SAFEnet

Panduan Keamanan Digital untuk Aksi



Panduan ini menggunakan lisensi Creative Commons Attribution-NonCommercial 4.0 (CC BY-NC 4.0). Anda bebas untuk untuk mendistribusikan, mencampur ulang, mengadaptasi, dan membuat materi dalam media atau format apa pun hanya untuk tujuan nonkomersial, dan hanya selama atribusi diberikan kepada pencipta. Informasi lebih lanjut di **https://creativecommons.org/licenses/by-nc/4.0/**

Pengantar

Sejak 2019, SAFEnet secara berkala melakukan pemantauan pelanggaran hak-hak digital. Selama proses tersebut banyak pula pengalaman dan pembelajaran yang bisa dibagikan, salah satunya tentang serangan digital yang kian hari kian politis. Terlebih, di saat terdapat isu atau kontroversi terkait kondisi politik dan kebijakan, peningkatan serangan digital selalu terjadi.

Dari deretan kejadian saat aksi #ReformasiDikorupsi hingga aksi terbaru #KawalPutusanMK, serangan digital selalu saja mengintai para aktivis, pembela hak asasi manusia (HAM), mahasiswa/i, atau jurnalis. Kondisi selama ini menunjukkan bahwa kerentanan bukan saja dalam ruang fisik, tetapi merambah pada ruang digital. Contoh lainnya adalah The People's Water Forum di Bali pada Mei 2024 lalu. Kegiatan tersebut tidak hanya mengalami represi fisik, tetapi juga berlanjut pada serangan digital.

Pelanggaran hak-hak digital saat masa #PeringatanDarurat hingga aksi #KawalPutusanMK pun tidak luput dari perhatian. Pembatasan/pemutusan akses internet, teror pembunuhan dan kriminalisasi, pembungkaman kebebasan berekspresi, upaya peretasan, hingga kekerasan berbasis gender *online* (KBGO) mewarnai aksi-aksi tersebut.



Saat ikut dalam sebuah demonstrasi, risiko serangan fisik tentu saja lebih signifikan, tetapi kita harus berupaya juga untuk mengambil tindakan mitigasi risiko serangan digital.

Buku saku ini menjelaskan langkah-langkah yang dapat diambil sebelum, selama, dan setelah demonstrasi atau aksi untuk membantu menjaga diri dan perangkat Anda lebih aman. Ada dua bagian besar dalam buku ini: Panduan Aksi Hindari Doxing dan Panduan Keamanan Digital Saat Aksi. Namun, perlu dicatat bahwa dengan berjalannya waktu, ragam dan variasi atau cara mitigasi serangan mungkin dapat berbeda. Oleh karena itu, pengamanan saat ini perlu disesuaikan kembali di masa mendatang untuk tetap relevan dan efektif.

Buku saku ini tentu saja masih jauh dari kata sempurna, tetapi kami berharap buku ini bisa membantu para aktivis, mahasiswa/i, pembela HAM, dan jurnalis yang akan mengikuti aksi unjuk rasa di lapangan. Bagi kami, ini adalah langkah awal untuk memastikan kita bisa menekan risiko serangan digital saat aksi berlangsung.

Panduan Aksi Hindari Doxing



Penggunaan teknologi pengawasan atau pelacakan semakin umum dilakukan, termasuk pada saat penanganan aksi. Teknologi ini bisa disalahgunakan untuk mengumpulkan identitas (*profiling*) aksi massa atau bahkan sebagai alat untuk melakukan *doxing*. Untuk melindungi hal tersebut, perlu upaya memilih tampilan yang dapat meminimalisir tindakan *doxing* dan melindungi keamanan fisik.



Dengan mengenakan kostum atau tampilan yang berbaur dengan kerumunan, hal tersebut dapat membantu untuk menutup identitas pribadi, serta mengurangi kemungkinan diidentifikasi dan dilacak. Selain hal tersebut, panduan berikut dapat membantu menghindari atau setidaknya meminimalisir potensi tindakan doxing.

Sebelum Aksi

- Gunakan pakaian netral tanpa identitas, kaos polos atau jaket tanpa nama lembaga/organisasi.
- Tutupi identitas yang mencolok, seperti tato atau warna rambut yang cerah.
- Jangan membawa perangkat terlalu banyak, bawa yang perlu saja.
- Usahakan perangkat yang dibawa tidak banyak kontak dan tidak banyak data.

- Pastikan perangkat dan media sosial sudah aman dengan menggunakan kata sandi kuat dan memasang dua faktor autentikasi (2FA).
- Selalu punya nomor darurat yang dihafal.
- Pastikan punya kawan jalan atau *buddy system*, di mana dua orang wajib saling memberi kabar dan bertanggung jawab satu sama lain ke kelompok lebih besar).
- Pastikan punya baju ganti yang bisa digunakan dengan cepat setelah aksi.

Ketika di Lokasi

- Hindari membagikan informasi berlebihan ketika aksi.
- Gunakan masker dan *face paint* ketika aksi.
- Persiapkan diri dengan perlengkapan pertama pada kecelakaan (P3K) pribadi.
- Lakukan dokumentasi seperlunya dan pastikan dari tempat aman.
- Matikan *geotag*, koneksi *bluetooth*, dan koneksi lainnya.
- Jangan gunakan Wifi publik.
- Tentukan titik kumpul untuk bersama dan berpisah dengan menggunakan deskripsi tempat, tidak perlu membagi lokasi.
- Selalu menyalakan *VPN* di perangkat.

Setelah Aksi dan Ketika Menemukan Diri Terkena Doxing

- Jangan balas komentar atau pesan yang berkesan mengintimidasi.
- Dokumentasikan setiap pesan/telepon (nomornya) dari pengirim.
- Lakukan penguncian akun media sosial.
- Informasikan ke organisasimu kalau Anda jadi korban *doxing*.
- Beri pemahaman dan pengertian ke orang sekitarmu apa yang terjadi dan pastikan kalau Anda sedang jadi korban teror *doxing*.
- Lakukan pengamanan data pribadi untuk diri sendiri dan bantu orang sekitarmu untuk melakukan hal yang sama.
- Laporkan ke situs web **aduan.safenet.or.id** atau **lapor.trace.mu**



Panduan Keamanan Digital Saat Aksi

Mengamankan perangkat digital ketika hendak melakukan aksi memerlukan perencanaan dan penerapan yang matang. Sudah seharusnya pengamanan dilakukan secara menyeluruh. Misalnya dari lapisan perangkat fisik, akun-akun, alat atau aplikasi komunikasi yang digunakan, dan perilaku. Masing-masing perencanaan ketika aksi juga perlu disesuaikan berdasarkan tahapnya, dari sebelum aksi, saat aksi, hingga setelah aksi.

Sebelum Aksi

Keamanan Perangkat

Perangkat tentu menjadi barang penting untuk dibawa ketika aksi protes. Baik untuk berkomunikasi dengan kawan-kawan, maupun untuk mendokumentasikan aksi. Penting untuk mengamankan perangkat karena umumnya di dalam perangkat kita ada data penting dan terkadang sensitif, utamanya bila berkaitan dengan aksi protes yang dilakukan.

Pengamanan perangkat sangat penting karena ini merupakan lapisan pertama yang dapat mengamankan keseluruhan data atau informasi dalam perangkat. Oleh karena itu, penting untuk mengamankan perangkat yang akan dibawa saat aksi.

Berikut ini adalah beberapa panduan praktis untuk mengamankan perangkat.

- **Aktifkan penguncian jaringan**, sehingga jaringan (wifi dan *mobile data*) tidak bisa dimatikan tanpa membuka kunci.
  Android: pengaturan > kunci layar > pengaturan kunci pengaman > matikan kunci jaringan pengaman
  iPhone: Setting > Face ID/Touch ID & Passcode > Allow Access When Locked > Control Center > Off
- **Kunci perangkat Anda.** Sebaiknya menggunakan kata sandi atau minimal PIN dengan 6 angka dan hindari menggunakan pembuka kunci biometrik seperti sidik jari atau Face ID. Penggunaan biometrik memungkinkan pihak lain untuk membuka ponsel anda dengan cara paksa.
- **Sebisa mungkin gunakan ponsel cadangan yang tidak** memuat banyak data dan nomor kontak terutama keluarga dan orang terdekat.
- Akan lebih baik jika ponsel cadangan tersebut menggunakan nomor yang tidak diketahui banyak orang (nomor khusus.
- **Pastikan perangkat ponsel terenkripsi**, dengan memastikan mengunci perangkat dan menggunakan kata sandi kuat.
- Untuk mencegah serangan teknis seperti *Cell-Site Simulators*, pengguna dengan perangkat terkait bisa:
  - Android: Menonaktifkan jaringan 2G
  - iPhone: Mengaktifkan mode Kuncitara (*Lockdown Mode)*

Keamanan Akun dan Data

Sebelum turun ke lapangan untuk aksi, penting untuk memastikan akun-akun, baik akun media sosial, akun percakapan, maupun akun email kita aman. Penting juga untuk memastikan data-data di perangkat kita tetap aman. Kita tidak pernah tahu apa yang akan terjadi selama dan setelah aksi. Risiko pembobolan akun atau pencurian data tetap ada.

Berikut ini adalah beberapa langkah untuk mengamankan akun dan data di perangkat digital.

- **Pastikan akses ke media sosial, e-mail dan apapun yang ada di perangkat digital dan komunikasi sudah dilindungi dengan kata sandi** yang tidak mudah ditebak. Gunakan sandi yang kuat yang merupakan gabungan dari angka, huruf, huruf besar, simbol, dan spasi.
- **Aktifkan 2FA (autentikasi dua langkah).** Pengamanan dua langkah ini berguna agar orang tidak mudah membobol akun kita, meskipun dia sudah memegang kata sandi. Hindari menggunakan pengamanan dua langkah menggunakan SMS, karena mudah untuk dicegat di tengah jalan.
- **Pastikan perangkat digital dan komunikasi selalu berada dalam keadaan terkunci.** Hindari menggunakan kunci pola, sidik jari, pengenalan wajah, atau PIN kurang dari 6 angka.

- **Cadangkan data di perangkat digital**, utamanya data yang penting dan sensitif. Pencadangan bisa dilakukan di perangkat berbeda, bisa juga dilakukan dengan menggunakan pencadangan komputasi awan *(cloud*).
- **Bila menggunakan kartu memori, gunakanyang baru/kosong dan aktifkan juga enkripsi untuk kartu memori.** Pastikan karu memori tidak digunakan untuk menyimpan data sensitif.
- **Aktifkan folder rahasia di perangkat untuk menyimpan foto atau dokumen rahasia.** Umumnya setiap perangkat berbasis android memiliki fungsi folder rahasia. Simpan atau masukkan data rahasia dan sensitif ke folder tersebut.
- **Pastikan sudah menonaktifkan akses lokasi di akun Google** yang terpasang di perangkat Anda. Ini bertujuan agar mengurangi risiko pelacakan lokasi dari pihak lain.



Perilaku

Kebiasaan menggunakan perangkat dengan nyaman harus diperhatikan, terutama ketika berada dalam kondisi yang memerlukan tingkat waspada dan kesadaran lebih tinggi, seperti pada saat melakukan aksi. Ada beberapa hal yang perlu diperhatikan saat akan melakukan aksi, termasuk:

- **Pastikan baterai perangkat digital dan komunikasi sudah terisi penuh** sebelum berangkat.

- **Siapkan nomor kontak darurat,** jika diperlukan nomor itu bisa diakses dengan cepat, akan lebih bagus kalau nomor itu dihapalkan atau bisa menghafalkan id lembaga/organisasi atau *buddy*. Jika dirasa susah menghafal nomor, bisa dengan mengafal *user name/id*, baik di Signal, Telegram, Twitter, Instagram atau jalur komunikasi lain yang sudah disepakati dan aman.
- **Pastikan setiap orang yang terlibat bisa termonitor,** bisa didata lebih dulu bisa juga dengan sistem *buddy*.
- **Siapkan perangkat digital dan komunikasi seminimal mungkin** (kalau dirasa cukup dokumentasi dengan ponsel, tidak perlu bawa kamera, begitu juga perekam suara). Bawa perlengkapan/peralatan seminim mungkin, sesuaikan dengan fungsi, tidak perlu membawa laptop. Agar mempermudah pergerakan.
- **Bersihkan media penyimpanan perangkat digital dan komunikasi,** terutama dari file-file pribadi dan yang berukuran besar, ini berguna untuk memperbanyak ruang dokumentasi juga sebagai mitigasi jika terjadi hal yang tidak diinginkan, data pribadi kita tidak apa-apa.
- **Siapkan media penyimpanan cadangan** seperti kartu memori, *flashdisk OTG*, dan pastikan mudah diakses/dijangkau jika sewaktu-waktu dibutuhkan.
- **Pertimbangkan menggunakan pelindung luar (*hardcase*)** untuk melindungi keadaan fisik perangkat serta menggunakan *privacy screen* untuk mencegah tampilan layar mudah dilihat dari sisi.

Saat Aksi

Ketika aksi, keamanan fisik memang krusial, tetapi keamanan digital juga tidak kalah penting. Utamanya, melindungi perangkat dan menerapkan kebersihan digital saat protes tidak serta merta bertujuan untuk melindungi diri sendiri. Namun, untuk melindungi juga upaya kolektif semua orang yang terlibat dalam gerakan tersebut.

Dengan memperhatikan keamanan, kita dapat memastikan keberlanjutan informasi terhadap kawan yang tidak mengikuti aksi, serta juga dapat melindungi keselamatan atau privasi kita, khususnya terkait dokumentasi atau pengorganisasian protes.

Pembagian tugas untuk kawan di lapangan juga bisa dilakukan. Tugas terkait dokumentasi dan kampanye aksi menggunakan media sosial milik lembaga/komunitas dapat diserahkan kepada satu orang yang berada di lokasi aksi untuk mengirimkan foto/video dan narasi aksi kepada admin media sosial yang tidak ada di lokasi aksi. Tujuannya untuk mengurangi risiko pengambilalihan akun lembaga/komunikasi karena lokasi adminnya tidak ditempat aksi.



Kemanan Perangkat

- **Jika jaringan bagus, pastikan untuk secara berkala mengunggah data ke penyimpanan berbasis *cloud*** untuk mengurangi risiko kehilangan data, jika perangkat hilang atau diambil paksa.
- **Pastikan tidak terhubung ke jaringan Wi-Fi terdekat**, lebih baik gunakan paket data pribadi. Penggunaan jaringan Wi-Fi yang tidak jelas sumbernya, rentan untuk mendapatkan serangan atau pengawasan digital.
- **Pastikan VPN selalu dalam kondisi menyala.**
- **Pastikan Wi-Fi Bluetooth tidak aktif** atau off jika tidak diperlukan, aktifnya fungsi tersebut rentan untuk menjadi bahan pelacakan atau pengawasan digital.
- **Pastikan menggunakan jalur komunikasi yang aman,** misalnya menggunakan Signal atau Wire.

Perilaku



Kebiasaan menggunakan perangkat dengan nyaman harus diperhatikan, terutama ketika berada dalam kondisi yang memerlukan tingkat waspada dan kesadaran lebih tinggi, seperti pada saat melakukan aksi. Ada beberapa hal yang perlu diperhatikan saat akan melakukan aksi, termasuk:

- **Tentukan rute** jika sewaktu-waktu diperlukan untuk meninggalkan area. Bagi perkelompok per rute, jangan gunakan satu rute yang sama untuk semua kelompok.

- **Tentukan titik kumpul.**
- **Tugaskan beberapa orang untuk cari tempat aman untuk monitor** keadaan sekitar.
- **Tugaskan 1-2 orang untuk monitor jalur komunikasi**, pastikan tidak ada yang anggota yang membuat unggahan dengan kalimat provokasi atau sebaran hoaks.
- **Pastikan mengambil foto dan video tanpa membuka kunci** (buat *shortcut*).
- **Pastikan urusan publikasi aksi hanya dipegang beberapa orang saja**, selain penanggung jawab, maka anggota lain hanya bertugas memberi informasi.
- **Pastikan juga menghapus metadata dari foto atau video** yang diunggah.
- **Jika terjadi hal yang tidak diinginkan, langsung cabut media penyimpanan yang sudah mendokumentasikan aksi, simpan dan amankan, ganti dengan media penyimpanan kosong.** Ini berguna untuk jaga-jaga, jika sampai ada pembukaan perangkat dengan paksa, dokumentasi sudah aman.

Setelah Aksi

Berakhirnya aksi tidak menjamin risiko akan turut berhenti. Jangan terlena meski situasi sudah dianggap aman dan semua personel sudah kembali ke tempat masing-masing dengan aman. Berikut ini adalah beberapa aktivitas yang bisa dilakukan untuk memastikan situasi benar-benar sudah aman.

- **Evaluasi kegiatan sekaligus saling cek kondisi masing-masing.** Pastikan semua personel benar-benar sudah kembali ke tempat dengan aman.

- **Pastikan semua perangkat elektronik dan perangkat komunikasi tidak tercecer dan tetap dipegang oleh pemiliknya.** Perhatikan apakah ada kondisi aneh pada perangkat setelah aksi, misalnya: akun WhatsApp mengirim pesan sendiri, atau keanehan lainnya. Periksa aplikasi di perangkat Android dengan VirusTotal untuk memastikan tidak ada aplikasi mencurigakan yang terpasang tanpa sepengetahuan Anda.

- **Pantau pembicaraan di media sosial terkait aksi yang dilakukan,** lakukan analisis apakah ada situasi lanjutan yang perlu diantisipasi atau tidak.

- Bila perangkat hilang atau diambil paksa, lakukan beberapa hal ini:
    - Bila memang dirasa perlu – misalnya ketika terjadi perampasan *ponsel* – **lakukan factory reset atau hapus semua data.** Ini bisa dilakukan dari jarak jauh dengan memanfaatkan fasilitas find my phone. Catatan: fitur ini membutuhkan pengaktifan lokasi di ponsel. Pertimbangkan risikonya, apakah perlu atau tidak terus menerus mengaktifkan lokasi di ponsel.
    - **Hapus semua isi telephone lewat jarak jauh** dengan memanfaatkan fitur milik Google atau iCloud
    - **Putuskan akun-akun (perpesanan, e-mail, Google, dsb.)** yang terpasang pada perangkat yang hilang melaui perangkat lain.
    - **Ada kemungkinan polisi atau pihak keamanan akan meminta kata sandi perangkat yang sudah disita**. Bila itu terjadi, minta bantuan pada pendamping hukum seperti LBH.

Aplikasi yang Berguna untuk Aksi

Berdasarkan pemantauan SAFEnet, terdapat beberapa aplikasi yang mengalami tingkat insiden peretasan tinggi. Serta, terdapat dugaan pembatasan akses internet saat aksi. Oleh karena itu, perlu upaya untuk menyiapkan aplikasi atau layanan yang dapat menanggulangi hambatan-hambatan tersebut.
Berikut ini adalah beberapa aplikasi alternatif yang bisa digunakan saat aksi:



Tella, untuk dokumentasi (ambil foto, video, recorder dan catatan) setelah terpasang bisa disamarkan menjadi aplikasi lain (fitur ini hanya tersedia untuk Android). Aplikasi ini bisa membantu Anda untuk menyamarkan dokumentasi di perangkat Android.



Session, untuk komunikasi, aplikasi ini menggunakan PIN jadi tidak ada perlu nomor ponsel dan e-mail. Kekurangannya proses pertukaran PIN yang mungkin akan jadi kendala. Kelebihannya, ketika aplikasi ini di logout atau dihapus, tidak ada percakapan yang tersimpan.

Signal, untuk aplikasi komunikasi lebih aman karena terenskripsi ujung ke ujung. Jika dibuka di tempat lain, pesan lama tidak akan muncul. Ini jelas lebih aman dari kemungkinan peretasan oleh pihak lain. Selain itu, terapkan juga beberapa tambahan pengamanan seperti berikut:

- Alih-alih menggunakan nomor di Signal, sebaiknya gunakan ID.
- Terapkan pengamanan tambahan dengan menggunakan PIN, dan gunakan PIN minimal dengan 6 angka.
- Aktifkan fitur Penguncian Registrasi (*Registration Lock*).
- Terapkan pengaman privasi tambahan untuk menonaktifkan pencarian menggunakan no telepon. Akun Anda hanya bisa dicari dengan ID dan bukan nomor telepon. Nomor telepon juga akan disembunyikan.
- Pertimbangkan mengaktifkan fitur penghapusan pesan secara otomatis sesuai pengaturan waktu *(dissapearing message)*.

Telegram, untuk komunikasi dengan catatan fitur keamanan harus difungsikan. Gunakan akun alih-alih nomor telepon dan aktifkan *secret chat* agar pesan bisa otomatis hancur dalam kurun waktu tertentu.



Gunakan VPN seperti Riseup vpn, Proton VPN, Tunnel Bear, Outline VPN (pilih salah satunya), VPN yang bisa digunakan dan ada fitur gratis jika belum menggunakan yang berbayar. Hindari menggunakan VPN yang diproduksi perusahaan dari Tiongkok.

Jika Anda membutuhkan akses VPN Tunnel Bear atau Outline VPN, silakan hubungi SAFEnet di Signal dengan ID safenetvoice.24.

bridgefy

BRIAR

Bridgefy atau Briar, aplikasi komunikasi tanpa internet. Keduanya punya kekurangan di sisi fitur yang hanya bisa mengakomodir percakapan teks. Namun, keduanya bisa digunakan tanpa sinyal internet dan hanya menggunakan Bluetooth dengan jarak tertentu.

Percakapan lewat kedua aplikasi itu juga menggunakan fitur *end to end encryption* dan diklaim lebih aman.

Referensi:
Electronic Frontier Foundation. "Attending a Protest." 02 Mei 2024, https://ssd.eff.org/module/attending-protest.

Germain, Thomas. "How to Protect Phone Privacy and Security During a Protest." Consumer Reports, 03 Juni 2020, https://www.consumerreports.org/electronics/privacy/protect-phone-privacy-security-during-a-protest-a5990476708/.

Amnesty International. "Tactics to secure your smartphone before joining a protest." 12 Juni 2020, https://www.amnesty.org/en/latest/campaigns/2020/06/tactics-to-secure-phone-before-a-protest/