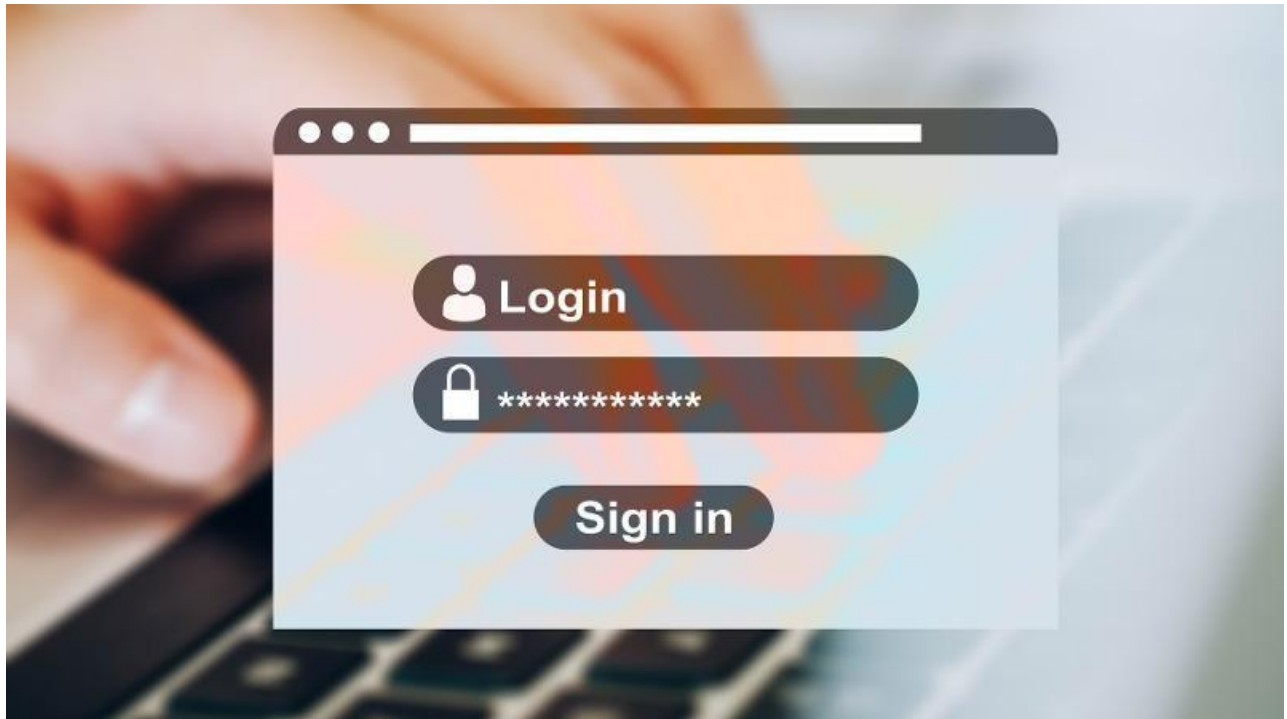


Two Factor Authentication (2FA)



Belakangan ini kerap kita dengar mengenai adanya kebocoran data atau hacking beberapa akun baik media sosial hingga akun e-commerce. Hal ini terjadi karena kurang kuatnya system keamanan yang diterapkan sehingga hacker dapat dengan mudah mengakses akun -akun tersebut.

Apa itu *Two factor authentication (2FA)*?

Two factor authentication sendiri adalah sistem keamanan yang membutuhkan dua jenis autentikasi yang dilakukan penggunanya. Sehingga jika biasanya untuk login pengguna hanya mengisi email & password maka jika menerapkan 2FA ini akan diminta Langkah lanjutan.

2FA Memiliki Beberapa Faktor

1. Something you know

Faktor pertama dari two factor authentication adalah something you know atau sesuatu yang kamu ketahui. Hal ini seperti email, PIN, atau password yang digunakan untuk log in ke suatu akun. Bisa juga merupakan pertanyaan seperti “nama ibu kandung”, atau “panggilan masa kecil” yang biasanya sudah diatur di awal membuat akun.

2. Something you have

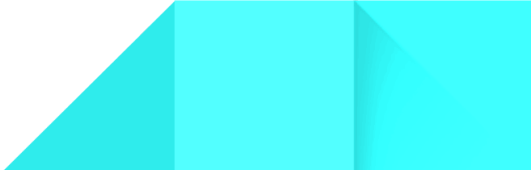
autentikasi yang dilakukan dengan mengandalkan sesuatu yang kamu punya. Contoh paling umum adalah autentikasi menggunakan smartphone. Pada contoh ini, sistem akan mengirimkan kode one-time password (OTP) atau link pada perangkat smartphone-mu. Tujuannya, untuk memastikan bahwa log in yang dilakukan akun tersebut memang dilakukan olehmu.

3. Something you are

Faktor terakhir pada two factor authentication adalah something you are, atau autentikasi yang dilakukan dengan sesuatu yang menjadi ciri khasmu. Faktor ini bisa dibilang hal yang paling sulit untuk dipalsukan atau bahkan ditiru oleh orang lain. Hal ini karena hanya kamu sendiri yang dapat melakukannya. Pada faktor ini, autentikasi dilakukan dengan pengamanan biometric seperti sidik jari, pengenalan wajah, hingga iris scanner.

Lalu Bagaimana Cara Kerja dari 2FA ini?

Ketika kamu melakukan login pada suatu website maka kamu diminta untuk memasukkan salah satu factor dari 2FA kemudian akan diminta memasukkan factor lain selain factor



pertama. Sebagai contoh : pertama kamu diminta untuk memasukkan password, disini password masuk dalam factor something you know kemudian Langkah selanjutnya kamu diminta verifikasi sidik jari, dimana sidik jari masuk dalam factor something you are. Maka ini dapat dibilang 2FA sudah diterapkan. Namun ketika keduanya masuk dalam 1 faktor yang sama (semisal sama sama something you know) maka ini bukan 2FA