BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Berdasarkan hasil survei APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) bahwa jumlah pengguna internet Indonesia mencapai 222 juta jiwa. Dari hasil survei penetrasi internet Indonesia 2024 yang dirilis APJII, maka tingkat penetrasi internet Indonesia menyentuh angka 79,5%. Dibandingkan dengan periode sebelumnya, maka ada peningkatan 1,4% dari sebelumnya.

Hasil survei tersebut mengonfirmasi bahwa kecepatan pertumbuhan pengguna internet di Indonesia sangat tinggi seiring dengan kualitas infrastruktur telekomunikasi perlahan mulai meningkat. Dampak positif dari fenomena ini adalah tingginya pemanfaatan teknologi berbasis digital di setiap aspek kehidupan sehari-hari. Namun, pada tahapan perkembangannya modus operasi kejahatan juga bergerak maju seiring perkembangan peradaban manusia. Sejalan dengan meningkatnya jumlah masyarakat dan penciptaan teknologi, manusia semakin tinggi memanfaatkan fasilitas teknologi digital untuk berinteraksi satu sama lain.

Hampir semua aktivitas perekonomian di dunia memanfaatkan media internet dengan menggunakan sarana sistem elektronik. Salah satu segi aktivitas ekonomi yaitu transaksi dengan memanfaatkan dunia internet yang populer dikenal dengan perdagangan melalui media internet (*e-commerce*). Kemajuan dunia internet melahirkan suatu dunia modern yang dikenal dengan dunia maya, di mana individu satu dengan individu lain bisa berinteraksi tanpa batas wilayah dan dilakukan tanpa bertemu muka secara langsung, melainkan melalui transaksi elektronik. Perkembangan teknologi informasi saat ini telah menciptakan jenis-

jenis dan peluang-peluang bisnis baru di mana transaksi-transaksi bisnis makin banyak dilakukan secara elektronik.

Perkembangan teknologi dapat menimbulkan dampak positif dan dampak negatif. Salah satu dampak negatif yang ditimbulkan karena perkembangan teknologi yaitu munculnya ancaman kejahatan-kejahatan modern. Ancaman kejahatan modern meliputi berbagai bentuk kejahatan siber seperti *phishing*, *malware*, dan *ransomware*, yang dapat merusak data pribadi dan sistem informasi. Selain itu, kejahatan ini sering kali memanfaatkan kemajuan teknologi untuk melakukan penipuan dan pencurian data secara lebih efektif. Adapun beberapa jenis-jenis ancaman kejahatan menurut artikel buletin IBM (https://www.ibm.com/id-id/think/topics/cyberthreats-types) di era modern :

a. *Cyber Crime* merupakan kejahatan siber mencakup berbagai aktivitas kriminal yang dilakukan melalui internet, seperti pencurian data, penipuan online, dan serangan siber. Pelaku kejahatan ini sering kali menggunakan teknik canggih untuk mengeksploitasi kelemahan sistem keamanan.
b. *Malicious Software (Malware)* adalah perangkat lunak berbahaya yang dirancang untuk merusak atau mengakses sistem komputer tanpa izin. Jenis *malware* termasuk virus, trojan, *ransomware*, dan *spyware*, yang dapat menyebabkan kerugian finansial dan pencurian data.
c. *Social Engineering* merupakan taktik melibatkan manipulasi psikologis untuk mendapatkan informasi sensitif dari individu. Contohnya termasuk penipuan telepon di mana penjahat berpura-pura menjadi pihak yang berwenang untuk meminta informasi pribadi.

d. Penjahat siber merupakan individu atau kelompok ini melakukan kejahatan siber, sebagian besar untuk mendapatkan keuntungan finansial. Kejahatan umum yang dilakukan oleh penjahat siber termasuk serangan *ransomware*, dan penipuan *phishing* yang mengelabui orang untuk melakukan transfer uang atau membocorkan informasi kartu kredit, kredensial login, kekayaan intelektual, atau informasi pribadi atau rahasia lainnya.

Kejahatan terus berkembang seiring dengan perkembangan peradaban manusia, dengan kualitas dan kuantitasnya yang kompleks dengan variasi modus operandinya dan penipuan *online* merupakan salah satu bentuk kejahatan yang semakin marak seiring dengan perkembangan teknologi informasi dan komunikasi (Suardi, 2022). Dalam konteks hukum pidana, penipuan *online* termasuk dalam tindak pidana yang diatur oleh Kitab Undang-Undang Hukum Pidana (KUHP) di Indonesia. Pasal 378 KUHP mendefinisikan penipuan sebagai tindakan menggunakan nama palsu, keadaan palsu, tipu muslihat, atau rangkaian kebohongan untuk menggerakkan orang lain menyerahkan barang, membuat utang, atau menghapuskan piutang. Dalam kasus penipuan *online*, modus operandi sering kali melibatkan penggunaan internet untuk menyebarkan informasi palsu atau untuk melakukan transaksi yang tidak sah (Bernoza, 2020).

Penipuan online adalah sebuah tindakan yang dilakukan oleh beberapa orang yang tidak bertanggung jawab untuk memberikan informasi palsu demi keuntungan pribadi (Risma Novia, 2023). Perbedaan antara penipuan *online* dengan konvensional yaitu penggunaan sistem elektronik (perangkat telekomunikasi, internet, dan komputer). Secara hukum, baik penipuan secara

online maupun konvensional dapat diperlakukan sama sebagai delik konvensional yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP) (Noor Rahmad, 2019). Di Indonesia, dampak dari kejahatan penipuan *online* telah mengakibatkan kerugian material di berbagai wilayah.

Penipuan *online* memiliki berbagai bentuk, termasuk *phishing*, *scam*, dan penipuan berkedok jual beli online (Sipahutar, 2021). *Phishing* adalah upaya mendapatkan informasi sensitif seperti kata sandi dan nomor kartu kredit dengan menyamar sebagai entitas tepercaya dalam komunikasi elektronik (Hasibuan & Sitompul, 2022). Scam biasanya melibatkan penawaran investasi palsu atau hadiah undian yang tidak pernah ada (Lestari, 2023). Penipuan jual beli *online* sering terjadi di platform *e-commerce*, di mana pelaku menawarkan barang dengan harga menarik namun tidak pernah mengirimkan barang tersebut setelah menerima pembayaran. Kejahatan ini sering kali menargetkan individu yang kurang waspada atau tidak memiliki pengetahuan yang cukup tentang keamanan digital (Wibisono & Mahanani, 2023). Sejumlah teknik umum yang digunakan penipu dalam transaksi *online* dirinci Kementerian Komunikasi dan Informatika (2021):

a. *Phishing.* Secara teknis, *phishing* adalah praktik penjahat dunia maya yang menyamar sebagai situs web terkemuka untuk mengelabui pengguna agar membocorkan informasi penting (Ghazi-Tehrani & Pontell, 2021). Pelaku akan menyamar sebagai perwakilan resmi dari organisasi yang sah untuk melakukan penipuan jual beli *online*. Panggilan telepon, email, dan pesan media sosial adalah cara utama penjahat mencoba menghubungi korbannya. Korban *phishing* rentan informasi sensitifnya dicuri dan

dimanfaatkan oleh penipu. Setelah mendapatkan informasi korban, pelaku akan memanfaatkannya untuk melakukan jual beli *online*.

b. *Pharming.* Salah satu metode melakukan penipuan, yang dikenal sebagai *pharming,* melibatkan pemalsuan nama domain situs web untuk mengelabui pengguna agar mengunjungi situs web jahat yang mencuri informasi sensitif (Prasad & Rohokale, 2020). Dalam kasus ini, penjahat akan membuat nama domain untuk situs web korban yang sangat mirip dengan domain asli organisasi yang sah. Menginfeksi situs web palsu ini dengan malware memungkinkan penipu mencuri informasi pribadi sensitif dari pengguna yang tidak menaruh curiga. Penjahat akan menggunakan informasi yang dicuri untuk melakukan transaksi *online* palsu, sehingga menyebabkan kerugian pada korban.

c. *Sniffing.* Sebuah metode serba guna untuk melanggar keamanan jaringan, sniffing melibatkan pengumpulan data sensitif dari jenis lalu lintas jaringan tertentu (Alemayehu, 2021). *Sniffing,* dalam definisi paling mendasarnya, adalah serangan terhadap data sensitif, seperti penemuan kata sandi atau informasi identitas pribadi lainnya. Korban mungkin mengalami perilaku ini jika mereka menggunakan WiFi publik atau koneksi internet publik lainnya. Penggunaan koneksi internet publik, khususnya untuk transaksi keuangan, membuat korban rentan terhadap serangan *sniffing*. Untuk melakukan pembelian dan penjualan *online* menggunakan data yang dicuri, penjahat akan memanfaatkan informasi pribadi korban.

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam cara masyarakat berinteraksi dan berkomunikasi. Namun, di balik kemudahan dan manfaat yang ditawarkan, muncul berbagai ancaman dan risiko baru akibat lengahnya literasi masyarakat mengenai dampak negatif yang dapat dimanfaatkan oleh pihak-pihak tidak bertanggung jawab dan salah satunya adalah penipuan *online*. Berikut adalah gambar mengenai kejahatan siber atau penipuan *online* di Indonesia dari tahun 2022 hingga 2024 :

Gambar 1.1 Statistik Kejahatan Siber atau Penipuan Online

Dari gambar statistik tersebut menjelaskan bahwa Polri telah menangani 1.062 tindak pidana kejahatan yang berkaitan dengan siber, internet, media *online*, media elektronik, dan media sosial. Polda Metro Jaya melakukan penindakan paling banyak yaitu 582 perkara. Data itu didapat dari aplikasi EMP Pusiknas Bareskrim Polri, dan berdasarkan data tersebut jumlah penindakan terhadap

kejahatan siber atau penipuan *online* mengalami peningkatan. Pada 2022, jumlah kejahatan siber atau penipuan *online* sebanyak 8.636 perkara dan angka tersebut terus meningkat hingga 2024 yang mencapai 13.913 perkara. Dalam tiga tahun berturut-turut, jumlah penindakan terhadap kejahatan siber atau penipuan *online* paling banyak ditangani oleh Polda Metro Jaya.

Sejak 2022 sampai 2025, Polri menangani 32.073 terlapor tindak pidana kejahatan siber atau penipuan online. Sementara jumlah korban mencapai 29.067 orang dan fenomena ini menunjukkan bahwa seiring dengan pesatnya pertumbuhan penggunaan internet, tingkat kerentanan masyarakat terhadap kejahatan digital juga semakin meningkat. Hal senada juga terjadi di kota Tanjung Balai, kota Tanjung Balai juga banyak terjadi kasus kasus penipuan secara *online*, jumlah kasus penipuan *online* yang terjadi di kota Tanjung Balai dapat di lihat dari jumlah terlapor dan di tangani bisa di lihat pada tabel berikut :

Tabel 1.1 Laporan Kasus Penipuan Online Di Kota Tanjung Balai

Tahun	Jumlah Terlapor	Jumlah Kasus Ditangani
2023	11	3
2024	20	8

Modus penipuan online kembali marak di Kota Tanjung Balai dan Polres Tanjung Balai mencatat pada tahun 2023 terdapat 11 terlapor dan 3 telah ditangani serta 8 kasus penipuan dari 20 pelapor modus penipuan online telah ditangani selama tahun 2024. Modus yang umum digunakan adalah pelaku menghubungi korban melalui pesan *WhatsApp* atau telepon, mengaku sebagai tokoh publik atau perwakilan instansi, dan menawarkan iming-iming hadiah atau

keuntungan finansial. Ujungnya, pelaku telah meminta transfer uang dari korban yang di mana nominalnya cukup besar bagi korban dan korban dengan tanpa sadar transfer uang ke pelaku modus penipuan *online*.

Kelurahan Bunga Tanjung sebagai bagian dari Kota Tanjung Balai tidak luput dari dampak negatif dan terkena imbas dari perkembangan teknologi ini. Dalam beberapa tahun terakhir terjadi peningkatan kasus penipuan online dengan mayoritas korban adalah ibu rumah tangga berusia di atas 50 tahun. Dari data kelurahan dan kepala lingkungan sepanjang tahun 2024, bahwa Kelurahan Bunga Tanjung tercatat memiliki 15 orang korban penipuan *online*, yang di mana dari jumlah tersebut 9 orang yang menjadi korban modus penipuan yang di gunakan pelaku melalui telepon menghubungi korban dan mengatakan bahwa anak korban atau kerabat korban saat ini dalam keadaan koma karena kecelakaan dan penipu telah meminta uang ratusan ribu rupiah hingga jutaan rupiah kepada korban dengan berdalih bahwa uang tersebut untuk biaya rumah sakit, dan pengurusan kepada pihak berwajib.

Selain itu, 6 orang yang menjadi korban modus penipuan *online* lainnya adalah dengan jual beli barang murah serta promo umroh, yang di mana karena promo ini akhirnya korban tergiur dengan promo yang dilakukan oleh pelaku modus kejahatan penipuan *online* dan korban mengalami kerugian ratusan ribu bahkan ada sampai dengan jutaan rupiah. Sayangnya, kebanyakan para korban memilih tidak melaporkan kasus penipuan *online* ini kepada pihak berwajib karena mereka telah berasumsi bahwa pelaku tidak akan dapat ditemukan dan ditindak secara hukum. Dampak dari modus penipuan terhadap korban adalah korban mengalami kerugian finansial yang di mana kerugian bukan di alami oleh

individu itu sendiri melainkan berdampak pada ekonomi di keluarga terebut yang menjadi korban oleh modus penipuan *online*.

Penipuan yang telah terjadi di kelurahan Bunga Tanjung, Kota Tanjung Balai para korbannya mengalami jenis penipuan *cyber crime* dan *phishing*. Yang di mana para korbannya adalah kebanyakan ibu rumah tangga yang berusia 50 tahun ke atas. Mereka ditipu melalui pesan dan panggilan serta jual beri barang yang dilakukan oleh pelaku. Kurangnya pemahaman tentang keamanan digital membuat para korban mudah terperdaya, hal ini mengindikasikan adanya kesenjangan digital yang signifikan di kalangan ibu rumah tangga, terutama pada kelompok usia tertentu. Dan adapun beberapa faktor kerentanan ibu rumah tangga berusia di atas 50 tahun terhadap penipuan *online* antara lain:

a. Kesenjangan Digital: Kelompok ini umumnya baru mengenal dan mengadopsi teknologi digital dalam beberapa tahun terakhir. Mereka mulai menggunakan *smartphone* dan sosial media, namun tidak dibekali dengan pengetahuan yang memadai tentang resiko keamanan *online*. Akibatnya, mereka seringkali tidak menyadari pentingnya verifikasi dan kehati-hatian dalam bertransaksi *online*.
b. Keterbatasan Akses Informasi: Ibu rumah tangga berusia di atas 45 tahun seringkali memiliki akses terbatas pada informasi terkini tentang modus-modus penipuan *online*. Mereka mungkin tidak secara aktif mengikuti perkembangan berita atau peringatan keamanan siber yang disebarluaskan melalui media digital. Keterbatasan ini membuat mereka kurang mampu mengantisipasi dan mengenali upaya penipuan.

c. Kurangnya Pendampingan: Minimnya program pendampingan dan edukasi digital yang spesifik ditujukan untuk kelompok ini membuat mereka harus belajar secara mandiri dalam menggunakan teknologi digital, seringkali melalui metode coba-coba yang berisiko.

Adapun beberapa cara dalam mencegah terjadinya penipuan *online* menurut artikel https://rgrfm.tulungagung.go.id/tips-menghindari-penipuan-online/ :

a. Kenali Jenis Penipuan *Online* : Penipuan online dapat berupa berbagai bentuk, seperti *phishing* modus penipu berupa mengirim email atau pesan palsu yang terlihat seperti dari sumber yang sah untuk mencuri informasi pribadi. Dan scam jual beli, modus penipu menjual barang yang tidak ada atau tidak sesuai dengan deskripsi untuk mengambil uang korbannya.
b. Jaga Informasi Pribadi Anda : Jangan pernah membagikan informasi pribadi seperti nomor KTP, nomor kartu kredit, kata sandi, atau informasi sensitif lainnya melalui email atau pesan yang tidak terpercaya. Selalu verifikasi sumber informasi sebelum memberikan data pribadi.
c. Email dan Pesan Palsu : Selalu waspada terhadap email dan pesan yang meminta informasi pribadi atau mengarahkan ke situs web yang mencurigakan. Penipu sering menggunakan taktik urgensi atau ancaman untuk membuat korbannya panik dan bertindak terburu-buru. Periksa alamat email pengirim dan pastikan itu berasal dari sumber yang sah.
d. Waspadai Tawaran yang Terlalu Menggiurkan : Penawaran yang menjanjikan keuntungan besar dengan risiko minimal seringkali merupakan modus penipuan dan lakukan riset dan periksa reputasi penjual sebelum melakukan transaksi.

e. Laporkan Penipuan : Jika menjadi korban penipuan *online*, segera laporkan ke pihak berwajib dan platform tempat terjadinya penipuan serta laporkan nomor telepon, email, atau akun media sosial yang digunakan untuk melakukan penipuan.

Berdasarkan dari fenomena dan hasil observasi awal di Kelurahan Bunga Tanjung, maka peneliti mengangkat judul penelitian "Pengaruh Peningkatan Kemampuan Literasi Digtal Ibu Rumah Tangga Terhadap Pencegahan Penipuan *Online* Di Kelurahan Bunga Tanjung Kota Tanjung Balai".

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah di jelaskan, identifikasi masalah pengaruh peningkatan kemampuan literasi digital ibu rumah tangga terhadap pencegahan penipuan *online* di Kelurahan Bunga Tanjung, Kota Tanjung Balai :

a. Kesenjangan digital terhadap ibu rumah tangga di atas 50 tahun dan baru mengerti teknologi digital dan keterampilan berinteraksi dengan perangkat digital.
b. Kekurangan pengetahuan keamanan digital pada ibu rumah tangga di atas 50 tahun dan tidak memiliki pengetahuan mengenai penipuan *online* dan cara-cara penipuan *online*.
c. Keterbatasan akses informasi terhadap ibu rumah tangga tentang informasi modus penipuan *online*.

1.3 Batasan Masalah

Peneliti membatasi masalah dengan menggunakan literasi digital untuk pelatihan peningkatan kemampuan literasi digital dalam pencegahan penipuan

online pada ibu rumah tangga berusia di atas 50 tahun.

1.4 Rumusan Masalah

1. Bagaimana kemampuan literasi digital ibu rumah tangga berusia di atas 50 tahun di Kelurahan Bunga Tanjung, Kota Tanjung Balai dalam menghadapi resiko penipuan *online*?
2. Seperti apa bentuk pencegahan penipuan online pada ibu rumah tangga berusia di atas 50 tahun di Kelurahan Bunga Tanjung?
3. Apakah terdapat pengaruh pelatihan peningkatan kemampuan literasi digital pada ibu rumah tangga berusia di atas 50 tahun dalam hal pencegahan penipuan *online* di Kelurahan Bunga Tanjung?

1.5 Tujuan Penelitian

Dari rumusan masalah diatas maka tujuan yang diharapkan dari penelitian ini adalah sebagai berikut :

1. Untuk mengetahui kemampuan literasi digital pada ibu rumah tangga berusia di atas 50 tahun di Kelurahan Bunga Tanjung, Kota Tanjung Balai dalam menghadapi risiko penipuan *online*.
2. Untuk mengetahui bentuk pencegahan penipuan online pada ibu rumah tangga berusia di atas 50 tahun di Kelurahan Bunga Tanjung?
3. Untuk mengetahui pengaruh pelatihan peningkatan kemampuan literasi digital pada ibu rumah tangga berusia di atas 50 tahun dalam hal pencegahan penipuan *online* di Kelurahan Bunga Tanjung.

1.6 Manfaat Penelitian

Peneliti berharap hasil penelitian ini dapat memberikan manfaat terhadap mayarakat di Kelurahan Bunga Tanjung Kota Tanjung Balai, maka manfaat penelitian ini sebagai berikut :

1.6.1 Manfaat Teoritis

Penelitian ini berharap dapat memberikan kontribusi dalam pnegembangan peningkatan literasi digital, khususnya bagi kelompok ibu rumah tangga berusia di atas 50 tahun dalam pencegahan kejahatan penipuan *online*.

1.6.2 Manfaat Praktis

Memberikan pemahaman tentang risiko penipuan *online* dan cara mengidentifikasinya serta menghindari penipuan online.