Security Culture 101/I (PC, Laptop, dan perangkat digital lainnya)

Kolaborasi Palang Hitam Anarkis dan Kolektif Eyes and Ears (Prancis)

Palang Hitam Indonesia,

23/12/2020

Daftar Isi

Panduan singkat mengenai Tor Browser dan RiseUp VPN

"Bisakah lembaga negara mengetahui situs web yang kita kunjungi, dan mengetahui apa yang kita lakukan di situs web tersebut?". Pertanyaan mendasar dalam hal ini:

- Jika menggunakan Tor untuk menjelajahi internet, maka komputermu tidak akan disusupi, lembaga Negara hanya dapat mengetahui bahwa kamu menggunakan Tor, dan tidak ada informasi yang lain.Untuk info lebih lanjut dan praktik yang lebih baik saat menggunakan Tor, kamu dapat membaca "Apakah saya benar-benar anonim jika saya menggunakan Tor?" kamu dapat lebih lengkap menpelajari tautan ini : `https://support.torproject.org`
- Dengan cara kerja yang serupa, jika kamu menggunakan riseup VPN untuk menjelajahi internet, jika komputermu serta layanan RiseupVPN tidak disusupi, maka lembaga Negara hanya dapat mengetahui bahwa kamu hanya menggunakan layanan VPN, dan tidak ada informasi yang lain.Untuk info lebih lanjut tentang batasan layanan VPN, kamu dapat membaca dokumentasi Riseup pada tautan ini: `https://riseup.net/en/vpn/limitations`
- Jika kamu tidak menggunakan Tor atau VPN untuk menjelajahi internet. Negara dapat mengklaim dan memutuskan untuk menargetkan kamu secara khusus, mereka dapat dengan mudah tahu di mana lokasi kamu mengakses Internet, mereka dapat meminta Penyedia Layanan Internet untuk memata-matai kamu, dan memberikan informasi pribadimu serta tahu situs web mana yang kamu kunjungi, atau bahkan mereka dengan mudah tahu aktivitas yang kamu lakukan di internet.

1) Tentang penyusupan komputer

Komputer dapat disusupi dengan dua tingkat:

- Pada tingkat perangkat lunak *(sofware)*, virus dapat diinstall pada komputermu (baik dari jarak jauh atau dengan akses langsung (fisik)). Kemungkinan ini sangat tergantung pada sistem operasi mana yang kamu gunakan (Windows, Linux, Tails…). Perangkat lunak yang kamu gunakan juga bisa memiliki bug (kelemahan), yang dapat digunakan dari jarak jauh untuk memata-mataimu. Ini kembali lagi bergantung pada sistem operasi mana yang kamu gunakan.
- Pada tingkat perangkat keras *(hardware)* , seseorang dengan akses langsung (fisik) ke komputermu dapat memodifikasinya untuk memata-matai kamu, meskipun praktik semacam ini mungkin jarang terjadi.

2) Untuk informasi lebih lanjut

Seperti yang kami katakan, jenis pengawasan atau kemanan digital ini bukan spesialisasi kami, jadi kami tidak begitu yakin untuk dapat menawarkan saran yang baik. Untuk informasi lebih lanjut tentang subjek ini, kamu dapat membaca panduan lain seperti, "panduan Riseup tentang keamanan" di tautan ini: `https://riseup.net/en/security`

3) Apakah saya benar-benar anonim jika saya menggunakan Tor?

Pada umumnya tidak mungkin untuk memiliki anonimitas yang sempurna, bahkan dengan Tor sekalipun. Meskipun ada beberapa hal lain yang dapat kamu praktikkan untuk meningkatkan anonimitas kamu saat menggunakan Tor maupun dalam aktivitas harian.

4) Gunakan Tor Browser dan perangkat lunak yang dikonfigurasi khusus untuk Tor.

Tor tidak melindungi semua lalu lintas internet komputermu saat kamu menjalakannya. Tor hanya melindungi aplikasi yang dikonfigurasi dengan benar untuk mengirim lalu lintas Internet mereka melalui Tor.

Aplikasi Browser

- Aman: Tor Browser
- Tidak aman: Browser lain yang dikonfigurasi untuk menggunakan Tor sebagai proxy

Aplikasi Berbagi Data

- Aman: OnionShare
- Tidak aman: BitTorrent melalui Tor

5) Mengontrol informasi apa yang akan kamu berikan melalui formulir web

Jika kamu mengunjungi situs web menggunakan Tor Browser, mereka tidak akan tahu siapa kamu atau dimana lokasi kamu yang sebenarnya. Sayangnya banyak situs web meminta informasi yang lebih personal, daripada yang mereka butuhkan melalui formulir web. Jika kamu masuk ke situs web tersebut, mereka masih belum tahu dimana lokasimu tetapi mereka tahu siapa kamu. Selanjutnya, jika kamu memberikan: nama, email, alamat, nomor telepon, atau informasi personal lainnya, kamu tidak lagi menjadi anonim di situs web tersebut. Pertahanan terbaik adalah waspada dan sangat berhati-hati saat mengisi formulir web.

6) Jangan gunakan Torrent melaui Tor

Aplikasi berbagi file Torrent telah diobservasi untuk mengabaikan pengaturan proxy dan membuat koneksi langsung bahkan ketika ada pemberitahun menggunakan Tor sebgai browser bawaan (*Default)* komputermu. Bahkan jika aplikasi torrent kamu hanya terhubung melalui Tor, kamu akan sering mengirimkan alamat IP asli dan mengizinkan pelacakan, karena itulah cara kerja torrents. Kamu tidak hanya meng deanonimkan lalu lintas torrent kamu dan lalu lintas web Tor simultanmu dengan cara ini, kamu juga memperlambat seluruh jaringan Tor untuk orang lain.

7) Jangan aktifkan atau instal plugin browser

Tor Browser akan memblokir plugin browser seperti Flash, RealPlayer, Quicktime, dan yang lainnya: mereka dapat dimanipulasi untuk mengungkapkan alamat IPmu. Demikian pula, kami tidak merekomendasikan untuk menginstal addons atau plugin tambahan ke Tor Browser, karena ini dapat memanipulasi Tor atau membahayakan anonimitas dan privasimu.

8) Menggunakan situs web versi https

Tor akan mengenkripsi lalu lintasmu ke dalam jaringan Tor, tetapi enkripsi lalu lintasmu ke situs web tujuanmu tergantung pada situs web tersebut. Untuk membantu memastikan enkripsi pribadi ke situs web, Tor Browser menyertakan *HTTPS Everywhere* untuk memaksa penggunaan enkripsi HTTPS untuk situs web yang mendukung. Namun, kamu masih harus melihat bilah URL browser untuk memastikan bahwa situs web yang kamu berikan informasi personal untuk menampilkan ikon gembok atau ikon bawang (lambang Tor) di bilah alamat, dan menyertakan https:// di URL. Lihat juga grafik interaktif EFF yang menjelaskan bagaimana Tor dan HTTPS berhubungan.

9) Jangan buka dokumen yang diunduh melalui Tor saat online

Tor Browser akan memperingatkan kamu sebelum secara otomatis membuka dokumen yang dimiliki oleh aplikasi eksternal (diluar Tor). **JANGAN ABAIKAN PERINGATAN INI.** Kamu harus sangat berhati-hati saat mengunduh dokumen melalui Tor (terutama file DOC dan PDF, kecuali kamu menggunakan penampil PDF yang disertakan dalam Tor Browser) karena dokumen-dokumen ini dapat berisi sumber data IP kamu yang akan diunduh di luar Tor oleh aplikasi yang membukanya. Ini akan mengungkapkan alamat IP non-Tor kamu. Jika Kamu harus bekerja dengan file yang diunduh melalui Tor, kami sangat menyarankan untuk menggunakan komputer yang terputus, atau menggunakan dangerzone untuk membuat file PDF aman sehingga dapat kamu buka. Namun, dalam keadaan apa pun lebih aman untuk menggunakan BitTorrent dan Tor serta memutus jaringan saat ingin membuka file yang telah terdownload dari aplikasi browser manapun.

10) Menggunakan *bridges*

Tor mencoba mencegah peretasan dan mempelajari situs web tujuanmu yang ingin disambungkan.Namun, secara *default*, itu tidak mencegah seseorang melihat lalu lintas Internet kamu, dari mengetahui bahwa kamu menggunakan Tor. **Jika ini penting bagi kamu**, kamu dapat mengurangi risiko ini dengan mengonfigurasi Tor untuk menggunakan *bridges* daripada terhubung langsung ke jaringan Tor. Pada akhirnya perlindungan terbaik adalah pendekatan sosial: semakin banyak pengguna Tor di dekat kamu maka semakin beragam minat mereka, semakin sedikit maka akan menjadi berbahaya jika kamu adalah salah satunya atau hanya satu satunya.Yakinkan orang lain untuk menggunakan Tor, juga!

Jadilah pintar dan pelajari lebih lanjut. Pahami apa yang dapat dilakukan dan tidak ditawarkan Tor.Daftar perangkat atau hambatan yang dijelaskan ditas belum lengkap, dan kami memerlukan bantuan kamu untuk mengidentifikasi dan mendokumentasikan semua masalah.

Riseup VPN berbagi beberapa batasan yang umum bagi semua VPN pribadi:

- **Peringatan hukum**: Jika Kamu tinggal dalam Negara/Wilayah non-demokrasi, mungkin ilegal untuk menggunakan VPN pribadi untuk mengakses internet.
- **Info lokasi**: Menggunakan VPN di perangkat selulermu akan mengamankan koneksi data, tetapi perusahaan telepon masih akan mengetahui lokasi kamu dengan merekam pemancar mana yang dikomunikasikan/ tersambung ke perangkatmu.
- **Keamanan Perangkat**: VPN membantu mengamankan informasimu saat menjelajahi internet, tetapi tidak mengamankan informasimu saat berada di penyimpanan internal komputer mu atau di server jarak jauh (cloud).
- **Koneksi yang tidak aman tetaplah tidak aman**: Meskipun Riseup VPN akan menganonimkan lokasi kamu dan melindungi kamu dari pengawasan ISP, setelah data kamu dialihkan dengan aman melalui riseup.net itu akan keluar di internet seperti biasanya. Oleh karena itu, kamu masih harus menggunakan koneksi aman (TLS) ketika tersedia (yaitu https, imap, dll).
- **VPN bukan obat mujarab**: meskipun VPN melakukan banyak hal, mereka tidak dapat memperbaiki semuanya. Misalnya, tidak dapat meningkatkan keamananmu jika komputer kamu sudah disusupi oleh virus atau spyware. Jika kamu memberikan informasi personal ke situs web, ada sedikit cara yang dapat dilakukan VPN untuk mempertahankan anonimitasmu di Internet. Untuk informasi selengkapnya, lihat VPN anonymity.
- **Internet mungkin menjadi lebih lambat**: Riseup VPN merutekan semua lalu lintas kamu melalui koneksi terenkripsi ke net sebelum melalui internet pada umumnya. Langkah ekstra ini dapat memperlambat segalanya. Untuk meminimalkan perlambatan, cobalah untuk memilih server VPN yang dekat dengan tempat kamu sebenarnya tinggal.

- **VPN mungkin sulit dikonfigurasi**: Meskipun kami telah mengambil langkah-langkah untuk membuatnya semudah mungkin, VPN apa pun memperkenalkan kompleksitas ekstra pada pengaturan jaringan kamu.

11) Keamanan / Anonimitas VPN

Koneksi yang tidak aman tetaplah tidak aman: Meskipun Riseup VPN akan menganonimkan lokasi kamu dan melindungi kamu dari pengawasan ISP, setelah data kamu dialihkan dengan aman melalui riseup.net itu akan keluar di internet seperti biasanya. Oleh karena itu, kamu masih harus menggunakan koneksi aman (TLS) ketika tersedia (yaitu https, imap, dll).

Selain itu, seberapa anonimkah RiseupVPN? Setiap kali kamu menjalankan RiseupVPN, sertifikat baru dibuat untuk mengautentikasi ke layanan. Kami tidak memerlukan pendaftaran nama pengguna/kata sandi untuk RiseupVPN, dan kami tidak memiliki informasi apa pun yang mengikat sertifikat data berumur pendek tersebut satu sama lain, atau kepada individu. Selain itu, log kami tidak berisi alamat IP pengguna , informasi sidik jari browser (informasi browser, plugin yang diinstal, font yang diinstal, resolusi layar, dll.), permintaan DNS, arus lalu lintas, informasi metadata , informasi identifikasi personal dalam bentuk apa pun, dan banyak lagi. Log yang kami miliki adalah minimum yang diperlukan untuk membuat layanan bekerja. Kami tidak menjual atau membagikan log data. Log yang ada disimpan dan dienkripsi, dan bertahan selama tidak lebih dari 5 hari sebelum dihapus.

Jika kamu tidak menggunakan RiseupVPN, dan masih menggunakan Riseup Red VPN yang sudah dihentikan peningkatan keamanannya **(silakan beralih ke RiseupVPN!)**, maka jawabannya tergantung pada informasi apa yang telah kamu kaitkan/berikan dengan login Riseup mu. Jika kamu khawatir tentang anonimitasmu, kami sarankan kamu membuat akun VPN terpisah yang hanya kamu gunakan untuk VPN pribadi. Untuk layanan ini, satu-satunya informasi tambahan yang berbeda dengan RiseupVPN adalah username yang terdaftar. Log ini juga disimpan dienkripsi dan tidak bertahan lebih dari 5 hari sebelum di hapus

Man-in-the-middle attacks (Serangan Man-in-the-middle)

Serangan Man-in-the-middle (atau MiTM) adalah salah satu bentuk penyadapan yang dapat melihat dan / atau memodifikasi lalu lintas jaringan . Serangan semacam itu dapat digunakan untuk mende-anonimisasi (membuka informasi personal) kamu, memodifikasi konten, mencuri kata sandi , atau menyusupkan virus, trojan, atau perangkat lunak lain yang dirancang untuk mendapatkan akses ke komputer.

Setiap koneksi internet rentan terhadap serangan MiTM karena sifat perusakannya mempengaruhi cara kerja internetmu. Dengan mengelabui protokol rute yang digunakan oleh internet, lalu lintas apa pun rentan terhadap serangan MITM di dunia belahan manapun.

Apakah VPN membantu melindungi terhadap MiTM?

Bisa iya bisa tidak. Menggunakan VPN akan mematikan banyak rute di mana serangan MiTM mungkin terjadi, tetapi tidak semuanya. Secara khusus, ini akan melindungi lalu lintasmu antar perangkat dan gateway VPN, mencegah ISP kamu, sebagian besar Pemerintah di berbagai Negara melakukan serangan MiTM yang ditargetkan gerakan sosial.

Namun, begitu lalu lintas internetmu melewati gateway VPN ke tujuan salah satu web, itu menjadi rentan terhadap serangan MiTM. Dengan VPN, lalu lintasmu kemudian semi-anonim, jadi jauh lebih sulit untuk menargetkan serangan apa pun terhadap orang tertentu, tetapi serangan sembarangan terhadap semua pengguna situs web tertentu masih sangat mungkin.

Contohnya, pada Januari 2011 pemerintah Tunisia, karena takut akan pemberontakan populer yang akhirnya akan menggulingkan rezim, mereka melakukan serangan MiTM pada pengguna Facebook yang teridentifikasi sebagai pemberontak, menyadap melalui login dan mendapatkan kata sandi mereka. Dalam hal ini, VPN akan melindungi selama gateway VPN terletak di luar negara Tunisia.

Keamanan Digital

Ditekan oleh waktu? Terlalu sibuk menolak penindasan atau membangun dunia yang lebih baik? Hebat! Kami sarankan mulailah melakukan peningkatan keamanan dengan langkah-langkah mudah yang dapat dilakukan semua orang untuk membuat kehidupan digitalmu jauh lebih aman dan menyenangkan.

1. Mulailah hati hati dalam mengelola pesan digital: Sebagian besar peretasan melalui kotak masukmu. Pelajari cara menjaga kehati-hatian yang tepat saat menggunakan email dan aplikasi pesan. Kami sarankan menggunakan aplikasi pesan yang terenkripsi dengan baik seperti, signal, wire dll.

2. Gunakan pengelola kata sandi: Dengan menggunakan pengelola kata sandi, kamu dapat melindungi diri dari sejumlah besar kemungkinan ancaman atau peretasan.

3. Aktifkan enkripsi perangkat : Enkripsi perangkat mudah diaktifkan, digunakan ke dalam sistem operasimu, dan melindungi data yang disimpan di perangkatmu.

4. Gunakan *browser* yang lebih aman: Dengan mengubah pengaturan browser web *default* dan menginstal beberapa ekstensi, Kamu dapat secara drastis meningkatkan keamanan dari penjelajahan web .

5. Jalankan perangkat lunak dengan aman : Menjaga perangkat lunak tetap *ter-update* adalah hal yang sederhana untuk dilakukan dan membuat sistem jauh lebih aman.

Mengapa Keamanan itu Penting

Semakin pentingnya keceptanan informasi dan komunikasi telah membawa fenomena baru: yaitu munculnya **“masyarakat pengawas”** .Dapat dianganggap pengawasan sebagai upaya oleh pemerintah untuk mempertahankan dominasi mereka dengan menegaskan kontrol atas komunikasi digital.

Negara-negara bangsa telah menggunakan teknologi komunikasi baru dengan mengejar upaya percepatan infrastruktur yang memfasilitasi pengawasan massal dan dapat dengan mudah digunakan kembali sebagai alat kontrol sosial total. Banyak Pemerintah juga melakukan kontrak dengan perusahaan swasta (penyedia layanan komunikasi) yang secara tidak etis digunakan untuk melacak aktivis dan meretas perangkat mereka.

Korporasi telah menemukan fakta bahwa pengumpulan dan analisis sejumlah besar data personal diperlukan jika mereka ingin tetap kompetitif di dunia yang kaya informasi. Secara gamblang, hampir semua iklan bergeser mengarah ke pelacakan berbasis pengawasan data dari perilaku masyarakat

Kriminal telah menemukan bahwa sangat menguntungkan untuk menyerang perangkat pribadi dan akun cloud (penyimpanan berbasis *digital external*) untuk meretas data atau memeras pengguna.

Dalam konteks ini, keamanan digital mesti menjadi salah satu prioritas.

- Pengawasan oleh Negara memiliki sejarah panjang yang mengakibatkan penindasan/penggembosan terhadap gerakan sosial.

- Bahkan secara tidak langsung, pengawasan yang terjadi secara masif memiliki efek pelemahan terhadap gerakan sosial.

- Pengawasan oleh Korporasi sama masifnya dengan pengawasan oleh Negara. Tidak hanya sejumlah besar data yang disimpan dari pengguna internet dengan mudah digunakan kembali untuk penindasan oleh Negara secara langsung, tetapi Korporasi hari ini berada di ambang mendapatkan kekuasaan yang belum pernah terjadi sebelumnya atas perilaku konsumen

Ketika mulai belajar tentang masifnya pengawasan beberapa orang mulai merasa kewalahan. Beberapa memutuskan bahwa tidak mungkin untuk aman, sehingga mereka mengundurkan diri agar tak hidup di bawah pengawasan atau meninggalkan semua bentuk komunikasi digital. Di Riseup, kami percaya ada cara ketiga: tujuan kami adalah membuat tingkat keamanan yang tinggi mudah dan dapat diakses oleh semua orang.

Gambaran Umum Keamanan Digital

Jenis Keamanan	Apa Itu?	Kapan itu berguna?
Keamanan Manusia	Perubahan sederhana yaitu merubah kebiasaan	Membantu mencegah kesalahan mebuka "tautan yang berbahaya" dalam sistem keamanan atau web apa pun.
Keamanan Perangkat	Langkah langkah untuk membuat keaman perangkat kamu lebih sulit diretas	Berguna untuk menjaga perangkatmu tahan terhadap serangan yang diketahui maupun tidak diketahui dan kemungkinan perangkatmu secara fisik jatuh ke tangan peretas
Keamanan Pesan	Cara untuk mengenkripsi pesan personal yang kamu kirim dan terima	Diperlukan jika Kamu ingin memastikan kerahasiaan pesan tertentu saat disimpan dan ditransmisikan.
Keamanan Jaringan	Memblokir situs yang melacakmu dan mengenkripsi lalu lintas internetmu.	Membantu melindungi dari pelacakan kriminal, negara, pembajakan akun, sensor, pemetaan jejaring sosial, penguntit, dan korporasi iklan.

Selain itu, lihat halaman *security resources* untuk tautan lebih lanjut ke panduan keamanan untuk aktivis yang aktif di gerakan sosial.

Artikel ini diterjemahkan dari berbagai sumber san ada beberapa tulisan yang ditambahkan agar menyesuaikan konteks di wilayah Indonesia. Serta kami menyediakan setiap text yang ditulis dalam artikel ini yang berwarna "biru", dapat langsung menuju kepada beberapa tautan bagi kalian yang ingin mempelajari soal kemanan digital lebih lanjut :

1. `https://support.torproject.org/`
2. `https://support.torproject.org/#staying-anonymous`
3. `https://riseup.net/en/vpn/security-issues`
4. `https://riseup.net/en/security`
5. `https://riseup.net/en/vpn/security-issues`
6. `https://riseup.net/en/vpn/limitations`

Spread Love
Palang Hitam Anarkis Indonesia

Palang Hitam Indonesia,
Security Culture 101/I (PC, Laptop, dan perangkat digital lainnya)
Kolaborasi Palang Hitam Anarkis dan Kolektif Eyes and Ears (Prancis)
23/12/2020

https://palanghitamanarkis.noblogs.org/post/2020/12/23/security-culture-101-i-pc-laptop-dan-pera

sea.theanarchistlibrary.org