Pintar
Opini Untar

Volume 1 | Halaman 141 – 143 | 8 Desember 2020
ISSN: 2746 - 9018

PENGATURAN KEAMANAN WI-FI ROUTER DI MASA PANDEMI

*Yohanes Calvinus

Editor: Bagus Mulyawan

Tentu kita sudah sangat dekat dengan penggunaan Wi-Fi dalam kehidupan sehari-hari bahkan tanpa sinyal Wi-Fi hidup rasanya sangat merana. Namun kita tak menyadari bahwa sinyal Wi-Fi bisa menjadi polusi. Mengapa bisa dibilang polusi? Ya, bagaimana tidak? pernahkah kita mencoba menggunakan sinyal Wi-Fi di salah satu tempat mall dan coba kita iseng mencari koneksi Wi-Fi di HP yang kita gunakan. Mungkin kita kaget nama koneksi Wi-Fi di dalam mall tersebut sangat banyak! Itulah terjadi polusi Wi-Fi.

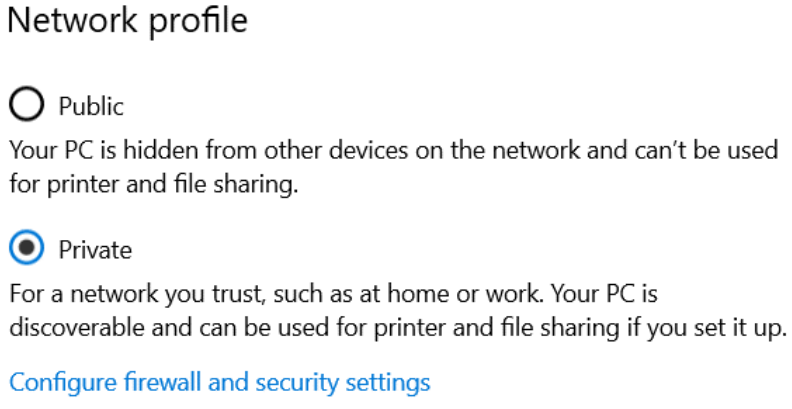
Kondisi pandemi saat ini membuat kebutuhan akan internet meningkat. Seiring peningkatan itu pula di area perumahan penggunaan *broadcast* Wi-Fi internet meningkat. Perlu diingat bahwa Wi-Fi bukanlah internet. Wi-Fi merupakan gelombang radio yang memiliki standar untuk digunakan sebagai media perantara pemancar dan penerima dalam hal ini seperti *Smartphone*, komputer dan lain-lain.

Untuk menghubungkan koneksi internet menggunakan Wi-Fi tentunya pemancar memancarkan suatu identitas melalui sebuah portal yang dinamakan *router* atau *internet gateway*. Identitas tersebut disebut SSID yang memiliki kepanjangan (*Service Set Identifier*) ibaratkan seperti KTP bagi Portal yang menyediakan jaringan internet dengan menggunakan jaringan gelombang Wi-Fi. Nah untuk di area perumahan, SSID internet Wi-Fi dapat saling dikenali dengan mudah apabila ternyata nama SSID tersebut disesuaikan dengan identitas si pemilik yang mengandung nama ataupun alamat. Tentunya hal ini dapat mengundang orang yang berniat jahil untuk melakukan peretasan pada alamat SSID Wi-Fi tersebut. Agar tidak menjadikan polusi SSID Wi-Fi di area perumahan dan mengundang niat jahil seseorang ada baiknya SSID Wi-Fi dibuat tersembunyi.

Keamanan router Wi-Fi di masa pandemi dirasa sangat perlu dikarenakan penggunaan di masa pandemi yang sangat tinggi menemani kebosanan di rumah. Ada 3 hal yang perlu diperhatikan dalam menjaga keamanan Wi-Fi *router* di rumah. Hal pertama yaitu pastikan Wi-Fi *router* anda menggunakan *password* yang aman yaitu mengandung Huruf besar dan kecil, angka dan huruf serta

Pintar
Opini Untar
Volume 1 | Halaman 141 – 143 | 8 Desember 2020
ISSN: 2746 - 9018

penggunaan tanda baca sangat dianjurkan. Hal Kedua, aktifkan sistem *Firewall* dan nyalakan fitur DMZ (*Demilitarized Zone*) yang merupakan fitur keamanan untuk membatasi jaringan Umum dan jaringan privasi. Hal Ketiga, menyembunyikan SSID Wi-Fi *Router* sehingga tidak mudah ditemukan dan diretas dengan mudah.



Pintar
Opini Untar

Volume 1 | Halaman 141 – 143 | 8 Desember 2020
ISSN: 2746 - 9018

Beberapa penyedia layanan sistem internet sebenarnya memiliki keamanan tersendiri yaitu dengan mengacak sistem keberadaan *IP Public* yang umumnya disebut *Dynamic Address*. Jaringan internet yang memiliki sistem *Dynamic Address* ini boleh dikatakan memiliki keuntungan pada sistem keamanan bagi penggunanya namun tidak lepas dari kerugian juga bagi beberapa pengguna. Kerugian yang dialami adalah jika pada suatu saat sistem pengacak *Dynamic IP* tersebut menempatkan pengguna pada alamat IP yang terekam untuk di blokir maka akan ada ketidaknyamanan bahwa pengguna tidak dapat mengakses suatu situs hingga halaman internet tertentu.

Jadi setiap internet yang terkoneksi akan memiliki 2 alamat IP yaitu *IP Public* (umum) dan *IP Private* (Privasi). *IP Public* dapat di cek dengan mengunjungi situs pengalamatan IP seperti *whatismyip.com, myip.com* dan masih banyak lagi. Untuk menjaga keamanan pastikan 3 hal utama dalam menjaga keamanan internet di rumah yaitu dengan p*assword* yang terkombinasi angka, huruf, dan tanda baca kemudian pastikan sistem *firewall* dan DMZ (*Demilitarized Zone*) pada Wi-Fi *router* aktif atau menyala dan yang paling penting adalah menyembunyikan SSID Wi-Fi *router*. Serta ketahui bahwa internet yang digunakan menggunakan *Dynamic IP address*. Pastikan menggunakan internet dengan bijak sebab banyak juga dari aplikasi internet yang berkedok menawarkan sistem VPN (*Virtual Private Network*) ternyata merupakan suatu sistem peretas yang berbahaya bagi keamanan pengguna internet di rumah.

Tips bagi penggunaan komputer juga perlu diatur agar dapat belajar dan bekerja dengan lebih cepat yaitu dengan tetap mengatur jaringan internet yang terhubung dengan Wi-Fi *router* di rumah dengan memilih jaringan *private* (pribadi) namun harus memperhatikan bahwa *setting* Wi-Fi *router* telah diatur sedemikian aman. Apabila sistem pada komputer diatur pada pengaturan publik atau umum maka sistem komputer akan menjalankan protokol keamanan sendiri yang akan menghambat koneksi internet sehingga penggunaan internet pada komputer akan terasa lambat.

*Dosen Fakultas Teknik Universitas Tarumanagara