How Secure is Your Password?

Oleh : Widyatari Hayuningtyas Winarto

Penggunaan username dan password sudah menjadi kebutuhan sehari-hari yang digunakan seseorang untuk dapat masuk ke suatu situs. Data-data penting akan tersimpan dalam akun online. Namun, dengan banyaknya aplikasi yang digunakan sering kali membuat penggunanya lupa dengan akun dan password. Salah satu solusi untuk permasalahan tersebut yaitu adanya sistem login Single Sign On (SSO). Sistem Single Sign On membuat pengguna hanya perlu sekali melakukan login untuk dapat mengakses beberapa aplikasi sehingga tidak perlu mengingat banyak username dan password yang digunakan.

Akhir-akhir ini, banyak sekali terjadi serangan cyber dan pembobolan data yang dilakukan oleh sekelompok orang tidak bertanggung jawab. Data maupun informasi menjadi target serangan sehingga perlu dijaga keamanannya. Kesalahan paling umum yang dilakukan pengguna akun adalah memilih password yang lemah dan umum. Oleh karena itu diperlukan otentikasi untuk mengamankan data atau sistem dari pihak ketiga. Password yang aman adalah password yang sulit atau tidak dapat ditebak atau dipecahkan menggunakan brute force attack, meskipun secara teoritis password apapun dapat diretas menggunakan serangan password bagaimanapun kompleksitas dari password tersebut. Berikut beberapa tips membuat password yang kuat dan aman.

1. Password terdiri dari kombinasi huruf besar dan huruf kecil, angka dan simbol khusus, seperti tanda baca.
2. Panjang password minimal 8 karakter. Semakin panjang password maka semakin bagus.
3. Penggunaan pola sebaiknya dihindari dalam pembuatan password, misalnya '12345'.
4. Password harus berupa sesuatu yang sulit ditebak oleh orang lain. Buatlah password seunik mungkin.
5. Jangan gunakan jalur keyboard berurutan dan sesuatu yang bersifat pribadi.
6. Gunakan password berbeda untuk setiap akun atau aplikasi.

Pembuatan password yang unik saja tidak cukup untuk mengamankan data. Penyimpanan password juga penting dilakukan untuk menjaganya tetap aman dan terlindungi dari peretas. Hal yang wajib dilakukan untuk meningkatkan sekuritas terhadap keamanan password yaitu :

1. Gunakan pengelola kata sandi yang bagus dan terpercaya.
   Pengelola kata sandi yang aman dapat menghasilkan, menyimpan, dan mengelola semua kata sandi atau password dalam satu akun online hanya dengan satu "kata sandi utama".
2. Gunakan otentikasi 2 faktor (2FA)
   Otentikasi 2 faktor adalah penambahan lapisan keamanan tambahan. 6Siapapun yang mencoba masuk ke akun kita harus memasukkan informasi kedua setelah password yang benar.
3. Jangan simpan password di ponsel, tablet, atau perangkat komputer.
4. Ganti password secara berkala.
5. Jaga kerahasiaan password dan jangan berikan kepada orang lain.

Sistem login merupakan suatu hal yang pasti ditemukan dalam dunia internet. Saat kita melakukan login, pasti akan memasukkan password dimana password tersebut bersifat privasi dan rahasia. Oleh karena itu, masalah keamanan menjadi masalah yang sangat penting. Seiring dengan banyaknya fasilitas internet yang membutuhkan akses masuk (login), maka kita perlu lebih berhati-hati terutama jika akun yang kita miliki sangat rahasia dan berharga mengingat internet merupakan jaringan publik. Salah satu upaya peningkatan keamanan data atau informasi adalah dengan penggunaan password yang unik dan panjang.

Referensi :

Khairina, D. M. (2016). Analisis Keamanan Sistem Login. *Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer*, 6(2), 64-67.

Komalasari, R. (2018). Kesadaran akan Keamanan Penggunaan Username dan Password. *Tematik: Jurnal Teknologi Informasi Komunikasi (e-Journal)*, 5(2), 141-152.

https://cybernews.com/best-password-managers/how-to-create-a-strong-password/

https://www.djkn.kemenkeu.go.id/artikel/baca/14939/Tips-Memilih-Password-Yang-Aman.html

Link video youtube : https://youtu.be/4eUm1pVbglA