**Pengertian Phising**  
Phising diambil dari kata dari bahasa inggris yakni “fishing” yang artinya memancing. Phising merupakan metoede kejahatan online dengan melakukan pencurian data untuk kepentingan individu yang tidak bertanggung jawab hingga merugikan orang lain.

Aktivitas phising memang bertujuan untuk memancing orang agar memberikan informasi pribadi tanpa di sadari korban. Umpan pancingan dapat berupa apa saja, mulai dari klik link internet sampai permintaan telepon. Setelah data berhasil dicuri, pelaku bebas menggunakan data korban untuk apa saja, termasuk kejahatan.

Cara kerja phising adalah korban dihubungi melalui berbagai kontak seperti telepon, email, atau pesan teks oleh seseorang menyamar sebagai lembaga sah untuk memancing korban agar memberikan data sensitif pribadi secara tidak sadar. Informasi pribadi paling umum diminta antara lain berupa no KTP, no rekening, rincian kartu kredit dan perbankan, hingga kata sandi.

**Jenis-Jenis Phising**

Ada beberapa jenis phising paling umum menimpa orang, yaitu antara lain:

1. Deceptive Phising

Deceptive phising adalah jenis penipuan dengan mengirimkan email atas nama lembaga untuk meminta korban melakukan beberapa aktivitas, seperti: verifikasi informasi akun, memberikan informasi username atau kata sandi, meminta korban untuk mengubah kata sandi, melakukan transaksi pembayaran.

Informasi di atas digunakan oleh peretas untuk mengakses kembali tanpa Anda ketahui kemudian dimanfaatkan agar memperoleh keuntungan.

Terdapat 2 cara deceptive phishing paling umum dilakukan oleh oknum. Cara pertama adalah pelaku menyamar atau mengklaim sebagai perwakilan dari lembaga resmi lalu meminta data diri korban. Sementara itu cara keduanya adalah pelaku berpura-pura menjadi lembaga dan memberikan situs berbahaya pada korban.

1. Smishing Phising

Smishing phising adalah jenis penipuan melalui SMS atau telpon guna memperoleh informasi pribadi. Kejahatan online ini lebih mudah memakan korban sebab orang cenderung lebih percaya dengan pesan teks atau telpon dibandingkan email.

Dalam smishing, pelaku akan berusaha membuat korban bersedia mengikuti apa yang dikatakannya. Setelah itu, pelaku biasanya akan memberi instruksi ke korban untuk melakukan hal-hal merugikan, seperti mengirim pulsa, menyebutkan nomor rekening, dan mengklik tautan tertentu.

1. Spear Phising

Spear phishing dilakukan dengan mengirim email ke target tertentu dengan mengaku sebagai pengirim terpercaya. Email tersebut berisi tautan yang mengarahkan calon korban ke situs web palsu penuh dengan malware, atau disebut juga dengan phising site.

Phising site adalah usaha penipuan untuk mengelabuhi korban menggunakan web atau situs palsu. Tujuannya agar pelaku mampu mencuri informasi sensitif seperti kredensial akun atau informasi keuangan dari korban.

1. Whale Phising

Whale phising adalah kejahatan phising ditujukan kepada seorang figur publik, dikenali banyak orang, kaya, dan memiliki kekuasaan. Sebab status calon korban besar, maka pelaku menganggapnya seperti ikan paus atau whale. Cara yang dilakukan sama dengan spear phising, tapi lebih terorganisir dan dilakukan oleh sekelompok orang.