BAB I
PENDAHULUAN

1.1 Latar Belakang

Criminal merupakan suatu tindakan kejahatan yang dapat melanggar nilai, norma, hukum serta perilaku yang dapat meresahkan dan merugikan banyak pihak. *Criminal* atau kriminalitas dapat dilakukan secara individu, kelompok maupun komunitas. Terdapat banyak faktor motif *criminal* terjadi, dengan beragam jenis sosial. Salah satu jenis kejahatan atau *criminal* ialah *Cyber crime* atau kejahatan di dunia maya. Terdapat banyak kejahatan di dunia maya yang menjadi kasus di Indonesia, salah satu kejahatan dunia maya yang sangat sering terjadi dan merugikan baik individu maupun perusahaan ialah *Phishing.*

Banyak kasus *phishing* yang terjadi di Indonesia baik perorangan maupun perusahaan dengan jumlah kerugian yang sangat tinggi. Terutama pada sektor perbankan. Dilansir dari Direktur Penelitian dan Pengaturan Perbankan Otoritas Jasa Keuangan atau yang biasa disebut OJK, Mohammad Miftah menyampaikan bahwa serangan siber menimbulkan kerugian bagi sektor perbankan, khususnya bank umum di Indonesia rugi hingga Rp 246,5 miliar. Terkutip pada https://www.republika.id/posts/21670/tak-semua-indah-di-era-digital.

Data menurut cisco pada laporan tren ancaman keamanan di tahun 2021 adalah sebanyak 86% organisasi memiliki setidaknya satu pengguna yang mencoba terhubung ke situs *phising*, 46% lalu lintas berbahaya di industri jasa keuangan yang dihasilkan dari *phising*, 48% organisasi menemukan aktivitas *malware* mencuri informasi, dan 90% pelanggaran data terjadi karena *phising*. Serta dampak yang

terjadi pada perusahaan apabila terkena *phishing* adalah kehilangan banyak pelanggan, reputasi organisasi atau perusahaan menjadi rusak, kehilangan nilai perusahaan, dan terjadinya gangguan bisnis. Dilansir dari https://www.cloudcomputing.id/berita/horangi-jelaskan-bahaya-phishing-terhadap-organisasi.

Serangan *phishing* tidak hanya mengincar individu tetapi juga mengincar para pekerja perusahaan tersebut, memanfaatkan mereka dengan pengetahuan minim mengenai *phishing*, sehingga data rahasia perusahaan yang dimiliki oleh karyawan akan dengan mudah diakses oleh pelaku.

Riset global Kaspersky pada tahun 2023, yang dilakukan di antara 834 pembuat keputusan TI dari Asia Pasifik, menunjukkan bahwa kehilangan atau terekspos nya informasi perusahaan dan pelanggan akibat pelanggaran data (59%) merupakan masalah besar bagi perusahaan. Apabila dilihat secara lebih spesifik tentang tantangan keamanan yang paling meresahkan, sebagian besar responden Asia Pasifik mengindikasikan kebocoran data dari sistem internal yang disebabkan oleh serangan dunia maya (29%) dan oleh karyawan (25%). Data tersebut dilansir dari https://voi.id/teknologi/257742/kaspersky-kebocoran-data-jadi-masalah-terbesar-bagi-perusahaan-di-asia-pasifik.

Riset dari *Haystax Technology* tahun 2017, ditemukan fakta bahwa 74% perusahaan merasa rentan dengan ancaman orang dalam, sementara 56% profesional keamanan menyakini bahwa dalam setahun terakhir ancaman dari orang dalam atau insider semakin sering terjadi. Kejahatan siber yang berkaitan dengan karyawan biasanya disebabkan oleh karyawan yang melakukan kelalaian, seperti

mengabaikan peringatan, gagal mengikuti prosedur atau kesalahan manusia sederhana. Banyak kasus pelanggaran data disebabkan karena ketidaktahuan karyawan, karyawan tidak menyadari jika perbuatannya merupakan sebuah kesalahan yang bisa memberikan dampak yang sangat besar dan mempengaruhi kelangsungan hidup sebuah perusahaan. Peristiwa ini biasanya terjadi secara internal tanpa melibatkan pihak ketiga. Bila ini terjadi, peretas bisa menggunakan informasi tersebut sebagai pemerasan atau sebagai aset bagi kelompok mereka. Riset tersebut dikutip dari https://news.prosperita.co.id/3-tipe-karyawan-penyebab-rentan-bahaya-siber/.

Phishing telah menjadi salah satu ancaman yang serius bagi perusahaan dan organisasi besar, dengan semakin banyaknya kasus yang terjadi, karena metode ini berhasil menciptakan ancaman yang sulit untuk diatasi. Para pelaku phishing menggunakan trik yang canggih dan menyesuaikan pesan palsu mereka untuk meniru situs *web* dan identitas resmi dari perusahaan atau organisasi yang dituju. Mereka mencari informasi melalui media sosial atau sumber lain untuk menciptakan pesan yang sangat meyakinkan dan kredibel. *Phishing* juga mengincar pegawai dalam perusahaan dan organisasi besar sebagai target utama.

Pada perusahaan PT Dinamika Sistem Integrasi Solusi, merupakan sebuah perusahaan yang bergerak dalam keamanan jaringan. Perusahaan ini memiliki klien rata-rata dari sector perbankan ternama di Indonesia. Salah satu program kerja pada perusahaan ini ialah untuk penyuluhan terhadap pegawai bank untuk *aware* dengan serangan / URL *phishing*. Fakta yang didapat dalam penyuluhan pada salah satu bank ternama di Indonesia ini ialah terdapat banyak pegawainya yang masih tertipu

dengan *link* yang mereka dapat yang merupakan *link phishing.* Penyuluhan ini dilakukan pada tahun 2023.

Ada 2 hal ketika data rahasia perusahaan berada di tangan pelaku, yaitu dengan menggunakannya untuk pribadi sehingga dapat langsung merugikan perusahaan tersebut atau dijual ke situs gelap. Tidak jarang juga komunitas dari situs gelap ini yang memberikan pekerjaan kepada pelaku untuk mendapatkan data rahasia milik seseorang atau suatu perusahaan.

Link phishing ini sendiri tidak hanya untuk mendapatkan data rahasia namun juga ketika *link* dibuka kemungkinan hal merugikan lainnya akan terjadi seperti mengunduh dan menjalankan *malware, ransomeware* dan sebagainya. Metode yang biasa digunakan sebagai sarana pengiriman *link phishing* ialah email atau sms.

Dalam mengidentifikasi sebuah *link phishing* juga harus memiliki pengetahuan dengan hal yang berkaitan dengan *phishing*, oleh sebab itu, sebagian besar individu kesulitan dalam memastikan *link* yang dia dapat adalah *link* aman atau *link* berbahaya.

Mengapa memilih algoritma *gradient boosting* dalam program? Karena *gradient boosting* merupakan algoritma dengan hasil akurasi yang tertinggi dengan begitu program dapat lebih akurat dalam menganalisa sebuah link. Akurasi yang dihasilkan oleh *gradient boosting* mencapai 0.974 tertinggi diantara algoritma lainnya.

1.2 Identifikasi Masalah

Berdasarkan latar belakang masalah tersebut, maka permasalahan yang muncul dapat di identifikasikan sebagai berikut :

1. Menjadi ancaman yang serius bagi perusahaan dan organisasi besar mengingat angka kasus *phishing* yang ada
2. Kurangnya pengetahuan terhadap *link-link phishing*
3. Sulitnya mengidentifikasi adanya *url link phishing*
4. Menjadi salah satu penyebaran *malware* dan *ransomeware* kedalam sistem

1.3 Rumusan Masalah

Berdasarkan masalah yang dihadapi, penulis merumuskan beberapamasalah yang ada dalam penelitian ini sebagai berikut :

1. Bagaimana mengurangi ancaman yang dapat merugikan individu dan organisasi?
2. Bagaimana mengetahui adanya *phishing* bagi pengguna?
3. Bagaimana mengidentifikasi adanya *phishing* yang semakin canggih?
4. Bagaimana melakukan pencegahan terhadap penyebaran *malware* dan *ransomeware*?

1.4 Batasan Masalah

Berdasarkan identifikasi masalah, penulis membuat batasan masalah dalam penelitian ini, yaitu :

1. Program berbentuk *platform Website*
2. Program berjalan untuk menganalisa sebuah *link phishing*

3. Program menggunakan algoritma *Gradient boosting*
4. Fokus pada kerugian individu yang berkaitan dengan perusahaan karena kurangnya pengetahuan terhadap bentuk *link phishing*

1.5 Tujuan dan Manfaat Penelitian

Dalam penelitian ini penulis memiliki tujuan dan manfaat berupa

1.5.1 Tujuan Penelitian

Adapun tujuan yang ingin di capai dari penelitian ini adalah sebagai berikut:

1. Membuat sistem untuk mengurangi ancaman dari *phishing*
2. Memberikan notifikasi bagi individu atau pengguna tentang adanya phishing
3. Mencagah data terinfeksi dengan adanya *malware* dan *ransomeware*

1.5.2 Manfaat Penelitian

Dalam penelitian ini diharapkan dapat memberikan manfaat berupa :

1. Memberikan perlindungan terhadap serangan *phishing*
2. Sebagai platform pengidentifikasi keamanan sebuah *url*
3. Meningkatkan keamanan perusahaan
4. Mengurangi resiko kerugian perusahaan akibat kelalaian pegawai

Sistematika Penulisan

Penyusunan skripsi ini, pada umumnya mencakup 5 (lima) bagian yang terdiri atas beberapa bab dan sub bab, yaitu :

BAB I PENDAHULUAN

Pada bab ini penulis menyajikan tentang latar belakang maksud dari tujuan indentifikasi masalah, batasan masalah, metode penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini memuat tinjauan pustaka tentang penelitian sebelumnya berkaitan dengan topik skripsi yang dipilih dengan teori-teori yang mendukung.

BAB III METODOLOGI PENELITIAN

Dalam bab ini setidaknya membahas mengenai objek penelitian dan kerangka dari penulisan skripsi ini.

BAB IV HASIL DAN PEMBAHASAN

Dalam bab ini menjelaskan tentang proses perancangan sistem perangkat keras serta perangkat lunak yang dibutuhkan dalam membangun sistem. Pada bab ini juga melakukan pengujian terhadap sistem yang dibuat untuk mengetahui apakah sudah benar-benar berjalan seperti yang diharapkan.

BAB V PENUTUP

Pada bab ini di menyajikan kesimpulan penelitian serta saran yang berhubungan dengan penyusunan laporan tugas akhir.