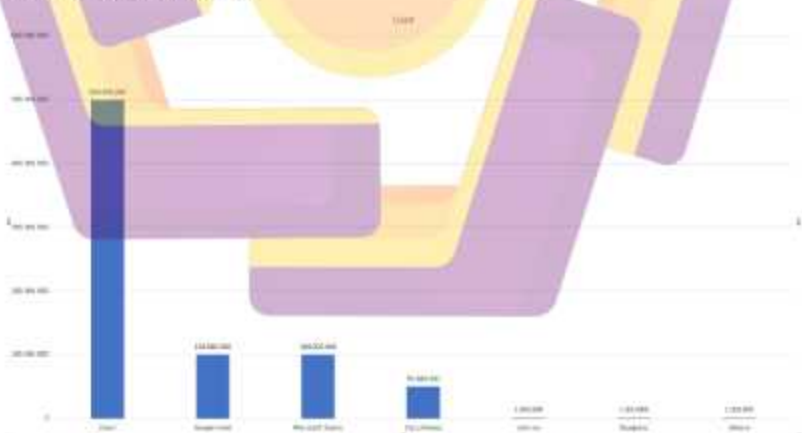
BAB I
PENDAHULUAN

1.1 Latar Belakang

Terjadinya pandemi di era perkembangan teknologi seperti sekarang, membuat manusia dihadapkan dengan pencegahan kontak fisik. Maka dari itu, di kondisi ini, teknologi telah menjadi alat yang digunakan untuk berkomunikasi dalam kegiatan sehari hari. Di masa *pandemic* ini kita diharuskan untuk mencegah penyebaran *virus covid* dengan mengurangi mobilitas di luar ruangan. Dengan begitu, manusia di paksa untuk menggunakan teknologi sebagai sarana untuk menunjang urusan mereka. Contohnya adalah dengan menggunakan aplikasi yang di sebut "*Zoom*". Dengan *zoom*, kita dapat berkomunikasi jarak jauh dengan hanya menatap layar *laptop*, atau *device* yang dapat menghubungkan kita ke server *zoom*. Akan tetapi, terdapat ancaman yang berasal dari pihak-pihak tidak bertanggung jawab. Mereka melakukan serangan-serangan siber demi mendapatkan informasi privat yang sangat *fatal* bila jatuh ke tangan orang yang tidak bertanggung jawab. Contohnya adalah serangan *Phishing*

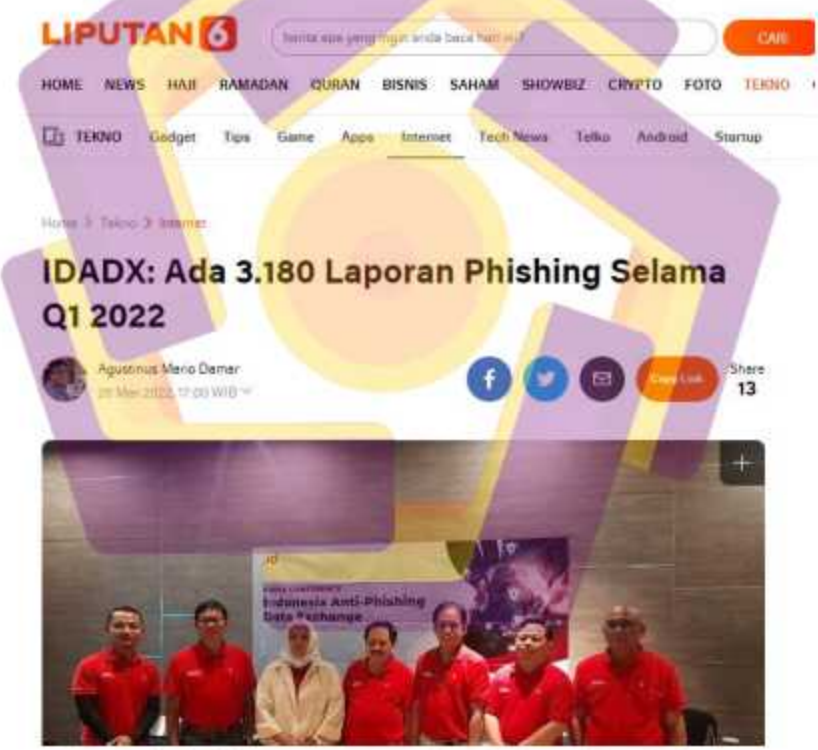


Gambar 1.1 Grafik jumlah pengguna zoom(Sumber: Playstore)

Pada gambar 1.1 diatas mejelaskan *grafik* jumlah pengguna *zoom* tahun 2022. Terlihat tabel diatas membuktikan bahwa *zoom* memiliki pengguna yang jauh lebih banyak di bandingkan dengan *platform* lain-nya, menurut data jumlah *download*

dari *playstore*. Yang di ambil pada tanggal 15 Juni 2022.

Serangan *Phishing* ini sering terjadi karena target tidak menyadari bahwa mereka sedang masuk kedalam jebakan dari si penyerang. Penyerang me*replikasi* sebuah *web* untuk menjebak korban masuk kedalam sebuah *web* yang tampilan-nya mirip dengan *platform* sasaran. Apabila penyerang mahir dalam pemrograman *web*, ini akan menjadi serangan yang sangat berbahaya. Karena mereka dapat me*replikasi* tampilan *web* sangat persis sama dengan pembuat atau *developer* aslinya. Sehingga, target tidak akan menyadari sama sekali kalau mereka meng*input*kan *data* akun mereka ke *web* yang salah.



Gambar 1.2 Artikel 26 Maret 2022 tentang banyaknya kasus phishing di tahun 2022

Pada gambar artikel diatas yang berasal dari *Liputan6* menunjukan bahwa jumlah serangan phishing di Indonesia mencapai Tiga ribu lebih kasus. Berbeda dengan serangan-serangan lain, phishing memanfaatkan kepolosan dari pengguna.

Yang mana ini bukan masalah dari system, melainkan human error. Hanya dengan penyedia hosting yang tidak memperhatikan bahaya serangan cyber atau siber dan kepolosan pengguna yang nantinya menjadi korban, penyerang dapat memanipulasi data email atau akun korban.

Oleh karena itu, dalam penelitian ini penulis akan memberikan pendalaman mengenai cara kerja serangan phishing ini. Dengan cara melakukan simulasi penyerangan, Sehingga di harapkan pembaca dapat sangat mengerti tentang bagaimana seorang penyerang atau attacker melancarkan serangan terhadap target dengan melakukan replikasi web. Dan bisa menjadi solusi untuk mengurangi kasus phishing yang terjadi di masa pendemi ini. Serta membuka wawasan pembaca dalam memahami apa yang di maksud dengan cyber attack dalam pembahasan ini, juga bahaya-nya terhadap manipulasi data yang dapat di salah gunakan oleh penyerang tersebut.

1.2 Rumusan masalah

Berdasarkan latar belakang masalah di atas, maka dapat disimpulkan permasalahan dari penelitian ini. yaitu:

a. Bagaimana melakukan identifikasi phishing lewat aplikasi zoom?
b. Bagaimana menganalisis perbedaan website phishing dibandingkan website asli dengan mengunakan zoom sebagai bahan analisis?

1.3 Tujuan Penelitian

Adapun tujuan yang ingin di capai dari penelitian ini adalah:

a. Memberikan Pemahaman kepada pengguna platform meeting zoom tentang bahaya-nya serangan phishing.
b. Dapat menganalisis perbedaan website phishing dan web asli.

1.4 Batasan Masalah

Adapun Batasan masalah pada penelitian ini, saya menentukan apa-apa saja yang akan saya gunakan untuk menyelesaikan penelitian ini :

a. Serangan phishing dilakukan melalui website.

b. Website dirancang menggunakan flutter. Flutter adalah framework multiplatform dengan Bahasa pemrograman Dart.
c. Hosting untuk menyimpan data website dan database server untuk menyimpan informasi korban. Database yang akan saya gunakan adalah Firebase dari google.
d. Platform *share* atau penyebaran phishing link menggunakan Gmail

1.5 Manfaat Penelitian

Adapun manfaat penelitian yang akan di dapatkan dari penelitian ini :

a. Penulis berharap masyarakat dapat memahami tentang bahaya dari salah satu serangan yang memanfaatkan kelalaian pengguna ini.
b. Masyarakat dapat membedakan seperti apa perbedaan bentuk antara website phising dan website aslinya.

1.6 Metodologi Penelitian

Pada penelitian ini penulis menggunakan metode penenlitian ekperimen yang menghasilkan data kualitatif. Lalu, terdapat juga beberapa elemen analisis dalam penelitian ini. Berikut ringkasan metode penelitian yang di gunakan:

a. Metode Penelitian Eksperimen, merupakan metode yang dilakukan melalui percobaan untuk menganalisis keberhasilan suatu penelitian.
b. Metode Analisis Komparatif, merupakan metode untuk menganalisis perbandingan antara dua hal.