BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Saat ini dimana teknologi sudah berkembang pesat, terdapat banyak manfaat yang dapat kita ambil dari perkembangan tersebut. Namun, hal ini juga menimbulkan permasalahan baru dimana kemudahan-kemudahan yang tercipta tersebut disalahgunakan oleh sejumlah pihak untuk mengambil keuntungan dengan cara yang tidak benar melalui media siber. Kegiatan tersebut biasa disebut dengan sebutan *Cybercrime* atau kejahatan siber. *Cybercrime* adalah kegiatan ilegal yang dilakukan di dunia maya dengan perantara komputer atau peralatan elektronik lainnya [1]

Salah satu jenis kejahatan yang paling marak terjadi di Indonesia adalah *phishing*. *Phising* dapat didefinisikan sebagai Tindakan yang dilakukan dengan tujuan untuk mencari informasi rahasia dengan cara mengirimkan pesan palsu kepada pengguna melalui media komunikasi elektronik[2]. Tercatat selama lima tahun terakhir, terdapat 34.622 kasus *phishing* dan tercatat sebanyak 7.988 kasus unik yang terjadi pada kuartal 3 tahun 2022 [3]. Namun, *phishing* hanyalah satu dari sekian banyak *cyber crime* yang mengancam masyarakat yang tidak bijak dalam memanfaatkan teknologi khususnya yang terhubung dengan jaringan internet. Penyebab dari permasalahan ini adalah kurangnya kepedulian pengguna internet untuk meningkatkan keterampilan digital sehingga menyebabkan berbagai permasalahan terkait *cybercrime*[4].

Untuk mengurangi dan mencegah tindak kejahatan ini terjadi, pemahaman tentang keamanan siber masyarakat (*cyber security*) perlu ditingkatkan[4]. *Cyber security* (Keamanan Siber) merupakan suatu aktivitas dengan maksud untuk melindungi perangkat komputer, perangkat mobile, server, sistem elektronik, jaringan, dan data dari beraneka jenis serangan jahat digital [5]. Meningkatkan kesadaran masyarakat terhadap kejahatan siber melalui edukasi *cyber security* diharapkan akan dapat mengurangi kasus-kasus kejahatan tersebut untuk terjadi.

Berdasarkan survei yang telah dilakukan, didapatkan dari 84,4% responden berusia 19-26 tahun. 93% dari responden mengatakan mereka mengetahui tentang kejahatan siber dengan kejahatan yang paling banyak mereka ketahui adalah *phishing* yaitu sebanyak 87%, *hacking* 53,1%, dan *ransomeware attack* 43,8

Dari hasil survey didapatkan juga sebanyak 62,5% responden mengatakan jika modus-modus kejahatan siber lebih dikenal akan dapat meminimalisir kejahatan siber, 37,5% lainnya mengatakan hal tersebut mungkin dapat meminimalisirnya. Hal ini menunjukkan bahwa dengan mengetahui modus dari kejahatan siber, maka tindak kejahatan siber tersebut akan dapat dminimalisir.

Mengedukasi masyarakat tentunya merupakan hal yang tidak mudah, oleh karena itu diperlukan suatu strategi untuk membuat kegiatan edukasi ini menjadi mudah. Salah satu caranya adalah dengan menggunakan gamifikasi. Gamifikasi dipahami sebagai penerapan sistem game - persaingan, hadiah, pengukuran perilaku pemain/pengguna - ke dalam domain yang bukan game, seperti pekerjaan, produktivitas, dan kebugaran[6]. Gamifikasi adalah strategi untuk memotivasi orang untuk melakukan tugas-tugas tertentu atau mencapai tujuan tertentu dengan cara mengubahnya menjadi bentuk yang lebih menarik dan menyenangkan seperti game.

Terdapat berbagai macam rangka kerja (*framework*) gamifikasi, seperti *Octalysis Framework* dan *Marczewski Framework*. Perbedaannya terdapat pada poin-poin yang diutamakan dalam pengembangan gamifikasinya. Marczewski Framework mengedepankan poin-poin *intrinsic motivation* menggunakan metode RAMP yang mengimplementasikan *Relatedness*, *Autonomy*, *Mastery*, dan *Purpose*. Sedangkan Octalysis Framework mengedepankan poin-poin berupa *8 core drives* manusia seperti *Meaning*, *Accomplishment*, *Social Influence*, *Empowerment* dan lainnya. Berbeda dengan *Octalysis framework*, *Marczewski framework* mengedepankan pembuatan sistem gamifikasi berdasarkan tipe pengguna tertentu yang terbagi menjadi 6 kelompok yang dikenal juga dengan sebutan *User Type Hexad* [7]. Pada *Marczewski framework* juga terdapat tahapan *planning* dan *Design Development* dimana tahap tersebut akan dilakukan suatu pengujian yang iteratif yang juga bergantung pada target tipe pengguna[8].

Pada penelitian ini, rangka kerja yang akan digunakan adalah rangka kerja *Octalysis*. Pemilihan rangka kerja ini dilakukan karena rangka kerja ini lebih cocok untuk pengerjaan penelitian yang cenderung berfokus kepada poin-poin *core drives* yang dimiliki oleh *Octalysis framework* dan *project* ini tidak dispesifikan kepada tipe pengguna tertentu. Selain itu, *Octalysis framework* juga sudah terbukti dalam beberapa riset berhasil meningkatkan kepuasan pengguna dalam menggunakan aplikasi berbasis gamifikasi [9]. Diharapkan dengan adanya aplikasi ini kesadaran pengguna terhadap keamanan siber dapat meningkat.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah, dapat dirumuskan permasalahan sebagai berikut:

1. Bagaimana merancang dan membangun sistem gamifikasi dan merancang website edukasi dengan memperhatikan *8 core drives* dari rangka kerja Octalysis?
2. Bagaimana mengukur penerimaan pengguna terhadap website edukasi keamanan siber menggunakan kuesioner berbasis *Technology Acceptance Model*?

1.3 Batasan Permasalahan

Untuk memperinci permasalahan dan menjadikannya tidak terlalu umum ditetapkan beberapa batasan masalah dalam penelitianini sebagai berikut:

1. Rangka kerja yang digunakan dalam pengembangan projek adalah rangka kerja Octalysis.
2. Materi edukasi yang akan diimplementasikan hanya materi mengenai kejahatan siber dasar.
3. Target user untuk pengembangan aplikasi ini adalah mahasiswa UMN yang mengetahui tentang kejahatan siber.

1.4 Tujuan Penelitian

Adapun tujuan penelitian uang ingin dicapai pada penelitian kali ini adalah sebagai berikut:

1. Merancang dan membangun website pembelajaran *cybercrime* dengan memperatikan *8 core drives* dari rangka kerja Octalysis
2. Mengukur penerimaan pengguna terhadap website edukasi keamanan siber?

1.5 Manfaat Penelitian

Manfaat dari penelitian yang dilakukan kali ini adalah sebagai berikut:

1. Website edukasi yang telah dirancang dan dibangun dapat digunakan oleh pengguna secara umum untuk mempelajari informasi *cybercrime* yang menerapkan metode gamifikasi.
2. Meningkatkan kesadaran pengguna mengenai kejahatan siber yang ada.

1.6 Sistematika Penulisan

Adapun sistematika penulisan yang dilakukan pada laporan skripsi ini terbagi menjadi lima bab. Sistematika penulisan laporannya adalah sebagai berikut:

- Bab 1 PENDAHULUAN
  Bab ini memberikan informasi mengenai latar belakang masalah, rumusan masalah, batasan masalah, tujuan penilitian, dan sistematika penulisan dari penulisan laporan penelitian ini.

- Bab 2 LANDASAN TEORI
  Bab ini memberikan informasi mengenai landasan teori yang digunakan pada penelitian ini. Landasan teori yang digunakan pada penlitian ini adalah *Octalysis Gamification Framework*, *Unified Theory of Acceptance and Use of Technology*(UTAUT), dan skala likert.

- Bab 3 METODOLOGI PENELITIAN
  Bab ini memberikan informasi mengenai metodologi penelitian yang digunakan dalam penelitian ini beserta perancangan website. Perancangan website akan terdiri dari perancangan sistem gamifikasi menggunakan *octalysis framework*, perancangan *mockup aplikasi*, pembuatan *flowchart*, dan perancangan antarmuka.

- Bab 4 HASIL DAN DISKUSI
  Bab ini berisi spesifikasi piranti yang digunakan dalam pembuatan website, hasil implementasi dan pengujian website, dan analisa hasil pengujian.

- Bab 5 SIMPULAN DAN SARAN
  Bab terakhir yang berisikan hasil dan kesimpulan dari penelitian yang

telah dilakukan serta saran yang ditujukkan untuk pengembangan aplikasi berikutnya.