

OUCH!

Buletin Bulanan Keamanan Komputer

# Virtual Private Networks (VPN)

## Sekilas

Anda terkadang perlu menggunakan Wi-Fi umum untuk mengakses internet pada saat di luar rumah, atau saat berada di restoran, kedai kopi, hotel atau lapangan udara. Seberapa aman jaringan Wi-Fi umum ini, adapa ada yang mengamati dan merekam setiap jejak langkah digital daring Anda? Bisa jadi Anda juga tidak percaya pada penyedia jasa internet (ISP) di rumah dan ingin memastikan bahwa setiap aktifitas daring Anda tidak diawasi. Aktifitas daring dan privasi bisa lebih diamankan dengan solusi VPN (Virtual Private Network). VPN merupakan solusi teknologi yang menciptakan jalur khusus terenkripsi sehingga menyulitkan pihak lain meneliti atau mengawasi aktifitas daring Anda. Selain itu, VPN juga menjaga kerahasiaan lokasi Anda, ini menyulitkan sebuah situs web untuk bisa menentukan lokasi Anda.

## Cara Kerja VPN

VPN bekerja dengan menciptakan jalur khusus terenkripsi ke penyedia jasa layanan VPN. Semua aktifitas daring akan melalui jalur ini, tersambung ke penyedia jasa VPN untuk diteruskan ke tujuan akhir. Sebagai contoh: bila Anda berada di Surabaya, Jawa Timur dan Anda terhubung ke server VPN Di Tokyo, Jepang, semua situs web yang Anda akses akan mengira Anda tersambung dari Tokyo, Jepang. VPN mudah sekali digunakan. Pertama-tama temukan penyedia jasa VPN yang bisa dipercaya dan lakukan registrasi. Setelah memiliki akun, dilanjutkan dengan mengunduh, install dan mengkonfigurasi perangkat lunak VPN. Sekali terpasang, sambungan ke internet akan berjalan seperti biasa. Perangkat lunak VPN secara otomatis menciptakan jalur khusus terenkripsi dan melakukan perlindungan privasi.

## Memilih Penyedia Jasa VPN

Memilih penyedia jasa layanan VPN adalah perlu dan penting. Ingat beberapa hal di bawah ini dalam proses seleksi penyedia jasa VPN.



**Logging:** Pilih penyedia jasa yang tidak melakukan logging/pencatatan aktifitas secara detail. Dengan tidak melakukan hal ini, tidak mudah bagi pihak lain untuk melacak ulang semua aktifitas Anda.



**Lokasi Fisik Perusahaan:** Penyedia jasa VPN ada di banyak negara. Pastikan perusahaan itu berada di negara dengan hukum privasi yang baik. Di tempat dimana hukum privasi lemah, tidak tertutup kemungkinan adanya tekanan/upaya untuk mendapatkan informasi seputar aktifitas Anda.



**Server:** Pilih penyedia jasa VPN dengan server di negara atau kota yang dibutuhkan. Beberapa bisnis VPN memiliki ribuan server tersebar di seluruh dunia. Bila Anda membutuhkan sambungan internet seakan-akan berasal dari sebuah negara, bisakah penyedia jasa VPN menyediakan solusinya.



**Kecocokan:** Cari solusi yang bisa menyediakan layanan di beragam komputer dan alkom. Misal: bisa digunakan di laptop Windows, tablet atau iPhone. Ada baiknya fasilitas VPN itu bisa memenuhi berbagai kebutuhan itu.



**Jangan Pilih Gratis:** Waspada pada label “Gratis” dalam jasa VPN. Bila tanpa bayar, bagaimana bisnis VPN itu bisa tumbuh dan berkembang. Bisa jadi dengan cara mengumpulkan dan menjual informasi Anda.

VPN adalah solusi jitu dalam perlindungan privasi. Namun VPN tidak memberikan perlindungan pada komputer, peralatan dan akun daring. Jadi, meskipun sudah menggunakan VPN, tetap patuhi langkah-langkah pengamanan dasar, diantaranya memastikan pembaruan peralatan, menggunakan kunci layar (screen-lock) dan selalu menggunakan sandi yang kuat dan berbeda untuk setiap akun.

## Versi Bahasa Indonesia

BIPIMax memberikan Pelatihan Optimasi Proses Bisnis (LSS) dan Pengenalan Keamanan & Proteksi Informasi. Informasi lengkap: <http://www.bipimax.net>

## Editor Tamu

**Phil Johnsey (@peakreflections)** adalah seorang profesional IT di Palm Beach County dalam bidang keamanan, forensik dan audit. Bersertifikat SANS dalam forensik digital, dasar-dasar keamanan dan sebagai anggota OUCH community review board. Phil berkeinginan menjadikan hal keamanan mudah dipahami setiap orang.



## Sumber Pustaka

Making Passwords Simple: <https://www.sans.org/u/Sd8>

Securing Your Mobile Devices: <https://www.sans.org/u/Sdd>

Stop Malware: <https://www.sans.org/u/Sdi>

OUCH! diterbitkan oleh SANS “Security Awareness” dan didistribusikan sesuai lisensi [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Anda diperkenankan menyebarkan buletin ini atau menggunakannya di dalam program pembelajaran sejauh tidak melakukan perubahan isi buletin. Untuk keperluan alih bahasa atau informasi lainnya, silakan menghubungi [www.sans.org/security-awareness/ouch-newsletter](http://www.sans.org/security-awareness/ouch-newsletter). Dewan Redaksi: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Diterjemahkan oleh: T. Gunawan