BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan internet membawa kemudahan dalam berbagai aktivitas digital, seperti transaksi keuangan, komunikasi, dan akses ke berbagai informasi lainnya. Tercatat pengguna internet di Indonesia mencatat 221 juta orang pada awal tahun 2025, atau sekitar 79,5% dari total populasi [1]. Angka ini menunjukkan pertumbuhan signifikan dalam adopsi internet di Indonesia. Tetapi, seiring dengan kemudahan tersebut, muncul berbagai ancaman keamanan, salah satunya adalah serangan *phishing*. *Phishing* merupakan upaya untuk memperoleh data ataupun informasi sensitif seperti data pribadi, password, akun sosial media dengan cara menyamar sebagai perusahaan atau individu yang terpercaya melalui media digital, yang sering kali dalam bentuk situs web palsu. Pada awal tahun 2025 di Indonesia, tercatat lonjakan serangan *phishing* sebesar 180% dibandingkan tahun 2023 [2]. Data tersebut menunjukan bahwa kesadaran keamanan Masyarakat Indonesia masih tergolong rendah, terutama dalam mengenali dan menghindari ancaman *phishing*. Oleh karena itu, diperlukan solusi yang dapat memberikan perlindungan untuk menghindari serangan *phishing*. Hal ini menjadi penting karena browser merupakan gerbang utama dalam aktivitas di Internet, termasuk transaksi keuangan, pengelolaan data pribadi, hingga komunikasi digital.

Salah satu kasus phishing yang terjadi adalah insiden yang menimpa satu platform *exchange* kripto Bybit pada awal tahun 2025. Pada insiden ini, peretas yang dikenal sebagai Lazarus Group berhasil mencuri sekitar $1,46 miliar dalam bentuk Ethereum dari Bybit [3]. Serangan ini bermula dari phishing yang mentargetkan pengguna dompet digital Bybit. Kode berbahaya tersebut disisipkan ke antarmuka pengguna dompet tersebut, sehingga pengguna melihat transaksi yang terlihat sah padahal telah dimodifikasi untuk memberikan kendali penuh kepada *hacker*. Serangan ini menegaskan bahwa phishing tidak hanya mengincar individu biasa, tetapi juga Perusahaan besar dengan sistem keamanan yang tinggi.

Kasus tersebut memperlihatkan betapa pentingnya perlindungan pada sisi pengguna, terutama ketika interaksi dengan website yang menjadi gerbang utama masuknya serangan *phishing*. Salah satu pendekatan yang dapat dilakukan adalah dengan menyediakan ekstensi *browser* yang mampu medeteksi dan memperingatkan pengguna saat mengakses situs web yang terindikasi sebagai *phishing* [4]. Google menyediakan layanan Safe Browsing API, yang dapat menjadi dasar pengembangan ekstensi *browser* sebagai solusi mitigasi *pshishing*. Sebetulnya, Google sudah menyediakan layanan Safe Browsing API tersebut, akan tetapi dalam beberapa kasus situs yang terindikasi *phishing* masih dapat berjalan dengan lancar. Pemerintah Indonesia juga sudah menerapkan hal serupa, hanya saja penerapannya kurang efektif untuk memblokir situs yang terindikasi *phishing* dan hanya memblokir situs yang bermuatan negatif, seperti berita hoax, konten yang berbau pornografi, mengandung muatan SARA [5].

Berdasarkan kondisi tersebut, penelitian ini dilakukan untuk merancang dan mengembangkan ekstensi browser berbasis Google Safe Browsing API sebagai upaya pencegahan terhadap serangan *phishing* dengan cara memblokir langsung situs yang tidak dikenali ataupun terindikasi berbahaya dengan memanfaatkan Google Safe Browsing *API*. Diharapkan dari penelitian ini dapat meningkat kesadaran dan membantu pengguna dalam pencegahan serangan *phishing*.

1.2 Rumusan Masalah

1. Bagaimana cara mengembangkan ekstensi browser yang memanfaatkan Google Safe Browsing API untuk mendeteksi situs *phishing*?
2. Bagaimana proses integrasi Google Safe Browsing API ke dalam ekstensi *browser* agar dapat bekerja secara *real-time*?
3. Apakah ekstensi *browser* yang dikembangkan dapat memberikan perlindungan terhadap potensi *phishing* berbasis *URL*?

1.3 Batasan Masalah

1. Penelitian hanya berfokus pada pengembangan ekstensi untuk *browser* Microsoft Edge.

2. Sistem deteksi *phishing* hanya menggunakan Google Safe Browsing API tanpa tambahan metode lain.
3. Uji coba dilakukan dengan situs terbatas yang sekiranya memiliki potensi *phishing*.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Mengembangkan sebuah ekstensi *browser* yang dapat mendeteksi situs *phishing* menggunakan data dari Google Safe Browsing API.
2. Menerapkan integrasi API dalam konteks pengembangan perangkat lunak keamanan berbasis *browser*.
3. Menghasilkan alat bantu keamanan siber sederhana yang dapat memberikan perlindungan awal terhadap serangan *phishing* berbasis *URL*.

1.5 Manfaat Penelitian

1. Memberikan solusi teknis berupa ekstensi browser yang mampu memblokir situs terindikasi *phishing* dengan memanfaatkan Google Safe Browsing API.
2. Membantu pengguna internet dalam mencegah akses ke situs berbahaya secara *real-time*.
3. Membuktikan bahwa integrasi Google Safe Browsing API ke dalam ekstensi *browser* merupakan pendekatan yang efektif dalam memperkuat keamanan siber, khususnya terhadap serangan *phishing*.

1.6 Sistematika Penulisan

Sistematika penulisan berisikan gambaran secara umum penelitian ini sehingga mempermudah alur isi. Adapun garis besar isi skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN

BAB II TINJAUAN PUSTAKA

BAB III METODE PENELITIAN

BAB IV HASIL DAN PEMBAHASAN

BAB V PENUTUP