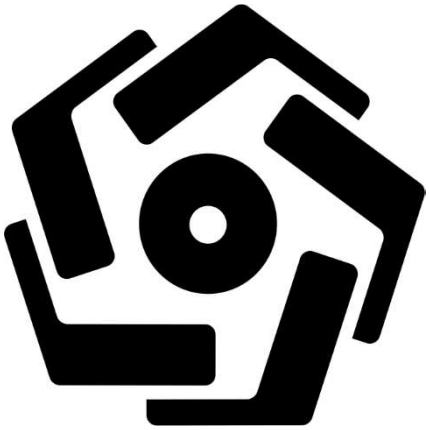
PENGEMBANGAN EKSTENSI BROWSER UNTUK PENCEGAHAN PHISHING BERBASIS GOOGLE SAFE BROWSING API

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi S1 Teknik Komputer



disusun oleh

PAUL DAVA NANDO SETYA

21.83.0632

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

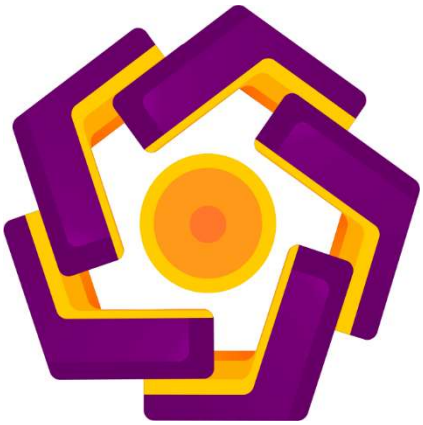
2025

PENGEMBANGAN EKSTENSI BROWSER UNTUK PENCEGAHAN PHISHING BERBASIS GOOGLE SAFE BROWSING API

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi S1 Teknik Komputer



disusun oleh

PAUL DAVA NANDO SETYA

21.83.0632

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN

SKRIPSI

PENGEMBANGAN EKSTENSI BROWSER UNTUK PENCEGAHAN PHISHING BERBASIS GOOGLE SAFE BROWSING API

yang disusun dan diajukan oleh

Paul Dava Nando Setya

21.83.0632

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 19 Agustus 2025

Dosen Pembimbing,

Wahid Miftahul Ashari, S.Kom., M.T
NIK. 190302452

ii

HALAMAN PENGESAHAN

SKRIPSI

PENGEMBANGAN EKSTENSI BROWSER UNTUK PENCEGAHAN PHISHING BERBASIS GOOGLE SAFE BROWSING API

yang disusun dan diajukan oleh

Paul Dava Nando Setya

21.83.0632

Telah dipertahankan di depan Dewan Penguji
pada tanggal 19 Agustus 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Dr. Dony Ariyus, S.S., M.Kom. **NIK. 190302128**	
Senie Destya, S.T., M.Kom. **NIK. 190302312**	
Wahid Miftahul Ashari, S.Kom., M.T. **NIK. 190302452**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 19 Agustus 2025

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

iii

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Paul Dava Nando Setya
NIM : 21.83.0632

Menyatakan bahwa Skripsi dengan judul berikut:

Pengembangan Ekstensi Browser Untuk Pencegahan Phishing Berbasis Google Safe Browsing API

Dosen Pembimbing : Wahid Miftahul Ashari, S.Kom., M.T

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 19 Agustus 2025

Yang Menyatakan,

Paul Dava Nando Setya

iv

KATA PENGANTAR

Puji Syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat-Nya sehingga penulis dapat meyelesaikan skripsi yang berjudul "Pengembangan Ekstensi Browser Untuk Pencegahan Phising Berbasis Google Safe Browsing API" dengan baik dan tepat waktu. Dalam proses penyusunan skripsi ini, penulis menyadari bahwa pencapaian ini tidak terlepas dari bantuan dan dukungan dari berbagai pihak. Oleh karena itu, penulis dengan tulus menyampaikan ucapan terima kasih kepada:

1. Bapak Prof. Dr. M. Suyanto, MM., selaku Rektor Universitas Amikom Yogyakarta
2. Ibu Prof. Dr. Kusrini, M.Kom. selaku Dekan Program Fakultas Ilmu Komputer
3. Bapak Dr. Dony Ariyus, M.Kom., selaku Ketua Program Studi Teknik Komputer
4. Bapak Wahid Miftahul Ashari, S.Kom., M.T sebagai dosen pembimbing yang telah memberikan arahan, masukan, dan bimbingan selama proses penyusunan skripsi.
5. Segenap Bapak dan Ibu Dosen Universitas Amikom Yogyakarta yang telah memberikan ilmu selama perkuliahan berlangsung.
6. Kedua orang tua dan teman-teman yang memberikan doa dan semangat tanpa henti.
7. Serta semua pihak yang telah membantu dan mendukung dalam proses penyusunan skripsi sampai akhir.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan demi perbaikan di masa mendatang. Semoga skripsi ini dapat memberikan manfaat bagi pembaca, khususnya dalam pengembangan keamanan perangkat lunak untuk pencegahan phishing

Yogyakarta, 16 Agustus 2025

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG DAN SINGKATAN

API	Application Programming Interface
SVM	Support Vector Machines
CNN	Convolutional Neural Network
LSTM	Long Short-Term Memory
IoT	Internet of Things
URL	Uniform Resource Locator
VPN	Virtual Private Network
DNS	Domain Name Server
UI	User Interface
ID	Identity
✓	Berhasil Mendeteksi Sebagai *Phishing*
×	Gagal Mendeteksi Sebagai *Phishing*

DAFTAR ISTILAH

Real-time	Proses atau respon secara langsung
Exchange	Platform penjualan dan pembelian aset digital
Dataset	Kumpulan berisi item data dari suatu sumber data
Blacklist	Daftar yang tidak diinginkan, berbahaya, atau melanggar aturan tertentu
Toolbar	Tombol navigasi yang terdapat di bagian atas atau samping tampilan perangkat lunak
Search Engine	Mesin pencari yang diperuntukkan untuk mencari informasi di dalam internet
Domain	Identitas untuk suatu website
Port	Protokol jaringan untuk mengidentifikasi aplikasi atau layanan yang berjalan pada sebuah perangkat
Login	Proses autentikasi di mana pengguna memasukkan data kredensial tertentu
Cloud	Teknologi yang menyediakan sumber daya komputasi untuk menyimpan, mengelola, dan memproses data
Linear	Urutan langkah-langkah yang teratur dan mengikuti alur yang sudah ada
Bug	Kecacatan ataupun error pada perangkat lunak
Database	Repositori digital untuk menyimpan, mengelola, dan mengamankan kumpulan data yang terorganisir

INTISARI

Phishing merupakan salah satu bentuk ancaman siber yang semamkin sering digunakan untuk mencari data sensitif pengguna dengan menyamar sebagai situs resmi. Permasalah ini menimbulkan risiko besar terhadap keamanan data pribadi dan finansial pengguna internet. Banyak pengguna yang masih sulit membedakan antara situs asli dan situs palsu, sehingga mereka rentan menjadi korban. Untuk mengatasi permasalahan tersebut, peneitian ini bertujuan untuk mengembangkan sebuah ekstensi browser yang dapat membantu pengguna mendeteksi dan menghindari *website phishing* secara otomatis menggunakan pendekatan berbasis *Google Safe Browsing API*. Pengembangan dilakukan melalui tahapan perancangan, implementasi ekstensi berbasis *HTML, JavaScript*, dan penggunan *API* dari *Google*, serta dilakukan pengujian terhadap *21 URL phishing* untuk mengevaluasi efektivitas ekstensi. Hasil pengujian menunjukkan bahwa ekstensi yang dikembangkan mampu mendeteksi *website phishing* sebanyak 15 *URL* dari 21 *URL* yang diuji. Performa ekstensi juga dibandingkan dengan ekstensi popular lainnya dan menunjukkan hasil yang cukup kompetitif. Penelitian ini berkontribusi pada pengembangan keamanan perangkat lunak yang praktis dan dapat digunakan oleh pengguna umum untuk meningkatkan keamanan saat menjelajahi *website*. Hasil dari penelitian ini dapat dimanfaatkan oleh pengguna internet secara luar, khususnya yang memiliki aktivitas digital yang rawan terhadap serangan *phishing*. Untuk Penelitian selanjutnya diharapkan dapat mengintegrasikan metode tambahan seperti machine learning agar dapat mendeteksi situs phishing baru secara lebih proaktif.

Kata kunci: ekstensi *browser, Google Safe Browsing API, machine learning, phishing, website.*

ABSTRACT

Phishing is a prevalent form of cyber threat increasingly employed to obtain sensitive user data by impersonating legitimate websites. This issue poses significant risks to the security of personal and financial information of internet users. Many individuals still struggle to distinguish between authentic and fraudulent websites, rendering them vulnerable to such attacks. To address this problem, this study aims to develop a browser extension capable of automatically detecting and preventing access to phishing sites by leveraging the Google Safe Browsing API. The development process was carried out through several stages, including design, implementation of the extension using HTML and JavaScript, integration of Google's API, and testing with 21 phishing URLs to evaluate its effectiveness. The testing results demonstrate that the developed extension successfully detected 15 out of 21 tested phishing URLs. Furthermore, its performance was compared with other popular extensions and showed relatively competitive results. This research contributes to the advancement of practical of software security solutions that can be readily adopted by general users to enhance their safety while browsing the web. The findings of this study can benefit a wide range of internet users, particularly those engaged in digital activities that are highly susceptible to phishing attacks. Future research may incorporate additional methods, such as machine learning, to proactively detect newly emerging phishing websites.

Keyword: *browser extension, Google Safe Browsing API, machine learning, phishing, website.*