PANDUAN PRAKTIS UNTUK MELINDUNGI IDENTITAS ANDA DAN KEAMANAN DARING DAN KETIKA MENGGUNAKAN PONSEL

UNTUK PENDUDUK TIMUR TENGAH, AFRIKA UTARA DAN LAINNYA

Panduan ini ditulis untuk penduduk di Timur Tengah dan Afrika Utara yang ingin menggunakan teknologi dengan aman untuk berkomunikasi, mengatur, dan berbagi data (laporan berita, informasi, media, dll.) – tetapi dapat digunakan oleh siapa pun, di mana pun, yang ingin melindungi rahasia pribadi dan keamanan di dalam jaringan (daring, *online*). Panduan ini ditujukan untuk kalangan luas dengan kemampuan komputer rata-rata yang ingin mengetahui langkah-langkah apa yang dapat diambil agar lebih aman ketika berada daring dan ketika menggunakan ponsel. Panduan ini memuat petunjuk dan pedoman untuk mengurangi pengawasan dan pemantauan, melindungi rahasia pribadi, dan menghadapi penyensoran. Beberapa hal yang dibahas adalah: penggunaan surat elektronik dan percakapan yang aman, kebiasaan kata sandi yang baik, bagaimana membuat komputer Anda bebas dari virus dan *spyware*, bagaimana menghindari penyensoran daring selagi anonim, taktik menggunakan ponsel dengan aman, dan memiliki tautan ke sumber-sumber yang lebih mendalam.

Walaupun semua informasi yang terdapat di sini dianggap akurat dan telah diperiksa pada Juli 2011, namun melindungi diri Anda di dalam jaringan merupakan suatu proses yang rumit dan dapat berubah-ubah seiring dengan munculnya teknologi baru dan ditemukannya kerentanan. Tidak ada solusi instan yang dapat menjamin keamanan dan privasi sepenuhnya, tetapi pedoman dan strategi di sini tentunya akan membantu membuat Anda menjadi lebih aman.

Dokumen ini telah disusun dan ditinjau oleh sejumlah organisasi dan individu yang memiliki spesialisasi di bidang daring dan keamanan ponsel. Apabila Anda menemukan masalah dalam dokumen ini atau memiliki saran-saran yang membangun, Anda dapat mengirimkan surat elektronik kepada info@accessnow.org.

(Apabila Anda memiliki masalah ketika mengakses tautan yang terdapat di dokumen ini dikarenakan situs yang diblokir setelah mengikuti pedoman yang diberikan berikut, silakan mengirim surat elektronik kepada info@accessnow.org dan beri tahu kami apa yang Anda ingin kami kirimkan lewat surat elektronik.)

Beberapa Hal Mendasar yang Penting

Mengamankan Surat Elektronik Anda

Dari seluruh layanan surat elektronik yang populer, Hotmail dan Gmail memberikan layanan aman yang menyediakan enkripsi koneksi (HTTPS) antara Anda dengan penyedia layanan surat elektronik.

Gmail sekarang telah menggunakan HTTPS sebagai pengaturan awal, tetapi untuk Hotmail Anda harus menyalakannya terlebih dahulu apabila Anda belum diminta sebelumnya (pergi ke Akun > Opsi Lainnya > Sambungkan menggunakan HTTPS > Gunakan HTTPS secara otomatis). Saat ini, Yahoo Mail belum aman; walaupun merepotkan, kami menyarankan agar Anda membuat dan menggunakan akun surat elektronik alternatif yang memiliki HTTPS untuk komunikasi Anda, terutama untuk segala sesuatu yang sensitif. Ingatlah bahwa HTTPS hanya melindungi koneksi antara Anda dengan penyedia layanan surat elektronik Anda dan pengiriman hingga ke tujuan akhir masih dapat tidak terenkripsi dan rentan apabila penerima tidak menggunakan HTTPS, atau mereka menggunakan penyedia layanan surat elektronik yang berbeda. Pilihan layanan surat elektronik lainnya yang aman adalah Riseup.net, dan Vaultletsoft. Lebih lagi, sistem yang unggul untuk mengenkripsi dan menandatangani surat elektronik Anda secara digital adalah PGP dan GPG (baca lebih lanjut dalam Bahasa Inggris dan Bahasa Arab).

Apabila Anda menggunakan Gmail dan ingin mengetahui lebih lanjut mengenai fitur keamanan lainnya (autentikasi 2-faktor, riwayat IP), silakan baca Daftar Periksa Keamanan Gmail. Apabila Anda menggunakan Hotmail, Anda dapat mengetahui lebih banyak mengenai fitur keamanan mereka, termasuk kata sandi sekali pakai untuk digunakan pada komputer publik di sini.

Membuat Kata Sandi yang Aman
Salah satu hal penting yang dapat Anda lakukan adalah menciptakan kata sandi yang baik dan kuat dan melakukan kebiasaan-kebiasaan kata sandi yang baik. Beberapa kiat yang mendasar:

- Gunakan frasa alih-alih hanya menggunakan satu kata.
- Buatlah frasa tersebut dengan dua belas karakter atau lebih; hal ini akan mempersulit berbagai program perangkat lunak untuk menembusnya.
- Gunakan kombinasi simbol, angka, huruf besar, dan huruf kecil. Salah satu cara penerapannya adalah dengan memasukkan simbol dan angka sebagai pengganti kata dan huruf dalam frasa, yang dapat berupa baris dari lagu atau puisi.
- Jangan gunakan kata sandi yang sama untuk semua akun; apabila kata sandi Anda diambil ketika dimasukkan daring di tempat yang tidak memiliki HTTPS maka info masuk Anda akan dengan mudah diketahui dan digunakan untuk mengakses akun Anda yang lain.

- Ganti kata sandi Anda setiap 3 bulan atau lebih sering apabila Anda menggunakan sistem warung internet atau komputer yang bukan milik Anda.
- Apabila Anda memiliki masalah dalam mengingat kata sandi, gunakanlah program enkripsi yang aman seperti KeePass untuk mengaturnya.
- Beberapa akun dilemahkan dengan adanya sistem pemulihan kata sandi. Pastikan pertanyaan keamanan dan jawaban untuk akun Anda tidak sederhana dan mudah ditebak.

Anti-virus dan Anti-spyware

Masalah serius bagi kebanyakan pengguna komputer adalah penggunaan perangkat lunak bajakan, terutama Microsoft Windows. Ketika Anda memperoleh perangkat lunak secara ilegal, Anda dapat menghemat uang, namun juga membuat diri Anda rentan terhadap masalah-masalah yang tidak dapat diatasi tanpa pemutakhiran dan perbaikan dari produsen perangkat lunak. Apabila Anda tidak dapat memperoleh sistem operasi dan perangkat lunak yang legal dan resmi, paling tidak Anda harus mengoperasikan perangkat anti-virus dan anti-spyware yang efektif untuk meminimalkan risiko. Namun, apabila memungkinkan, gunakanlah perangkat lunak yang resmi untuk keamanan Anda.

- Apabila saat ini Anda tidak menggunakan perangkat lunak yang efektif, program anti-virus yang unggul dan gratis untuk Windows adalah Avast, yang dapat membantu melindungi data di komputer Anda agar tidak rusak dan terinfeksi. Malwarebytes adalah program lainnya yang beroperasi dalam modus aman jika komputer Anda sudah terinfeksi.
- Yang juga penting adalah perangkat lunak anti-spyware, yang dapat mengidentifikasi dan menghilangkan perangkat perusak yang dapat mengikuti jejak aktivitas Anda baik di dalam maupun luar jaringan; program anti-spyware yang efektif dan gratis adalah Spybot.
- Untuk mengurangi kemungkinan Anda terkena virus dan *spyware*, jangan membuka surat elektronik dan lampiran dari sumber yang tidak dikenal dan tidak tepercaya. Apabila Anda tidak yakin akan suatu lampiran, berkas, atau situs web, Anda dapat mengujinya dengan mengunggah ke VirusTotal atau mengirimkannya kepada scan@virustotal.com dengan menuliskan “SCAN” di bagian subjeknya (atau SCAN+XML apabila Anda ingin hasilnya dalam format XML).
- Tempat masuk lainnya bagi kode berbahaya adalah skrip yang Anda temukan ketika sedang menjelajah jaringan. Kami sangat menyarankan agar Anda mengunduh dan menggunakan tambahan NoScript pada peramban Firefox Anda, yang memungkinkan Anda untuk memblokir sebagian besar skrip dan mengizinkan skrip yang Anda percaya.
- Tempat masuk umum lain bagi virus dan *spyware* adalah USB dan peranti mudah lepas lainnya. Jangan memasukkan peranti mudah lepas ke komputer Anda kecuali bila peranti tersebut dari sumber yang

diketahui dan tepercaya. Selain itu, gunakan anti-virus dan anti-*spyware* seperti Spybot dan Avast untuk memindai peranti mudah lepas.

Beralihlah ke Ubuntu, sistem operasi berbasis Linux, kecuali apabila ada alasan penting untuk terus menggunakan Windows. Ubuntu memungkinkan diska keras terenkripsi sebagai setelannya dan pada dasarnya bebas dari virus dan perangkat perusak. Meskipun tetap menjadi target serangan, pengguna Ubuntu lebih aman daripada pengguna Windows bajakan yang tidak diperbarui dan diperbaiki. Mint adalah sistem operasi lainnya yang berbasis Ubuntu dan memungkinkan penggunaan aplikasi dalam cakupan yang luas.

Pesan Instan yang Aman
Skype dan Google Chat di dalam Gmail yang dilindungi HTTPS adalah pilihan yang baik apabila Anda yakin akun Anda tidak menjadi target para peretas. Pilihan yang lebih aman adalah dengan menggunakan Pidgin untuk mengakses beberapa klien obrolan (Google Talk, dll.) dengan pengaya Off The Record (OTR) – ini menjamin agar sekalipun menggunakan kunci enkripsi Anda, data info masuk sebelumnya menjadi tidak berguna. Baca lebih lanjut mengenai properti keamanan OTR untuk memahami sebuah contoh dari Privacy by Design.

Amankan keberadaan daring Anda dengan cara-cara lainnya:

- Untuk menjaga kerahasiaan identitas Anda ketika berpartisipasi dalam aktivitas daring, Anda dapat menggunakan nama lain ketika diminta mengidentifikasi diri Anda dalam jaringan sosial atau situs media. Sampai mana Anda membuat diri tidak dikenal tergantung pada keinginan Anda sendiri; sangatlah umum untuk membuat penanganan anonim di Twitter, tetapi kebanyakan orang memiliki akun atas nama asli mereka di situs jaringan sosial seperti Facebook. Ini terserah kepada Anda dan pemikiran Anda akan seberapa mungkin Anda menjadi target untuk diawasi daring. Sangatlah penting untuk diketahui bahwa bagi Facebook, Anda harus membuat nama palsu yang meyakinkan daripada nama samaran yang terdiri dari satu kata dan sudah jelas palsu, yang akan dihapus oleh Facebook karena melanggar perjanjian persyaratan layanan.
- Apabila Anda memutuskan untuk menggunakan nama asli Anda di Facebook dan menggunakan HTTPS untuk mengakses atau menggunakan situs tersebut, sangatlah penting agar Anda tidak memberikan informasi personal yang sensitif seperti nomor telepon.
- Ada banyak pilihan untuk menggunakan teknologi GPS yang menunjukkan keberadaan Anda secara fisik ketika daring. Ini dapat menjadi alat yang sangat berguna ketika digunakan sebagai bagian dari kampanye terkoordinasi untuk merancang laporan dari lapangan dengan menggunakan ponsel pada saat krisis atau saat acara kunci, tetapi ini juga memberitahukan informasi yang sangat sensitif mengenai aktivitas dan lokasi Anda. Kami menyarankan agar Anda mematikan pelacak GPS

untuk program seperti Twitter dan Bambuser kecuali apabila itu hanya sementara dan penting untuk proyek aktivis yang sedang Anda ikuti. Bahkan apabila GPS tidak ditampilkan, sangatlah penting untuk menghilangkan kumpulan informasi ini pada peramban web Anda atau klien lainnya.

- Ketika Anda mengirimkan informasi yang sensitif kepada orang lain, ingatlah bahwa ada kemungkinan mereka tidaklah aman; daftar kontak mereka, surat elektronik, dan komunikasi lainnya mungkin saja diawasi. Berhati-hatilah terutama ketika berkomunikasi dengan pihak yang belum Anda verifikasi identitasnya. Sebagai tambahan, pesan langsung yang Anda kirim kepada seseorang (kenal maupun tidak) melalui Facebook dan Twitter dapat dibaca apabila mereka belum mengambil beberapa langkah tertentu (lihat lebih lanjut mengenai HTTPS dan alat pengelakan di sebelah ini).
- Batasi penggunaan aplikasi pihak ketiga yang dapat mengakses akun Anda atau jangan gunakan sama sekali (contohnya aplikasi yang mengakses akun Anda di Twitter, Facebook, Gmail, dll.) Aplikasi tersebut sering kali memiliki kerentanan dalam keamanan dan dapat digunakan untuk membobol akun yang dinyatakan aman.

Keamanan Daring

Internet sangat disensor di banyak negara di wilayah seperti Bahrain, Kuwait, Oman, Uni Emirat Arab, Qatar, Syria, dan Saudi Arabia. Internet juga diawasi di negara-negara tersebut, walaupun tidak diketahui sampai sebatas mana. Apabila Anda dapat menghindari penyensoran ini, bukan berarti Anda juga menghindari pengawasan, yang lebih sulit untuk dilakukan. Anda harus mencoba menggunakan proxy yang aman dan anonim dengan asumsi bahwa aktivitas Anda dapat diawasi dan direkam. Sebagai tambahan, kami sangat menganjurkan agar Anda tidak menggunakan Internet Explorer sebagai peramban web Anda, karena memiliki beberapa kerentanan, terutama pada versi tak berlisensi dari perangkat lunak tersebut. Sebuah alternatif baik yang gratis dengan sejumlah tambahan yang berguna adalah Mozilla Firefox.

Mengenkripsi aktivitas daring Anda menggunakan HTTPS

Apabila Anda ikut serta dalam aktivitas daring, sangatlah penting untuk mengikutinya dengan cara yang membuat identitas dan kata sandi Anda aman. Baru-baru ini kami melihat Tunisia melaksanakan kampanye pengelabuan besar-besaran sewaktu mereka mengeksploitasi suatu kerentanan dengan tujuan untuk mengumpulkan data info masuk dan kata sandi bagi penduduk yang mengakses Facebook. Untungnya, Facebook merespons dengan mengaktifkan HTTPS, yang sangat membantu. Apabila memungkinkan, Anda harus selalu menggunakan HTTPS. Bila Anda tidak dapat menggunakan HTTPS, sangatlah penting agar Anda menggunakan suatu sistem proxy yang aman. Sebuah sensor dapat menargetkan pengguna tertentu atau situs tertentu dan menolak akses ke situs HTTPS.

Jikalau Anda menggunakan proxy anonim seperti Tor, sangatlah sulit, bahkan hampir tidak mungkin, untuk melakukan serangan terencana yang demikian.

HTTPS

Tambahan yang mudah digunakan dan sangat baik adalah HTTPS Everywhere. Ini adalah tambahan untuk Firefox yang “memaksa” sebuah situs untuk menggunakan HTTPS apabila tersedia. **Mengunduh tambahan ini merupakan salah satu hal yang harus Anda lakukan untuk memiliki enkripsi *end-to-end* pada situs-situs seperti Facebook, Twitter, Penelusuran Google, dan lainnya.** Ini juga akan mengurangi kemungkinan kata sandi Anda diambil ketika berbagi jaringan wi-fi yang terbuka dan tidak terlindungi.

- Apabila belum, unduhlah versi terbaru Firefox. Kemudian unduh HTTPS Everywhere dan/atau Force TLS, nyalakan ulang komputer Anda, dan atur preferensi. Catatan: HTTPS Everywhere memiliki beberapa situs bawaan yang dapat diubah. Force TLS memerlukan lebih banyak modifikasi, yang mengharuskan pengguna untuk membuat daftar situs untuk memaksa HTTPS.
- Jikalau Anda menggunakan Google Chrome, unduh KB SSL Enforcer Extension. (Catatan: Ini tidaklah seefektif tambahan untuk Firefox yang disebutkan di atas. Masih ada beberapa kesalahan dengan SSL Enforcer, walaupun begitu kami berasumsi hal tersebut akan diperbaiki seiring dengan waktu.)

Facebook

Meskipun tambahan Firefox yang dijelaskan di atas memaksa HTTPS untuk beberapa situs, apabila sering menggunakan Facebook, sebaiknya Anda memastikan bahwa Facebook diatur ke HTTPS sebagai setelan awal, terutama apabila Anda mengaksesnya dengan lebih dari satu komputer.

- Untuk memungkinkan HTTPS bagi Facebook, pergi ke Akun di pojok kanan atas > pengaturan akun > pada tab pengaturan, pilih “ganti” keamanan akun > tandai kotak di sebelah “penjelajahan aman (HTTPS)”.
- Penggunaan beberapa permainan dan tambahan Facebook lainnya akan menonaktifkan penggunaan HTTPS.
- Facebook sekarang juga mempunyai fitur keamanan lainnya yang dapat Anda gunakan, termasuk keluar log dari jauh dan notifikasi info masuk yang memungkinkan Anda untuk membatasi perangkat yang dapat mengakses akun Anda. Sebuah video yang mengulas fitur keamanan mereka dapat ditemukan pada situsnya. Panduan menyeluruh lainnya mengenai pemakaian Facebook dengan aman dapat ditemukan di sini.

Twitter

Meskipun tambahan Firefox yang dijelaskan di atas akan memaksa HTTPS untuk Twitter juga, merupakan ide yang bagus untuk mengganti pengaturan Twitter ke HTTPS sebagai setelan awal kapan pun Anda terhubung, terutama

apabila Anda mengaksesnya dengan lebih dari satu komputer atau dengan menggunakan komputer umum.

- Untuk mengaktifkan HTTPS bagi Twitter, klik tombol Twitter pada pojok kanan atas > pengaturan > turun ke bagian bawah halaman dan tandai kotak di sebelah “Selalu gunakan HTTPS”.
- Catatan: Mengganti pengaturan akun Twitter menjadi “selalu menggunakan HTTPS” tidak memaksa HTTPS pada ponsel. Sampai hal ini diperbaiki, selalu tuju ke https://mobile.twitter.com.

Pengelakan: Mengunjungi situs yang diblokir

Beberapa negara di wilayah ini melaksanakan penyaringan ketat terhadap sejumlah besar situs web dan blog dan sangatlah beralasan untuk mencurigai bahwa penyaringan ini juga menandakan adanya pengawasan yang tidak sedikit jumlahnya, walaupun tingkat pengawasan itu sendiri berbeda di tiap-tiap negara. Untuk mengunjungi dan mengunggah media apa pun ke situs yang diblokir, Anda dapat menggunakan alat pengelakan. Sangatlah penting untuk diketahui bahwa ada perbedaan antara enkripsi dan privasi/anonimitas: alat pengelakan yang baik mengenkripsi lalu lintas antara pengguna dan penyedia pengelakan, tetapi tidak dapat mengenkripsi lalu lintas antara penyedia pengelakan dan situs yang dikunjungi. Di sinilah pentingnya untuk selalu menggunakan HTTPS apabila memungkinkan, karena ia menyediakan enkripsi *end-to-end*. Namun, hanya menggunakan HTTPS saja tidak akan membantu Anda mengakses situs yang diblokir dan karena itulah alat pengelakan menjadi sangat penting. Alamat IP Anda selalu disimpan melalui layanan jarak jauh – hanya dengan menggunakan proxy anonim (seperti Tor) barulah alamat IP Anda menjadi benar-benar tersembunyi secara aman. Banyak layanan yang akan memperlihatkan info masuk terakhir Anda dan apabila akun Anda dibobol, lokasi Anda sebelumnya akan diketahui.

Melompati firewall

Proxy sederhana berbasis web memungkinkan pengguna untuk mengakses situs yang diblokir melalui formulir halaman web. Pengguna dapat mengunjungi sebuah situs proxy dan memasukkan URL untuk situs yang ingin mereka kunjungi, dan proxy tersebut akan memperoleh dan menampilkan halaman tersebut. Proxy HTTP/SOCKS menyalurkan lalu lintas jaringan melalui protokol yang membuka jalan melalui firewall. Alamat IP dan nomor porta ditemukan di situs direktori proxy publik dan dimasukkan ke dalam konfigurasi peramban. Meskipun proxy sederhana berbasis web dan proxy HTTP/SOCKS umum digunakan untuk mengelakkan penyaringan, keduanya tidak menyediakan anonimitas (penggunaannya dapat dilihat/dipantau) dan sangatlah jarang diketahui siapa yang menyediakannya. Ada beberapa risiko yang terkait dengan ini, jadi sebaiknya gunakanlah sistem seperti Tor, yang dapat menyediakan pengelakan dan anonimitas.

Solusi lain yang berbasis proxy adalah Psiphon. Ia memiliki beberapa konfigurasi yang berbeda. Psiphon 1 adalah sebuah proxy web ringan yang dapat dijalankan lewat komputer yang menggunakan MS Windows atau Linux. Psiphonode biasanya bukan merupakan proxy publik yang terbuka. Sebaliknya, tujuan dari Psiphon adalah agar orang-orang biasa tanpa perangkat keras komputer khusus dapat menyediakan kemampuan pengelakan berbasis proxy kepada sejumlah kecil 'teman' yang berada di negara lain tempat pemblokiran situs terjadi. Hal ini dikenal sebagai model jaringan kepercayaan, sebab 'teman' yang menyediakan proxy psiphon akan dapat mengakses lalu lintas apa pun yang melewati psiphonode mereka dan karenanya harus ada hubungan tepercaya antara penyedia psiphonode dengan mereka yang memanfaatkan node tersebut. **Psiphon mencatat data tentang pengguna**, **tetapi IP-nya merupakan anonim.** Psiphon 2 adalah solusi berbasis awan yang diatur secara sentral dan dijalankan oleh Psiphon Inc. yang terdiri dari proxy penulisan ulang tautan. Psiphon 1 dan 2 memiliki kesulitan berhubungan dengan HTTPS dan situs Web 2.0. Keterbatasan ini telah diatasi melalui PsiphonX yang lebih baru.

Tor: Anonimitas daring
Tor adalah perangkat yang unggul dan mutakhir untuk mengelakkan penyaringan Internet dan membantu Anda melindungi anonimitas daring Anda, walaupun kekurangan utamanya adalah lebih lambat dalam menjelajah dibandingkan dengan solusi lainnya. Tor Browser Bundle menangani seluruh pengaturan dan menggunakan Tor bridge dapat membantu mendapatkan akses di lingkungan dengan penyaringan tinggi.

Walaupun ada beberapa cara dalam menggunakan Tor, kami menyarankan Anda untuk mengunduh Tor Browser Bundle, yang memungkinkan Anda menggunakan Tor melalui Windows, Mac OS X, atau Linux tanpa mengharuskan Anda memasang berbagai aplikasi. Luncurkan saja Tor Browser Bundle, dan Firefox dengan versi yang disesuaikan akan berjalan bersama dengan Vidalia, aplikasi pengawas Tor, yang telah terkonfigurasi untuk terhubung dan mengirimkan semua lalu lintas melalui jaringan Tor. Anda dapat memasang Tor Browser Bundle pada USB, sehingga Anda dapat menggunakannya pada komputer mana pun yang Anda butuhkan. Untuk Browser Bundle dengan ataupun tanpa pesan instan yang aman dalam banyak bahasa (termasuk Bahasa Arab dan Persia) kunjungi situs unduh Tor. Karena penggunaan Tor dapat memperlambat pengalaman penjelajahan web, kami menyarankan untuk menggunakan dua peramban, satu dengan Tor untuk mengakses informasi yang sensitif atau diblokir dan peramban lainnya untuk yang tidak sensitif. Apabila dibiarkan terhubung, Tor dapat meningkatkan efisiensinya sejalan dengan waktu dan Anda akan melihat kemajuan dalam kecepatan. Apabila Anda merasa menjelajah web dengan Tor masih lambat dan konten yang ingin Anda lihat berbasis teks, Anda dapat mematikan gambar dan pemuatan JavaScript pada peramban Anda.

Melakukan hal ini dapat meningkatkan kecepatan pemuatan halaman melalui Tor secara dramatis.

Sayangnya, situs web utama Tor yang ditautkan di atas biasanya diblokir di kebanyakan negara di wilayah ini. Anda tetap dapat mengakses perangkat lunak tersebut dengan:

- Mengunjungi situs web Tor dengan HTTPS – https://www.torproject.org/
- Menemukan cermin torproject.org dengan melakukan pencarian "tor mirror" di Google. Anda juga dapat melihat daftar cermin resmi apabila Anda mencari "site:torproject.org mirrors" di Google dan melihat hasil singgahan dari halaman "Tor Project: Mirrors".
- Atau Anda dapat meminta paket dengan mengirimkan surat elektronik kepada robot "gettor" di gettor@torproject.org. Catatan: demi keamanan dan hasil yang terbaik, gunakanlah akun Gmail yang dilindungi HTTPS untuk mengirim surat elektronik kepada gettor@torproject.org. Pilihlah salah satu dari nama-nama paket berikut ini dan masukkan nama paket tersebut di mana saja di isi surat elektronik Anda:
    - tor-im-browser bundle for Windows (Tor & pesan instan)
    - tor-im-browser bundle for Windows ATAU Intel Mac OS X ATAU Linux (Peramban Tor)

Tidak lama setelah Anda mengirim surat elektronik, Anda akan menerima balasan dari robot "Gettor" dengan perangkat lunak yang diminta dalam bentuk berkas zip. Untuk bantuan lebih lanjut dengan Tor, kirimkan surat elektronik kepada tor-assistants@torproject.org.

Pilihan lain untuk pengelakan yang mengenkripsi komunikasi dan menyediakan anonimitas adalah sebuah jaringan VPN. Anda dapat membaca lebih lanjut mengenai bagaimana mempersiapkannya di sini, atau mengunduh versi gratis dari VPN Hotspot Shield di sini atau mengirimkan surat elektronik kepada hss-sesawe@anchorfree.com (baris subjek dari pesan Anda harus memiliki paling tidak satu dari kata-kata "hss", "sesawe", "hotspot", "shield".)

Perangkat pengelak lain yang juga umum dipakai adalah Ultrasurf dan Freegate. Ketiga VPN ini merupakan perangkat yang baik untuk mengakses situs yang diblokir, namun penting untuk dicatat bahwa seperti halnya proxy sederhana berbasis web atau proxy HTTP/SOCKS, anonimitas tidak disediakan (contohnya mereka tidak menyembunyikan identitas Anda ketika Anda menggunakannya). Selain itu, layanan tersebut diketahui menyaring dan memblokir situs yang tidak didukung atau tidak disukai oleh operator. Terlebih lagi, situs-situs tersebut diketahui mencatat data mengenai semua pengguna. Mereka adalah perusahaan komersial dan memperoleh pendapatan dengan menargetkan iklan kepada Anda berdasarkan informasi personal Anda (situs yang Anda lihat, istilah pencarian yang Anda gunakan,

dll.) -- hal ini merupakan masalah penting bagi mereka yang mencari anonimitas atau privasi dalam penggunaan perangkat lunak pengelak.

Catatan Penting:
Ketika pemerintah memiliki kemampuan untuk mengatur layanan Internet di suatu negara, mereka juga dapat menggunakan beberapa strategi lainnya untuk berkompromi dengan keamanan dan rahasia pribadi melalui kode dan injeksi sertifikat keamanan. Untuk mengatasi hal ini, gunakan pedoman dan taktik di atas, dan cobalah untuk mengikuti berita atau peringatan dari aktivis daring di negara Anda yang mungkin mengenali tipe-tipe taktik ini dan memberikan peringatan dini.

Sumber lainnya: Video tutorial bagaimana menggunakan berbagai alat pengelakan dalam Bahasa Inggris dan Bahasa Arab (12 pm Tutorials).

Ponsel

Banyak aktivis yang telah dilacak melalui ponsel mereka dan beberapa negara melakukan pengawasan dengan lebih gencar dibandingkan negara lainnya. Aktivis di Mesir mengalami pengawasan dalam tingkat yang tinggi dan otoritas Mesir menggunakan sejenis teknologi yang mengubah ponsel menjadi perangkat pendengar di sekitarnya dari jarak jauh, walaupun ponsel tersebut berada dalam keadaan tidak aktif ketika itu. Anda harus menilai risiko terhadap aktivitas Anda dalam penerapannya di negara Anda, seberapa menonjolnya pekerjaan Anda, dan apa yang telah dialami orang lain di komunitas Anda. Perusahaan ponsel memiliki kapasitas untuk melacak dan mengumpulkan informasi mengenai penggunaan ponsel Anda, termasuk lokasi Anda, dan dapat membagikan informasi tersebut kepada pemerintah apabila diminta. Selain itu, ada juga kemungkinan untuk dipasangnya perangkat lunak pengawas di ponsel yang beroperasi di latar belakang tanpa diketahui pengguna. Risiko ini muncul apabila ponsel Anda telah berada jauh dari Anda untuk waktu yang lama.

Ketika ponsel Anda menyala, ponsel tersebut terus menerus mengomunikasikan informasi sebagai berikut ke menara terdekat:

- Nomor IMEI - nomor yang secara unik mengidentifikasi perangkat keras ponsel Anda.
- Nomor IMSI - nomor yang secara unik mengidentifikasi kartu SIM – di sinilah nomor ponsel Anda tertaut.
- Nomor TMSI, sebuah nomor sementara yang ditetapkan ulang secara berkala sesuai dengan lokasi atau perubahan cakupan, tetapi dapat dilacak oleh sistem pendengaran diam-diam yang tersedia secara komersial.
- Jaringan sel tempat ponsel tersebut sedang berada. Sel dapat mencakup area dari beberapa meter hingga kilometer, dengan sel yang lebih kecil di daerah perkotaan dan bahkan sel kecil di bangunan-

bangunan yang menggunakan alat penguat udara untuk memperbaiki sinyal dalam ruangan.

- Lokasi dari pelanggan di dalam sel tersebut, ditentukan dengan melakukan triangulasi dari sinyal yang berasal dari tiang-tiang terdekat. Sekali lagi, keakuratan lokasi bergantung pada ukuran dari sel – semakin banyak tiang-tiang di suatu daerah, semakin akurat posisinya.

Karena hal ini, ketika ponsel Anda menyala dan sedang berkomunikasi dengan menara jaringan, ponsel tersebut dapat digunakan sebagai perangkat pengawas untuk mereka yang memiliki akses kepada informasi yang dikumpulkan oleh perusahaan telekomunikasi, termasuk:

- Panggilan masuk dan keluar Anda
- SMS keluar dan masuk Anda, termasuk informasi pengirim dan penerima
- Layanan data yang Anda gunakan (contohnya aktivitas penjelajahan web yang tidak menggunakan HTTPS, pesan instan yang tidak aman) juga volume dari data yang dipindahkan, misalnya “apakah Anda mengunggah ke YouTube”
- Perkiraan lokasi Anda (dalam perkiraan beberapa meter sampai beberapa kilometer tergantung dari kepadatan menara)

Sangatlah penting untuk diketahui bahwa apabila Anda merasa sedang dilacak, tidaklah cukup hanya dengan mengganti kartu SIM, karena Anda dapat dilacak hanya dengan menggunakan ID (IMEI) dari ponsel Anda.

Ada banyak informasi di ponsel Anda yang dapat digunakan untuk memberatkan Anda apabila ponsel tersebut disita atau diambil dari Anda. Semua ponsel memiliki ruang penyimpanan dalam jumlah kecil di kartu SIM, dan juga di memori internal ponsel. (Sebagai tambahan, beberapa ponsel memiliki kartu penyimpanan SD [atau mikroSD] untuk berkas multimedia). Secara umum, menyimpan data di kartu SIM dan kartu SD (apabila memungkinkan) lebih baik daripada menyimpannya secara internal di ponsel, karena Anda akan dapat dengan mudah menghapus atau menghancurkan data di kartu SIM atau kartu SD.

Data yang disimpan di SIM Anda, memori internal ponsel, dan kartu penyimpanan SD (apabila ada) termasuk:

- Buku telepon Anda – nama kontak dan nomor telepon
- Riwayat panggilan Anda – siapa yang Anda telepon, siapa yang menelepon Anda dan kapan panggilan tersebut dilakukan
- SMS yang Anda kirim atau terima
- Data dari aplikasi yang Anda gunakan, seperti kalender atau daftar agenda
- Foto atau video yang Anda ambil menggunakan kamera ponsel, apabila ponsel Anda memilikinya. Kebanyakan ponsel menyimpan kapan foto tersebut diambil, dan dapat juga termasuk informasi lokasi.

Untuk ponsel yang dapat menjelajah web, Anda harus juga mempertimbangkan seberapa banyak riwayat penjelajahan Anda yang tersimpan di ponsel. Apabila memungkinkan, jangan menyimpan riwayat penjelajahan. Surat elektronik adalah potensi bahaya lainnya apabila akses terhadap kartu SIM atau memori ponsel telah diperoleh.

Seperti halnya diska keras di komputer, memori SIM di ponsel Anda menyimpan data yang pernah ada di dalamnya sampai penuh, lalu barulah data yang lama ditimpa. Ini berarti SMS, catatan panggilan, dan kontak yang telah dihapus dapat diperoleh kembali dari SIM tersebut. (Ada aplikasi gratis untuk melakukan ini dengan menggunakan alat baca kartu pintar). Hal yang sama berlaku pada ponsel yang memiliki memori tambahan, baik yang terdapat di dalam ponsel atau pun yang menggunakan kartu memori. Biasanya, semakin banyak penyimpanan yang dimiliki suatu ponsel, maka semakin lama waktu perolehan kembali berkas-berkas yang telah dihapus.

Jadi apa maksudnya ini bagi Anda?
Ponsel dapat menjadi perangkat yang berguna bagi aktivis, tetapi dapat juga menimbulkan ketidakbebasan yang luar biasa apabila pemerintah atau badan keamanan dengan giat bekerja sama dengan perusahaan telekomunikasi untuk melacak Anda. Apabila Anda berada di negara yang menggunakan ponsel secara ekstensif untuk pengawasan, terutama apabila Anda merasa Anda sedang diawasi untuk aktivitas yang menarik perhatian, disarankan agar Anda tidak menggunakan ponsel untuk berkomunikasi. Adakan pertemuan tatap muka.

Pada akhirnya, risiko yang Anda ambil bergantung pada diri Anda sendiri: apabila Anda tidak merasa Anda sedang diincar sebagai aktivis berposisi tinggi atau sebagai bagian dari pengawasan yang lebih besar dan ingin menggunakan ponsel Anda untuk berkomunikasi dengan aktivis lainnya, mengambil foto dan video, atau membagikan informasi, Anda dapat menggunakan taktik sebagai berikut:

- Ciptakan dan gunakan sistem kode untuk berkomunikasi dengan aktivis lainnya.
- Gunakan “bunyi” sebagai sistem untuk berkomunikasi dengan aktivis lainnya (menelepon sekali atau dua kali dan menutupnya sebagai tanda bahwa Anda telah sampai di lokasi, atau menyatakan bahwa Anda aman, dll.)
- Jangan gunakan nama sungguhan untuk aktivis lainnya di buku alamat Anda; gunakan nomor atau nama samaran. Dengan begitu, apabila ponsel atau kartu SIM Anda diambil oleh badan keamanan, mereka tidak memiliki seluruh jaringan aktivis lainnya.
- Bawalah cadangan kartu SIM bersama Anda ke demonstrasi-demonstrasi apabila Anda tahu itu akan disita dan sangatlah penting untuk membawa ponsel yang berfungsi pada suatu acara. Apabila Anda

harus membuang kartu SIM, cobalah untuk menghancurkannya secara fisik.

- Apabila ponsel Anda dapat dikunci menggunakan kata sandi, gunakanlah. Ini dapat juga berarti nomor PIN kartu SIM Anda: semua kartu SIM memiliki nomor PIN awal; apabila Anda bisa, gantilah nomor PIN tersebut dan gunakan penguncian PIN di SIM Anda. Anda kemudian akan diminta untuk memasukkan kata sandi (nomor PIN Anda) setiap kali Anda menggunakan ponsel Anda.
- Apabila Anda merasa bahwa suatu demonstrasi akan mendapat tindakan keras dari badan keamanan, Anda dapat menyetelnya menjadi mode pesawat dalam suatu acara; Anda tidak akan dapat melakukan atau menerima panggilan, tetapi Anda tetap dapat mengambil video dan foto dan mengunggahnya ke situs daring kemudian. Taktik ini juga berguna apabila Anda merasa badan keamanan akan menindak semua orang dengan ponsel pada suatu acara. Di kemudian hari pemerintah dapat meminta catatan panggilan/SMS atau data untuk semua individu yang berada di lokasi tertentu pada waktu tertentu untuk melakukan penangkapan massal.
- Matikan pelacak lokasi dan geotag untuk berbagai aplikasi kecuali Anda menggunakan fitur ini sebagai bagian dari proyek terencana untuk melakukan geotag pada media tertentu di sebuah acara atau sebagai bagian dari sebuah tindakan. Apabila Anda menggunakan ponsel untuk menyiarkan video secara langsung, matikan pilihan GPS/geotag (Petunjuk untuk Bambuser).
- Apabila Anda memiliki ponsel yang beroperasi dengan Sistem Operasi Android, Anda dapat menggunakan beberapa perangkat untuk mengenkripsi penjelajahan web, pesan instan, SMS, dan panggilan suara melalui perangkat yang diciptakan oleh Guardian Project dan Whispersys.
- Ketika menggunakan ponsel untuk menjelajahi web, gunakan HTTPS selalu apabila memungkinkan.

Sumber lainnya:

- Mobile in a box dari Tactical Tech (Bahasa Inggris)
- Mobile Security Risks Primer dari MobileActive (Bahasa Inggris)

Catatan untuk pengguna BlackBerry:
Pembuat BlackBerry, Research in Motion (RIM), menyediakan dua tipe akun dengan level-level enkripsi yang sesuai. Bagi pelanggan individu biasa, tidak pernah ada enkripsi *end-to-end* yang sejati pada komunikasi BlackBerry Anda – RIM atau penyedia layanan ponsel Anda selalu dapat menangkap panggilan, surat elektronik, penjelajahan web, dll. yang Anda lakukan. Sebaliknya, pengguna yang perusahaannya menggunakan BlackBerry Enterprise Server (BES) akan mendapatkan enkripsi *end-to-end* pada surat elektronik, pengirim pesan instan (BBM), dan peramban web. Walaupun

begitu, apabila Anda adalah seorang pengguna perusahaan, ingatlah bahwa siapa pun yang menjalankan server perusahaan Anda, biasanya admin TI, memiliki sarana untuk mendekripsi semua komunikasi Anda, dan ada beberapa jenis proses legal (dan tidak legal) tempat pemerintah dapat memperoleh komunikasi Anda yang telah didekripsi.

Baru-baru ini Uni Emirat Arab mencoba memaksa Research in Motion untuk memberikan mekanisme yang dapat mendekripsi semua komunikasi BlackBerry, tetapi RIM menolak melakukannya. Pengguna BlackBerry harus selalu mengikuti berita mengenai negosiasi antara pemerintah mereka dan RIM mengenai permasalahan ini. Mereka harus sadar akan upaya-upaya lainnya untuk memotong komunikasi BlackBerry yang terenkripsi. Pada 2009, Etisalat dari UEA mengirimkan pengguna BlackBerry sebuah “pemutakhiran” tidak resmi yang memungkinkan perusahaan telekomunikasi tersebut untuk menerima salinan dari semua pesan pengguna. RIM kemudian mengirimkan semua pengguna sebuah pemutakhiran yang menghapus perangkat lunak tipuan tersebut, tetapi pengguna BlackBerry harus sadar akan pemutakhiran perangkat lunak yang mencurigakan yang tidak berasal dari RIM langsung.

Lainnya

Blog

Apabila Anda memiliki blog atau ingin memulai blog, ada banyak sumber untuk membuatnya. Perhatian utama Anda adalah untuk membuat identitas Anda aman dan memastikan orang-orang tetap dapat membaca blog Anda kalau-kalau pemerintah memblokir blog tersebut. Berikut ini adalah sumber-sumber untuk membuat dan mencerminkan situs Anda jikalau di blokir pada URL aslinya:

- Membuat blog secara anonim dengan WordPress dan Tor (Global Voices)
- Membuat cerminan dari blog WordPress yang disensor (Global Voices)
- Kiat bagaimana blogging yang aman (EFF)
- Pedoman untuk Narablog (Reporters without Borders)

Merekam video
Buku: Video untuk Perubahan dalam Bahasa Arab
& Video: Cara Membuat Video untuk Perubahan dengan teks Bahasa Arab (Witness)

Sumber lainnya mengenai keamanan dan aktivitas digital:
Tactical Tech & FrontLine –
Security in a Box: Bahasa Arab dan Bahasa Inggris

The Electronic Frontier Foundation –
Panduan mendalam: Surveillance Self-Defense;

Panduan singkat: International Edition of SSD (keduanya dalam Bahasa Inggris)