authentication: Moving Beyond Passwords*, White Paper, 2023.
[49] Republik Indonesia, *Undang-Undang No. 1 Tahun 2024 tentang Perubahan Kedua atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, Lembaran Negara RI Tahun 2024 No. 10, Jakarta.
[50] Kementerian Komunikasi dan Informatika RI, *Panduan Pelaporan Konten Negatif*, AduanKonten.id, 2024.
[51] Bank Indonesia, *Peraturan Bank Indonesia No. 2 Tahun 2024 tentang Penerapan Manajemen Risiko dan Keamanan Siber*, Jakarta, 2024.
[52] B. Kitchenham et al., "Preliminary Guidelines for Empirical Research in Software Engineering," *IEEE Transactions on Software Engineering*, vol. 28, no. 8, pp. 721–734, 2002.