

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Penggunaan internet yang semakin meluas di kalangan masyarakat tidak lantas menjadi baik, karena dengan semakin banyaknya pengguna internet maka keamanan informasi dan data pribadi juga dipertaruhkan. Salah satu faktor penyebab terjadinya pencurian data pribadi adalah karena pengguna dengan mudahnya menyebarkan data pribadi melalui *webiste phising* [1]. *Phishing* merupakan kejahatan dengan menggunakan teknik rekayasa sosial. *Phisher* (sebutan penipu *Phishing*) berupaya menipu untuk mendapatkan informasi yang sangat rahasia, seperti *username, password* sampai kartu kredit, dengan menyamar sebagai orang terpercaya dalam sebuah komunikasi elektronik. *Phishing* rata rata menyerang sektor Industri berbasis daring, seperti *ecommerce, social media* dan perbankan [2].

Pada perkembangannya, serangan *phising* saat ini menunjukkan jumlah yang cukup banyak, dimana merujuk dari *Anti-Phishing Working Group (APWG)* pada periode ke 4 tahun 2018 sampai dengan periode ke-1 tahun 2019 dengan total 180,768 web *phising* [3]. Dengan data seperti ini menandakan masih maraknya tindak kejahatan *phising* di dunia maya yang menyerang dan tersebar secara masif dikalangan masyarakat umum, selain itu dengan perkembangan serangan web *phising* yang masih tinggi dibutuhkan juga peningkatan kewaspadaan dari *user* atau pengguna terkait bahaya serangan *phising* melalui media sosial

Tindakan *Phishing* mengincar informasi yang bersifat rahasia pengguna untuk digunakan oleh pihak yang tidak bertanggung jawab. Pengguna dirugikan dalam banyak hal seperti privasi, penyalahgunaan data hingga *hacking* bahkan kerugian Finansial [4]. Dasarnya *phising* dikaitkan dengan kejahatan dunia maya, penjahat mengirim sebuah link palsu ke media sosial *whatsapp* yang nantinya memikat korban ke situs *website* yang merupakan klon visual dari halaman sosial

media ataupun website lainnya, di website klon tersebut biasanya anda memasukkan data – data pribadi anda ke formulir palsu dan mengirimkannya langsung ke para penjahat. Namun dalam skala kecil bisa saja *website phishing* disebar melalui pihak-pihak yang awam terhadap *phishing* contohnya masyarakat yang awam akan hal ini. Dalam masalah *phishing* ini harus dicarikan solusi agar kejahatan *phishing* bisa berkurang sedikit demi sedikit, karena data pribadi merupakan harta yang paling berharga di dunia serba digital saat ini.



Gambar 1.1 Contoh *website phishing*

A screenshot of a phishing website. The text is in Indonesian and reads: "WOW! Adidas menawarkan 3100 Sepatu Gratis, T-shirt dan Masker untuk semua orang. Dapatkan milik Anda di sini GRATIS". Below this is a URL: "http://adidas-id.offers247.online". A timestamp "14:30" is visible in the bottom right corner.

Gambar 1.2 contoh *website phishing*

Dapat dilihat dari 2 contoh gambar di atas penyebaran link palsu dapat dengan mudah dilakukan, hanya dengan mengandalkan iming – iming hadiah pulsa dan sepatu gratis para korban akan mengunjungi tautan link tersebut. Lalu para korban akan mulai mengisi *form* yang ada pada website palsu / *phishing* tersebut tanpa mengerti akibat dari mempercayai tautan tersebut. Dalam hal ini data pribadi korban akan menjadi target pelaku, biasanya pelaku akan mengincar data pribadi yang sangat privasi seperti : Nama Ibu, No kartu kredit, No Ktp, *Email*, No Hp, hingga alamat rumah. Hal ini menjadi sangat berbahaya jika

korban benar benar mengisi form tersebut [5]. Seperti yang diketahui dalam perbankan nama ibu dan no kartu atm menjadi hal yang penting, apabila data tersebut ada di tangan orang lain maka bisa terjadi hal hal yang sangat merugikan.

Website phishing tidak akan bekerja ataupun memakan korban apabila masyarakat yang masih awam akan *phising* diberikan informasi tentang bahaya nya kejahatan dunia maya ini. Dalam penelitian yang saya lakukan akan mengarah ke tingkat kewaspadaan masyarakat tentang seberapa paham nya para responden akan bahaya kejahatan *phising*. Dalam penelitian yang dilakukan menggunakan metode kuantitatif yang menggunakan kuesioner dan diisi oleh para responden . Isi dari kuesioner tersebut adalah pertanyaan –pertanyaan yang berkesinambungan terhadap permasalahan penelitian. Hasil dari kuesioner tersebut akan terlihat persentase angka yang akan dibahasakan agar mudah dipahami dan terlihat seberapa pentingkah para responden menjaga data pribadi mereka dan seberapa seringkah para responden mendapatkan pesan berupa link palsu *phising*.

Pada latar belakang yang sudah dijelaskan secara rinci diatas maka penelitian ini adalah melakukan “ Analisis Tingkat Kewaspadaan Masyarakat terhadap Ancaman Keamanan Data Pribadi Melalui *Webiste Phising* Di Sosial Media *Whatsapp* Menggunakan Metode Kuantitatif ” Dalam hal ini responden merupakan masyarakat umum yang awam akan dunia *Phising* dan pencurian data. Hasil dari penelitian akan memberikan edukasi terhadap para responden akan bahaya nya *Phising* dan pencurian data pribadi di internet, sebab dalam masa covid19 seperti ini akan banyak kejahatan *phising* yang mengincar masyarakat khususnya yang awam akan dunia teknologi.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang ada pada penelitian ini didapatkan rumusan masalah yaitu seberapa besar tingkat kewaspadaan masyarakat terkait tindak kejahatan web *phising* yang marak terjadi dan tersebar di media pesan singkat *Whatsapp*.

1.3 Batasan masalah

- a. Penelitian ini terfokus pada *Website phishing* dan ancaman pencurian data Pribadi melalui media sosial *whatsapp*.
- b. Penelitian ini menggunakan Metode kuantitatif dalam pengambilan data responden.
- c. Jumlah responden berjumlah 80 orang yang masih awam terhadap Phising.
- d. Pembuatan Kuesioner menggunakan *google form* yang diisi oleh para responden .
- e. Menggunakan *Aplikasi SPSS versi 25* dalam pengolahan data

1.4 Tujuan penelitian

Tujuan yang ingin diraih dalam pembuatan laporan skripsi ini adalah mendapatkan nilai persentase dari tingkat kewaspadaan masarakat terkait ancaman tindak kejahatan web *phising* yang sering tersebar di media sosial *whatsapp*, serta cara menghindari tindak kejahatan *web phising* ini.

1.5 Sistematika penulisan

Pada bagian ini terdapat 5 bab yang dimana pada masing-masing bab memiliki peran dan bagian yang berbeda.

Bab I Pendahuluan, berisi: latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan.

Bab II Landasan Teori, berisi: hasil penelitian sejenis atau sebelumnya yang sudah pernah dilakukan sebelumnya, serta referensi dari jurnal atau pun skripsi, dan penjelasan mengenai *phising* serta bagaimana cara mengamankan data pribadi akan tidak terjadi pencurian

Bab III Metodologi Penelitian, berisi : penjelasan mengenai metode penelitian yang digunakan untuk mengolah data dan mendapatkan data dari responen, serta menganalisis hasil dari data yang sudah dikumpulkan.

Bab IV Pembahasan, berisi : pembuktian yang menunjukkan bahwa url yang digunakan sebagai sample telah terindikasi *phising* dan pengolahan data dari hasil

penelitian, serta proses penerapan metode penelitian, dan melakukan perhitungan hasil kuesioner/data yang sudah dikumpulkan agar bisa diambil kesimpulan dari kuesioner tersebut.

Bab V Penutup, berisi : kesimpulan dari hasil akhir penelitian Tingkat Kewaspadaan Masyarakat terhadap Ancaman Keamanan Data Pribadi Melalui *Webiste Phising* Di Sosia Media *Whatsapp*. Menggunakan Metode Kuantitatif dan saran .

