Panduan Dasar #AmanInternetan

versi 1.0

Februari 2018

Menjelang tahun politik 2018-2019, besar potensi media sosial/digital makin penuh dengan kampanye hitam, *hoax*, *fake news*, ujaran kebencian, dan persekusi.

Karena itu, makin penting bagi kita untuk meningkatkan kapasitas dan wawasan kita perihal kebebasan berekspresi dan kemanan digital, khususnya dalam melindungi data pribadi yang beredar di internet.

Tentunya, tidak ada solusi keamanan tunggal, dan tidak ada sistem keamanan yang tidak dapat dirusak. Namun ada hal-hal dasar yang dapat dilakukan untuk mencegah (atau setidaknya mempersulit) data Anda di(salah)gunakan.

“A chain is only as strong as its weakest link. Computer security relies on a great number of links, hardware, software and something else altogether: people.

Di balik semua sistem teknologi dan prosedur keamanan yang ada, tetap terdapat faktor penting, yaitu: manusia.

Bukan hanya dirimu, tapi yang perlu diperhitungkan adalah bagaimana jika orang-orang sekitarmu tidak memperkuat kapasitas keamanan digital mereka—misalnya menggunakan password yang mudah ditebak, atau menuliskannya di layar komputernya, lupa *logout*, atau dengan mudahnya memberikan akses kepada teman, rekan, kliennya, atau dikelabui dengan *phishing* dan berbagai *social engineering*? Atau kalau pemerintah menuntut perusahaan telko atau perusahaan media sosial, aplikasi, yang kita gunakan seperti Telegram, Facebook, dsb. untuk membagikan data pribadi penggunanya (dan ini bukannya belum terjadi)?

Tidak ada sistem yang tidak melibatkan interaksi manusia. Begitu pula keamanan digital bersifat menyeluruh, melibatkan semua orang, bukan semata bergantung pada kemampuan individual ataupun perangkat tertentu. **#AmanInternetan dimulai dari dirimu, dan orang-orang sekitarmu**.

Kebebasan Berekspresi dan Keamanan Digital

khususnya memasuki tahun politik 2018-2019

Seberapa aman situasi keamanan berinternet di Indonesia, dengan jumlah pengguna internet mencapai 132,7 juta orang dari total penduduk 265,4 juta jiwa? Juga seberapa aman pengguna media sosial aktif yang mencapai 130 juta orang atau nyaris 100 persen dari total pengguna internet menghadapi Era Pasca-Kebenaran yang ditandai dengan persoalan *political hoax*, *hate speech* dan persekusi? Bagaimana pula dengan keamanan saat menyampaikan pendapat, di tengah catatan memburuknya indeks kebebasan ekspresi seperti yang tertuang dalam laporan Freedom on Net 2017 lalu?

Apalagi bila melihat bahwa penyebab merosotnya indeks itu adalah praktik pemblokiran konten oleh pemerintah, tingginya kriminalisasi warganet dengan UU ITE pasal 27 ayat 3 tentang defamasi, dan kegagalan dalam mengantisipasi serta mengatasi manipulasi dan intimidasi yang datang dari kelompok etnis dan agama garis keras yang menyasar pada kaum-kaum rentan, seperti LGBT dan kelompok minoritas, kaum tani dan buruh, serta berbagai aksi solidaritas. Bulan Februari 2018 juga menyaksikan disahkannya UU MD3 yang mempermudah kriminalisasi terhadap siapapun yang mengkritik DPR; serta perumusan RKUHP yang memuat pasal penghinaan presiden, wapres dan pemerintah.

Southeast Asia Freedom of Expression Network (SAFEnet) mencatat dalam tempo satu tahun sejak revisi UU ITE disahkan pada 28 November 2016, ada 385 warganet yang diadukan ke polisi dengan pasal-pasal karet dalam UU ITE. Setidaknya 363 aduan tercatat terkait pasal pencemaran nama baik, 21 aduan terkait pasal penodaan agama, 1 aduan terkait pasal pengancaman online. Dibanding sebelumnya, ini menunjukkan adanya lonjakan aduan yang menggunakan pasal-pasal karet UU ITE. Tidak direvisinya atau dicabutnya pasal 28 ayat 2 dan pasal 29 pada saat pembahasan Komisi I dan Kemkominfo juga berakibat mendorong pelaporan-pelaporan kasus penodaan agama dan

pengancaman yang definisinya diartikan seenaknya sendiri dan cenderung mengada-ada.

Pada tahun 2017 juga, SAFEnet menyoroti tentang fenomena persekusi yang terjadi di media sosial dan semakin menguat dengan terjadinya pemidanaan mereka yang dipersekusi dengan pasal 28 ayat 2 UU ITE.

Dalam Monitoring Kasus Persekusi yang dikerjakan SAFEnet bersama dengan Koalisi Anti Persekusi, ada 100 kasus persekusi ekspresi yang terjadi sejak awal tahun 2017 sampai akhir November 2017. Dari 100 kasus persekusi ekspresi, 12 kasus di antaranya telah masuk ke persidangan dan diputus bersalah dengan kisaran vonis antara 2 sampai 4 tahun penjara. Namun sebaliknya para pelaku persekusi hingga hari ini belum terungkap apalagi dipidanakan sekalipun apa yang mereka lakukan sudah jelas melanggar hukum.

Dari fenomena persekusi ini, SAFEnet juga melihat adanya kewalahan dan kegagapan di kalangan warganet dan informasi yang tidak tersampaikan oleh pemangku kepentingan lainnya dalam mengantisipasi unsur-unsur persekusi, seperti *doxing* (tindakan mencari dan menyebarkan data-data pribadi atau hal-hal yang bersifat mengidentifikasi seseorang dengan niat jahat di internet). Di sisi lain, survei Mastel di awal 2017 menemukan bahwa *political hoax* dan SARA yang berpotensi memecah kerukunan masyarakat merajalela, terutama melalui media sosial dan aplikasi *chatting*.

Problem keamanan berinternet juga berkaitan dengan keterbatasan kapasitas warganet untuk mengenali persoalan keamanan digital dan bagaimana memanfaatkan jalur yang telah dibuat untuk menciptakan pengalaman berinternet yang aman. Karenanya, selama bulan Februari 2018, SAFEnet mengadakan Bulan Aman Internetan 2018, bekerjasama dengan ICT Watch dan SIBERKREASI. Tujuan dari kegiatan ini adalah menggandeng para pemangku kepentingan untuk meningkatkan kapasitas dan wawasan masing-masing, utamanya warganet, agar dapat menciptakan situasi internet yang lebih aman dan antisipatif terhadap berbagai ancaman kebebasan berekspresi di Indonesia. Di Surabaya, kegiatan ini diadakan pada hari Senin, 26 Februari 2018, bekerjasama dengan PERIN+1S dan C2O library & collabtive sebagai rekan pelaksana, dengan dukungan narasumber dari AJI Surabaya.

Tidak ada sistem keamanan yang tidak dapat dibobol, dan tiap orang memiliki kebutuhan dan solusi keamanan yang berbeda. Kebutuhan dan solusi keamanan untuk anak kecil akan berbeda dengan seorang jurnalis, aktivis buruh. Namun ada praktek-praktek keamanan dasar yang dapat dilakukan untuk mencegah data Anda di(salah)gunakan.

Nyebut *digital security* bisa membuat keder banyak orang. Dalam film Hollywood, penggambaran berita dan media populer, *digital security* dan *hacking* sering digambarkan sebagai sesuatu yang hampir magis: aktor-aktor misterius dengan panik (atau fokus) mengetik di depan layar hijau yang huruf-huruf dan angka-angkanya bergerak dengan sangat cepat, dan dengan ajaib bisa menyelesaikan masalah setelah mengetik kode misterius. Banyak orang percaya bahwa mereka memerlukan keahlian teknis khusus untuk memahami dan mengurangi ancaman terhadap keamanan mereka. Ini tidak selalu betul.

Mengasosiasikan *digital security* melulu pada *hacking* dan hal "teknis" seperti *encryption*, *zero days*, *XSS*, dan *surveillance* NSA ibaratnya membatasi isu kesehatan pada kemoterapi kanker, lupus, dan HIV tanpa meningkatkan praktek dasar untuk menjaga kesehatan seperti cuci tangan, sikat gigi, atau vaksinasi.

Dan, ahli komputer, informasi dan teknologi tidak selalu melakukan praktek keamanan digital yang lebih baik.

KLIPING

Mark Zuckerberg hacked on Twitter and Pinterest

Facebook founder apparent victim of 2012 LinkedIn password dump

▲ Mark Zuckerberg's social media accounts were targeted by a hacker going by the name OurMine. Photograph: Eric Risberg/AP

Mark Zuckerberg is having a bad Monday.

The Facebook founder briefly lost control of both his Twitter and Pinterest accounts this morning, after a hacker broke in to both, defacing the pages.

MOTHERBOARD

A Hacker Has Wiped a Spyware Company's Servers—Again

"I don't want to live in a world where younger generations grow up without privacy."

"The hacker found the key and credentials to those containers inside the Android app of PhoneSheriff, one of Retina-X's spyware products. The API key and the credentials were stored in plaintext, meaning the hacker could take them and gain access to the server."

Individu ahli teknologi maupun perusahaan teknologi pun rentan ancaman keamanan digital. Akun Mark Zuckerberg, CEO Facebook, dibobol karena **menggunakan password yang sama** untuk 3 situs: LinkedIn, Path, Twitter. Sementara satu perusahaan spyware ("stalkerware") **menyimpan data sensitif dengan *plaintext*, tanpa *encryption***.

KOMPAS.com
RAYAKAN PERBEDAAN

Rabu, 20 Januari 2016 | 16:03 WIB

Kebocoran Go-Jek Memuncak, Rute Sehari-hari Pengguna Bisa Dilacak

Selasa, 12 Januari 2016 | 14:49 WIB

Go-Jek Klaim Data Pengguna dan "Driver" Aman, Faktanya?

GO-JEK

Anda dengan ini setuju dan memberikan wewenang pada kami untuk memberikan Informasi Pribadi anda kepada Penyedia Layanan sebagai suatu bagian dari ketentuan Layanan. Walaupun informasi pribadi anda secara otomatis akan dihapus dari perangkat bergerak milik Penyedia Layanan setelah anda menggunakan Layanan, terdapat kemungkinan dimana Penyedia Layanan dapat menyimpan data anda di perangkat mereka dengan cara apapun. Kami tidak bertanggung jawab atas penyimpanan data dengan cara tersebut dan anda setuju untuk membela, memberikan ganti rugi dan membebaskan kami dan kami tidak akan bertanggung jawab atas segala penyalahgunaan Informasi Pribadi anda oleh Penyedia Layanan setelah berakhirnya Layanan yang diberikan.

"Kami tidak menjamin keamanan *database* kami dan kami juga tidak menjamin bahwa data yang anda berikan tidak akan ditahan/terganggu ketika sedang dikirimkan kepada kami. Setiap pengiriman informasi oleh anda kepada kami merupakan risiko anda sendiri. Anda tidak boleh mengungkapkan sandi anda kepada siapa pun. Bagaimanapun efektifnya suatu teknologi, tidak ada sistem keamanan yang tidak dapat ditembus."

Contoh hal-hal yang tercantum dalam **Terms & Conditions (Syarat & Ketentuan),** seringkali kita abaikan dan langsung klik "Setuju" atau "Accept" tanpa membaca.

Kenapa harus hati²?

Apa saja yang ada di sini? Silakan ditambahkan/kurangi.

Dompet	Media sosial	HP
- Beberapa foto pasangan/keluarga? - Kartu identitas (KTP, SIM, STNK) - Uang - Kartu kredit/debit	- Puluhan, ratusan foto dan video, beberapa dengan rincian lokasi dan waktu - Peta jaringan kawan, keluarga - Riwayat kerja, riwayat tinggal - Hobi - Puluhan, ratusan status	- Ratusan, ribuan foto - Puluhan video - Daftar alamat dan no HP kawan, kolega, dsb. - Aplikasi media sosial - Password berbagai aplikasi, website, bank - Bank details - Log semua telpon dan SMS Anda - Email dan password² - Aplikasi chat dan log-nya? - Catatan pembelian melalui aplikasi - Geolokasi Anda - Dokumen2 - Jadwal kegiatan

Tersebarnya data pribadi tersebut membuat rentan penggunanya pada:

- *Cyberbullying*, doxing (penyingkapan data-data pribadi, berpotensi memalukan)
- Pencurian identitas, misalnya menggunakan identitas/akun Anda untuk melakukan kejahatan atau mempermalukan Anda
- Kehilangan pekerjaan atau kawan
- *Stalking*
- *Surveillance*, mengawasi gerak-gerik Anda
- Pencurian uang
- Mendapatkan data pribadi Anda
- Mencari sensasi
- Membuat konflik adu domba
- Kepentingan politik
- Lainnya….?

Basic digital hygiene

Sekali lagi, tidak ada solusi tunggal, dan tidak ada sistem keamanan yang tidak dapat dibobol. Begitu pula, kebutuhan dan solusi keamanan setiap orang berbeda-beda. Seorang jurnalis memiliki kebutuhan keamanan yang berbeda dengan ibu rumah tangga, website administrator, atau Snowden. Kebutuhan ini pun berganti-ganti seiring waktu. Namun ada praktek-praktek keamanan dasar yang dapat dilakukan untuk mencegah (atau setidaknya mempersulit) data Anda di(salah)gunakan.

- **Periksa data pribadimu yang tersebar di internet** Semakin tersebar datamu, semakin mudah orang lain mentarget dirimu, dan semakin besar kemungkinan data tersebut di(salah)gunakan, untuk manipulasi psikologis, dsb.
  - Google dirimu sendiri untuk melihat seberapa banyak datamu dapat ditemukan orang biasa
  - Cek juga pipl.com, peekyou.com, beenverified.com, archive.org.
  - Jika memiliki website, cek data WHOIS websitemu
  - Perika ulang data pribadi yang sudah dipasang di media sosial: Alamat? Tempat kerja? No. telpon? Keluarga? Hobby? Foto-foto diri? Siapa saja yang dapat melihat data pribadimu?

- Biasakan **memeriksa setelan privasi dan keamanan perangkat yang kamu gunakan secara berkala** (sering berubah karena update OS, aplikasi, dsb).
  - **Facebook**: masuk ke Settings > Security & login dan Privacy
  - **Google**: masuk ke https://myaccount.google.com
  - **iPhone**: masuk ke Settings > Privacy. Cek apps apa saja yang mendapat akses ke kamera, foto, daftar kontak, kalender, microphone di dalam iPhonemu. Cek juga Location Services > System Services

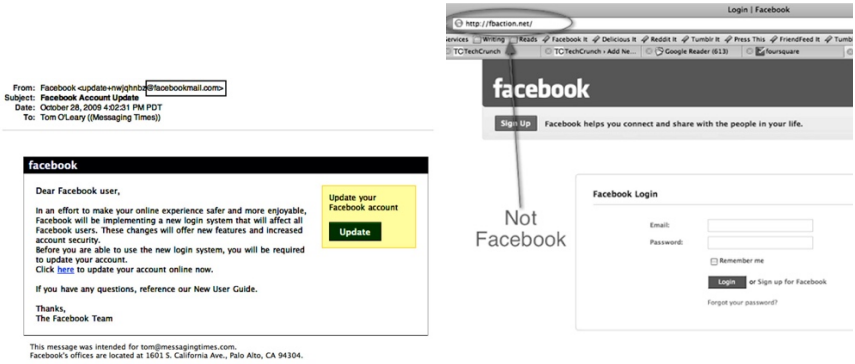
- **Android**: masuk ke Settings > Apps (atau Application Manager) > Permissions. Lebih jauh, cek: https://support.google.com/googleplay/answer/6270602

☐ Resah melihat iklan-iklan online semakin memahami kebiasaanmu? Gunakan **berbagai browser** untuk kebutuhan yang berbeda-beda agar pertukaran data pribadimu terbatasi. Misalnya, gunakan Chrome untuk mengakses Google, Firefox untuk mengakes Facebook, Tor untuk berselancar, dsb. Bisa juga gunakan *private mode* atau *incognito* di browser.

☐ **Perkuat *password*** — gunakan sedikitnya 12 karakter. Pikirkan sebagai *passphrase*, frasa kunci. Gabungkan dari berbagai kata, simbol, angka, dan huruf besar kecil. Contoh: `(JerBasukiM0w0b3yo!)`
- Gunakan **password manager** seperti KeepassXC (open source dan gratis) untuk menyimpan banyak password. Namun ingat juga bahwa menggunakan password manager juga berarti menciptakan satu titik serangan yang menggiurkan.
- Lebih jauh, cek: https://securityinabox.org/id/guide/passwords/ https://ssd.eff.org/en/module/creating-strong-passwords

☐ Aktifkan **two-factor authentication (2FA)**
Biasanya, pilihan untuk mengaktifkan 2FA ada di setelan keamanan & privasi perangkat yang Anda gunakan. Namun ingat juga bahwa 2FA yang berbasis SMS dapat disadap. Dan, ada kemungkinan terkunci tidak bisa login jika sedang di luar negeri tanpa *roaming* atau akses ke no HP biasanya ☺
Tutorial 2FA untuk berbagai perangkat dapat dilihat di: https://www.turnon2fa.com/tutorials/

- Waspadai ***phishing*** yang biasanya berupaya meyakinkan Anda untuk mengklik link, membuka dokumen, menginstall software dalam gadget Anda, atau memasukkan username dan password dalam laman web yang terlihat legit (*credential harvesting*). Ada juga *phishing* yang lebih tertarget, dengan mencari-cari informasi dulu tentang Anda (seperti siapa ibu, ayah, paman atau teman Anda, kemudian mengemail Anda dengan mengaku-aku sebagai mereka; apa profesi atau minat Anda, untuk kemudian memberi tawaran yang sesuai—misalnya, untuk peneliti, peluang untuk mengikuti konferensi di luar negeri dengan dibiayai penuh).



- **Install anti-virus**. Anti-virus cukup berguna untuk menangkis malware pada umumnya (meski tidak untuk *targeted attack*). Mitos bahwa Mac ataupun Linux kebal serangan virus adalah, ya… mitos. Install dan pastikan Anda update. Baiknya jangan jalankan lebih dari 1 anti-virus agar computer tidak berat atau *crash*.

- Sebisa mungkin, pastikan **software dan OS rajin diupdate**. Ini memang cukup kendala, apalagi jika kita menggunakan software bajakan. Pertimbangkan menggunakan versi open source (misal, Linux, LibreOffice, dsb.)

- Jika Anda banyak memiliki data sensitif (Anda bekerja sebagai—atau dengan—jurnalis, system administrator, peneliti, aktivis, dsb.) yang membuat Anda rentan sebagai target serangan, baiknya Anda memastikan bahwa **data dan komunikasi menggunakan *encryption***. Antara lain:
  - Aplikasi chat dapat menggunakan **Signal** atau **Wire**
  - Email dapat menggunakan PGP encryption. Ada beberapa penyedia email dengan encryption seperti Protonmail atau Riseup.

Langkah-langkah di atas hanya sekedar langkah dasar keamanan digital. Masih banyak praktek dan perangkat keamanan digital, yang dapat dibaca lebih lanjut di hal. 14-15. Mencoba untuk melindungi semua data Anda dari semua orang sepanjang waktu tentunya tidak praktis dan tidak realistis.

Yang perlu diingat: **keamanan adalah suatu proses, dan *tradeoff***, yang cukup menyita sumber daya. *Tradeoff* dalam proses ini bisa bermacam-macam: waktu (login jadi lebih lama, tidak langsung bles login karena *cookies* sering Anda hapus), kemudahan (harus mengingat banyak password), biaya (harus *upgrade* software, sementara hardware Anda tidak kuat), dan sebagainya.

Ada baiknya setelah Anda memahami dasar *digital hygiene* di atas, Anda melakukan analisis keamanan di halaman berikut untuk menilai apa yang tepat untuk Anda. Terkadang ini disebut sebagai *threat modelling* atau *risk assessment*. Poin utamanya, keamanan bukan tentang alat atau perangkat (lunak maupun keras) yang Anda gunakan. Ini dimulai dengan memahami konteks potensi ancaman yang Anda hadapi—sesuai kondisi, pekerjaan, dan identitas—dan bagaimana Anda dapat mencegahnya.

ANALISIS KEMANAN (*SECURITY ANALYSIS*)

1 ASET: apa yang mau kamu lindungi?

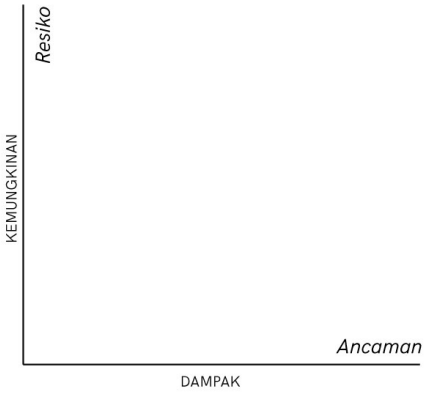
Apa yang membuatmu menjadi target?
Bisa **berwujud** (barang, uang, gedung, website, organisasi atau akun media sosial yang berpengaruh dengan banyak followers (*influencers*), dsb) dan **tak berwujud** (reputasi, informasi, identitas)

2 PENILAIAN RESIKO (RISK ASSESSMENT)

Siapa saja yang ingin/dapat menyerang asetmu?

Apa motivasi musuh menyerang asetmu?
Uang? Ideologi? Reputasi? Diangkat media? Dikenal banyak orang?

Apa saja resiko dan ancaman terhadap asetmu?
Seberapa besar kemungkinan ini terjadi?
Seberapa serius dampaknya jika terjadi?
Petakan di bawah ini



3 PENGAMAN apa yang sudah dan dapat diterapkan?

Seberapa baik pengaman ini mengurangi resiko dan ancaman tersebut?

4 RESIKO LAIN yang mungkin timbul

Apa resiko lain yang dapat ditimbulkan dari solusi pengaman tersebut?
Apakah ada konsekuensi tak terduga, ripple effect?
Apakah masalah lama lebih kecil daripada masalah baru yang ditimbulkan?

5 COST & TRADE-OFF (BIAYA & PENGORBANAN)

Apa biaya, pengorbanan yang dibutuhkan dari solusi pengaman tersebut?
Kemudahan? Kenyamanan? Privasi?

LAYAK & SEIMBANG KAH SOLUSI PENGAMAN TERSEBUT?

Apakah hasil yang didapat dari upaya pengamanan (3) seimbang dengan resiko lain (4) serta biaya & pengorbanan (5) yang timbul?

Bacaan lebih lanjut

Ada banyak sekali perangkat dan panduan kemanan digital, tapi yang perlu diingat adalah: teknologi digital berubah dan menjadi usang dengan sangat, sangat cepat. Karenanya, ketika melakukan (atau mengajar) keamanan digital, cantumkan dan verifikasi *kapan* panduan tersebut dibuat.

Di bawah ini adalah daftar panduan yang ditujukan untuk non-spesialis atau khalayak umum, yang saya adaptasi dari artikel "Current Digital Security Resources" oleh Martin Shelton, UX Security Researcher di Google Chrome. Saya tambahkan juga referensi untuk pengguna berbahasa Indonesia.

Meski ada banyak panduan lainnya, panduan-panduan di bawah ini dipilih dengan pertimbangan relevansi, saran-saran yang praktis, bahasa yang mudah dipahami, struktur yang jelas, dan tentu saja, informasi yang *update* (diperbarui).

- (Frequently updated) **Surveillance Self-Defense (https://ssd.eff.org), by the Electronic Frontier Foundation**. Surveillance Self-Defense is a thorough resource organized into multiple "playlist" of step-by-step guides for several different groups. Each playlist includes a list of modules with information relevant to each group.
- (Frequently updated) **A DIY Guide to Feminist Cybersecurity (https://hackblossom.org/cybersecurity/), by Noah Kelley**, **HACK*BLOSSOM**. This fairly exhaustive guide covers tools for blocking online tracking, circumvention and anonymity tools, defending against malware, strong authentication practices, privacy on social media, as well as device and communication encryption. *Note: There's a lot of great information for defending against untargeted mass surveillance (e.g., using a VPN) which is not directly related to the threat model outlined.*
  Related reading: (April 2017) DIY Online Security Guide for Every Woman, by Chayn (@chaynhq).

- (Last updated May 2017) **A First Look at Digital Security (https://www.accessnow.org/a-first-look-at-digital-security/), by Anqi Li & Kim Burton, Access Now.** A short, beginner-friendly primer booklet on threat modeling, illustrated through personas for multiple security needs.
- (Last updated December 2017) **Security Planner (https://securityplanner.org/), by the Citizen Lab.** This interactive guide is designed to help readers quickly identify the security tips most relevant to them by walking through questions about where you handle private information (e.g., which devices and services?), specific security concerns, as well as information about your unique circumstances. In turn, it provides a detailed list of security recommendations with step-by-step articles on how to learn more.
- **Security in a Box (https://securityinabox.org), by Tactical Tech.** Panduan keamanan digital yang diperuntukkan bagi para aktivis dan pejuang hak asasi manusia di seluruh dunia. Tersedia dalam berbagai bahasa, termasuk **bahasa Indonesia (https://securityinabox.org/id/)**

Kunjungi juga **SAFEnet (http://id.safenetvoice.org/), ICT Watch (http://ictwatch.id/), Internet Sehat (http://internetsehat.id/)** dan **SIBERKREASI (http://siberkreasi.id/)** untuk membaca seputar kesehatan dan keamanan internet di Indonesia. Kemenkominfo juga baru saja menerbitkan situs **Literasi Digital (http://literasidigital.id/)** yang memuat banyak video, infografis, buku dan modul pelatihan dalam bahasa Indonesia.

Untuk lebih banyak lagi daftar sumber keamanan digital (bahasa Inggris) yang sering diperbarui, untuk khalayak umum maupun kelompok pengguna khusus (misalnya jurnalis, aktivis, pelatih kemanan, pengacara), lihat:
Martin Shelton, "Current Digital Security Resources"
https://medium.com/@mshelton/current-digital-security-resources-5c88ba40ce5c.

Booklet ini disusun sebagai materi pendamping (*handout*) untuk lokakarya kemanan digital yang diselenggarakan pada 26 Februari 2018 di C2O library & collabtive.

Penyusun: kathleen azali, dari berbagai sumber

Acara Bulan Aman Internetan 2018 diselenggarakan SAFEnet, ICT Watch, SIBERKREASI dan didukung oleh:

Jakarta:
LSPR Graduate School
Relawan TIK
Nurul Fikri

Depok:
Program Sarjana Ilmu Komunikasi FISIP UI

Bali:
Balebengong

Pontianak:
Jurnalis Perempuan Khatulistiwa
Mafindo Pontianak
Telkomsel

Surabaya:
PERIN+1S
C2O Library
AJI Surabay