

## BAB V PENUTUP

### 5.1 Kesimpulan

Dari penelitian yang dilakukan, didapat hasil bahwa:

1. Pengembangan ekstensi browser dapat dilakukan dengan memanfaatkan HTML, CSS, dan Javascript dan mengikuti struktur standar ekstensi browser.
2. Integrasi API dilakukan dengan cara API dimasukkan kedalam file manifest.json untuk mendapatkan permission dari browser dan pada file background.js untuk endpoint dari Google Safe Browsing API.
3. Ekstensi browser yang dikembangkan dapat mendeteksi website phishing dengan memanfaatkan Google Safe Browsing API. Berdasarkan pengujian terhadap 21 URL phishing, ekstensi ini berhasil mendeteksi sebanyak 15 website phishing. Hal ini menunjukkan bahwa pendekatan ini cukup efektif dan relevan untuk digunakan dalam pencegahan terhadap situs phishing. Jika dibandingkan dengan tiga ekstensi keamanan peuler, yaitu Avira Browser Security, Bitdefender TrafficLight, dan Netcraft, ekstensi yang dikembangkan ini memiliki performa yang kompetitif. Meskipun tidak unggul, tingkat deteksinya mendekati beberapa ekstensi tersebut. Dengan demikian, ekstensi yang dikembangkan mampu memberikan kontribusi nyata terhadap upaya mitigasi website phishing melalui pendekatan yang memanfaatkan Google Safe Browsing API.

### 5.2 Saran

Dalam proses pengembangan dan pengujian, terdapat beberapa hal yang dapat ditingkatkan di masa mendatang. Salah satunya adalah memperluas cakupan deteksi dengan menambahkan metode seperti *machine learning*, agar tidak hanya bergantung pada *Google Safe Browsing API* dan supaya mampu mengenali situs *phishing* baru yang belum masuk dalam jangkauan daftar *blacklist* Goole. Selain

itu, ekstensi ini juga masih dapat dioptimalkan dalam hal tampilan *UI* (antarmuka) agar lebih menarik.

