PANDUAN

KEAMANAN DIGITAL UNTUK JURNALIS

ALIANSI JURNALIS INDEPENDEN
Alliance of Independent Journalist

PANDUAN

KEAMANAN DIGITAL UNTUK JURNALIS

Adi Marsiela,
Luh De Suriyani

Diterbitkan oleh:

ALIANSI JURNALIS INDEPENDEN
Alliance of Independent Journalist

2022

PANDUAN

KEAMANAN DIGITAL UNTUK JURNALIS

Penulis:
Adi Marsiela
Luh De Suriyani

Editor:
Ika Ningtyas

Diterbitkan oleh:

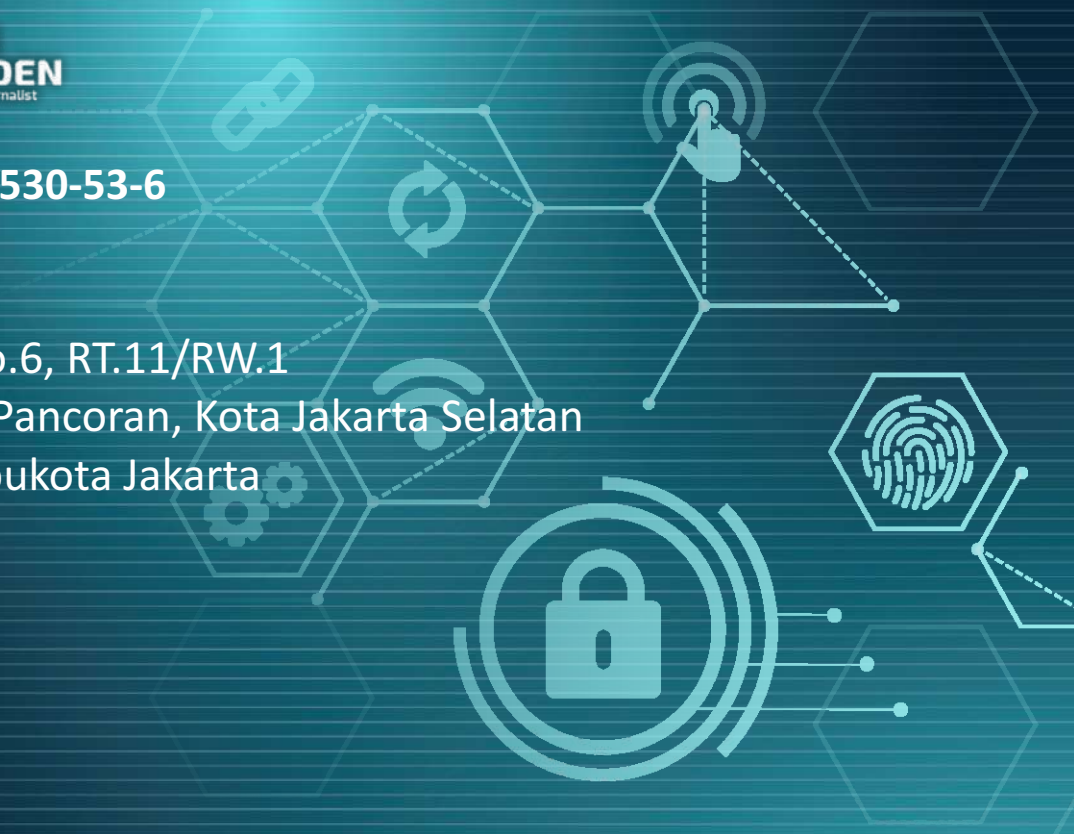
ALIANSI JURNALIS INDEPENDEN
Alliance of Independent Journalist

ISBN : 978-979-3530-53-6

Alamat:
Jl. Sigura Gura No.6, RT.11/RW.1
Duren Tiga, Kec. Pancoran, Kota Jakarta Selatan
Daerah Khusus Ibukota Jakarta

Telepon/Fax:
(6221)3151214
(6221)3151261

Email
sekretariat@ajiindonesia.or.id



Pengantar

Aliansi Jurnalis Independen (AJI) mencatat serangan digital menjadi tren baru yang digunakan sejak 2019 untuk menghambat kerja-kerja jurnalistik. Pada 2020, AJI mendokumentasikan 14 kasus serangan digital dan 5 kasus pada 2021.

Jenis serangan digital yang dominan menyerang jurnalis berupa doxing dan peretasan akun media sosial. Kemudian jenis serangan pada media yang sering terjadi adalah *denial-of-service* (DDoS) dan peretasan terhadap situs.

Pelaku serangan digital terhadap anggota AJI dan jurnalis pada umumnya, bisa datang dari pihak-pihak yang merasa tidak senang dengan aktivisme yang dijalankan anggota AJI, kerja-kerja jurnalistik maupun untuk melecehkan secara seksual. Mereka bisa perorangan hingga pihak-pihak yang memiliki otoritas. Tren di Indonesia, para pendengung (*buzzer*) telah digunakan sebagai alat untuk menyerang aktivis atau kelompok kritis di media sosial, termasuk jurnalis yang kritis terhadap kebijakan pemerintah.

Serangan digital, apapun bentuknya, tidak bisa diabaikan karena kerap menjadi pintu masuk terjadinya kekerasan fisik dan seksual. Dengan skala lebih luas, serangan digital dapat berdampak secara psikis karena informasi pribadi dapat tersebar masif.

Panduan keamanan digital ini dibuat agar anggota AJI dan jurnalis lainnya dapat memahami prinsip keamanan digital yang paling mendasar seperti mengelola informasi pribadi dan memperkuat perangkat digital. Mencegah dan mengurangi risiko tentunya lebih baik, untuk mendukung kerja-kerja organisasi.

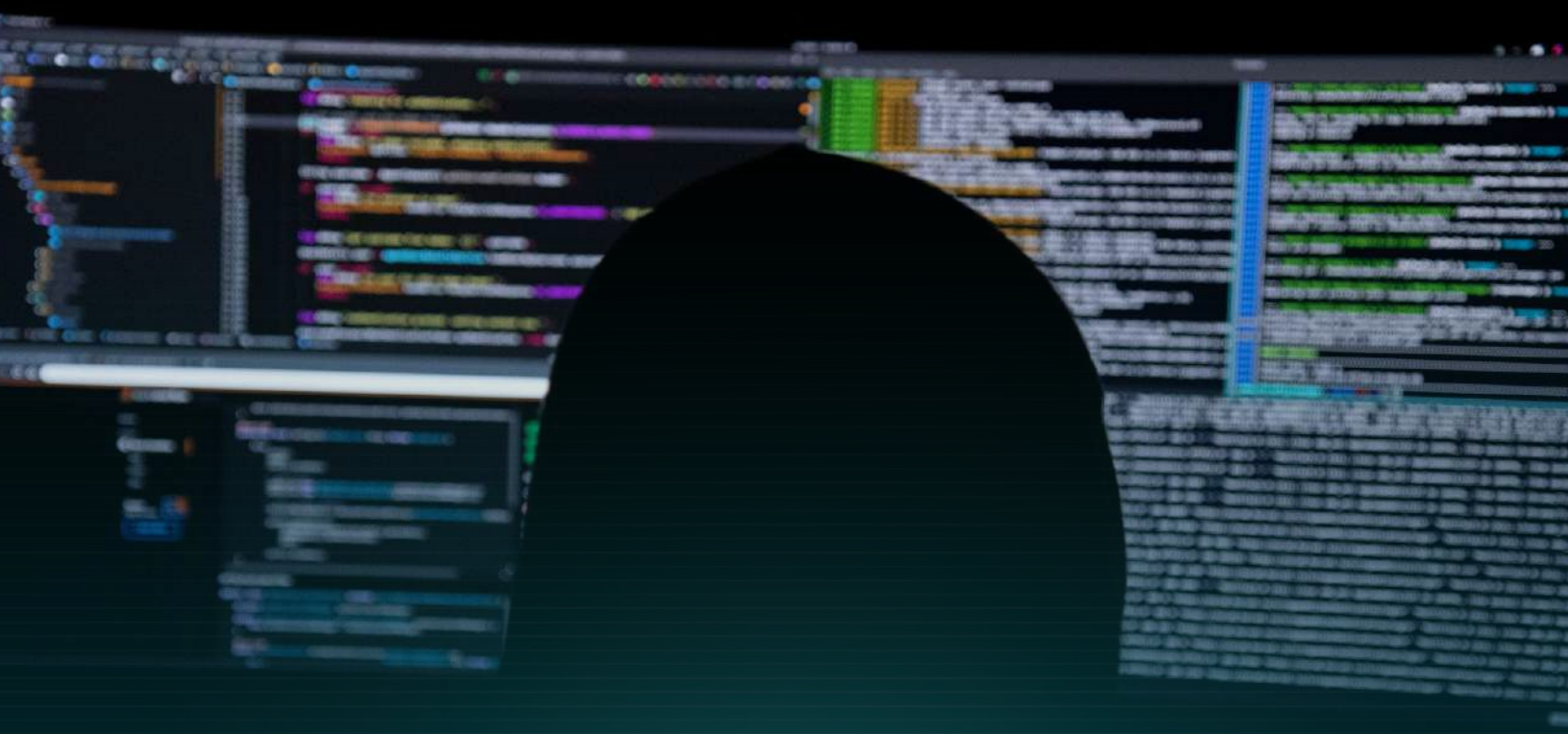
AJI Indonesia berharap panduan Keamanan Digital ini bisa menjawab kebutuhan anggota AJI dan jurnalis lainnya dalam mengantisipasi risiko-risiko yang mungkin muncul di masa depan. Salah satu yang paling penting adalah jurnalis menyadari risiko dan mau mengubah perilakunya.

Panduan ini akan diperbaharui secara berkala karena kebijakan privasi aplikasi terus berubah, demikian juga teknologinya.

Jakarta, Januari 2022

Sasmito
Ketua Umum AJI Indonesia

Daftar isi



BAB 1

Memahami Jenis Ancaman Digital

ALIANSI JURNALIS INDEPENDEN
Alliance of Independent Journalist

BAB 1
Memahami Jenis Ancaman Digital

Ancaman digital adalah tindakan kejahatan yang berupaya merusak data, mencuri data, atau mengganggu kehidupan di dunia maya secara umum. Di era digital, jurnalis memiliki kerentanan ganda menerima ancaman digital, sebagai individual maupun karena risiko dari pekerjaan. Hal ini karena kerja-kerja jurnalis saat ini menggunakan berbagai perangkat teknologi yang terhubung dengan internet, baik dalam berkomunikasi, menggali data, serta mempublikasikan laporannya.

Kekerasan digital bisa menjadi pintu atau bersamaan atas terjadinya bentuk-bentuk kekerasan fisik. Berikut ini adalah bentuk-bentuk ancaman digital yang bisa menyerang jurnalis:

1. Malware

Akronim dari *malicious software* (perangkat lunak berbahaya) adalah program atau file yang berbahaya bagi pengguna komputer atau ponsel. Jenis malware dapat mencakup virus, worm, trojan horse, dan spyware. Program jahat ini dapat melakukan berbagai fungsi berbeda seperti mencuri, mengenkripsi, atau menghapus data, mengubah atau membajak fungsi komputasi inti dan memantau aktivitas komputer atau ponsel pengguna tanpa izin mereka.

2. Phishing

Phishing adalah salah satu kejahatan siber dengan teknik menghubungi target melalui email, telepon atau pesan teks oleh seseorang yang menyamar sebagai lembaga yang sah. Tujuannya untuk memanipulasi individu agar memberikan data sensitif seperti informasi pribadi, rincian kartu kredit dan perbankan, serta kata sandi. Informasi tersebut kemudian digunakan untuk mengakses akun-akun penting dan dapat mengakibatkan pencurian identitas dan kerugian finansial.

3. Peretasan

Peretasan atau *hacking* adalah mengakses perangkat seperti laptop atau ponsel, akun dan jaringan tanpa diketahui oleh pemiliknya. Tujuannya untuk mencari keuntungan financial, memperburuk citra, hingga teror. Peretasan terkait dengan rendahnya keamanan digital dalam perangkat atau akun seseorang.

4. Doxing

Doxing adalah mengumpulkan dan mengumbar informasi pribadi seseorang di internet dengan tujuan mempermalukan atau mengundang pelecehan ke dalamnya. Informasi pribadi yang diumbar melibatkan apa saja mulai dari foto, nomor telepon, alamat rumah, nomor kartu kredit dan riwayat dukungan politik. Pelaku doxing menggunakan informasi pribadi kita yang tersebar di internet untuk menyerang balik dengan narasi yang mengandung fitnah dan kebencian.

5. Pemalsuan (*impersonating*)

Pemalsuan akun (*impersonating*) adalah saat pihak tertentu membuat profil palsu, situs web atau email yang menggunakan nama atau identitas Anda sehingga mirip seperti akun asli Anda. Impersonating bertujuan untuk membuat kampanye kotor, informasi yang menyesatkan, rekayasa sosial atau mencuri identitas seseorang untuk menciptakan kebisingan di medsos, menurunkan kepercayaan, dan pelanggaran data yang berdampak pada reputasi Anda sebagai jurnalis.

6. Pelecehan

Pelecehan online (*online harassment*) adalah perilaku di internet yang mengintimidasi, mengancam, dan mempermalukan nama seseorang di internet. Bentuknya, bisa berupa menyebarkan pernyataan online yang memfitnah atau merendahkan, membuat dan membagikan informasi palsu atau disinformasi tentang seseorang dengan tujuan merusak reputasi mereka, memberi pernyataan cabul, mengirim materi yang ofensif atau cabul, mengedarkan pesan intim seksual (baik berupa foto atau video online) tanpa persetujuan seseorang.

7. Kekerasan berbasis gender online (KBGO)

Jurnalis perempuan atau yang bergender minoritas (LGBT), rentan menjadi korban kekerasan berbasis gender online (KBGO). Survei IFJ pada 2018 menunjukkan bahwa dua pertiga jurnalis wanita (66%) mendapatkan serangan online berbasis gender. Namun hanya setengah kasus serangan ini dilaporkan dan hanya 13 persen pelakunya dapat diungkap atau dibawa ke pengadilan.[1]

Temuan baru atas survei itu mengungkap, bahwa pelecehan yang ditujukan kepada jurnalis perempuan sebagian besar berupa pelecehan seksual, penghinaan atas penampilan fisik mereka, delegitimasi pekerjaan karena identitas gender, menerima gambar atau video cabul dan ancaman berupa pemerkosaan. Bentuk-bentuk pelecehan seperti ini tak dialami jurnalis pria. Temuan lainnya bahwa 75% dari jurnalis perempuan dalam survei yang mendapatkan pelecehan online memilih tidak melaporkan serangan ini. Fenomena tersebut sangat mengkhawatirkan karena meski jurnalis perempuan sering mendapat pelecehan online tetapi mereka menganggap situasi ini sebagai hal "biasa". Padahal salah satu tujuan utama pelaku KGBO adalah membungkam jurnalis.

Bentuk-bentuk ancaman digital terhadap jurnalis tentunya semakin kompleks dan berkembang. Seperti Cyber Amok, Spam Calls, hingga Ddos Attack yang dulunya hanya menyasar pihak-pihak tertentu saja. karena itu masih dibutuhkan lagi pemetaan lebih lanjut yang berbasis survei atau riset mendalam. Selain itu, dari kasus yang pernah terjadi, ancaman digital tersebut tidak datang sendiri-sendiri tapi bisa bersamaan. Doxing yang dialami jurnalis Detik, misalnya, disertai dengan ancaman pembunuhan. Seorang jurnalis yang mengalami peretasan, bisa juga menjadi korban KBGO sekaligus.

[1] Selengkapnya baca di: https://www.ifj.org/media-centre/news/detail/article/ifj-global-survey-shows-massive-impact-of-online-abuse-on-women-journalists.html

BAB 2

Keamanan Perangkat dan Akun

ALIANSI JURNALIS INDEPENDEN
Alliance of Independent Journalist

BAB 2
Keamanan Perangkat dan Akun

1. Keamanan untuk Ponsel

Selain menjadi alat komunikasi pribadi, ponsel digunakan sebagai perangkat penunjang kerja-kerja jurnalistik. Perekaman wawancara, pengambilan foto dan video, memantau informasi dari berbagai belahan dunia hingga proses pengiriman karya jurnalistik. Akan tetapi, kelebihan dan kemudahan itu dibayangi oleh pelbagai kerentanan seperti kehilangan data karena ponsel hilang, peretasan dan penyusupan. Oleh karena itu, anggota AJI harus mengetahui langkah-langkah untuk mengurangi risiko.

1.1 Perlindungan fisik ponsel

a. Hindari membeli ponsel bekas karena berisiko adanya virus atau malware tertentu yang tidak diketahui.
b. Jangan meletakkan ponsel sembarangan, terutama di tempat tempat publik untuk menghindari pencurian dan peretasan.
c. Ponsel perlu diberi pelindung (*casing*) untuk mencegahnya pecah saat terjatuh.
d. Hindari mengisi ulang baterai menggunakan port USB di tempat-tempat publik untuk menghindari *juice jacking* atau pembajakan data. Lebih baik mengisi daya hanya untuk *powerbank*. Apabila tidak membawa *powerbank*, sebaiknya mengisi baterai ponsel dengan kepala charger dan kabel USB milik sendiri. Saat pengisian baterai, ponsel harus dalam kondisi mati (*off*) agar data tidak dibajak.
e. Saat ponsel rusak, perbaiki di *service center* resmi.

Form Penilaian Mandiri
*Silakan tandai pengalaman sendiri dengan mengisi tanda centang sebagai asesmen mandiri**

Perilaku	Ya (Y)	Tidak (N)
Beli ponsel bekas		
Meletakkan ponsel sembarangan		
Belum memakai pelindung (casing)		
Isi ulang baterai menggunakan port USB di tempat publik		
Tidak memperbaiki di *service center* resmi		

**Semakin banyak jawaban anda yang (N) maka semakin baik mitigasi sekaligus perlindungan digital pada ponsel anda. Jika masih banyak jawaban anda (Y) maka sebaiknya segera ubah perilaku anda seperti yang disarankan dalam SOP ini.*

1.2 Perlindungan digital ponsel

a. Gunakan kunci untuk membuka ponsel. Kunci ponsel biasanya berupa sidik jari, pin dan *password*. Penggunaan sidik jari memang unik, namun jika anda lengah dan sedang tertidur, orang lain bisa menguasai ponsel dan mencoba menarik jari Anda guna membuka kunci ponsel. Gunakan pin yang unik untuk mencegah seseorang memasuki ponsel Anda. Hindari pin dari tanggal lahir atau salah satu anggota keluarga.

b. Segera perbarui (update) sistem operasi dan aplikasi di ponsel saat muncul pemberitahuan. Jangan ditunda! Pembaruan perangkat lunak tersebut berfungsi untuk memperbaiki celah keamanan (*bug*) dan peningkatan keamanan yang membantu menjaga ponsel Anda dari pelanggaran dan gangguan data, menutup celah kerentanan dan membuat peretas sulit untuk menerobos.

c. Tambahkan kunci ganda berupa sidik jari/pin/kata kunci di masing-masing aplikasi yang penting di ponsel seperti email, akun media sosial, aplikasi percakapan, dan galeri. Ada beberapa aplikasi yang sudah menyediakan pin. Namun apabila tidak tersedia, Anda bisa unduh beberapa kunci ganda di playstore seperti: AppLock yang dikembangkan oleh ThinkYeah Mobile.

Rekomendasi ini diberikan karena aplikasi tersebut memungkinkan penggunanya mengunci pengaturan sistem hingga panggilan masuk. Kelebihannya, tidak ada iklan yang mengganggu, ringan untuk perangkat, mudah digunakan, fitur berlimpah. Kekurangannya, terkadang terjadi error pada beberapa perangkat.

d. Matikan *bluetooth* saat tidak digunakan atau berada di tempat publik untuk menghindari peretasan dan pencurian data. Pada 2017 diumumkan adanya *bug blueborne* yang bisa menyerang melalui bluetooth yang aktif dan menjadi pintu masuk pencurian data ke ponsel.

e. Hindari menggunakan WIFI publik seperti di kafe, bandara, pusat perbelanjaan atau tempat umum lainnya. WIFI publik bisa jadi pintu terjadi pencurian data, penyadapan dan peretasan di ponsel.

f. Apabila terpaksa menggunakan WIFI publik, akseslah dengan menggunakan *virtual private network* (VPN). VPN menjadi semacam 'terowongan pribadi' yang mengenkripsi semua data Anda untuk membantu mencegah penjahat siber yang bersembunyi dalam jaringan. Layanan VPN gratis yang direkomendasikan adalah RiseUp VPN, Proton VPN, atau TunnelBear (gratis hingga penggunaan 500 MB). Meski begitu, hindari membuka situs yang memungkinkan penjahat siber bisa mengakses identitas, kata sandi, informasi pribadi, atau pekerjaan Anda, seperti layanan perbankan online, email, dan situs jejaring sosial.

   Layanan RiseUp VPN ini dikelola oleh The Riseup Collective, badan otonom yang berbasis di Seattle dengan anggota kolektif di seluruh dunia.
   Rekomendasi penggunaan ProtonVPN terkait dengan pengembangnya yang berasal dari Swiss, negara yang mengedepankan perlindungan data pribadi. Jika menggunakan layanan yang tidak berbayar, pengguna dapat memilih koneksi dari tiga negara. Namun semua server dalam layanan ini dilengkapi lebar pita tak terbatas dan rute DNS untuk mencegah serangan DNS. Peladen ProtonVPN hanya menggunakan protokol aman yang terkenal, seperti OpenVPN. Mereka tidak menggunakan PPTP atau L2TP/IPSec.

   Aplikasi berbayar yang dasar akan memberi akses pada beberapa peladen di 50 negara dengan kecepatan lebih tinggi. Paket plus memiliki akses pada peladen premium, termasuk Secure Core, Tor, P2P, dan server yang dibutuhkan untuk Netflix.

   Rekomendasi penggunaan TunnelBear karena aplikasi VPN ini dapat bekerja pada beragam platform, mulai dari Android, iOS, macOS, hingga Windows. Selain itu, aplikasi ini terbilang stabil dalam kecepatan internetnya. Versi yang gratis memiliki kuota hingga 500MB per bulan. Untuk dapat mengakses VPN sepuasnya perlu

berlangganan. Kekurangan dari aplikasi ini adalah perlu berlangganan premium guna mengakses fitur ekstra.

g. Pasang antivirus untuk mencegah *malware* yang dapat mencuri *password* atau informasi akun Anda. Beberapa android jenis baru telah dilengkapi dengan antivirus.

h. Batasi aplikasi yang akan diunduh. Semakin banyak aplikasi, artinya, semakin banyak informasi pribadi yang direkam dan tersebar. Selain itu, unduh aplikasi hanya dari Google playstore untuk android dan app store untuk iphone dengan membaca ulasan mengenai aplikasi tersebut. Jangan pernah mengunduh aplikasi melalui pesan teks (baik via sms, chat atau email) karena itu adalah metode terkenal yang digunakan peretas untuk menyuntikkan *malware* langsung ke ponsel Anda.

i. Hindari menekan tautan mencurigakan yang dikirim melalui pesan teks. Sebab tautan bisa berisi *malware*. Untuk memeriksa apakah tautan tersebut aman atau tidak, Anda bisa memeriksanya dengan virustotal.com tanpa perlu mengunduh aplikasi. Ini adalah salah satu produk layanan online gratis yang berguna untuk menganalisis berkas dan pranala (URL) dari virus, worm, trojan, dan segala jenis perangkat perusak dengan menggunakan 54 mesin antivirus.

j. Jangan menyimpan data sensitif di ponsel (foto/video *nude*, dokumen atau file penting, rekaman dari sumber anonim dll). Audit sesering mungkin file yang tersimpan di ponselmu dan segera pindahkan data yang penting ke *hard disk external* atau laptop.

k. Rutin menghapus informasi atau percakapan yang sensitif di aplikasi percakapan daring.

l. Apabila android Anda hilang, lakukan penghapusan data jarak jauh dengan membuka tautan ini: https://www.google.com/android/find. Metode ini akan menghapus semua data di ponsel secara permanen, terkecuali data di kartu SD.

Bagaimana risiko anda terkait perlindungan digital ponsel? Silahkan nilai sendiri dengan membaca perilaku di sisi kiri dan tuliskan perilaku anda (Ya/Tidak) di bawah ini.*

Perilaku	Ya (Y)	Tidak (N)
Melindungi ponsel dengan password atau pola agar tidak mudah diakses orang lain		
Memperbarui sistem operasi (OS) jika tersedia		
Memperbarui aplikasi jika tersedia di OS		
Mengganti nama ponsel agar tidak mudah dikenali saat terkoneksi bluetooth, wi-fi		
Menonaktifkan sambungan wi-fi, bluetooth jika tidak digunakan		
Menggunakan (install) aplikasi dari sumber resmi		
Mengaktifkan lokasi saat diperlukan saja		
Menghapus riwayat wifi pada ponsel agar tidak meninggalkan jejak digital		
Selalu log-out dari aplikasi email jika tidak dipergunakan dalam waktu lama, misal satu pekan		
Mengetahui akses (data dan fungsi) dari setiap aplikasi di smartphone		
Melakukan pencadangan data ponsel minimal sebulan sekali		
Rutin mengecek serta menghapus aplikasi dan data apa saja yang sudah tidak dipergunakan		
Menggunakan/mengaktifkan VPN saat mengakses wifi publik		
Sudah memasang antivirus di ponsel		
Akses masuk ke ponsel menggunakan PIN		
Sudah mengaktifkan enkripsi pada ponsel		

**Semakin banyak jawaban anda yang (Y) maka semakin baik mitigasi sekaligus perlindungan digital pada ponsel anda. Jika masih banyak jawaban anda (N) maka sebaiknya segera ubah perilaku anda seperti yang disarankan dalam SOP ini.*

2. Keamanan Laptop/Komputer

Selain ponsel, laptop atau komputer menjadi perangkat yang sering digunakan untuk pekerjaan. Prinsip keamanan untuk laptop/komputer, tidak jauh berbeda dengan gawai.

2.1 Perlindungan fisik laptop/komputer

a. Hindari membeli laptop/komputer bekas karena berisiko adanya virus atau malware tertentu yang tidak diketahui.

b. Jangan meletakkan laptop sembarangan, terutama di tempat tempat publik untuk menghindari pencurian dan peretasan.

c. Laptop perlu diberi pelindung (casing) untuk mencegahnya rusak saat terjatuh.

d. Saat laptop rusak, perbaiki di *service center* resmi.

Form Penilaian Mandiri keamanan laptop/komputer:

Perilaku	Ya	Tidak
Menggunakan laptop baru		
Menggunakan pelindung/casing body laptop		
Memperbaiki laptop di tempat resmi		
Tidak memasang stiker/label di body laptop yang identik dengan pekerjaan atau sikap politik		

**Semakin banyak jawaban anda yang (Y) maka semakin baik mitigasi sekaligus perlindungan digital pada ponsel anda. Jika masih banyak jawaban anda (N) maka sebaiknya segera ubah perilaku anda seperti yang disarankan dalam SOP ini.*

2.2 Perlindungan digital laptop/komputer

a. Selalu perbarui *operating system* agar terlindung dari malware atau virus.

b. Selalu perbarui dan install aplikasi resmi.

c. Pasang antivirus.

d. Tutup kamera bawaan pada laptop atau webcam saat tidak dipergunakan.

e. Pasang kombinasi frasa untuk sandi mengakses laptop/komputer anda.

f. Pasang sandi buat window.

g. Ketuk ikon *window> setting> sign-in option>* lalu pilih mau pakai apa PIN/security key.

h. Pasang sandi buat Mac OS. Ketuk ikon apel > *system preferences* > *security & privacy* > *general* > ketuk simbol gembok di kanan bawah agar terbuka> atur password.

i. Aktifkan fitur enkripsi pada laptop/komputer anda untuk menyamarkan file atau dokumen.

j. Pasang enkripsi buat windows dengan langkah-langkah berikut:

https://support.microsoft.com/en-us/windows/turn-on-device-encryption-0c453637-bc88-5f74-5105-741561aae838

atau unduh dan install https://www.veracrypt.fr/code/VeraCrypt/

Langkah-langkah untuk pemasangan enkripsi di Mac OS: Ketuk ikon apel > *system preferences* > *security & privacy* > *FileVault* > nyalakan jadi ON, tentu sebelumnya harus buka gembok di kiri bawah.

k. Aktifkan Firewall

Langkah-langkah mengaktifkan Firewall di Windows:

Settings > *Update and security* > klik *Firewall and protection*

Mengaktifkan Firewall di Mac OS:

Ketuk ikon apel > *System Preference* > *security & privacy* > aktifkan *Firewall*

l. Mematikan fitur lokasi pada laptop

Langkah-langkah untuk mematikan fitur lokasi pada Windows:

Setting > *Privacy* > *Location* (matikan 'Pin to Start')

Mematikan fitur lokasi di Mac OS:

Sistem *Preference* > *security & privacy* > matikan *location*

m. Hapus riwayat koneksi WIFI

Langkah-langkah untuk Windows:

Cari ikon WIFI di kanan bawah > ketuk kanan > *Open Network and Internet Setting* > cek jaringan yang terkoneksi otomatis > padamkan

Langkah-langkah untuk Mac OS:

System preferences > *network* > *advanced* > WIFI (tinggal dipilih nama jaringan lalu pilih kurangi dengan icon untuk jaringan yang ingin dilupakan)

n. Ganti nama device

o. Bersihkan dokumen atau file yang sudah dihapus dengan aplikasi https://www.ccleaner.com/ccleaner

Formulir penilaian mandiri perlindungan digital laptop/komputer

Perilaku	Ya	Tidak
perbarui *operating system*		
perbarui dan install aplikasi resmi		
Pasang antivirus		
Tutup kamera bawaan pada laptop atau webcam saat tidak dipergunakan		
Kata sandi di laptop/komputer		
Aktifkan fitur enkripsi pada laptop/komputer		
Aktifkan Firewall		
Mematikan fitur lokasi		
Hapus riwayat koneksi Wifi		
Ganti nama device		

**Semakin banyak jawaban anda yang (Y) maka semakin baik mitigasi sekaligus perlindungan digital pada ponsel anda. Jika masih banyak jawaban anda (N) maka sebaiknya segera ubah perilaku anda seperti yang disarankan dalam SOP ini.*

3. Keamanan Akun

Ciri-ciri akun medsos yang diretas:

a. Ada email yang masuk dan menerangkan ada pihak dengan perangkat tertentu yang coba masuk ke akun medsos kita padahal kita tidak pernah melakukan hal tersebut.
b. Ada masalah saat login ke akun medsos.
c. Medsos tiba-tiba dibanjiri banyak iklan.
d. Secara tiba-tiba follow akun-akun tidak dikenal.
e. Ada unggahan pada medsos padahal kita tidak melakukannya.

3.1 Cara mengamankan akun medsos

a. Hapus permanen akun yang sudah tidak digunakan, bukan sekedar logout tapi hapus untuk selamanya.
b. Cek aplikasi apa saja yang terhubung dengan aplikasi sosial media.
c. Praktikkan penggunaan password yang aman: setiap akun medsos memiliki password yang berbeda, jangan lupa sertakan huruf kapital, huruf kecil, angka, karakter (tapi jangan lupa juga sama password) atau penggunaan sebuah kalimat atau frase.
d. Update aplikasi medsos secara reguler.
e. Pakai email berbeda-beda untuk masing-masing akun sosial media/aplikasi cuma-cuma yang terhubung via internet.

3.2 Jika akun medsos diretas, apa yang bisa dilakukan?

a. Cek perangkat apa saja yang terhubung dengan akun medsos kita, jika ada perangkat tidak dikenal, maka hapus.
b. Jika kita tidak login dengan username dan password yang bisa kita gunakan, laporkan kondisi itu pada *help center* aplikasi medsos yang kita pakai.
c. Ganti password dengan menggunakan karakter unik dan beda-beda untuk masing-masing akun medsos.
d. Aktifkan juga *two factor authentication.*
e. Cek kembali *account permissions* dan batas akses dari aplikasi yang kita gunakan/hendak install.
f. Install anti-virus pada perangkat seluler.

Tautan untuk mengecek aplikasi lain yang memiliki akses ke medsos:

Facebook: https://www.facebook.com/settings?%20tab=applications&section=all
Instagram: https://www.instagram.com/accounts/manage_access/
LinkedIn: https://www.linkedin.com/psettings/permitted-services
Twitter: https://twitter.com/settings/applications

BAB 3

Manajemen Identitas

ALIANSI JURNALIS INDEPENDEN
Alliance of Independent Journalist

BAB 3
Manajemen Identitas

Dengan banyaknya aktivitas anggota AJI dan jurnalis lain di media digital, maka kita perlu untuk lebih mawas diri dalam menjaga keamanan personal. Apalagi, keamanan kita juga juga bisa berdampak terhadap keamanan orang lain maupun organisasi. Untuk bisa menerapkan keamanan digital di tingkat personal, kita perlu memahami beberapa hal.

Serangan digital sering kali dilakukan dengan mengumpulkan data-data pribadi tentang kita yang berserak di Internet. Pada dasarnya, data ini bisa berupa data itu sendiri maupun metadata atau data tentang data. Contohnya, data yang kita unggah adalah foto ketika kita sedang berada di lapangan sedangkan metadata adalah data berupa waktu (hari, tanggal, dan jam) pengambilan foto, tipe kamera untuk mengambil foto, atau bahkan lokasi pengambilan foto jika fungsi GPS pada perangkat tersebut.

Contoh lain data dan metadata bisa kita lihat pada komunikasi kita dengan surel. Laporan dan lampiran kita dalam surel adalah data sedangkan metadata adalah apa layanan surel yang kita pakai, kapan surel dikirim, apa alamat surel kita dan surel tujuan, alamat IP kita, hingga apa layanan Internet yang kita pakai.

Data bisa kita sembunyikan, tetapi metadata tidak bisa disembunyikan begitu saja. Semua data yang kita tinggalkan saat beraktivitas daring menjadi jejak digital. Bagi orang yang memang dengan sengaja mengincar kita, jejak-jejak digital yang tersebar di berbagai platform itu bisa menjadi bahan untuk melakukan rekayasa sosial (*social engineering*).

Pelaku bisa menarget kita berdasarkan data-data pribadi tersebut. Berikut beberapa tindakan yang bisa kita lakukan sebagai bagian dari meningkatkan keamanan digital personal.

2.1 Menemukan identitas digital

a. Coba cek nama Anda di mesin pencari seperti Google atau DuckDuckGo.
b. Perhatikan apa saja identitas Anda yang bisa ditemukan di sana.
c. Refleksikan seberapa besar risiko terhadap keamanan, jika identitas pribadi tersebut beredar di ranah digital.
d. Siapakah pemilik identitas digital Anda tersebut dan di mana identitas itu berada?
e. Jika Anda tidak nyaman dan merasa berisiko, bisakah Anda menghapusnya? Bisa dengan menghubungi penyelenggara platform dan menyatakan konten yang ada berkaitan dengan informasi pribadi.

Untuk mengajukannya, Anda bisa membuka fitur legal help di laman Google Support atau mengikuti petunjuk pada tautan ini.

Langkah selanjutnya pilih opsi ‘create a request’. Kemudian pilih produk Google yang kontennya ingin dihapus. Masukkan alasan permohonan penghapusan konten. Ada enam pilihan yang disediakan, di antaranya, ‘right to be forgotten’, melaporkan phishing, pencemaran nama baik, masalah hak cipta, hingga masalah hukum lainnya.

Ada tautan yang disertakan untuk setiap konten dari produk Google yang Anda pilih untuk dihapus. Isi seluruh data dan informasi yang diperlukan. Kirimkan formulir permohonan tersebut.

Google bakal meninjau laporan yang masuk secara manual terlebih dulu. Setelah ada keputusan, pemohon/pelapor akan menerima surat elektronik berisi notifikasi terkait permohonannya. Proses permohonan pengguna oleh Google ini bakal memakan waktu lama dan tidak serta merta selesai berdasarkan telaah informasi yang kami lakukan.

2.2 Memeriksa kebocoran identitas

a. Periksa apakah surel Anda pernah menjadi korban kebocoran data atau tidak.
b. Untuk memeriksa kebocoran email, gunakan www.haveibeenpawned.com atau https://monitor.firefox.com/. Masukkan alamat email Anda. Situs tersebut akan memberikan hasil analisis, apakah email Anda pernah bocor atau tidak.
c. Jika email Anda pernah bocor di layanan tertentu, segera ganti kata sandinya di layanan tersebut.

2.3 Mengelola identitas digital

a. Gunakan surel berbeda untuk jenis kegiatan berbeda, seperti antara surel untuk pekerjaan, belanja, dan hiburan.
b. Gunakan peramban berbeda untuk kegiatan yang berbeda pada saat berselancar agar tidak terdeteksi satu sama lain.
c. Periksa akun-akun yang sudah lama tidak digunakan dan hapus akunnya jika memang sudah tidak diperlukan.

2.4 Memperkuat kata sandi

a. Periksa ulang seberapa tinggi tingkat keamanan kata sandi yang kita gunakan. Misalnya di www.howsecuremypassword.com. Ingat tuliskan saja pola kata sandinya, bukan kata sandi yang sebenarnya, untuk menghindari perekaman di situs itu. Misal, kata sandi anda hanya terdiri dari 9 karakter huruf seperti kilimanjaro. Coba kombinasikan format kata sandi anda dengan huruf kapital dan angka menjadi Kil1m4nj4r0. Bakal terlihat waktu yang digunakan untuk menjebol kata sandi Anda yang baru akan lebih lama dibandingkan sebelumnya.
b. Perkuat keamanan kata sandi dengan menggunakan kombinasi antara huruf, angka, simbol, dan besar kecilnya huruf.
c. Disarankan untuk membuat kata sandi berupa kalimat yang mudah diingat, tetapi tidak terkait dengan kita setidaknya yang diketahui publik.

2.5 Mengelola kata sandi

a. Gunakan kata sandi berbeda untuk akun berbeda-beda sehingga ketika satu akun mengalami kebocoran data, akun lainnya tak akan otomatis diketahui juga. Kata sandi yang direkomendasikan adalah frasa atau berbentuk kalimat. Gunakan pola yang memudahkan mengingatnya.
b. Gunakan aplikasi penyimpan atau pengelola kata sandi (password manager) untuk memudahkan pengelolaan kata sandi berbeda-beda untuk semua identitas digital.
c. Gantilah kata sandi secara berkala, misalnya setahun sekali, untuk mengantisipasi jika kata sandi tersebut sudah bocor.

2.6 Menggunakan keamanan dua lapis

a. Aktifkan autentikasi dua langkah (2FA) pada tiap akun yang memiliki fungsi tersebut.
b. Pengaturan 2FA tiap akun berbeda-beda, tetapi pada dasarnya dia menggunakan kata sandi satu kali pakai, biasanya dalam bentuk angka, ke aplikasi atau perangkat yang dipakai untuk melakukan autentikasi dibandingkan pakai SMS karena SMS bisa disadap dan tidak terenkripsi.
c. Sebaiknya gunakan aplikasi autentikasi seperti Google Authenticator atau ESET. Layanan dari Google ini menawarkan kemudahan tapi saat pindah HP harus melakukan kloning dulu sebelum pindah ke HP baru, jika tidak maka semua kunci akan hilang dan tidak bisa dikembalikan.

   Jika memiliki waktu lebih dapat menggunakan Twilio Authy. Kelebihan dari Twilio jika perangkat seluler di-*instal* ulang, bisa menggunakan informasi log-in di perangkat yang baru. Kekurangannya adalah menggunakan nomor untuk login.
d. Khusus untuk staf admin TI dan website bisa ditambah dengan Yubikey sebagai pengamanan tambahan. Perangkat keras itu berfungsi sebagai langkah kedua untuk mengakses server data, server web dan aplikasi yang lain. Jadi, pemegang akun root tidak bisa melakukan perintah root kalau tidak menggunakan yubikey/ yubico.
e. Pengaktifan 2FA juga bisa dilakukan pada peralatan untuk mengelola koneksi Mikrotik agar tidak bisa diakses pihak lain dengan mudah.

2.7 Mengatur privasi pada layanan

a. Periksalah pengaturan privasi di platform digital yang kita gunakan.
b. Periksa lagi, informasi pribadi apa yang direkam oleh platform. Pengaturan di Google misalnya, bisa dicek di tautan https://policies.google.com/privacy. Sedangkan pengaturan privasi pada Google bisa dicek di https://myaccount.google.com/intro/privacycheckup.
c. Untuk informasi pribadi yang direkam oleh Facebook, bisa dicek melalui https://www.facebook.com/about/privacy. Sedangkan pengaturan privasi pada Facebook melalui tautan ini:

https://www.facebook.com/about/basics/manage-your-privacy.

d. Lakukan pemeriksaan serupa pada platform lain yang kita gunakan, seperti Twitter, Instagram, YouTube, dan lain-lain.

2.8 Mengecek terjadinya phising

Seperti yang dijelaskan di bab sebelumnya, phising adalah salah satu jenis kejahatan online untuk menipu atau mengelabui dengan tujuan buruk. Misalnya mengirimkan tautan atau link berisi virus atau malware untuk mencuri password dan data penting lainnya. Bentuk phising saat ini makin beragam dan sulit dikenali. Kita harus terus mengasah kepekaan untuk bisa melakukan deteksi awal. Intinya, jangan membuka sesuatu yang tidak pernah dicari, dibutuhkan, atau tidak dikenali.

Salah satu cara melatih diri mengenali phising bisa melalui kanal ini:
https://phishingquiz.withgoogle.com/

2.9 Penilaian Risiko

Berikut tabel yang bisa Anda gunakan untuk menilai risiko terkait manajemen identitas yang terkait dengan pekerjaan atau kebutuhan pribadi. Silahkan identifikasi ada berapa banyak identitas pribadi Anda berdasarkan jenis-jenis layanan dan aplikasi berbasis internet yang digunakan atau dimiliki. Semakin detail kita menuliskannya, semakin bisa kita menilai risiko terkait ancaman digital.

Formulir penilaian risiko manajemen identitas

Jenis	Layanan	Peruntukan	ID	Password	Terkait dengan
Email 1	(Gmail/Yahoo/Proton/email kantor/dll)	(Pekerjaan kantor/komunikasi pribadi/akses ke aplikasi dll)		Kombinasi (angka, huruf, simbol, KAPITAL, huruf biasa). Saat ini juga direkomendasikan bentuk kalimat sebagai sandi yang lebih kuat.	(Google Drive, aplikasi apa saja, Youtube, Canva, Tableau, Linkedin, dll).
Medsos 1	Twitter	Pekerjaan		Kombinasi angka, huruf besar dan kecil, atau kalimat.	Ada informasi akun Instagram

Medsos 2	Twitter 2	Pribadi (contoh)		Kombinasi angka, huruf besar dan kecil, atau kalimat.	Akun alternatif
Web 1	instink.net	Pekerjaan		Kombinasi angka, huruf besar dan kecil, atau kalimat.	Portal media siber
canva	desain	Pekerjaan desain		Kombinasi angka, huruf besar dan kecil, atau kalimat.	Email kerja
Silakan tambahkan seterusnya sesuai jumlah akun yang Anda miliki					

Petunjuk pengisian:

Kolom (1) Jenis : Diisi dengan berbagai layanan/aplikasi yang Anda gunakan di internet
Kolom (2) Layanan : Diisi dengan layanan spesifik. Contoh jika email maka tuliskan platform email yang Anda gunakan seperti Gmail, Yahoo, Proton, Thunderbird, termasuk alamat portal dan lainnya sesuai yang dimiliki.
Kolom (3) Peruntukan : Diisi dengan keterangan untuk kebutuhan pekerjaan atau pribadi.
Kolom (4) ID : Diisi dengan nama akun/ID/profil di layanan atau aplikasi.
Kolom (5) Password : Diisi dengan penerapan password, seperti apakah menggunakan angka, tanda baca, huruf kecil, huruf kapital, atau kalimat (bukan password-nya)
Kolom (6) Terkait dengan: Diisi dengan koneksi antara layanan itu dengan layanan lainnya. Misalnya untuk mengakses layanan Twitter Anda, maka 2FA-nya akan terhubung dengan email atau Google Authenticator.

BAB 4

Keamanan Komunikasi

ALIANSI JURNALIS INDEPENDEN
Alliance of Independent Journalist

BAB 4
Keamanan Komunikasi

Sebagaimana disebutkan dalam salah satu prinsip keamanan digital, keamanan diri Anda secara pribadi, juga ditentukan oleh pihak lain, terutama orang yang kita ajak berkomunikasi dan perangkat yang digunakan. Dalam komunikasi digital, komunikasi menjadi lebih kompleks. Sebab dapat melibatkan banyak pihak, tidak hanya pengirim dan penerima pesan, tetapi juga beragam perangkat dan alur seperti modem, penyedia jasa Internet, peladen, pintu gerbang antar-negara (national gateway), dan seterusnya.

Agar komunikasi melalui Internet tersebut lebih aman, berikut adalah beberapa tindakan yang bisa dilakukan.

3.1 Memilih dan mengelola peramban (*browser*)

a. Gunakan peramban yang memberikan pilihan privasi pada penggunanya, seperti Firefox dan Brave. Sejumlah peramban menyimpan aktivitas kita, mulai website yang pernah dibuka, kata kunci, IP address, lokasi dll.
b. Aturlah agar hanya seminimal mungkin aktivitas pribadi yang direkam oleh peramban tersebut. Perbandingan privasi dan keamanan peramban bisa dicek di https://www.mozilla.org/en-US/firefox/browsers/compare/.
c. Pengaturan privasi dan keamanan pada Chrome bisa dicek di chrome://settings/privacy. Sedangkan pengaturan privasi dan keamanan pada Firefox bisa dicek di about:preferences#privacy. Periksalah apa saja jejak digital yang direkam oleh peramban tersebut dan pikirkan ulang apakah Anda memang harus membiarkannya direkam atau tidak.
d. Bersihkan riwayat penelusuran atau aktivitas daring yang tersimpan di peramban.
e. Jangan pernah merekam identitas ataupun aset digital yang berisiko tinggi, seperti kata sandi, nomor kartu kredit, dan semacamnya.
f. Pilihlah agar semua akun Anda akan otomatis keluar ketika peramban ditutup

3.2 Memastikan keamanan protokol situs/laman

a. Pastikan situs web yang kita akses sudah menggunakan protokol *https* (*hypertext transfer protocol secure*) bukan *http*. Protokol *https* artinya situs tersebut sudah menggunakan enkripsi. Sehingga data yang Anda masukkan tidak bisa dibaca oleh pihak ketiga yang berada di tengah-tengah.
b. Jangan memasukkan nama pengguna dan kata sandi pada situs web yang masih menggunakan protokol *http*, misalnya untuk membuka email atau akun media sosial, dan rekening bank.

3.3 Menambah plugin atau add-ons untuk deteksi awal

Ada beberapa *plugin* atau *add-ons* yang dapat berfungsi untuk meningkatkan keamanan dan memberikan pemberitahuan (alert) saat terjadi aktivitas yang mencurigakan saat Anda berkomunikasi menggunakan internet.

a. Privacy Badger berguna untuk mengetahui aplikasi apa saja yang merekam aktivitas Anda saat mengunjungi situs tertentu. Tambahkan add-ons privacy badger untuk Mozilla di tautan ini: https://addons.mozilla.org/en-US/firefox/addon/privacy-badger17/

   Sedangkan untuk Chrome, tambahkan dari tautan ini: https://chrome.google.com/webstore/detail/privacy-badger/pkehgijcmpdhfbdbbnkijodmdjhbjlgp

b. HTTPS Everywhere berguna untuk mengenkripsi protokol situs web yang belum menggunakan https. Untuk Mozilla tambahkan dari tautan ini: https://addons.mozilla.org/en-US/firefox/addon/https-everywhere/

   Untuk pengguna Chrome tambahkan dari : https://chrome.google.com/webstore/detail/https-everywhere/gcbommkclmclpchllfjekcdonpmejbdp?hl=en

c. Cookie AutoDelete berguna untuk menghapus cookies (remah-remah jejak digital) begitu kita menutup peramban.

   Bagi pengguna chrome, tambahkan cookie autodelete dari tautan ini: https://chrome.google.com/webstore/detail/cookie-autodelete/fhcgjolkccmbidfldomjliifgaodjagh?hl=en

   Bagi pengguna Mozilla: https://addons.mozilla.org/en-US/firefox/addon/cookie-autodelete/

d. No Script. Perlindungan maksimal untuk browser: NoScript mengizinkan konten aktif hanya untuk domain tepercaya pilihan untuk mencegah eksploitasi.

   Bagi pengguna chrome: https://chrome.google.com/webstore/detail/noscript/doojmbjmlfjjnbmnoijecmcbfeoakpjm

3.4 Berbagi berkas pekerjaan (*file sharing*)

Gunakan layanan berbagi berkas yang lebih peduli pada keamanan dibandingkan Google Drive. Alternatif yang tersedia yakni:

a. Untuk berbagi dokumen pekerjaan secara bersama-sama, Anda bisa menggunakan: www.cryptpad.fr.
b. Untuk berbagi berkas dalam ukuran besar bisa menggunakan https://send.tresorit.com/
c. Untuk berbagi dokumen ataupun berkas lain dengan www.mega.nz

3.5 Mengelola aplikasi percakapan

a. Gunakan aplikasi percakapan yang memberikan fungsi enkripsi ujung ke ujung (*end to end encryption*). Enkripsi dari ujung ke ujung artinya sistem komunikasi yang hanya bisa dibaca oleh pengguna yang berkomunikasi.
b. Hindari menggunakan WhatsApp untuk berkomunikasi informasi yang berisiko tinggi. Karena meskipun whatsapp mengklaim sudah menggunakan enkripsi ujung ke ujung, tetapi rentan diserang karena popularitasnya, berdasarkan sejumlah kasus peretasan yang terjadi.
c. Gunakan alternatif aplikasi percakapan yang menyediakan fasilitas untuk menghancurkan pesan secara otomatis, seperti Telegram, Signal, dan Wire.
d. Matikan fungsi pencadangan otomatis terutama jika aplikasi itu untuk percakapan berisiko tinggi.
e. Kombinasikan penggunaan aplikasi percakapan berbeda-beda agar bisa memecah komunikasi

3.6 Mengelola aplikasi panggilan video

a. Gunakan aplikasi panggilan video sesuai dengan kebutuhan dan kondisi.
b. Zoom merupakan aplikasi yang sudah terenkripsi dari ujung ke ujung, tetapi dia berbayar untuk panggilan lebih dari 1 jam, dan menyimpan riwayat penggunanya.
c. Jitsi merupakan aplikasi panggilan video terenkripsi dari ujung ke ujung dan gratis tanpa terikat waktu. Jitsi juga sangat menjaga anonimitas pengguna karena tidak perlu login untuk menggunakannya.
d. BigBlueButton juga bisa menjadi pilihan panggilan video yang aman.

3.7 Menyamarkan jejak komunikasi dengan VPN

a. Gunakan virtual *private network* (VPN) jika mengakses wifi di tempat umum seperti kafe, hotel, bandara, dan lain-lain. Pilih VPN yang sudah dikenal dan dipercaya oleh komunitas, seperti ProtonVPN, RiseUp VPN, TunnelBear, NordVPN, dan semacamnya.
b. Hindari penggunaan VPN yang menggunakan peladen di negara negara otoriter seperti

Rusia dan Cina.

c. Menggunakan VPN yang tidak kredibel justru rentan membuat Anda jadi korban kejahatan digital.

3.8 Memilih surel (email) yang aman

a. Gunakan layanan email yang menyediakan fungsi enkripsi seperti Rise Up, Protonmail, Disroot, dan Tutanota.
b. Tambahkan fungsi enkripsi pada email kantor seperti PGP-Key atau Enigmail pada aplikasi pengelola surel Thunderbird.
c. Tambahkan aplikasi enkripsi seperti Mailvelope pada layanan email yang tidak terenkripsi.

3.9 Memeriksa lampiran dan tautan

a. Jika Anda menerima email berisi tautan (link) dan lampiran (attachment) dari orang yang tidak dikenal sama sekali, hindari langsung membuka tautan dan lampiran tersebut. Sebab bisa saja, tautan atau lampiran tersebut telah ditanam malware yang bisa menginjeksi laptop/handphone Anda. Malware dapat mematai-matai aktivitas atau mencuri data dari perangkat.
b. Periksalah tautan dan lampiran tersebut secara daring pada platform pemeriksa keamanan seperti https://urlscan.io/ atau https://www.virustotal.com/gui/home/upload

3.10 Memilih mesin pencari

Gunakan mesin pencari yang tidak merekam jejak pencarian, seperti DuckDuckGo (https://duckduckgo.com/), StartPage (https://www.startpage.com/), atau Qwant (https://www.qwant.com/).

3.11 Memastikan keamanan website berita/organisasi

Ada sejumlah cara sederhana untuk menilai keamanan website berita atau situs organisasi yang Anda miliki. Penilaian awal ini menjadi langkah untuk memitigasi serangan *denial-of-service.* Namun, untuk menguji secara detail, harus berkoordinasi dengan tim keamanan jaringan.

a. https://sitecheck.sucuri.net/
b. https://www.webpagetest.org/

BAB 5

Keamanan Liputan

ALIANSI JURNALIS INDEPENDEN
Alliance of Independent Journalist

BAB 5
Keamanan Liputan

Pekerjaan keluar kota atau kunjungan lapangan merupakan kegiatan berisiko tinggi sebab ada beberapa situasi yang tidak bisa sepenuhnya bisa Anda kendalikan. Hal ini juga akan mempengaruhi situasi, risiko, dan potensi ancaman digital terhadap Anda. Untuk itu ada beberapa tindakan yang bisa kita lakukan untuk mencegah terjadinya serangan digital atau kerusakan aset digital yang tidak kita inginkan, terutama jika topik liputan tersebut memang berisiko tinggi.

Tindakan mitigasi yang bisa dilakukan sebelum dan saat Anda liputan adalah:

a. Menyiapkan ponsel khusus atau cadangan

- Siapkan ponsel cadangan atau ponsel khusus jika perusahaan media Anda tidak menyediakan.
- Gunakan identitas berbeda di ponsel cadangan tersebut, misalnya nama alias dengan email berbeda untuk menghindari penggunaan identitas sama di dua perangkat berbeda.
- Dalam situasi tertentu, ponsel jadul atau murahan justru lebih membantu karena tidak terkoneksi langsung ke internet. Meski begitu, waspadai penggunaan panggilan seluler atau SMS karena tidak terenkripsi.

b. Kurangi informasi sensitif di perangkat

- Sebelum berangkat, periksalah apa saja data penting yang ada di ponsel.
- Hapus data-data penting di ponsel yang tidak kita perlukan selama perjalanan, misalnya dokumen atau rekaman wawancara hasil investigasi, atau data pribadi yang sensitif.
- Matikan fungsi lokasi.
- Periksa fungsi lokasi pada ponsel atau laptop agar tidak otomatis menunjukkan lokasi di mana Anda berada.
- Jika memerlukan petunjuk lokasi, usahakan bertanya kepada warga sekitar dibandingkan menggunakan aplikasi di ponsel.
- Jika terpaksa menggunakan fungsi penunjuk lokasi seperti GPS, lakukanlah dari ponsel pintar cadangan jika memang perangkatnya memungkinkan.

c. Pelajari lokasi tujuan

- Bekali diri dengan informasi terkait lokasi liputan, seperti ketersediaan akses Internet atau bahkan listrik jika di daerah terpencil.
- Pahami situasi sosial politik budaya atau bahkan hukum di lokasi tujuan. Misalnya, ada negara yang melarang warga untuk menggunakan VPN atau memblokir situs web dan aplikasi tertentu.

- Pelajari juga bagaimana risiko terhadap identitas dan aset digital yang mungkin terjadi selama Anda dalam perjalanan tersebut dan siapkan antisipasinya.

d. Menjaga kewaspadaan selama perjalanan

- Gunakan perangkat digital seperlunya selama perjalanan, tidak dengan terus menerus hanya terfokus pada pemakaian intensif seperti media sosial atau percakapan.
- Jangan pernah tinggalkan perangkat ponsel ataupun laptop di luar jangkauan Anda, apalagi jika dalam posisi terbuka. Selain risiko kehilangan, juga bisa digunakan orang yang sudah mengincar Anda untuk memasukkan malware dan perangkat fisik maupun lunak lain yang berbahaya.
- Jangan pernah memasukkan perangkat penyimpan, stik (*flashdisk)* ataupun diska keras (*hard disk*) dari orang lain. Jika toh terpaksa, pindailah dulu perangkat keras tersebut.

e. Membatasi pengungkapan kegiatan

- Batasi mengungkapkan lokasi dan kegiatan Anda secara terus menerus, terutama jika berisi data pribadi. Misalnya mengunggah tiket perjalanan, boarding pass, kamar hotel, dan semacamnya.
- Waspada terhadap penggunaan fungsi GPS secara otomatis pada perangkat karena bisa menunjukkan lokasi persis di mana Anda berada.
- Jika tetap ingin berbagi foto melalui media sosial sebagai bagian dari sosialisasi dan advokasi, lakukan setelah kita kembali ke kantor atau tempat aman.

f. Menyimpan nomor kontak darurat

- Simpanlah nomor kontak darurat pada ponsel, tetapi buatlah agar tidak mencolok. Misalnya tidak dengan menyebut hubungan kita sehari-hari, seperti istri, anak, saudara, bos, dan semacamnya.
- Simpan pula kontak-kontak yang bisa kita hubungi ketika di lapangan dalam situasi darurat.
- Penyimpanan kontak bisa sebagai kontak itu sendiri maupun di catatan ponsel dan atau catatan terpisah seperti di buku perjalanan.

g. Penyimpanan data cadangan

- Bawalah penyimpanan memori tambahan, seperti kartu *SSD* ataupun diska keras (*external hard disk*). Memori tambahan mudah disembunyikan, untuk mengantisipasi jika terjadi situasi di luar kendali kita, misal potensi alat kerja Anda dirampas.
- Lakukan pencadangan sesering dan sebanyak mungkin terutama untuk materi penting dan berisiko tinggi.
- Jika tersedia koneksi Internet, segera lakukan pencadangan berbasis komputasi awan (*cloud*) yang terenkripsi.
- Dalam situasi tertentu, disarankan menggunakan aplikasi percakapan yang memungkinkan adanya sinkronisasi dengan komputasi awan seperti Telegram

sehingga bisa langsung mengunggah data berkapasitas besar dan berisiko tinggi.

h. Saat mengakses Wifi publik

- Gunakan VPN ketika mengakses Wifi publik seperti di hotel, bandara, atau kafe agar tidak diketahui admin Wifi.
- Hindari memasukkan nama pengguna dan kata sandi identitas digital.
- Jangan melakukan aktivitas rentan seperti belanja daring atau memesan layanan seperti hotel yang mengharuskan kita memasukkan nomor kartu kredit.
- Hapus segera riwayat penggunaan Wifi dari perangkat setelah selesai menggunakannya.
- Matikan fungsi gabung Wifi otomatis agar perangkat tidak langsung terhubung pada Wifi dalam jangkauan perangkat tanpa kita tahu.

i. Komunikasi tanpa internet

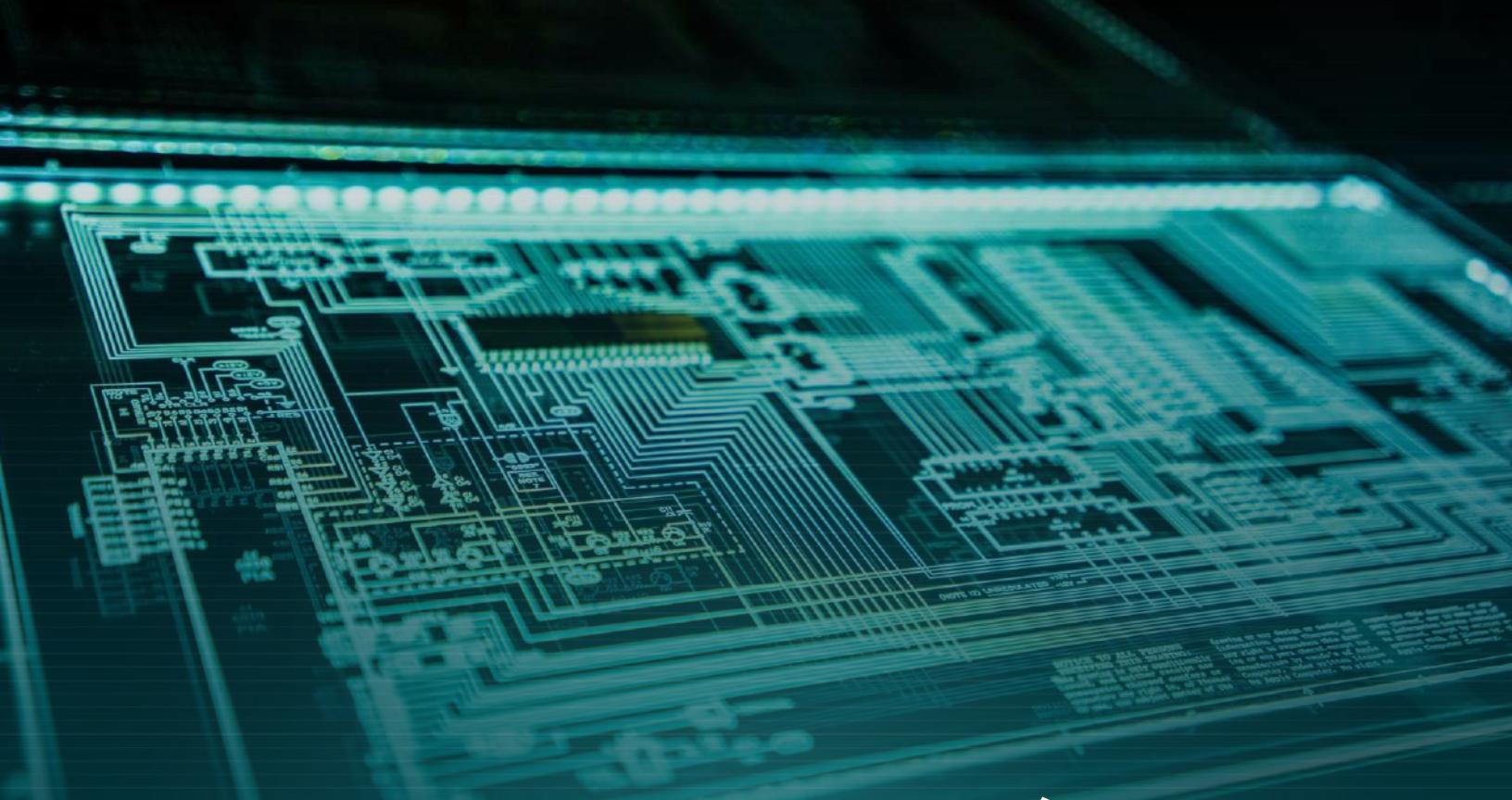
- Untuk berkomunikasi tanpa menggunakan koneksi Internet, beberapa aplikasi berikut bisa jadi pilihan yaitu Briar (https://briarproject.org/), Bridgefy (https://bridgefy.me/) dan Silence (https://silence.im/).
- Gunakan aplikasi untuk bertukar berkas melalui komunikasi nirkabel seperti Bluetooth, AirDrop, atau NFC jika ponsel memiliki fitur tersebut.
- Selain tindakan teknis seperti bentuk-bentuk di atas, perlu juga untuk mempertimbangkan hal-hal nonteknis sebagai mitigasi terhadap serangan digital seperti antisipasi selama perjalanan, kewaspadaan selama di tempat publik, hingga membatasi pengungkapan data-data pribadi.

j. Aplikasi teks/foto/video terenkripsi

Kadangkala dalam peliputan atau perjalanan yang berisiko tinggi, Anda harus menghadapi situasi yang bisa mengancam. Misalnya perampasan ponsel yang berisi hasil liputan. Jika Anda menghadapi situasi tersebut, sebaiknya Anda menggunakan aplikasi terenkripsi untuk mengirim teks, pengambilan foto/video. Aplikasi semacam ini tidak bisa dibuka oleh orang lain yang tak mengetahui password, tak bisa, disalin, dan dilihat isinya. Selain itu, data di dalam aplikasi mudah dihapus, jika ponsel diambil alih oleh pihak lain.

Berikut sejumlah aplikasi yang bisa diunduh:

- Aplikasi Tella (https://tella-app.org/) yang bisa diunduh di playstore.
- Aplikasi Cryptocam bisa diakses di:
  https://f-droid.org/en/packages/com.tnibler.cryptocam/
  https://cryptocam.gitlab.io/



BAB 6

Menghadapi Serangan Digital

ALIANSI JURNALIS INDEPENDEN
Alliance of Independent Journalist

BAB 6
Menghadapi Serangan Digital

Setelah melakukan serangkaian upaya untuk mengurangi risiko, setiap jurnalis harus tetap mewaspadai setiap bentuk-bentuk serangan digital. Pengetahuan berupa langkah-langkah darurat yang harus dilakukan saat serangan terjadi harus dimiliki oleh jurnalis. Selain mengetahui langkah-langkah teknis di bawah ini, melapor ke perusahaan media tempat Anda bekerja dan organisasi tempat Anda berserikat adalah hal penting untuk meminta dukungan dan bantuan darurat. Saat kasus terjadi, perusahaan media dan organisasi profesi jurnalis harus memantau kondisi korban, membantu mencari rumah aman, dan mengadvokasi kasus.

5.1 Peretasan Yahoo Mail

a. *Reset* password Anda dengan masuk ke tautan ini: Reset Password Yahoo
b. Masukkan alamat email akun Yahoo Mail Anda.
c. Pilih metode *reset* yang diinginkan, melalui nomor HP atau email pemulihan yang sudah Anda daftarkan. Namun pemulihan melalui email lebih direkomendasikan. Lalu klik *next*/lanjut.
d. Sebuah kode akan dikirimkan ke email pemulihan atau via SMS. Masukkan kode itu ke halaman Yahoo.
e. Buat password baru yang lebih kuat dengan kombinasi angka, huruf dan spasi.

5.2 Peretasan Gmail

a. Apabila Anda masih bisa mengakses akun Gmail Anda, segera ubah password dan tambahkan autentikasi 2 langkah (bagi yang belum mengaktifkannya).
b. Apabila Anda tidak bisa login, buka halaman pemulihan akun dengan klik tautan ini: https://s.id/PemulihanGmail. Jawab pertanyaan-pertanyaan yang diajukan oleh Google. Jika diminta sandi terakhir yang Anda ingat, masukkan sandi paling baru yang diingat. Semakin terbaru sandinya, akan semakin baik. Masukkan alamat email pemulihan yang dapat membantu Anda untuk kembali login dan menjadi email tujuan pengiriman pemberitahuan keamanan.
c. Selengkapnya mengenai peretasan dan pemulihan akun Gmail, bisa mengikuti langkah-langkah dalam tautan ini: Pemulihan akun Gmail

5.3. Pengambilalihan akun Whatsapp

a. Copot*/uninstall* WA ponsel Anda lalu Install kembali.
b. Daftarkan nomor Anda dan tunggu kode verifikasi melalui SMS dan masukkan segera kode verifikasi 6 digit dari SMS.

c. Jika Anda tidak menerima kode 6 digit melalui SMS, tunggu hingga bilah kemajuan selesai dan coba lagi. Waktu tunggu dapat berlangsung hingga 10 menit.
d. Jika waktu berakhir sebelum Anda menerima kode verifikasi, sebuah opsi akan muncul untuk meminta panggilan telepon. Pilih opsi "Panggil saya" untuk meminta panggilan telepon. Ketika Anda menerima panggilan, mesin suara otomatis akan memberitahu Anda kode verifikasi 6 digit. Masukkan kode ini untuk memverifikasi akun WhatsApp Anda.
e. Saat akun Anda kembali, segera tambahkan PIN dan email agar akun Whatsapp Anda tidak dicuri kembali.
f. Apabila Anda masih sulit masuk dan diminta untuk memasukkan kode verifikasi dua langkah, peretas mungkin telah mengaktifkan PIN di Whatsapp tersebut. Anda harus menunggu selama 7 hari sebelum dapat masuk ke akun tanpa kode verifikasi dua langkah.
g. Laporkan bahwa akun Anda telah dicuri ke alamat email: *support@whatsapp.com* dengan subyek 'Hilang / Dicuri: Silakan nonaktifkan akun saya' di badan email.

5.4 Pengambilalihan Akun Facebook

a. Untuk mengetahui apakah ada orang lain yang mengakses akun Anda secara diam-diam, Anda bisa memeriksa di Pengaturan (*setting*) ⇒ Keamanan dan Info Login. Lalu periksa "Tempat Anda Login" untuk mengecek daftar perangkat (laptop atau ponsel) yang mengakses akun Anda. Jika menemukan perangkat yang bukan milik Anda, klik tiga titik di sebelah kanan, lalu pilih keluar. Anda juga perlu mengganti password yang lebih kuat.
b. Saat akun Anda telah diretas dan password diubah, Facebook akan mengirimkan notifikasi melalui email yang Anda daftarkan. Cek apakah ada notifikasi tersebut!
c. Dalam email notifikasi, Facebook menyediakan tautan "Klik di sini" bagi Anda yang tidak membuat perubahan password tersebut. Tautan tersebut akan mengarahkan Anda untuk menjawab pertanyaan yang diminta oleh Facebook untuk memulihkan akun Anda.
d. Atau Anda bisa mengakses tautan berikut untuk melaporkan peretasan yang terjadi: https://www.facebook.com/hacked.

5.5 Pengambilalihan Akun Instagram

a. Jika Anda menggunakan laptop, Anda bisa mengetahui apakah ada orang lain yang mengakses akun Anda secara diam-diam, dengan memeriksa di Pengaturan (setting) ⇒ *Login activity*. Anda akan dibawa pada sebuah halaman yang berisi informasi tentang jenis perangkat dan lokasi login. Apabila Anda menemukan adanya perangkat yang tidak Anda gunakan, klik tanda panah di sebelah kanan, lalu klik *logout*.
b. Apabila Anda sudah tidak bisa masuk ke akun Instagram, cek pemberitahuan (*notice*)

di alamat email yang Anda daftarkan. Instagram akan mengirimkan pemberitahuan pada setiap perubahan yang terjadi pada akun Instagram Anda, seperti *login* dari perangkat berbeda atau perubahan password.

c. Klik fitur *Secure Your Account Here* dan Anda akan dibawa pada halaman untuk mengubah password Instagram Anda. Segera masukkan password baru yang lebih kuat dan unik.
d. Apabila Anda tetap kesulitan mengambil-alih akun, laporkan ke Instagram dengan langkah-langkah:

Ponsel Android:

- Di layar login, ketuk "dapatkan bantuan untuk login" di bawah fitur Login.
- Masukkan nama pengguna, email, atau nomor telepon Anda, lalu ketuk "Berikutnya". Pelajari selengkapnya tentang apa yang bisa Anda lakukan jika tidak tahu nama pengguna Anda.
- Ketuk "Perlu bantuan lain?" lalu ikuti petunjuk di layar.
- Pastikan Anda memasukkan alamat email yang aman dan hanya bisa diakses oleh Anda. Setelah mengirimkan permintaan, tunggu email dari Instagram yang berisi langkah berikutnya.

Ponsel IOS:

- Di layar login, ketuk "lupa kata sandi?"
- Ketuk "Perlu bantuan lain?" di bawah tombol "Berikutnya" dan ikuti petunjuk di layar.
- Pastikan Anda memasukkan alamat email yang aman dan hanya bisa diakses oleh Anda. Setelah mengirimkan permintaan, tunggu email dari Instagram yang berisi langkah berikutnya.
- Selengkapnya terkait pemulihan akun yang diretas di: https://help.instagram.com/

5.6 Peretasan Akun Gojek/Grab

a. Copot/*uninstall* akun Gojek/Grab Anda untuk sementara waktu. Lalu hubungi dan jelaskan kronologi kasus Anda ke *customer service* Gojek di 021-5084-9000 atau via email ke *customerservice@gojek.com*. Sedangkan untuk *customer service* Grab hubungi 021-50816600.
b. Untuk memulihkan akun Anda, Gojek/Grab biasanya akan meminta untuk menginstal dan memasukkan akun Anda kembali.

5.7 Menghadapi Doxing

a. Jika *doxxer* (pelaku doxing) mengungkap alamat rumah Anda dan berpotensi membahayakan keselamatan Anda dan keluarga, pertimbangkan untuk mencari

rumah aman sementara waktu hingga serangan mereda.

b. Laporkan postingan yang mengandung doxing ke platform dan blokir akun pelaku *doxxer*. Fitur *report* tersedia di masing-masing platform.
c. Jika doxxer mengungkap nomor telepon dan Anda menerima banyak gangguan, matikan telepon Anda sementara waktu. Pertimbangkan untuk mengganti nomor telepon di kemudian hari.
d. Jika *doxxer* telah mengekspos nomor rekening bank, kartu kredit, atau informasi akun keuangan Anda lainnya, segera hubungi semua lembaga keuangan yang terlibat dan laporkan pelanggarannya.
e. Menutup sementara akun media sosial menjadi pilihan terbaik jika serangan *doxxer* meningkat.
f. Laporkan ke polisi atas *doxing* yang Anda alami dengan membawa hasil dokumentasi dan tautan. Arsipkan melalui https://perma.cc/ atau https://archive.is/

5.8. Menghadapi pemalsuan akun (impersonating)

a. Buat pengumuman atas pemalsuan akun Anda ke keluarga, rekan kerja dan teman-teman Anda agar mereka tidak tertipu.
b. Laporkan akun yang menggunakan identitas Anda ke penyedia platform agar akun palsu tersebut ditutup.

Pelaporan akun palsu di Facebook : https://s.id/akunpalsuFB
Pelaporan akun palsu di Twitter : https://help.twitter.com/forms/ impersonation
Pelaporan akun palsu di Instagram : https://s.id/akunpalsuIG
Pelaporan akun palsu Gmail : https://s.id/akunpalsuGmail

5.9. Menghadapi Pelecehan Online dan KGBO

a. Laporkan/blokir akun, postingan atau komentar yang mengandung pelecehan termasuk KBGO (kekerasan berbasis gender online) ke platform. Per Januari 2020, Facebook dan Instagram telah memperluas jenis laporannya untuk pelecehan seksual, kekerasan dan ujaran kebencian yang mengandung SARA.
b. Minta dukungan dari organisasi profesi tempat Anda berserikat atau ke lembaga penyedia layanan pendamping pelecehan/kekerasan seksual.
c. Laporkan ke polisi atas kekerasan dan pelecehan yang Anda terima, baik melalui telepon, sms, chat, atau di media sosial lainnya dengan menyertakan dokumentasi atas kekerasan/ pelecehan yang dialami.
d. Minta dukungan perusahaan media atau AJI (bagi anggota AJI) untuk memfasilitasi layanan pemulihan trauma.

BAB 7

Pengaduan dan Studi Kasus Penanganan Serangan Digital

ALIANSI JURNALIS INDEPENDEN
Alliance of Independent Journalist

BAB 7
Pengaduan dan Studi Kasus Penanganan Serangan Digital

Penanganan kasus kekerasan berbasis digital sedang terus dikembangkan karena banyaknya modus yang digunakan pelaku. Sejumlah studi kasus ini mungkin membantu untuk mencari jalan terbaik menangani kasus karena tidak bisa dilakukan dengan solusi tunggal.

Bagi jurnalis yang mendapatkan serangan digital karena kerja-kerja jurnalistik, Anda bisa melapor ke AJI melalui kanal https://advokasi.aji.or.id/. Pengaduan bisa diisi korban langsung atau kuasa/perwakilan medianya.

Pelaporan Anda akan menjadi dokumentasi bagi AJI dan tahap awal bagi Anda yang membutuhkan bantuan. Pendokumentasian kasus sangat penting sebagai upaya mitigasi kasus-kasus berikutnya dan pelaporan publik. Terutama mendesak perubahan kebijakan negara dan Dewan Pers untuk melindungi jurnalis dari ancaman kekerasan digital.

Bidang Internet AJI Indonesia juga bergabung dalam Tim Reaksi Cepat (TRACE) yang pembentukannya difasilitasi oleh SAFEnet. TRACE terdiri dari aktivis lintas organisasi dengan pengalaman pendampingan dan penanganan serangan digital.

Anda juga bisa membaca lebih lanjut panduan keamanan digital yang telah diterbitkan oleh organisasi lain:

1. https://gijn.org/digital-security/
2. https://cpj.org/2019/07/digital-safety-kit-journalists.php#protect
3. https://digitalrightswatch.org.au/2019/06/10/digital-security for-journalists/
4. https://cpj.org/2020/05/digital-safety-protecting-against targeted-online-attacks/
5. https://coconet.social/digital-hygiene-safety-security-indonesia/
6. https://freedom.press/training/your-smartphone-and-you handbook-modern-mobile-maintenance/
7. https://www.accessnow.org/issue/digital-security/
8. https://digitalfirstaid.org/en/index.html
9. https://securityinabox.org/en/guide/basic-security/android/
10. https://id.safenet.or.id/wp-content/uploads/2019/11/Panduan KBGO-v2.pdf
11. https://digsec.safenet.or.id

Berikut ini adalah beberapa studi kasus serangan digital yang bisa kita pelajari bersama.

Studi kasus 1: Serangan online dan offline jurnalis media Papua

Sejumlah jurnalis mengalami ancaman setelah mengelola sebuah media Papua yang cukup kritis atas kebijakan pemerintah dalam menangani konflik. Sebuah akun anonim di Twitter menyebarkan informasi pribadi para jurnalis termasuk nama jajaran redaksi, dengan menuduh mereka bagian jaringan gerakan papua merdeka. Penyebaran informasi pribadi dengan tujuan negatif seperti ini disebut doxing.

Perbuatan doxing tentu sangat membahayakan bagi para jurnalis dan keluarga mereka. Sebab mereka dapat menjadi target sasaran dari kelompok-kelompok tertentu yang terhasut dengan unggahan yang beredar. Padahal jurnalis bekerja untuk kepentingan publik sesuai etika jurnalistik.

Selain doxing, serangan langsung juga menimpa Pemimpin Umum Tabloid Jubi, Victor Mambor di Jayapura, Papua. Mobil Victor yang diparkir di tepi jalan di samping rumahnya, dirusak oleh orang tak dikenal pukul 00.00 hingga pukul 02.00 WIT.

Kerusakan terjadi pada kaca depan mobil (diduga dipukul dengan benda tumpul hingga retak) dan kaca mobil sebelah kiri (kaca depan dan belakang) yang dipukul yang diduga dengan benda tajam hingga hancur. Selain itu pintu depan dan belakang sebelah kiri dicoret-coret dengan cat pilox berwarna orange.

Diduga kuat, teror yang dialami Victor terkait pemberitaan Tabloid Jubi yang tidak disukai pihak tertentu. Ini merupakan rentetan dari sejumlah serangan terhadap Victor maupun Tabloid Jubi yang terjadi sebelumnya, yakni serangan melalui digital, doxing, dan penyebaran flayer di media sosial yang kontennya menyudutkan Tabloid Jubi maupun Victor Mambor, dan ancaman untuk melaporkan media maupun pribadi Victor ke polisi.

Penanganan kasus ini dimulai dengan asesmen kronologis dan dampaknya bagi korban. Penanganan dan penguatan keamanan digital pada korban juga dilakukan oleh jaringan pembela HAM dan hak digital.

Studi kasus 2: Doxing kepada jurnalis pemeriksa fakta

Dua jurnalis pemeriksa fakta Tempo, Ika Ningtyas dan Zainal Ishaq mengalami doxing di medsos Facebook oleh salah seorang dokter hewan, yang kerap membagikan narasi menyesatkan terkait Covid-19. Doxing terjadi setelah keduanya menerbitkan 4 artikel cek fakta atas klaim-klaim dokter hewan itu di Facebook sepanjang April hingga Juli 2020.

Dokter hewan tersebut melakukan doxing pada Jumat, 31 Juli 2020 dan Sabtu, 1 Agustus 2020 dengan membagikan foto Zainal dan Ika. Dia juga menulis artikel berjudul "Lawan Teroris Wabah" yang menuduh keduanya sebagai jurnalis penyebar ketakutan.

Atas kejadian tersebut, Ika dan Zainal melaporkan kasus itu ke perusahaan media dan organisasi profesinya, AJI. Mereka juga menutup sementara akun Facebook selama sepekan, untuk menghindari serangan makin meluas. Selain itu, perusahaan medianya juga melaporkan unggahan dokter hewan itu ke Facebook, baik melalui fitur "report" yang tersedia, sekaligus via email. AJI juga menerbitkan siaran pers untuk mengecam tindakan doxing.

Namun saat itu FB belum menurunkan (takedown) postingan doxing tersebut karena kebijakan FB belum mengatur doxing. Tapi pada kasus berikutnya yang juga menimpa jurnalis cek fakta di Tirto dan Liputan6, Facebook menurunkan unggahan terkait doxing.

Studi kasus 3: Pengambilalihan Akun Medsos

Pada awal Juni 2021, pihak tertentu yang lokasinya terdeteksi di Singapura, mencoba meretas akun Instagram *@watchdoc_insta* milik Watchdoc. Instagram mengirimkan notifikasi ada pihak tertentu yang berupaya mengganti email akun Instagram Watchdoc menjadi rosob30301@vvai.com. Upaya mengganti email tersebut diketahui terjadi tiga kali pada rentang pukul 15:22 WIB hingga 18:33 WIB.

Pada usahanya yang ketiga, peretas menggunakan username capd2jyxrybubpc+977@protonmail.com. Peretas berhasil menghapus seluruh konten di akun @watchdoc_insta, mengganti username Instagram menjadi @watchwatchwatchhehe serta display name menjadi Dogwatch.

Tim media sosial yang berusaha menyelamatkan akun Instagram Watchdoc tidak berhasil. Meski sudah berusaha me-reset password beberapa kali lewat tautan yang dikirimkan Instagram via email yang terintegrasi ke akun tersebut. "*Sorry, there was a problem. Please try again*." Demikian respon yang muncul.

Pemilik akun kemudian melayangkan pengaduan melalui Instagram Support. Facebook merespon pengaduan pada 18:34 WIB yang mendeteksi bahwa akun mungkin tidak mengikuti Syarat Penggunaan. Pada pukul 22:17 WIB dengan mengetuk tautan *secure your account* pada email yang dikirim oleh Instagram, pemilik akun berhasil melakukan peninjauan profil pengguna dan me-reset password dan menggantinya dengan password baru.

Akan tetapi, Tim Watchdoc belum berhasil mendapatkan akun Instagram mereka, karena tidak mendapatkan kode autentifikasi dua langkah via sms ke nomor handphone yang didaftarkan oleh pengguna. Nomor telepon tersebut merupakan milik salah satu tim Watchdoc.

Dalam notifikasi yang muncul, bahwa Tim Watchdoc harus memasukkan kode autentifikasi dari aplikasi Authenticator. Kemungkinan peretas telah mengubah pengaturan autentifikasi 2 langkah yang semula berbasis SMS menjadi aplikasi Authenticator.

Upaya log in dari pemilik akun terakhir dilakukan pada 7 Juni 2021 pukul 06:45 WIB melalui aplikasi Instagram di perangkat iPhone 7, tetapi tidak berhasil juga. Muncul two factors authentication menggunakan aplikasi Authenticator. Pemilik akun harus memasukkan kode yang ada di aplikasi authenticator milik peretas.

Upaya login yang dilakukan sejak 7 dan 8 Juni 2021 belum membuahkan hasil juga.

Pemilik akun akhirnya melaporkan kasus ini ke pihak Facebook melalui bantuan Safe Net dan Tim Facebook Concierge Support dengan mengirimkan kronologi peretasan melalui email. Respon mereka cukup cepat.

Pihak Facebook meminta pemilik akun memberikan 2 informasi pendukung, yaitu email yang aman yang tidak pernah dikaitkan ke akun Instagram/Facebook. Tim Watchdoc disarankan membuat email baru menggunakan Protonmail.

Setelah mengirimkan informasi tersebut pada 8 Juni 2021 pukul 14:06 WIB, Facebook berhasil memulihkan akun dengan pemberitahuan melalui email pada hari yang sama pukul 18:35 WIB.

Pihak Facebook mengirimkan link untuk reset password ke email Protonmail. Setelah melakukan reset password, pihak Facebook juga menyarankan agar kami menerapkan autentifikasi dua langkah berbasis aplikasi Authenticator.

Akun Instagram kembali pulih dengan jumlah postingan yang sama sebelum akun diretas. Pemilik akun hanya perlu mengatur ulang foto profil dan bio akun Instagram.

Studi kasus 4: Doxing yang bermula dari pemberitaan media

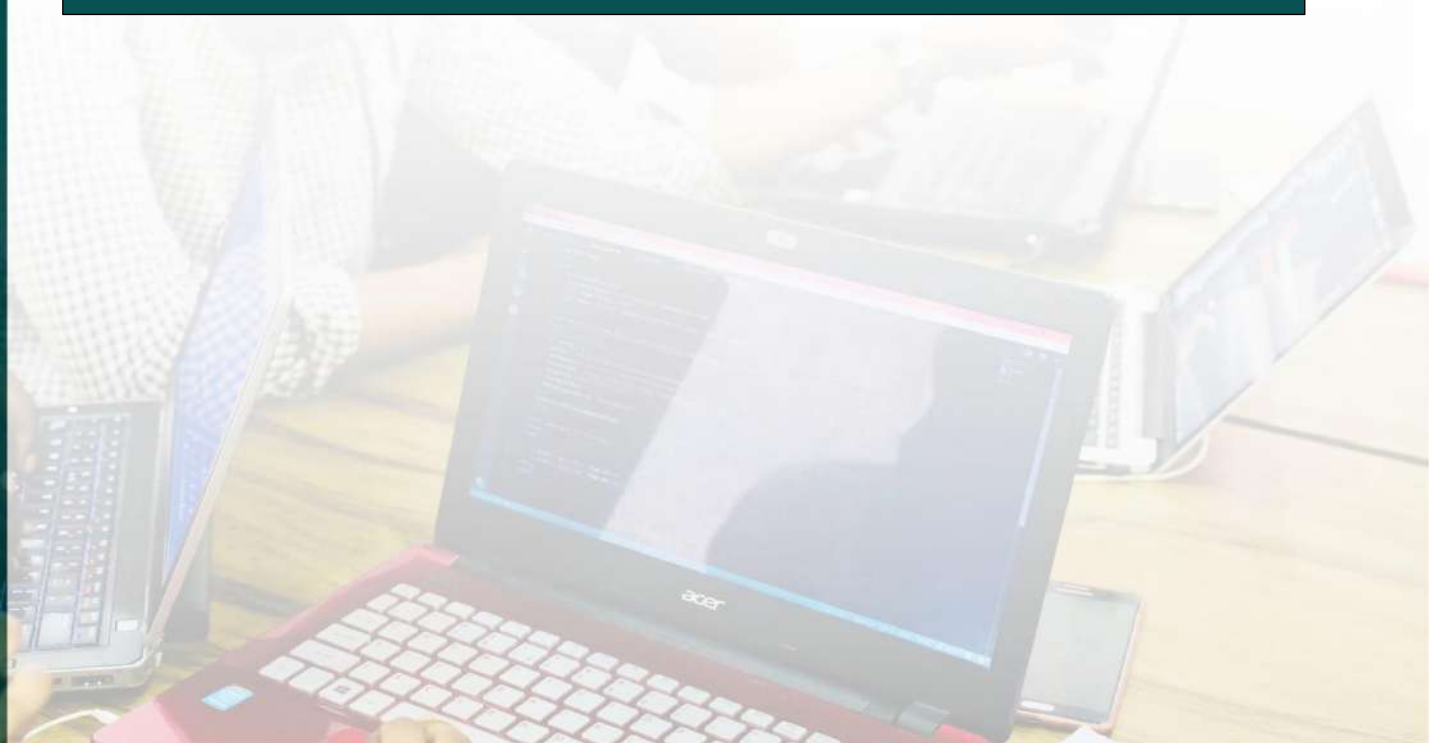
Nama jurnalis Viva.co.id, Ridho Permana menjadi viral di sela sela perhelatan Olimpiade Tokyo 2020. Namanya jadi perhatian warganet setelah ia menulis beberapa pemberitaan seksis tentang seorang atlet perempuan antara April 2020-Januari 2021. Namanya juga sempat masuk dalam jajaran trend di Twitter pada Kamis, 29 Juli 2021.

Kondisi ini membuat beberapa media mengangkat profil tentang Ridho yang dapat mengarah pada doxing, seperti berjudul *Agama dan Instagram Ridho Permana Viva co.id*. Belakangan pemberitaan berisi informasi pribadi Ridho telah diturunkan tanpa penjelasan atau permintaan maaf seperti yang telah diatur oleh Pedoman Pemberitaan Media Siber.

Konten bernuansa doxing tersebut muncul setelah Ridho menulis pemberitaan, salah satunya berjudul *Reputasi bulutangkis Indonesia rusak gara-gara Praveen Melati*. Berita ini menuai kritik dari warganet karena dianggap tidak memberikan motivasi dan apresiasi pada atlet Indonesia yang berjuang di Olimpiade Tokyo 2020.

Dari sana, warganet mulai mencari rekam jejak pemberitaan Ridho. Hingga akhirnya warganet menemukan rekam jejak pemberitaan yang seksis dan tidak ramah gender yang kerap ditulis oleh Ridho. Sejumlah akun kemudian membuat kolase dari berbagai pemberitaan itu dan mengedarkan meme ke berbagai media sosial.

Doxing terhadap Ridho ini berbeda dengan kebanyakan kasus karena doxing dilakukan oleh media massa arus utama.



Referensi

Amnesty International Indonesia. *Selamat tinggal serangan digital*. Dapat diakses melalui:
https://www.amnesty.id/selamat-tinggal-serangan-digital/

LBH Pers. Panduan Penanganan Perkara Informasi dan Transaksi Elektronik. Dapat diakses melalui:
Pandungan Penanganan Perkara Informasi dan Transaksi Elektronik

LBH Pers. Protokol Keamanan dalam Meliput Isu Kejahatan Lingkungan. Dapat diakses melalui:
https://lbhpers.org/protokol-keamanan-dalam-meliput-isu-kejahatan-lingkungan/

Southeast Asian Freedom of Expression Network (SAFEnet). *Kursus Keamanan Digital*. Dapat diakses melalui:
https://digsec.safenet.or.id/panduan-kursus/

Tactical Tech. *Data Detox Kit*. Dapat diakses melalui:
https://tacticaltech.org/projects/data-detox-kit/

Profil Penulis

Luh De Suriyani

Luh De Suriyani, jurnalis sejak 2002, mukim di Bali. Alumni Pers Mahasiswa Akademika Universitas Udayana kemudian bergabung dengan AJI Denpasar. Saat ini juga mengelola media nonprofit jurnalisme warga BaleBengong.id bersama relawan lain sejak 2007. Tertarik menekuni keamanan digital sebagai bagian keamanan holistik karena ancamannya meningkat, dan pembelajaran ini sebuah proses. Bukan tujuan.

Adi Marsiela

Adi Marsiela, bekerja sebagai jurnalis sejak 2003. Saat ini tinggal dan bekerja dari Bandung. Belajar Jurnalistik di FIKOM Universitas Padjadjaran. Bergabung dengan kepengurusan Aliansi Jurnalis Independen bidang internet sejak 2021. Masih belajar soal keamanan digital dan jurnalistik berbasis data.

PANDUAN

KEAMANAN DIGITAL UNTUK JURNALIS

Diterbitkan oleh:

ALIANSI JURNALIS INDEPENDEN
Alliance of Independent Journalist

2022

ALIANSI JURNALIS INDEPENDEN (AJI) INDONESIA
Jalan Sigura Gura No.6A, Duren Tiga,
Jakarta Selatan 12760 - Indonesia
Telepon : (6221)3151214
E-mail : sekretariat@ajiindonesia.or.id
Web : www.aji.or.id

ISBN 978-979-3530-53-6 (PDF)