BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi dapat mengubah ekonomi, budaya, politik, dan hukum. Selain menghasilkan manfaat bagi banyak orang, perkembangan teknologi informasi juga memicu kejahatan baru yaitu sebagai serangan *cyber* dari Internet (Kharisma Putra et al., 2023). Jumlah pengguna internet yang meningkat juga menimbulkan ancaman terhadap privasi yang dapat mengancam data pribadi (Aklani et al., 2024). Pesatnya perkembangan teknologi saat ini sangat membantu orang dalam berkomunikasi dan mengakses berbagai aplikasi *online*, seperti fintech, *game online*, belanja, kartu kredit, aplikasi perbankan, streaming video, musik, dan lainnya (Hayati et al., 2021). *Cybercrime* merupakan fenomena yang sangat mengkhawatirkan, mengingat tindakan *carding*, *hacking*, penipuan, terorisme, dan penyebaran informasi yang mengganggu menjadi bagian dari aktivitas pelaku *cybercrime* (Guloet al.,, 2021).

Perkembangan teknologi tidak hanya mengubah cara kita berkomunikasi, bekerja, dan mengakses informasi, tetapi juga bagaimana kita bermain *game*. Game *online*, terutama yang berbasis *online*, telah menjadi bagian penting dari kehidupan sehari-hari banyak orang. Game *online* sebagai permainan yang menggunakan teknologi internet, yang memberikan dampak positif seperti meningkatkan relasi sosial, namun juga memiliki dampak negatif jika tidak dikontrol (A Andoyo, 2021). Popularitas *game online* ini diikuti oleh munculnya berbagai ancaman, salah satunya adalah serangan *social engineering*.

Social engineering dipahami sebagai strategi yang memanfaatkan kelemahan manusia dalam proses manipulasi untuk mendapatkan informasi sensitif atau mengakses data penting, terutama di era digital (DR Triwahono et al. 2023). Dalam konteks *game online*, pelaku kejahatan menggunakan teknik *social engineering* untuk mengeksploitasi pemain, mengakses akun mereka, atau mencuri data sensitif seperti informasi *login* atau pembayaran. Serangan *social engineering* sering memanfaatkan perangkat pribadi pengguna, seperti ponsel atau tablet, untuk mengeksploitasi kerentanan manusia dalam memberikan informasi pribadi (Aldawood et al., 2019).

Serangan *social engineering* memanfaatkan kesalahan manusia untuk melewati langkah-langkah keamanan teknis, dan terbukti sangat efektif di platform dengan interaksi pengguna tinggi, seperti *game online* (A Kučs et al.,2022).

Temuan ENISA menunjukkan bahwa 84% serangan siber berbasis pada beberapa bentuk *social engineering*, menyoroti peran kesalahan manusia dalam kegagalan keamanan platform, termasuk layanan permainan daring (I Stamelos et al.,2024).

Komunikasi di dalam komunitas virtual *game online* sering kali menjadi jalan masuk bagi pelaku serangan *social engineering* untuk memanipulasi korban mereka (Zakaria et al., 2022). Framework yang dirancang untuk memahami pola serangan *social engineering* dapat membantu mengidentifikasi metode yang paling sering digunakan oleh penyerang (Abu Hweidi et al.,2023).

Metode serangan yang paling sering dipakai untuk ini adalah *pretexting*, *impersonation*, dan *phishing*. Taktik rekayasa sosial, seperti *phishing* dan *pretexting*, semakin sering digunakan dalam platform *game online* untuk memanfaatkan kepercayaan pengguna dan mengambil informasi sensitif (Nyusti et al., 2024). Selain itu, popularitas multi*player online game*s membuat mereka menjadi target utama serangan cyber, terutama metode *social engineering* yang menipu pemain untuk mengungkapkan kredensial akun (Mahmor et al., 2024). Serangan ini semakin berbahaya selama pandemi COVID-19, ketika waktu bermain

game online meningkat secara signifikan (King et al., 2020).

Cybercriminals juga sering menggunakan teknik seperti *impersonation* dan hadiah palsu untuk memancing pemain ke dalam penipuan (Galekwa et al., 2024). Deepfake kini mulai digunakan di lingkungan *game* virtual untuk menciptakan ilusi identitas palsu, membuka peluang baru bagi serangan *social engineering* (Tariq et al., 2023). Dalam *game online*, pelaku serangan sering kali menciptakan skenario atau persona palsu untuk memanipulasi pemain agar memberikan informasi sensitif (Ariya et al., 2024).

Selain itu, pelatihan berbasis *game* telah terbukti efektif meningkatkan respons manusia terhadap ancaman keamanan siber, termasuk serangan *social engineering* (Muhly et al., 2023). Pendekatan berbasis kesadaran seperti model PROTECT (Prepare,Recognize, Observe, Think, Engage, Communicate) memungkinkan pemain untuk lebih tanggap terhadap ancaman, sementara mitigasi berbasis riset menjadi penting dalam mengurangi dampak serangan ini (Goeke et al., 2019; Ligsay, 2020).

Fenomena ini menarik untuk diteliti, mengingat banyaknya kasus yang melibatkan *social engineering* di *game online*. Permainan *online* menjadi target karena sifatnya yang interaktif dan melibatkan banyak pemain yang mungkin tidak sepenuhnya memahami risiko keamanan. Selain itu, di dalam *game* mobile, metode serangan ini sering kali lebih efektif karena interaksi pengguna yang cepat dan tidak jarang kurang hati-hati. Kesadaran pengguna terhadap serangan *social engineering* masih rendah, sehingga diperlukan pendekatan pendidikan yang komprehensif (Syafitri et al., 2022).

Berdasarkan fenomena ini, penelitian ini akan mencoba menganalisis metode-metode serangan *social engineering* yang umum terjadi di *game online*, khususnya *game* mobile. Penelitian ini juga akan mengidentifikasi faktor-faktor yang mempengaruhi keberhasilan serangan tersebut serta memberikan rekomendasi untuk meningkatkan kesadaran dan perlindungan pengguna terhadap ancaman *social engineering*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, dapat mengembangkan rumusan masalah sebagai berikut:

1. Bagaimana metode serangan *social engineering*, seperti *pretexting*, *impersonation*, dan *phishing* terjadi dalam lingkungan *game online*, khususnya di PUBG Mobile dan Mobile Legends ?
2. Faktor-faktor apa yang mempengaruhi keberhasilan serangan *social engineering* dalam permainan *online* PUBG Mobile dan Mobile Legends?
3. Bagaimana metode *social engineering* seperti *pretexting*, *impersonation*, dan *phishing* diterapkan di dalam *game* mobile PUBG Mobile dan Mobile Legends ?
4. Bagaimana meningkatkan kesadaran dan perlindungan pengguna terhadap *social engineering*, khususnya *pretexting*, *impersonation*, dan *phishing*, dalam lingkungan *game* mobile PUBG Mobile dan Mobile Legends ?

1.3 Batasan Masalah

Agar penelitian ini lebih fokus, ada beberapa batasan masalah yang diterapkan, yaitu:

1. Penelitian ini akan mengkaji metode serangan *social engineering* yang terjadi dalam lingkungan *game online* dan mobile, dengan fokus pada PUBG Mobile dan Mobile Legends.
2. Metode *social engineering* yang akan dibahas meliputi *pretexting*, *impersonation*, dan *phishing*, yang melibatkan manipulasi psikologis terhadap *player*, tanpa membahas aspek keamanan jaringan secara mendetail.
3. Fokus penelitian adalah pada *game* PUBG Mobile dan Mobile Legends, sehingga *game* offline atau platform selain *game* mobile tidak akan dibahas.

Batasan-batasan ini diambil agar penelitian dapat berjalan secara sistematis dan mencapai hasil yang lebih spesifik.

1.4 Tujuan dan Manfaat Penelitian

Tujuan dari penelitian ini adalah untuk memberikan pemahaman yang mendalam tentang ancaman serangan *social engineering* dalam lingkungan *game* mobile *online*. Penelitian ini berfokus pada analisis metode serangan seperti *pretexting*, *impersonation*, dan *phishing*, serta faktor-faktor yang memengaruhi keberhasilannya dengan sasaran sebagai berikut :

1. Menganalisis berbagai metode serangan *social engineering*, seperti *pretexting*, *impersonation*, dan *phishing*, yang sering terjadi dalam *game online* PUBG Mobile dan Mobile Legends.
2. Mengidentifikasi faktor-faktor yang mempengaruhi keberhasilan serangan *social engineering* dalam permainan *online*, khususnya di PUBG Mobile dan Mobile Legends.
3. Menguji metode-metode serangan *social engineering* seperti *pretexting*, *impersonation*, dan *phishing* yang diterapkan di *game* mobile PUBG Mobile dan Mobile Legends.
4. Menyusun rekomendasi untuk meningkatkan kesadaran dan perlindungan pengguna terhadap serangan *social engineering*, khususnya *pretexting*, *impersonation*, dan *phishing*, dalam *game* mobile PUBG Mobile dan Mobile Legends.

Manfaat Penelitian:

1. Akademis:

Memberikan kontribusi ilmiah dalam literatur keamanan siber, khususnya yang berhubungan dengan *social engineering* di lingkungan *game online*.

2. Praktis:

Menyediakan panduan bagi *player game online* dan mobile agar lebih waspada terhadap serangan *social engineering*.

3. Industri Game:

Membantu pengembang *game* memahami ancaman yang ada

sehingga dapat meningkatkan sistem keamanan di platform *game* mereka.

1.5 Sistematika Penulisan

BAB I Pendahuluan

Bab ini menjelaskan latar belakang penelitian yang mendasari pentingnya kajian tentang serangan *social engineering* dalam *game* mobile. Disajikan pula rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, serta solusi yang ditawarkan

BAB II Tinjauan Pustaka

Pada bab tinjauan pustaka berisi teori yang digunakan untuk mendukung penelitian. Teori tersebut berupa penjelasan mengenai apa itu social engineering, pretexting, impersonation, phishing,

BAB III Metodologi Penelitian

Bab ini membahas pendekatan penelitian yang digunakan, yaitu metode kualitatif, untuk mengamati dan menganalisis teknik *social engineering* seperti *pretexting*, *impersonation*, dan *phishing*. Penjelasan rinci mencakup alur penelitian, metode pengumpulan data, teknik pengujian, dan analisis data yang dilakukan.

BAB IV ANALISIS DAN PEMBAHASAN

Bagian ini memaparkan hasil dari pengujian metode serangan *social engineering* terhadap pemain PUBG Mobile dan Mobile Legends. Hasil penelitian mencakup tingkat keberhasilan serangan, faktor-faktor yang memengaruhi keberhasilan serangan, serta distribusi usia dan latar belakang pendidikan responden yang

rentan terhadap serangan. Diskusi terkait dampak serangan dan implikasinya juga dibahas secara rinci.

BAB V PENUTUP

Bab ini merangkum hasil utama penelitian dan menjawab rumusan masalah yang telah diajukan. Selain itu, diberikan rekomendasi strategis untuk meningkatkan kesadaran dan perlindungan pengguna, seperti edukasi keamanan digital, implementasi fitur keamanan tambahan, dan kolaborasi dengan komunitas *game*.