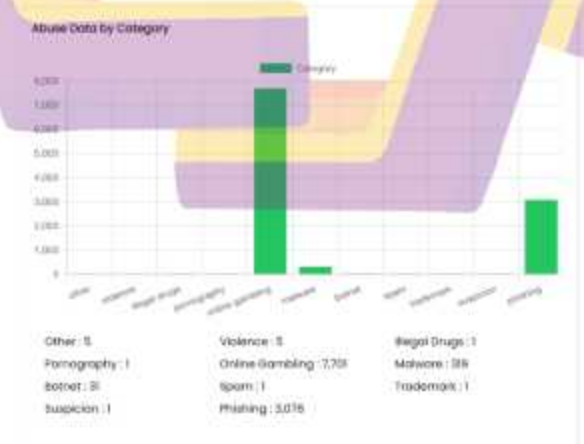
BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada era teknologi yang semakin berkembang, digitalisasi merupakan sebuah hal yang tidak dapat dihindari dan menjadi sebuah kebutuhan. Digitalisasi menawarkan kemudahan dalam mengakses berbagai macam informasi dan komunikasi yang dapat mempermudah masyarakat dalam melakukan pekerjaan. Digitalisasi diterapkan pada beberapa sektor salah satunya adalah sektor keuangan. Digitalisasi pada sektor keuangan menawarkan sebuah system yang dapat secara signifikan memberikan kemudahan dalam mengakses informasi terkait keuangan seperti pembuatan rekening, transfer uang, investasi, dan sebagainya secara daring. Namun, dengan adanya digitalisasi dalam sektor keuangan ini secara bersamaan menciptakan celah keamanan baru yang dapat dieksploitasi oleh penjahat siber. Kerentanan tersebut berupa *phishing*. *Phishing* didefinisikan sebagai serangkaian metode penipuan yang bertujuan untuk mendapatkan data sensitif terkait korban seperti nama pengguna dan kata sandi dengan cara menyamar sebagai entitas terpercaya.



Gambar 1. 1 laporan *domain abuse* dari IDADX [1]

Peningkatan frekuensi dan kompleksitas serangan *phishing* di Indonesia menunjukkan adanya evolusi pada taktik yang digunakan pelaku. Situasi terbaru menunjukkan bahwa kasus penipuan dan penipuan online di Indonesia semakin meningkat. Berdasarkan data dari Indonesia Anti-Scam Centre (IASC) yang berada di bawah Otoritas Jasa Keuangan (OJK), hingga 17 Agustus 2025, tercatat 225.281 laporan penipuan digital sejak November 2024. Dari total rekening yang terverifikasi, sebanyak 72.145 rekening telah diblokir. Total kerugian yang dilaporkan mencapai sekitar Rp4,6 triliun.[2]

Salah satu modus yang terjadi dalam tiga tahun terakhir adalah *phishing* dengan memanfaatkan isu perubahan tarif transfer yang menimpa nasabah bank BRI. *Phishing* tersebut dilakukan oleh seseorang yang mengatasnamakan pihak bank untuk mengarahkan korban untuk memasukkan data kredensial seperti *username* dan *password* pada situs yang diberikan.

Dampak dari kasus *phishing* ini sangat luas, tidak hanya menyebabkan kerugian finansial bagi nasabah yang saldonya terkuras, tetapi juga memicu krisis kepercayaan terhadap sistem keamanan perbankan digital secara keseluruhan [3].

Dengan mengkaji kasus tersebut, penelitian ini bertujuan untuk memberikan pemahaman secara garis besar terkait pola *phishing* dan memberikan edukasi agar terhindar dari *phishing*.

1.2 Rumusan Masalah

Berdasarkan apa yang sudah dijelaskan sebelumnya, adapun rumusan masalah dalam penelitian ini adalah :

1. Bagaimana tahapan serangan *phishing* tersebut dilakukan, ditinjau dari model *cyber kill chain*?
2. Prinsip manipulasi psikologis apa yang digunakan berdasarkan teori Cialdini?

1.3 Batasan Penelitian

Agar penelitian ini lebih terarah dan sesuai dengan rumusan masalah yang sudah disebutkan sebelumnya, peneliti membuat batasan masalah. Batasan masalah yang ditetapkan adalah:

1. Fokus analisis adalah temuan artefak digital terkait kasus *phishing* perubahan tarif yang terjadi pada periode 2022-2025.
2. Artefak digital yang dianalisis berupa tangkapan layar chat WhatsApp, tampilan situs *phishing*, dan struktur URL
3. Tidak melakukan investigasi forensik secara mendalam, tidak melacak server pelaku, dan tidak menganalisis sisi *backend* situs *phishing*
4. Demonstrasi bersifat ilustratif dengan menggunakan *tools open-source* (*zphisher*) berdasarkan template yang tersedia, bukan merekonstruksi situs asli.

1.4 Manfaat Penelitian

Dengan adanya penelitian ini, diharapkan dapat memberikan manfaat sebagai berikut:

Bagi nasabah

- Memberikan edukasi tentang ciri-ciri *phishing*
- Membantu masyarakat untuk mengenali pola rekayasa social yang sering digunakan pelaku *phishing* agar terhindar dari kasus yang sama

Bagi pihak perbankan

- Memberikan informasi mengenai kelemahan yang dimanfaatkan
- Menjadi dasar pengembangan system deteksi dan edukasi nasabah

1.5 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Mendeskripsikan tahapan *phishing* berdasarkan model *cyber kill chain*
2. Mengidentifikasi artefak digital yang digunakan pada kasus ini.
3. Mengidentifikasi faktor-faktor psikologis yang dieksploitasi berdasarkan teori yang dikemukakan oleh Cialdini.
4. Memberikan gambaran teknis melalui simulasi pembuatan situs *phishing* sebagai ilustrasi proses *credential harvesting*

1.6 Sistematika Penulisan

BAB I PENDAHULUAN, Bab ini berisis latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan penelitian, serta sistematika penulisan. Bab ini menjadi dasar bagi pembaca untuk memahami konteks dari penelitian ini

BAB II TINJAUAN PUSTAKA, Bab ini berisi tentang studi literatur yang mencakup penelitian-penelitian terdahulu yang relevan serta keaslian penelitian yang ditampilkan kedalam bentuk tabel.

BAB III METODE PENELITIAN, Bab ini berisi objek penelitian, alur penelitian dan alat dan bahan yang digunakan selama penelitian.

BAB IV HASIL DAN PEMBAHASAN, Bab ini merupakan tahapan dimana peneliti melakukan pembahasan hasil dari analisis dan melakukan demonstrasi *phishing*.

BAB V PENUTUP, berisi kesimpulan dan saran yang dapat peneliti rangkum dan sampaikan kepada pembaca.