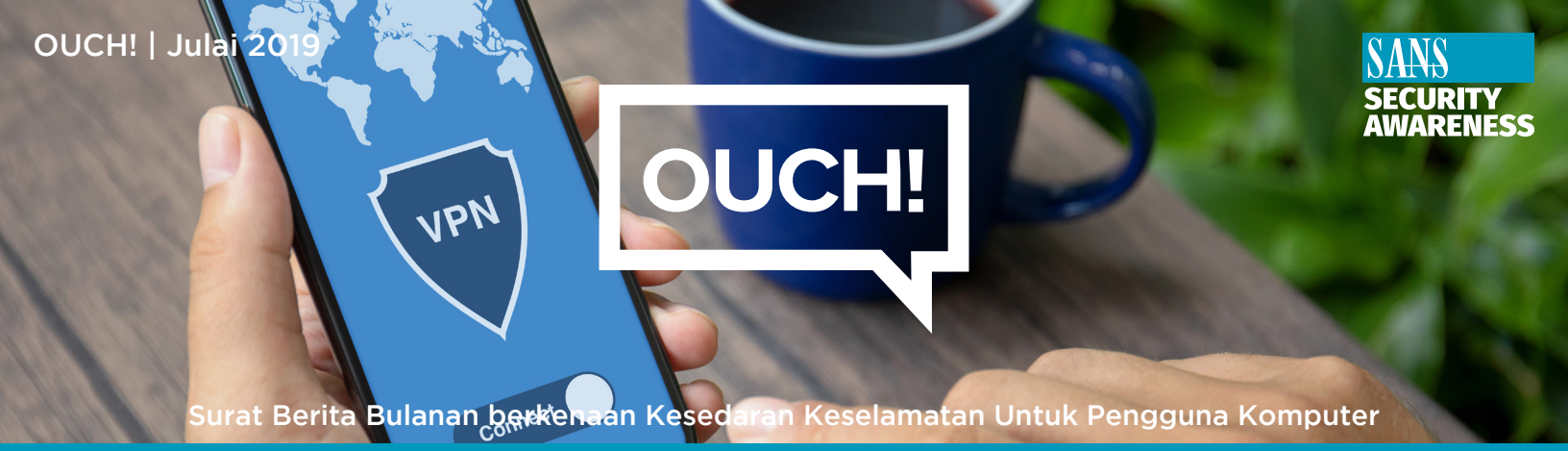

SANS SECURITY AWARENESS

Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

Rangkaian Peribadi Maya (VPN)

Gambaran Keseluruhan

Anda mungkin berada di dalam situasi yang memerlukan anda untuk menggunakan Wi-Fi umum untuk mendapatkan capaian Internet ketika anda keluar dari rumah, seperti ketika anda berada di restoran atau kedai kopi atau ketika anda sedang berada di dalam hotel sewaktu melancong atau di dalam lapangan terbang. Tetapi apakah tahap keselamatan rangkaian umum tersebut atau siapa yang sedang memerhati atau merakamkan apa yang anda sedang lakukan dalam talian? Mungkin juga anda tidak mempercayai penyedia perkhidmatan Internet (ISP) untuk rumah anda dan ingin memastikan mereka tidak boleh memantau apa yang anda lakukan dalam talian. Anda boleh lindungi aktiviti dalam talian dan privasi anda dengan menggunakan Rangkaian Peribadi Maya (VPN). VPN adalah teknologi yang mewujudkan sebuah terowong peribadi dan tersulit untuk aktiviti dalam talian anda sehingga menjadikannya lebih sukar bagi sesiapa untuk menonton atau memantau apa yang anda lakukan dalam talian. Di samping itu, VPN membantu menyembunyikan lokasi anda menjadikannya lebih sukar bagi laman web yang anda lawati untuk menentukan lokasi anda.

Bagaimana VPN berfungsi?

VPN berfungsi dengan mencipta sebuah terowong peribadi dan tersulit kepada penyedia VPN yang anda pilih. Segala aktiviti dalam talian anda akan melalui terowong ini, kemudian melepasi rangkaian penyedia VPN kepada destinasi yang dituju. Contohnya, jika anda berada di Tampa, Florida dan anda bersambung kepada pelayan VPN di Munich, Jerman, sebarang laman web yang anda layari akan menganggap anda sedang berhubung dari Munich, Jerman. VPN mudah untuk digunakan. Langkah pertama ialah mencari penyedia VPN yang anda percaya kemudian mencipta akaun dengan penyedia tersebut (selalunya anda perlu membeli perkhidmatan tersebut). Apabila anda sudah mempunyai akaun, anda perlu memuat turun, memasang dan membuat konfigurasi perisian VPN tersebut. Setelah anda membuat pemasangan dan konfigurasi, anda boleh menggunakan Internet seperti biasa. Perisian VPN tersebut akan mencipta terowong tersulit secara senyap untuk anda dan mula melindungi privasi anda tanpa anda sedari.

Memilih Penyedia VPN

Aktiviti dalam talian anda selamat dan peribadi bergantung kepada penyedia VPN anda. Oleh itu, pastikan anda memilih penyedia perkhidmatan yang anda boleh percaya. Berikut merupakan beberapa perkara utama ketika memilih penyedia perkhidmatan VPN.

Pengelogan: Pilih penyedia perkhidmatan yang tidak menyimpan sebarang log dan memberikan tumpuan kepada privasi. Sekiranya penyedia perkhidmatan VPN anda tidak mengumpul sebarang log, lebih sukar bagi sesiapa untuk menjejak apa yang anda pernah lakukan dalam talian.

Pusat Syarikat: Penyedia VPN yang berlainan berpusat di negara yang berbeza. Pastikan anda memilih penyedia VPN yang berpusat di negara yang menguatkuasakan undang – undang privasi. Penyedia VPN yang berpusat di negara yang tidak menekankan penguatkuasaan undang – undang privasi barangkali akan dipaksa untuk menyerahkan maklumat yang di kumpul mengenai anda.

Pelayan: Cari penyedia perkhidmatan VPN yang mempunyai pelayan di negara atau bandar yang anda mahukan. Sekiranya anda perlu memastikan perhubungan anda kelihatan datang dari negara tertentu, adakah penyedia perkhidmatan VPN anda mampu melakukan perkara tersebut?

Keserasian: Cari perkhidmatan yang berfungsi dengan komputer dan peranti mudah alih yang berlainan. Sebagai contoh, anda mungkin menggunakan komputer riba Windows, tablet dan iPhone. Justeru, anda perlu menggunakan perkhidmatan VPN yang berfungsi dengan semua peranti tersebut.

Elakkan yang Percuma: Berwaspada dengan perkhidmatan VPN yang "percuma", bagaimana mereka menjana pendapatan dan masih kekal dalam perniagaan? Perkhidmatan yang percuma mungkin sebenarnya mengumpul dan menjual maklumat anda.

VPN merupakan cara yang hebat untuk membantu melindungi privasi dalam talian. Walaubagaimanapun, VPN tidak melakukan apa-apa untuk menjamin komputer, peranti atau akaun dalam talian anda. Jadi, walaupun anda menggunakan VPN, pastikan anda sentiasa mematuhi langkah asas keselamatan, termasuklah memastikan peranti anda sentiasa dikemaskini, menggunakan pengunci skrin dan sentiasa gunakan kata laluan yang kukuh dan unik untuk semua akaun anda.

Penterjemahan oleh SNSC.

Pusat Keselamatan Rangkaian SKMM (SKMM Network Security Centre- SNSC) beroperasi di bawah Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) dengan matlamat menjamin keselamatan maklumat, kebolehpercayaan dan keutuhan rangkaian di Malaysia. Laman Web: http://snsc.skmm.gov.my/.

Editor Jemputan

Phil Johnsey *(@peakreflections) merupakan seorang pakar IT di Palm Beach County yang berpengalaman di dalam bidang keselamatan, forensik dan audit. Beliau mempunyai sijil pentauliahan dari SANS di dalam bidang forensik digital, asas keselamatan, dan merupakan salah seorang ahli lembaga di dalam komuniti pengulas OUCH. Beliau cenderung untuk menjadikan keselamatan mudah untuk semua orang.*

Sumber

Memudahkan Kata Laluan: https://www.sans.org/u/Sd8
Menjamin Peranti Mudah Alih: https://www.sans.org/u/Sdd
Hentikan Perisian Hasad: https://www.sans.org/u/Sdi