BAB I
PENDAHULUAN

1.1 Gambaran Umum Objek Penelitian

1.1.1 Profil Objek Penelitian

Dalam studi ini, penelitian dilakukan di Indonesia dengan fokus pada pengguna media sosial. Media sosial yakni salah satu sarana teknologi informasi yang digunakan sebagai alat komunikasi untuk berinteraksi secara global dan sangat populer di berbagai kalangan di Indonesia. Media sosial adalah platform online yang memungkinkan pengguna dengan mudah menggunakannya untuk memenuhi kebutuhan komunikasi mereka (Widada, 2018). Menurut McLuhan, fungsi media sosial adalah sebagai media interaktif yang mengandung konsep "*the medium is the message*" berarti media itu sendiri adalah pesan yang mengubah pola komunikasi dan bahasa dalam interaksi antar manusia.

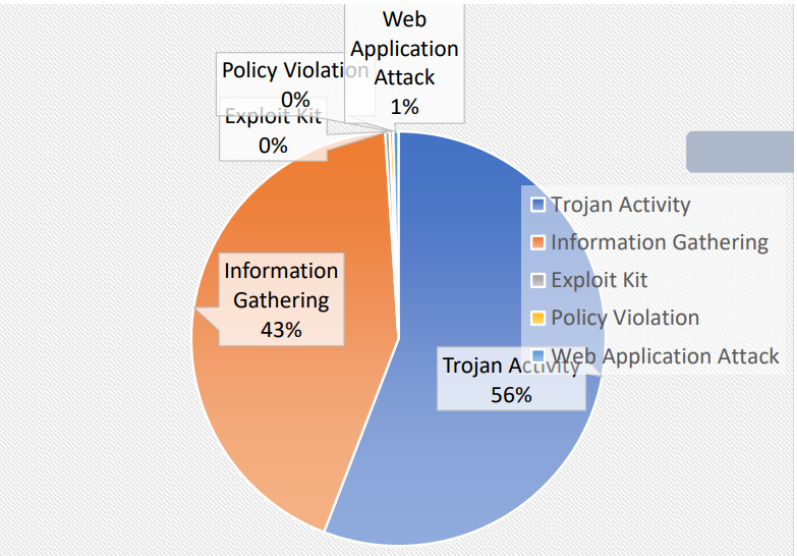
Pengguna media sosial saat ini telah meningkat secara signifikan. Menurut laporan We Are Social (Annur, 2024), pada Januari 2024 ada 185 juta individu pengguna internet di Indonesia, setara 66,5% dari total populasi nasional yang berjumlah 278,7 juta orang. Lebih lanjut data berdasarkan laporan “Digital Indonesia 2024” menunjukkan frekuensi penggunaan masyarakat indonesia rata-rata menghabiskan 3 jam 11 menit per harinya.

Laporan lainnya dari We Are Social (2024), mencatat bahwa terdapat sekitar 139 juta identitas pengguna media sosial di Indonesia pada Januari 2024, yang mewakili 49,9% dari total populasi nasional. WhatsApp merupakan aplikasi media sosial yang paling dominan digunakan di Indonesia pada Januari 2024. Dari seluruh pengguna internet di Indonesia yang berusia 16—64 tahun, sekitar 90,9% menggunakan aplikasi ini. Instagram menempati peringkat kedua dengan 85,3% pengguna, diikuti oleh Facebook dengan 81,6%, dan TikTok dengan 73,5%. Sementara itu, Telegram digunakan oleh 61,3% pengguna, sedangkan X (sebelumnya Twitter) oleh 57,5%. Aplikasi lain seperti Facebook Messenger, Pinterest, Kuaishou (Kwai dan Snack Video), dan LinkedIn juga digunakan oleh sebagian kecil pengguna.

Media sosial telah menciptakan platform di mana individu dapat membentuk komunitas online yang luas untuk berbagi minat, pengalaman, dan pemikiran mereka, tidak hanya memungkinkan berbagi informasi pribadi, tetapi juga memfasilitasi akses yang lebih besar terhadap informasi umum dan berita (Aldan Nur Zen & Sitanggang, 2023).

1.2 Latar Belakang Penelitian

Di era digital ini, Teknologi Informasi dan Komunikasi (TIK) telah menjadi bagian tak terpisahkan dari kehidupan manusia. Hampir semua aspek kehidupan, mulai dari pekerjaan, pendidikan, hingga hiburan kini bergantung pada TIK. Kemajuan teknologi ini membawa banyak manfaat namun juga membuka celah bagi para penjahat siber untuk melancarkan aksinya. Seiring dengan meningkatnya ketergantungan pada TIK, risiko serangan siber pun semakin tinggi. Salah satu tindak kejahatan yang sering terjadi yaitu *social engineering* (Rusyda, 2023). Menurut Anders (2020), *social engineering* adalah serangan psikologis di mana penyerang menipu korban untuk melakukan sesuatu yang seharusnya tidak dilakukan. Konsep *social engineering* bukanlah hal baru namun yang membuat teknologi saat ini jauh lebih efektif bagi para penyerang dunia maya adalah korban tidak dapat melihatnya secara fisik. Pelaku dapat dengan mudah berpura-pura menjadi apa pun atau siapa pun yang mereka inginkan dan menargetkan jutaan orang di seluruh dunia. Selain itu, serangan *social engineering* dapat melewati banyak teknologi keamanan. Kesalahpahaman umum yang dimiliki kebanyakan orang tentang penyerang dunia maya adalah bahwa pelaku menggunakan alat dan teknik yang sangat canggih untuk meretas ke komputer atau akun korban. Padahal, penyerang dunia maya telah belajar bahwa seringkali cara termudah untuk mencuri informasi pribadi, meretas akun, atau menginfeksi sistem korban adalah dengan menipu korban agar melakukan kesalahan.



Gambar 1. 1 Klasifikasi serangan siber
Sumber : www.bssn.go.id (2020)

Menurut rekapitulasi insiden web defacement yang dirilis oleh Badan Siber dan Sandi Negara (BSSN) Indonesia dilihat dari gambar 1.1 klasifikasi serangan siber untuk periode

Januari hingga April 2020, berbagai bentuk serangan siber telah terjadi di Indonesia. Dari beragam jenis serangan ini, *trojan activity* menjadi serangan siber tertinggi. *Trojan* sendiri adalah satu jenis *malware* yang menyamar atau berperilaku sebagai program yang bermanfaat dengan tujuan memberikan akses yang tidak sah kepada *attacker* ke sistem komputer pengguna(Nugraha et al., 2019). Misalnya, pelaku kejahatan mungkin mengirim email dengan lampiran yang terlihat sah (misalnya, berkedok sebagai faktur atau *resume*) yang sebenarnya berisi *Trojan*. *Trojan activity* ini juga termasuk ke dalam kategori *social engineering* karena seringkali melibatkan manipulasi psikologis untuk mengelabui pengguna agar mengunduh dan menginstal perangkat lunak berbahaya.

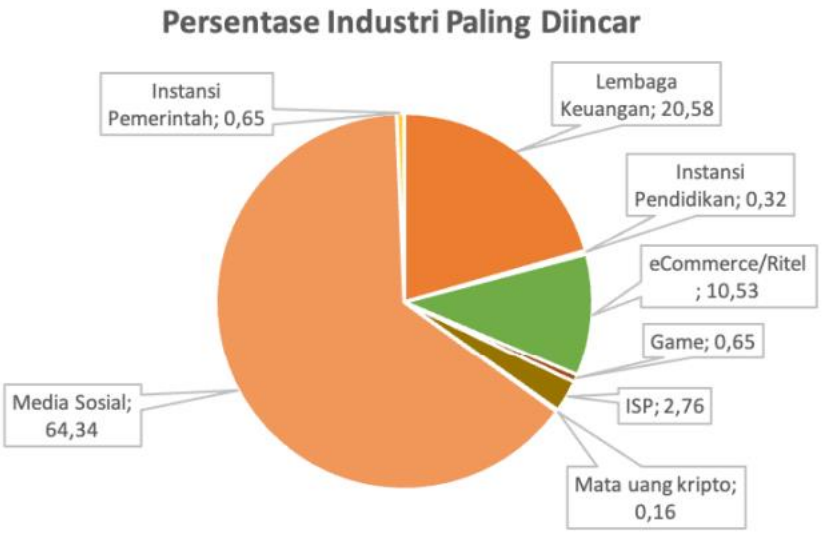
Penelitian yang dilakukan oleh Bakhshi (2017) melalui eksperimen serangan *social engineering* menunjukkan hasil yang cukup tinggi, yaitu antara 45-60 % partisipan gagal mengenali serangan dan menjadi korban. Hal ini menunjukkan tingginya tingkat keberhasilan serangan tersebut, yang disebabkan terutama oleh kurangnya kesadaran dan pemahaman masyarakat tentang bahaya dan taktik yang digunakan dalam serangan *social engineering*. Hal ini mendukung paragraf sebelumnya mengapa *trojan activity* menjadi kejahatan siber yang tinggi.

Gambar 1. 2 Laporan phising Q4 2023

Sumber : Indonesia-Anti Phising Data Exchange (IDADX) (2023)

Pada Gambar 1.2 dapat dilihat laporan *phising* pada akhir tahun 2023. *Phising* adalah adalah sebuah kejahatan dengan upaya mendapatkan informasi pribadi seseorang hingga kredensial akun keuangan. Pada saat ini, *phishing* biasanya dilakukan dengan skema *social engineering* dan *technical subterfuge*. Dalam kuartal keempat tahun 2023, IDADX menerima

sebanyak 3.605 laporan terkait *phishing*, dengan peningkatan yang signifikan dari bulan November ke bulan Desember.



Gambar 1. 3 Industri yang sering diincar

Sumber: Indonesia-Anti Phising Data Exchange (2024)

Pada Gambar 1.3 mengungkapkan sektor-sektor industri yang paling sering menjadi target serangan phishing pada kuartal keempat tahun ini. Sektor media sosial menempati posisi teratas dengan 64,34% dari total serangan phishing yang terjadi. Di posisi kedua, sektor lembaga keuangan menjadi target dengan persentase sebesar 20,58%. Selama beberapa kuartal terakhir, sektor media sosial terus berada di peringkat tertinggi sebagai target utama serangan phishing, melebihi sektor lembaga keuangan. Kondisi ini menjadi peringatan penting bagi masyarakat Indonesia untuk lebih berhati-hati dan waspada dalam menggunakan *platform* media sosial.

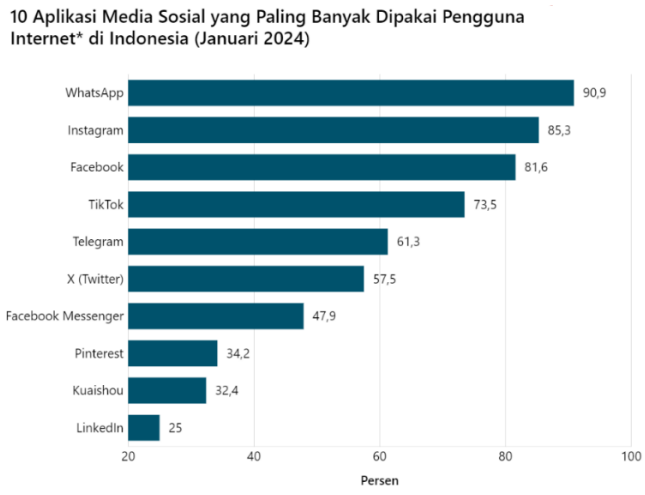
Gambar 1. 4 Contoh *social engineering* melalui media sosial

Sumber: Surat Imbauan BSSN (2023)

Banyaknya kasus kejahatan siber yang dipicu oleh teknik *social engineering* menimbulkan kekhawatiran yang semakin mendalam mengenai keamanan informasi pribadi dan kerahasiaan data. Gambar 1.4 merupakan salah satu contoh *social engineering* yang memanfaatkan media ssosial adalah penipuan melalui undangan palsu yang dikirimkan lewat WhatsApp. Undangan tersebut berisi Modus Berkas Aplikasi Berbasis Android. Aplikasi tersebut meminta izin untuk melakukan beberapa aktivitas di perangkat Android pengguna, termasuk membaca pesan SMS atau MMS yang tersimpan di perangkat atau kartu SIM.

Dengan mendapatkan izin, aplikasi dapat mengakses informasi rahasia yang mungkin terdapat dalam pesan tersebut. Selain itu, aplikasi juga dapat menerima dan memproses pesan SMS tanpa memberitahukan pengguna, serta mengirim pesan SMS yang dapat mengakibatkan biaya tanpa persetujuan langsung dari pengguna. Jika aplikasi terpasang pada perangkat korban, penipu memiliki potensi untuk mengakses data SMS yang mengandung informasi sensitif seperti kode PIN dari riwayat SMS-Banking. Banyak pengguna tidak menghapus riwayat transaksi SMS-Banking mereka, yang dapat dimanfaatkan oleh penyerang untuk meminta token SMS secara ilegal. Dengan akses ini, penyerang dapat mengeksploitasi dan melakukan transfer uang dari rekening korban tanpa izin.

Dalam situasi tersebut, media sosial menjadi salah satu alat yang berfungsi untuk mencari dan berbagi informasi terkait *social engineering* (Aldan Nur Zen & Sitanggang, 2023). Generasi sekarang yakni generasi remaja merupakan generasi *digital native*. Teknologi menjadi hal yang melekat pada kehidupan mereka. Tercatat pengguna internet di Indonesia menurut laporan We Are Social (Annur, 2024), pada Januari 2024 ada 185 juta individu pengguna internet di Indonesia, setara 66,5% dari total populasi nasional yang berjumlah 278,7 juta orang.



Gambar 1. 5 Media sosisal yang digunakan
Sumber: We Are Social (2024)

Pada Gambar 1.5 menurut laporan terbaru dari We Are Social (2024). WhatsApp mendominasi sebagai aplikasi media sosial yang paling banyak digunakan di Indonesia pada Januari 2024, dengan 90,9% dari seluruh pengguna internet berusia 16—64 tahun memanfaatkannya. Diikuti oleh Instagram dengan 85,3%, Facebook dengan 81,6%, dan TikTok dengan 73,5%. Pengguna Telegram mencapai 61,3%, sementara X (dahulu Twitter) mencatat 57,5%. Aplikasi lain seperti Facebook Messenger, Pinterest, Kuaishou (Kwai dan Snack Video), serta LinkedIn juga memiliki proporsi pengguna yang lebih kecil, sesuai dengan data yang terlihat dalam grafik. Secara total, We Are Social mencatat bahwa terdapat sekitar 139 juta identitas pengguna media sosial di Indonesia pada Januari 2024, yang mewakili 49,9% dari total populasi nasional.

Dengan memanfaatkan fenomena ini, memanfaatkan platform media sosial untuk membagikan dan mencari informasi mengenai *social engineering*. Dengan begitu, individu yang sedang mengalami kejahatan *social engineering* dapat menemukan jawaban dari beberapa pengalaman yang dibagikan di *platfrom* media sosial. Dalam penelitian ini, variabel-variabel yang digunakan dipilih berdasarkan relevansi dan dukungan empiris yang kuat dari berbagai studi sebelumnya yang berfokus pada perilaku berbagi informasi, keamanan informasi, dan social engineering. Variabel utama yang diteliti mencakup *Information Creation Ability* (ICA), Information Sharing Experience (ISE), *Information Sharing Self Efficacy* (ISSE), *Information Security Behaviour* (ISB), *Intention to Share* (ITSha), *Subjective Norm* (SN), *Attitude Towards Behaviour* (ATB), dan *Intention to Seek* (ITSee).

Information Creation Ability (ICA) diambil dari penelitian Tamrin et al. (2021), yang menunjukkan bahwa kemampuan individu untuk menghasilkan informasi yang relevan dan bermanfaat sangat penting dalam kegiatan berbagi informasi. Variabel ini digunakan karena informasi yang akurat dan bermanfaat dapat meningkatkan kualitas dan efektivitas berbagi informasi, terutama terkait *social engineering*. *Information Sharing Experience* (ISE) juga berasal dari penelitian Tamrin et al. (2021), yang menekankan pentingnya pengalaman berbagi informasi dalam mempengaruhi perilaku berbagi. Pengalaman ini dianggap penting karena membantu individu menjadi lebih percaya diri dan kompeten dalam berbagi informasi terkait *social engineering*. *Information Sharing Self Efficacy* (ISSE) didasarkan pada konsep dari penelitian Tamrin et al. (2021), yang menunjukkan bahwa keyakinan diri dalam berbagi informasi berperan penting dalam menentukan perilaku berbagi informasi. *Self Efficacy* mempengaruhi seberapa yakin individu terhadap kemampuan mereka dalam berbagi informasi yang akurat dan bermanfaat, yang pada gilirannya mendorong mereka untuk lebih aktif dalam berbagi informasi terkait ancaman *social engineering*. *Information Security Behaviour* (ISB)

diambil dari penelitian Tamrin et al. (2021), yang menunjukkan bahwa perilaku terkait keamanan informasi dapat dipengaruhi oleh *self-efficacy* dalam berbagi informasi dan niat untuk berbagi informasi. Memahami perilaku keamanan informasi penting untuk mengetahui bagaimana individu melindungi diri mereka dari ancaman *social engineering* dan menunjukkan sejauh mana mereka sadar akan pentingnya menjaga keamanan informasi pribadi. *Intention to Share* (ITSha) mengacu pada niat individu untuk berbagi informasi yang mereka miliki terkait social engineering. Variabel ini penting karena mencerminkan seberapa besar keinginan individu untuk membantu orang lain dengan membagikan pengetahuan mereka. Penggunaan variabel ini didukung oleh penelitian Tamrin et al. (2021).

Perceived Threat (PT) diambil dari penelitian Vrhovec et al. (2023), yang menunjukkan bahwa persepsi individu terhadap ancaman dapat mempengaruhi niat mereka untuk mencari dan berbagi informasi. Tingkat ancaman yang dirasakan oleh individu dapat mendorong mereka untuk lebih proaktif dalam mencari informasi terkait *social engineering*. *Attitude Towards Behaviour* (ATB) mencerminkan sikap individu terhadap perilaku tertentu, dalam hal ini pencarian dan berbagi informasi terkait social engineering. Sikap positif terhadap perilaku tersebut dapat meningkatkan niat dan tindakan nyata dalam mencari informasi. Penggunaan variabel ini didukung oleh penelitian Vrhovec et al. (2023) yang menunjukkan bahwa sikap individu dapat mempengaruhi niat dan perilaku mereka. *Subjective Norm* (SN) mengacu pada persepsi individu tentang pandangan dan harapan orang lain terhadap perilaku mereka Vrhovec et al. (2023). Variabel ini relevan dalam konteks penelitian ini karena pandangan dan dukungan dari lingkungan sosial dapat mempengaruhi niat dan tindakan individu dalam mencari informasi terkait *social engineering*. *Intention to Seek* (ITSee) didasarkan pada penelitian Vrhovec et al. (2023), yang menunjukkan bahwa niat untuk mencari informasi dapat dipengaruhi oleh pesan yang menekankan ancaman dan cara mengatasi social engineering. Niat untuk mencari informasi penting untuk memahami seberapa proaktif individu dalam mencari pengetahuan tentang ancaman *social engineering* dan cara menghadapinya, serta mencerminkan kesadaran mereka terhadap pentingnya informasi tersebut dalam menjaga keamanan pribadi.

Dengan memanfaatkan fenomena ini, memanfaatkan platform media sosial untuk membagikan dan mencari informasi mengenai *social engineering*. Dengan begitu, individu yang sedang mengalami kejahatan *social engineering* dapat menemukan jawaban dari beberapa pengalaman yang dibagikan di *platfrom* media sosial. Berdasarkan penelitian (Tamrin et al., 2021) dilakukan untuk mencari faktor yang berpengaruh dalam kegiatan berbagi suatu informasi. Hasil menunjukan bahwa *information creation ability* dan *information sharing*

experience merupakan faktor dari *information sharing-self efficacy*. Sementara itu, *information sharing-self efficacy* dimediasi oleh *information security behaviour* yang berpengaruh pada kegiatan berbagi suatu informasi. Penlitian ini juga didukung oleh penelitian Vrhovec et al. (2023) yang hasilnya menyampaian pesan yang menekankan pada ancaman yang dirasakan dapat secara langsung meningkatkan niat mencari informasi.

Dalam konteks penelitian yang dilakukan, konsep ini relevan karena memahami faktor-faktor yang mempengaruhi perilaku pencarian dan berbagi informasi terkait keamanan informasi khususnya *social engineering* menjadi sangat penting. Kesadaran akan ancaman dan tindakan preventif terhadap serangan siber sangat bergantung pada bagaimana informasi tersebut dicari, diakses, dan disebarluaskan di masyarakat.

Latar belakang yang telah dijelaskan diatas memberikan ketertarikan kepada penulis untuk melakukan penelitian yang berjudul **ANALISIS FAKTOR-FAKTOR YANG BERPENGARUH DALAM PENCARIAN DAN BERBAGI INFORMASI *SOCIAL ENGINEERING* PADA MEDIA SOSIAL.**

1.3 Rumusan Masalah

Adapun rumusan masalah dari penelitian sebagai berikut:

1. Bagaimana *Information Creation Ability* (ICA) mempengaruhi *Information Sharing Self Efficacy* (ISSE) ?
2. Bagaimana *Information Sharing Experience* (ISE) mempengaruhi *Information Sharing Self Efficacy* (ISSE) ?
3. Bagaimana *Information Sharing Self Efficacy* (ISSE) mempengaruhi *Information Security Behaviour* (ISB) ?
4. Bagaimana *Information Security Behaviour* (ISB) mempengaruhi *Intention To Share* (ITSha) ?
5. Bagaimana *Perceived Threat* (PT) mempengaruhi *Intention To Seek* (ITSee) ?
6. Bagaimana *Attitude Towards Behaviour (ATB)* mempengaruhi *Intention To Seek* (ITSee) ?
7. Bagaimana *Subjective Norm* (SN) mempengaruhi *Intention To Seek* (ITSee) ?
8. Bagaimana *Intention To Seek* (ITSee) mempengaruhi *Intention To Share* (ITSha) ?

1.4 Tujuan Penelitian

Tujuan kegiatan ini adalah:

1. Untuk mengetahui bagaimana pengaruh *Information Creation Ability* (ICA) dengan *Information Sharing Self Efficacy* (ISSE).
2. Untuk mengetahui bagaimana pengaruh *Information Sharing Experience* (ISE) dengan *Information Sharing Self Efficacy* (ISSE).
3. Untuk mengetahui bagaimana pengaruh *Information Sharing Self Efficacy* (ISSE) dengan *Information Security Behaviour* (ISB).
4. Untuk mengetahui bagaimana pengaruh *Information Security Behaviour* (ISB) dengan *Intention To Share* (ITSha).
5. Untuk mengetahui bagaimana pengaruh *Perceived Threat* (PT) dengan *Intention To Seek* (ITSee).
6. Untuk mengetahui bagaimana pengaruh *Attitude Towards Behaviour (ATB)* dengan *Intention To Seek* (ITSee).
7. Untuk mengetahui bagaimana pengaruh *Subjective Norm* (SN) dengan *Intention To Seek* (ITSee).
8. Untuk mengetahui bagaimana penggaruh *Intention To Seek* (ITSee) dengan *Intention To Share* (ITSha).

1.5 Manfaat Penelitian

1.5.1 Manfaat Teoritis

Secara teoritis hasil Penelitian ini diharapkan dapat bermanfaat sebagai referensi pada Penelitian-Penelitian selanjutnya dan mengetahui faktor apa yang paling berpengaruh terhadap perilaku information seeking dan information sharing. Khususnya dalam konteks ancaman *social engineering*.

1.5.2 Manfaat Praktis

Secara praktis hasil Penelitian ini bermanfaat bagi pengguna media sosial karena dengan memahami faktor-faktor yang paling berpengaruh pada *seeking and sharing* informasi dalam *social engineering*, pengguna dapat lebih waspada dan mengembangkan langkah-langkah pencegahan yang lebih efektif untuk melindungi diri dari potensi ancaman.

1.6 Sistematika Penulisan

Berisi tentang sistematika dan penjelasan ringkas laporan Penelitian yang terdiri dari Bab I sampai Bab V dalam laporan Penelitian.

a. BAB I PENDAHULUAN

Dalam bab ini membahas mengenai gambaran umum objek Penelitian, latar belakang Penelitian yang berkaitan dengan fenomena yang terjadi, rumusan masalah, tujuan Penelitian, manfaat Penelitian dari aspek teoritis dan aspek praktis yang diambil dari Penelitian, dan sistematika Penelitian tugas akhir.

b. BAB II TINJAUAN PUSTAKA

Dalam bab ini berisi teori dari umum sampai ke khusus, disertai Penelitian terdahulu dan dilanjutkan dengan kerangka pemikiran Penelitian yang diakhiri dengan hipotesis jika diperlukan.

c. BAB III METODE PENELITIAN

Dalam bab ini menegaskan pendekatan, metode dan teknik yang digunakan untuk mengumpulkan serta menganalisis temuan yang dapat menjawab masalah Penelitian. Bab ini meliputi uraian tentang: Jenis Penelitian, Operasionalisasi Variabel, Populasi dan Sampel (untuk kuantitatif) / Situasi Sosial (untuk kualitatif), Pengumpulan Data, Uji Validitas dan Reliabilitas, serta Teknik Analisis Data.

d. BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Dalam bab ini hasil Penelitian dan pembahasan diuraikan secara sistematis sesuai dengan perumusan masalah serta tujuan Penelitian disajikan dalam sub judul tersendiri. Bab ini berisi dua bagian: bagian pertama menyajikan hasil Penelitian dan bagian kedua menyajikan pembahasan atau analisis dari hasil Penelitian. Setiap aspek pembahasan hendaknya dimulai dari hasil analisis data, kemudian diinterpretasikan dan selanjutnya diikuti oleh penarikan kesimpulan.

e. BAB V KESIMPULAN DAN SARAN

Dalam bab ini berisi kesimpulan merupakan jawaban dari pernyataan Penelitian, kemudian menjadi saran yang berkaitan dengan manfaat Penelitian.