

# PANDUAN

# KEAMANAN DIGITAL

# PEMBUAT KONTEN

PERETASAN  
INTERSEPSI  
FITNAH  
DOKING

Phishing



# PANDUAN **KEAMANAN DIGITAL** PEMBUAT KONTEN

**Penulis:**

Sasmito  
Adib Muttaqin Asfar

**Reviewer:**

Arif Kurniawan

**Penata Isi:**

Eko Punto Pambudi

**Ilustrasi Sampul:**

Imam Yunni

Januari 2025



**Aliansi Jurnalis Independen (AJI) Indonesia**

Jalan Kembang Raya No. 6, Kwitang, Senen  
Jakarta Pusat 10420

Telp 021-3151214, Fax 3151261  
Email: sekretariat@ajindonesia.or.id  
Web: www.aji.or.id

Didukung oleh:



Funded by  
the European Union

## DAFTAR ISI

|  |           |
|--|-----------|
| Daftar Isi   | 3         |
| Kata Pengantar   | 5         |
| <b>I. Pendahuluan</b>  | <b>7</b>  |
| <b>II. Jenis-jenis Serangan Digital</b>                      | <b>8</b>  |
| A. Penyebaran rumor/fitnah                                   | 8         |
| B. Doxing  | 8         |
| C. Intersepsi/penyadapan                                     | 9         |
| D. Peniruan identitas  | 9         |
| E. Pembuatan akun palsu atas nama korban                     | 9         |
| F. Peretasan/pengambilalihan akun media sosial               | 10        |
| G. Social engineering  | 10        |
| H. Phishing  | 10        |
| I. Perampasan perangkat digital                              | 10        |
| J. Serangan digital berbasis gender                          | 11        |
| <b>III. Mitigasi Serangan Digital</b>                        | <b>12</b> |
| A. Perlindungan Perangkat                                    | 12        |
| 1. Perlindungan Fisik  | 12        |
| a. Menghindari membeli ponsel/laptop bekas.                  | 12        |
| b. Tidak meletakkan ponsel/laptop sembarangan.               | 13        |
| c. Memasang pelindung (casing).                              | 13        |
| d. Tidak isi ulang baterai dengan port USB di tempat publik. | 13        |
| e. Memperbaiki di service center resmi.                      | 13        |
| 2. Perlindungan Digital                                      | 14        |
| Pada Ponsel  | 14        |
| Pada Laptop  | 18        |
| B. Perlindungan Data Online                                  | 21        |
| 1. Cek Data Anda yang Tersebar Online                        | 22        |
| 2. Cek Kebocoran Data  | 23        |
| 3. Hapus atau Batasi Akses                                   | 23        |
| C. Pengamanan Akun   | 24        |
| 1. Memperkuat Sandi  | 25        |
| 2. Pengamanan 2 Lapis  | 26        |
| 3. Mengatur Privasi Akun                                     | 27        |
| 4. Manajemen Penggunaan Akun                                 | 27        |

|                                       |           |
|---------------------------------------|-----------|
| <b>IV. Mekanisme Penanganan</b>       | <b>30</b> |
| A. Kehilangan Akses Terhadap Akun     | 31        |
| 1. Identifikasi masalah               | 31        |
| 2. Peretasan Whatsapp                 | 32        |
| 3. Peretasan akun Gmail               | 33        |
| 4. Peretasan Yahoo Mail               | 34        |
| 5. Pengambilalihan Akun Facebook      | 35        |
| 6. Pengambilalihan Akun Instagram     | 35        |
| 7. Pengambilalihan Akun Tiktok        | 36        |
| 8. Pengambilalihan Akun Youtube       | 38        |
| B. Serangan Pendengung (Buzzer)       | 41        |
| a. Doxing                             | 41        |
| b. Impersonating                      | 41        |
| c. Pelecehan Online dan KGBO          | 42        |
| C. Menjadi Target Penangkapan         | 42        |
| <b>V. Kontak Darurat</b>              | <b>43</b> |
| A. Kontak Bantuan Penanganan          | 43        |
| 1. Aliansi Jurnalis Independen (AJI)  | 43        |
| 2. Tim Reaksi Cepat (TRACE)           | 43        |
| 3. SAFEnet                            | 43        |
| 4. Access Now                         | 43        |
| B. Kontak Bantuan Hukum               | 44        |
| Wilayah Jabodetabek                   | 44        |
| Wilayah Jawa Barat dan Banten         | 44        |
| Wilayah Jawa Tengah dan DIY           | 44        |
| Wilayah Jawa Timur                    | 45        |
| Wilayah Bali dan Nusra                | 45        |
| Wilayah Aceh dan Sumatera Utara       | 45        |
| Wilayah Sumatera Barat dan Riau       | 46        |
| Wilayah Sumatera Selatan dan Lampung  | 46        |
| Wilayah Kalimantan                    | 46        |
| Wilayah Sulawesi dan Papua            | 47        |
| C. Kontak Penanganan Psikososial      | 47        |
| 1. Yayasan Pulih                      | 47        |
| 2. Jaringan LBH Apik di berbagai kota | 47        |

## KATA PENGANTAR

Di era digital yang semakin berkembang, para pembuat konten memiliki peran yang sangat penting dalam membangun narasi, menyampaikan informasi, serta mempengaruhi opini publik.

Meskipun berbeda dengan jurnalis yang bekerja dengan standar jurnalistik dan kode etik, para pembuat konten ini juga memberikan informasi beragam di platform media sosial dengan menarik, dan kadang isi konten mereka cukup kritis.

Para pembuat konten ini acapkali memberikan kritik, saran dan informasi ke pengikut media sosial mereka. Bahkan boleh dibilang jumlah pengikut mereka lebih banyak dibanding media sendiri. Kehadiran mereka kini sama pentingnya dengan media yang memberikan informasi.

Keaktifan ini, terutama bagi mereka yang memiliki audiens besar atau membahas isu-isu sensitif, meningkatkan kemungkinan menjadi target peretas. Serangan seperti doxxing, peretasan akun, serta intimidasi digital kerap dialami oleh pembuat konten yang dianggap mengganggu kepentingan tertentu.

Sayangnya, tidak semua pembuat konten memiliki pemahaman yang mendalam tentang ancaman-ancaman digital, seperti *phishing*, *malware*, atau serangan *brute force*, yang membuat mereka lebih rentan menjadi korban serangan.

Data dari riset PR2Media dan Aliansi Jurnalis Independen (AJI) pada Agustus 2024 mengungkap fakta mengejutkan: 63,5 persen dari 312 pembuat konten di Indonesia pernah menjadi korban serangan digital dalam lima tahun terakhir.

Beberapa jenis serangan yang paling sering dialami meliputi: pengawasan atau *stalking* oleh pihak tak dikenal, *phishing*, yakni penipuan melalui email dan pesan untuk mencuri data pribadi, *bullying*, ancaman, serta intimidasi non-gender, dan peretasan atau pengambilalihan akun media sosial.

Dampak dari serangan-serangan ini tidak bisa dianggap remeh. Selain kehilangan privasi, para korban juga menghadapi ancaman terhadap keamanan fisik dan emosional mereka. Lebih dari itu, hilangnya akses ke akun digital bisa berakibat fatal, seperti kehilangan sumber penghasilan yang selama ini bergantung pada platform digital.

Karena itu, memahami ancaman digital dan cara mengatasinya bukan sekadar pilihan, tetapi sebuah keharusan bagi pembuat konten. Penting bagi pembuat konten untuk memahami dan menerapkan langkah-langkah keamanan digital guna melindungi diri dan karya mereka.

Buku *Panduan Keselamatan Digital untuk Pembuat Konten* ini hadir sebagai jawaban atas kebutuhan mendesak para kreator dalam menghadapi berbagai ancaman digital.

Tidak sekadar mengidentifikasi ancaman, buku panduan ini juga memberikan langkah-langkah praktis untuk menjaga keamanan perangkat, melindungi data pribadi, serta mengelola risiko di lingkungan digital yang semakin dinamis. Dengan memahami langkah-langkah perlindungan yang tepat, para pembuat konten dapat memastikan keberlanjutan karya mereka sekaligus menjaga kepercayaan audiens.

Panduan ini ditulis dengan metode yang praktis dan mudah diterapkan. Selain bagaimana memastikan data terenkripsi, password yang kuat juga apa yang bisa dilakukan seandainya terjadi serangan pada media sosial.

Dengan menerapkan prinsip-prinsip keamanan yang dijelaskan dalam panduan ini, diharapkan para pembuat konten dapat terus berkarya dengan aman dan bebas dari ancaman digital.

Aliansi Jurnalis Independen (AJI) Indonesia mengucapkan terima kasih pada Sasmito dan Adib Muttaqin Asfar yang sudah menulis buku yang penting ini. Juga International Media Service (IMS) dan European Union yang telah mendukung hadirnya panduan ini.

Selamat membaca dan tetap jaga keamanan digital Anda!

**Nany Afrida**

Ketua Umum AJI

## I. PENDAHULUAN

Sebanyak 63,5 persen dari 312 pembuat konten menyatakan pernah mengalami setidaknya satu jenis serangan digital selama lima tahun terakhir. Kondisi ini terungkap dalam riset “Keamanan Digital Pembuat Konten di Indonesia” yang diterbitkan Pemantau Regulasi dan Regulator Media (PR2Media) dan Aliansi Jurnalis Independen (AJI) pada Agustus 2024.<sup>1</sup>

Ada empat jenis serangan digital yang perlu mendapat perhatian khusus karena paling sering dialami pembuat konten, yaitu “diawasi/*stalked*”, “*phishing*”, “*bullying*”, ancaman, dan intimidasi yang bukan berbasis gender”, dan “peretasan/pengambilalihan akun media sosial”.

Riset ini juga menunjukkan serangan digital terhadap pembuat konten yaitu terancamnya keamanan fisik maupun emosional dan privasi, serta hilangnya akses terhadap sumber pendapatan. Karena itu, penting bagi pembuat konten untuk memahami jenis-jenis konten, pencegahan serangan digital, dan penanganan serangan digital.

---

<sup>1</sup> <https://t.ly/ajilaporan>

## II. JENIS-JENIS SERANGAN DIGITAL

Berikut ini jenis serangan digital yang diidentifikasi PR2Media dan AJI dalam riset “Keamanan Digital Pembuat Konten di Indonesia” 2024:

### A. PENYEBARAN RUMOR/FITNAH

Penyebaran rumor/fitnah digital adalah penyebaran informasi palsu, tidak berdasar, atau menyesatkan melalui media digital seperti media sosial, situs web, aplikasi pesan instan, dan platform komunikasi online lainnya. Informasi ini biasanya dirancang atau disampaikan dengan maksud tertentu, seperti merugikan seseorang, kelompok, institusi, atau bahkan menciptakan keresahan di masyarakat.

Ciri-ciri penyebaran rumor/fitnah digital adalah:

- Tidak berdasarkan fakta
- Mengandung emosi
- Anonim atau tidak jelas sumbernya
- Viral atau cepat menyebar
- Menggunakan format yang menarik

Penyebaran rumor/fitnah digital sering disampaikan dalam bentuk teks, gambar, atau video dengan narasi menarik atau provokatif untuk meningkatkan daya tariknya.

### B. DOXING

*Doxing* adalah serangan digital yang dilakukan seseorang atau kelompok dengan sengaja mengumpulkan dan memublikasikan informasi pribadi orang lain secara online tanpa izin, biasanya dengan niat jahat atau untuk merugikan korban. Istilah “doxing” berasal dari kata “documents” (dox), yang merujuk pada dokumen atau data pribadi yang diekspos kepada publik.

Pelaku *doxing* biasanya memiliki berbagai tujuan, seperti:

- Membalas dendam atau mengintimidasi: agar korban merasa tidak aman.
- Merusak reputasi: menyebarkan informasi yang memalukan untuk mencoreng nama baik seseorang.
- Mendorong serangan lain: membuka informasi agar orang lain bisa melakukan ancaman, intimidasi, atau kekerasan.

- Aktivisme atau hacktivisme<sup>2</sup>: terkadang digunakan untuk membocorkan informasi tentang pihak yang dianggap “berbahaya” secara sosial atau politik.

### C. INTERSEPSI/PENYADAPAN

Intersepsi atau penyadapan adalah tindakan mencuri atau menyadap komunikasi digital tanpa izin, yang dilakukan melalui metode hacking seperti *Man-in-the-Middle (MITM)*<sup>3</sup>, *packet sniffing*, atau aplikasi berbahaya seperti aplikasi mata-mata *spyware* dan aplikasi perekam keyboard *keylogger*. Penyadapan menjadi serangan digital karena melanggar privasi, mengeksploitasi data sensitif, mengancam keamanan nasional, serta sering digunakan untuk aktivitas kriminal seperti pemerasan atau penipuan.

### D. PENIRUAN IDENTITAS

Peniruan identitas digital adalah tindakan jahat yang dilakukan seseorang dengan berpura-pura menjadi individu lain secara online untuk tujuan tertentu, seperti mencuri data, melakukan penipuan, atau merusak reputasi korban. Pelaku biasanya menggunakan informasi pribadi korban, seperti nama, foto, atau kredensial akun, yang didapat melalui phishing, hacking, atau eksploitasi data yang bocor.

### E. PEMBUATAN AKUN PALSU ATAS NAMA KORBAN

Pembuatan akun digital palsu atas nama korban adalah tindakan ilegal yang dilakukan pelaku dengan membuat akun online menggunakan identitas korban tanpa izin. Biasanya untuk tujuan jahat seperti penipuan, penyebaran informasi palsu, atau merusak reputasi. Pelaku sering memanfaatkan data pribadi korban, seperti nama, foto, atau email, yang diambil dari media sosial atau sumber lain.

---

2 Hacktivisme adalah bentuk serangan siber yang dilakukan oleh para peretas (hacker) dengan tujuan politis atau sosial. Mereka menggunakan keterampilan teknis untuk mengakses, merusak, atau mengganggu situs web, sistem, atau jaringan sebagai cara untuk menyuarakan protes, mempengaruhi opini publik, atau melawan kebijakan yang dianggap tidak adil. Hacktivisme bisa berupa serangan *DDoS* (menyebabkan gangguan akses ke situs), *defacing* (mengubah tampilan situs web), atau membocorkan informasi yang sensitif untuk mengekspos pelanggaran. Tujuan utamanya adalah untuk memengaruhi perubahan sosial atau politik melalui kekuatan teknologi.

3 Serangan *Man-in-the-Middle (MITM)* adalah jenis serangan siber yang dilakukan penyerang secara diam-diam menyusup di antara dua pihak yang sedang berkomunikasi untuk mencuri atau memanipulasi data mereka. Dalam serangan ini, penyerang dapat memonitor, mengubah, atau bahkan mengarahkan ulang pesan tanpa sepengetahuan korban.

## F. PERETASAN/PENGAMBILALIHAN AKUN MEDIA SOSIAL

Peretasan atau pengambilalihan akun media sosial adalah tindakan seseorang secara ilegal mengakses dan mengambil alih kendali atas akun media sosial milik orang lain. Hal ini biasanya dilakukan melalui metode seperti *phishing*, *brute force attack*<sup>4</sup>, *malware*<sup>5</sup>, atau memanfaatkan data pribadi yang bocor. Tujuannya bisa berupa pencurian identitas, penipuan, penyebaran konten berbahaya, atau merusak reputasi korban.

## G. SOCIAL ENGINEERING

Social engineering adalah teknik manipulasi psikologis yang digunakan oleh pelaku kejahatan untuk mengelabui seseorang agar memberikan informasi sensitif atau melakukan tindakan tertentu, seperti membocorkan kata sandi, data pribadi, atau akses ke sistem. Metode ini sering memanfaatkan kepercayaan, rasa takut, atau urgensi melalui taktik seperti *phishing*, *pretexting*, *baiting*, atau *vishing (voice phishing)*. Social engineering berbahaya karena memanfaatkan kelemahan manusia alih-alih celah teknis, membuatnya sulit diantisipasi.

## H. PHISHING

*Phishing* adalah serangan siber yang dilakukan pelaku dengan menyamar sebagai entitas atau individu tepercaya untuk menipu korban agar memberikan informasi sensitif seperti kata sandi, nomor kartu kredit, atau data pribadi. Serangan ini biasanya dilakukan melalui email, pesan teks, atau situs web palsu yang tampak sah untuk memancing korban masuk perangkap.

## I. PERAMPASAN PERANGKAT DIGITAL

Perampasan perangkat fisik digital adalah tindakan mengambil secara paksa atau mencuri perangkat digital seperti ponsel, laptop, atau perangkat lainnya dengan tujuan mengakses data sensitif, menyabotase, atau mengeksploitasi informasi

---

4 Serangan *brute force attack* adalah metode peretasan yang dilakukan penyerang dengan mencoba semua kemungkinan kombinasi kata sandi atau kunci enkripsi hingga menemukan yang benar. Proses ini dilakukan secara otomatis menggunakan perangkat lunak untuk mencoba berbagai kombinasi dengan kecepatan tinggi. Meskipun metode ini sederhana, serangan brute force bisa sangat efektif jika kata sandi yang digunakan lemah atau mudah ditebak.

5 *Malware* adalah jenis program komputer yang dirancang untuk merusak atau mengganggu komputer, ponsel, atau perangkat elektronik lainnya. *Malware* bisa masuk ke perangkat kita tanpa kita tahu, dan ketika itu terjadi, ia bisa mencuri informasi pribadi, merusak file, atau membuat perangkat menjadi lambat. Ada berbagai jenis malware, seperti virus, *trojan*, atau *ransomware*, yang bisa menyebar lewat email, situs web, atau aplikasi yang tidak aman.

yang ada di dalamnya. Ancaman ini tidak hanya melibatkan kehilangan perangkat fisik, tetapi juga risiko keamanan digital jika perangkat tidak terlindungi dengan kata sandi, enkripsi, atau fitur pelacakan.

## **J. SERANGAN DIGITAL BERBASIS GENDER**

Serangan digital berbasis gender adalah jenis serangan siber yang menargetkan individu berdasarkan identitas gender mereka, dengan tujuan untuk merendahkan, mengintimidasi, atau mengendalikan korban. Serangan ini dapat berupa pelecehan seksual, intimidasi verbal, perundungan online, penyebaran gambar atau video pribadi, hingga *doxing* (penyebaran informasi pribadi). Korban, terutama perempuan dan kelompok gender minoritas, sering menjadi sasaran karena ketidaksetaraan gender dan stereotip sosial. Serangan ini dapat menimbulkan dampak psikologis yang berat, serta mengancam hak privasi dan keselamatan individu.

Dari serangan di atas, setidaknya ada empat jenis serangan paling sering dialami pembuat konten, yaitu “diawasi/stalked”, “phishing”, “bullying, ancaman, dan intimidasi yang bukan berbasis gender”, dan “peretasan/pengambilalihan akun media sosial”.

Sedangkan faktor terbanyak yang menjadi pemicu serangan digital adalah jenis konten yang diunggah, diikuti oleh relasi tertentu dengan pihak lain (figur publik atau individu yang diberitakan media), dan keyakinan pribadi.

### III. MITIGASI SERANGAN DIGITAL

Pembuat konten perlu memiliki langkah-langkah mitigasi untuk mencegah sembilan jenis serangan digital di atas. Utamanya mitigasi dari empat serangan yang paling sering dialami pembuat konten. Sejumlah langkah yang bisa dilakukan di antaranya yaitu melindungi data pribadi yang ada di ranah digital dan perlindungan aset digital.

Namun demikian, panduan perlindungan keamanan digital bagi pembuat konten ini dimulai dari perlindungan perangkat, perlindungan data online, hingga penanganan serangan digital. Panduan ini memprioritaskan perlindungan data pribadi secara sistematis, agar pembuat konten tidak kena serangan yang sering terjadi.

#### A. PERLINDUNGAN PERANGKAT

Ancaman serangan di atas selalu ada selama perangkat, baik ponsel maupun laptop, terkoneksi dengan jaringan. Perilaku kita menentukan seberapa besar risiko atau kerentanan terhadap serangan.

Hal-hal yang perlu dilakukan dalam melakukan perlindungan perangkat digital:

##### 1. Perlindungan Fisik

###### a. Menghindari membeli ponsel/laptop bekas.

Ponsel bekas berisiko membawa virus atau *malware* yang tidak pernah kita ketahui. Sebaiknya, hindari membeli ponsel bekas. Jika terpaksa membeli ponsel atau laptop bekas, pastikan untuk memeriksa secara teliti kondisi perangkat dan riwayatnya. Periksa apakah perangkat tersebut terdaftar sebagai barang curian atau memiliki masalah keamanan, misalnya dengan memeriksa IMEI<sup>6</sup> atau nomor seri untuk memastikan keasliannya. Pastikan perangkat telah dipulihkan sepenuhnya ke pengaturan pabrik dan tidak ada data lama yang tertinggal. Gunakan alat keamanan seperti antivirus dan enkripsi pada perangkat untuk melindungi data pribadi. Jika memungkinkan, beli dari penjual tepercaya dengan garansi atau

---

<sup>6</sup> IMEI (*International Mobile Equipment Identity*) adalah nomor unik yang diberikan kepada setiap ponsel atau perangkat mobile. Nomor ini seperti “nomor identitas” ponsel yang membedakan satu perangkat dengan yang lainnya. Dengan IMEI, kita bisa melacak atau memblokir ponsel jika hilang atau dicuri, karena nomor ini tidak bisa diubah. Jadi, kalau ponsel kita hilang, IMEI bisa membantu untuk melacak atau mematikannya agar tidak disalahgunakan.

kebijakan pengembalian, serta hindari transaksi dengan individu yang tidak dapat diverifikasi.

**b. Tidak meletakkan ponsel/laptop sembarangan.**

Meletakkan perangkat secara sembarangan meningkatkan risiko pencurian atau akses yang tidak sah, terutama jika perangkat jatuh ke tangan yang tidak bertanggung jawab. Selain itu, meletakkannya di tempat yang sembarangan juga bisa menyebabkan kerusakan fisik akibat benturan atau cairan yang tumpah, yang dapat merusak komponen perangkat. Untuk menjaga privasi dan keamanan informasi pribadi, serta memastikan perangkat tetap berfungsi dengan baik, penting untuk selalu menyimpannya di tempat yang aman dan terkontrol.

**c. Memasang pelindung (casing).**

*Casing* melindungi ponsel dari risiko kerusakan fisik yang bisa memicu hilangnya data dan akses terhadap akun-akun digital.

**d. Tidak isi ulang baterai dengan port USB di tempat publik.**

Hindari menggunakan port USB untuk mengisi ulang baterai karena bisa jadi ada *malware* (biasa disebut *juice jacking* atau pembajakan data menggunakan USB)<sup>7</sup>. *Port charge* USB di tempat umum seperti stasiun, bandara, atau pusat perbelanjaan sering kali tidak terjamin keamanannya. Sebaiknya gunakan charger pribadi atau power bank untuk menghindari risiko ini.

**e. Memperbaiki di service center resmi.**

Upayakan memperbaiki ponsel/laptop rusak di *service center* resmi. Kita tidak pernah tahu apa yang terjadi pada ponsel selama proses perbaikan.

Jika tempat service resmi tidak tersedia, cari layanan non-resmi terpercaya dengan reputasi baik dan ulasan positif, namun pastikan untuk mempertimbangkan risiko pada garansi. Hubungi service

---

<sup>7</sup> Committee to Protect Journalist, "Digital Safety Kit", 30 Juli, 2019, <https://cpj.org/2019/07/digital-safety-kit-journalists/#device>

resmi secara online, sebab beberapa pabrik menyediakan panduan perbaikan jarak jauh.

## 2. Perlindungan Digital

### *Pada Ponsel*

- a. *Melindungi ponsel dengan kunci (password, pola, atau sidik jari) agar tidak mudah diakses orang lain.*

Jangan membiarkan layar ponsel Anda tanpa kunci. Kunci bisa berupa pin atau pola (kombinasi angka), password (kombinasi angka, huruf, dan karakter lain), atau sidik jari. Jangan gunakan tanggal lahir, nomor rumah atau kantor, atau yang mudah dikenali untuk membuat pin atau *password*.

- b. *Selalu memperbarui sistem operasi (OS), khususnya jika ada peringatan pada ponsel.*

Selalu ada celah keamanan (*bugs*) pada setiap versi Android, IOS, atau OS lain dan pembaruan berfungsi menambal celah itu.

- c. *Memperbarui aplikasi jika tersedia.*

Kita sebaiknya memperbarui aplikasi jika tersedia karena pembaruan tersebut seringkali mencakup perbaikan bug, peningkatan kinerja, dan yang paling penting, perbaikan keamanan. Pembaruan aplikasi membantu menutupi celah keamanan yang mungkin dieksploitasi oleh peretas untuk mengakses data pribadi atau perangkat kita.

- d. *Pasang kunci tambahan pada masing-masing aplikasi berupa pin, password, atau sidik jari.*

Pada berbagai ponsel pintar, ada fitur enkripsi untuk mengunci berbagai aplikasi. Beberapa aplikasi juga menyediakan pilihan kunci berupa pin (seperti Whatsapp atau Signal).

- e. *Ganti nama ponsel agar tidak mudah dikenali saat terkoneksi dengan jaringan via bluetooth atau WiFi.*

Nama perangkat yang terlihat secara publik dapat memberi informasi tentang jenis ponsel, merek, atau bahkan identitas pengguna. Hal ini bisa memudahkan orang lain untuk menjadikan perangkat kita sebagai target hacking, misalnya dengan mencoba

mengaksesnya melalui serangan *brute force* atau metode lain.

f. *Menonaktifkan sambungan WiFi dan bluetooth*

Semua perangkat pintar yang terhubung di internet memiliki alamat. Nama lain dari alamat itu adalah internet protocol (*IP Address*). Jika tidak digunakan untuk mencegah perangkat kita terdeteksi perangkat lain. *IP address* dapat terdeteksi orang lain dan jadi pintu masuk *software* jahat alias *malware*.

g. *Menonaktifkan fitur lokasi saat tidak diperlukan.*

Menonaktifkan fitur lokasi saat tidak diperlukan sangat penting untuk melindungi privasi dan mencegah penyalahgunaan data. Dengan menonaktifkan fitur lokasi, kita dapat mengurangi risiko pelacakan aktivitas atau perjalanan kita oleh pihak ketiga, termasuk pengiklan, aplikasi yang tidak dipercaya, atau bahkan potensi ancaman kejahatan siber.

h. *Menghindari penggunaan WiFi publik seperti di kafe, bandara, dan tempat umum lainnya.*

WiFi publik bisa menjadi pintu masuk jadi pintu masuk *malware*, pencurian data, dan peretasan ponsel.

i. *Menggunakan VPN saat mengakses WiFi publik*

WiFi publik, seperti yang ada di kafe, bandara, atau hotel, sering kali tidak memiliki enkripsi yang cukup kuat, membuatnya rentan terhadap serangan *Man-in-the-Middle* dan pencurian data. Tanpa VPN, data pribadi seperti kata sandi, informasi kartu kredit, atau riwayat browsing bisa dengan mudah disadap oleh pihak ketiga yang berbahaya. VPN mengenkripsi koneksi internet kita, sehingga menjaga data kita tetap aman meskipun sedang menggunakan jaringan WiFi publik yang tidak terlindungi.

Jangan menggunakan sembarang layanan VPN karena berpotensi membahayakan keamanan seperti mengambil data pribadi, meminta akses terhadap informasi sensitif, hingga meminta akses memindai aplikasi yang terinstal di perangkat kita. Jika tidak mampu menggunakan VPN berbayar, gunakan VPN yang menawarkan perlindungan tanpa terlalu banyak pembatasan pada versi gratis seperti Proton VPN. Proton VPN masih direkomendasikan karena dikembangkan developer

dari Swiss dan berada di bawah hukum Swiss, negara yang mengedepankan perlindungan data pribadi. Jika memilih versi yang tidak berbayar, pilihan *server* (peladen) sangat sedikit tetapi bisa diakses tanpa batasan waktu maupun kuota.

j. *Memasang antivirus pada ponsel.*

Memasang antivirus pada ponsel sangat penting untuk melindungi perangkat dari berbagai ancaman siber seperti malware, spyware, virus, dan aplikasi berbahaya. Umumnya ponsel, terutama buka flagship, sangat rentan terhadap serangan yang dapat mencuri data pribadi, merusak perangkat, atau bahkan mengambil alih kontrol atas ponsel untuk tujuan ilegal. Antivirus juga membantu melindungi informasi sensitif seperti kata sandi, nomor kartu kredit, dan pesan pribadi yang dapat disalahgunakan jika jatuh ke tangan yang salah. Selain itu, antivirus pada ponsel juga dapat memblokir situs web berbahaya, memperbarui sistem keamanan secara otomatis, serta memindai dan membersihkan perangkat dari potensi ancaman yang terdeteksi.

k. *Tidak menyimpan file/dokumen sensitif pada ponsel*

karena berisiko, terutama saat ponsel hilang, diretas, atau disusupi *malware*.

l. *Pasang enkripsi ponsel Anda.*

- Enkripsi adalah proses mengubah data menjadi kode rahasia yang tidak mudah terbaca. Jika ponsel Anda terenkripsi, data-data di dalamnya tak bisa terbaca oleh orang yang tidak sah.
- Fitur ini memungkinkan kita mengatur aplikasi mana saja yang hendak dienkripsi. Misalnya mengunci aplikasi secara otomatis setelah ditutup, atau menyembunyikan aplikasi-aplikasi kredensial (seperti *mobile banking*, *cloud drive*, atau penyimpanan data penting).

1) *Pada Android*

Nama fitur ini berbeda-beda pada setiap ponsel Android. Sebagian bernama "File-Based Encryption." Untuk menemukannya, buka menu Setting dan Privacy & Security.

## 2) Pada IOS

Berbeda dari Android yang fitur enkripsinya perlu diaktifkan, hampir seluruh perangkat iPhone memiliki fitur *full device encryption* (FDE) atau enkripsi penuh yang aktif sejak pengaturan pabrik.

### m. Membatasi izin akses aplikasi terhadap perangkat (lokasi, kamera, mikrofon, dan lainnya).

Aplikasi yang baik tidak membutuhkan akses terhadap semua alat pada ponsel. Aplikasi yang baik tetap bisa bekerja meskipun kita tidak mengizinkannya mengakses seluruh peralatan.

Batasi izin akses setiap aplikasi agar mereka hanya mengakses peralatan yang dibutuhkan. Misalnya aplikasi percakapan (*chat*) tidak membutuhkan akses lokasi. Jika aplikasi chat Anda memiliki akses terhadap fitur lokasi ponsel Anda, hapus izin aksesnya jika tidak diperlukan.

## 1) Pada Android

Buka menu Settings (pengaturan), masuk Privacy, lalu masuk Permission Manager. Di sana terdapat daftar fitur pada ponsel Anda.

Cek fitur tersebut satu-satu dan lihat aplikasi apa saja yang mendapatkan izin akses. Misalnya cek fitur mikrofon dan lihat aplikasi apa yang bisa mengaksesnya.

Anda bisa mengganti izin akses setiap aplikasi terhadap fitur mikrofon tersebut dan hapus izin akses jika tidak diperlukan.

Misalnya, Anda hanya mengizinkan Whatsapp untuk mengakses mikrofon “hanya saat digunakan” (*allowed only while in use*), bukan “sepanjang waktu” (*allowed all the time*)

## 2) Pada IOS

Buka menu Settings (pengaturan), masuk ke Privacy & Security, lalu cek aplikasi apa saja yang mendapatkan izin atau masuk *list of permissions* (daftar izin) ke fitur-fitur

perangkat Anda<sup>8</sup>.

Aturlah aplikasi mana yang Anda izinkan mengakses fitur-fitur itu. Misalnya tentukan aplikasi mana saja yang bisa mengakses kamera, dokumen foto, atau lokasi Anda.

### ***Pada Laptop***

- a. *Mengunci laptop dengan password, kode, atau PIN.*

Pasang password atau PIN yang lebih kuat lebih sulit ditembus. Buat password dengan kombinasi frasa, huruf kapital dan kecil, angka, dan karakter lain. Saat ini, usahakan minimal sandi yang kita miliki adalah 8 kombinasi karakter.

- b. *Selalu memperbarui sistem operasi dan aplikasi.*

Sama seperti perangkat digital kita lainnya, pasti akan selalu ada celah keamanan (*bugs*) pada setiap versi sistem operasi di perangkat laptop kita. Pembaruan sistem berfungsi menambal celah itu.

Contoh adalah jumlah celah keamanan yang ditemukan pada sistem operasi Windows setiap tahunnya dapat bervariasi, tergantung pada kompleksitas dan ukuran sistem operasi tersebut<sup>9</sup>.

- c. *Menggunakan sistem operasi yang legal.*

Pembaruan sistem operasi hanya akan bisa dilakukan jika sistem operasi tersebut orisinal atau legal (bukan bajakan). Sistem operasi yang ilegal tidak bisa diperbarui sehingga semua celah (*bugs*) yang menimbulkan kerentanan tidak bisa ditutup<sup>10</sup>. Jika yang legal terlalu mahal, sistem operasi *open source* yang

---

8 David Nield, "How to manage app permissions on your iPhone", 2 Maret, 2024, <https://www.theverge.com/24087604/iphone-app-permissions-how-to>

9 Sistem Operasi Windows milik Microsoft secara rutin merilis pembaruan keamanan bulanan yang mencakup perbaikan untuk berbagai kerentanannya. Misalnya, pada 2023, ditemukan sebanyak 2.860 celah keamanan dengan tingkat risiko yang beragam. Namun, tidak semua celah keamanan ditemukan atau diumumkan secara publik oleh Microsoft, karena beberapa di antaranya mungkin belum diketahui atau belum dieksploitasi.

10 WannaCry adalah ransomware pada 2017. Aplikasi berbahaya ini menyebar melalui kerentanannya pada sistem operasi Windows, terutama versi yang tidak diperbarui atau menggunakan salinan bajakan. Ransomware ini mengenkripsi data pengguna dan meminta tebusan untuk membuka akses kembali, yang mengancam kehilangan data berharga. Indonesia menjadi negara kedua yang paling banyak terkena WannaCry sebab menggunakan OS bajakan.

berbasis Linux bisa menjadi pilihan.

d. *Pasang antivirus atau antimalware pada komputer.*

Setiap sistem operasi menanamkan *software antivirus/antimalware*, misalnya Windows Defender pada laptop Windows serta XProtect dan Malware Removal Tool (MRT) pada MacBook. Memasang antivirus dan antimalware lain dengan reputasi baik layak dipertimbangkan sebagai *backup* jika antivirus/antimalware bawaan gagal mendeteksi virus/*malware*.

e. *Backup data/file yang tersimpan pada laptop secara reguler.*

Mem-*backup* data/file sangat penting dilakukan untuk mengurangi risiko komputer hilang, dicuri, atau rusak. Simpan salinan sebagai *backup* di *hard drive* lain seperti *hardisk* eksternal yang aman. Jika bisa, gunakan metode backup 3-2-1: *Backup* 3-2-1 adalah strategi cadangan data yang bertujuan untuk mengurangi risiko kehilangan data. Prinsip utamanya adalah memiliki tiga salinan data:

- Salinan pertama adalah data asli yang ada di perangkat utama (seperti ponsel, laptop, atau komputer).
- Salinan kedua adalah salinan cadangan yang disimpan di perangkat penyimpanan terpisah, seperti hard drive eksternal atau server lokal.
- Salinan ketiga adalah salinan cadangan lain yang disimpan di lokasi berbeda, seperti layanan penyimpanan *cloud* atau *server remote*.

Dengan cara ini, jika terjadi kerusakan perangkat utama atau penyimpanan lokal, data tetap aman dan dapat dipulihkan dari salinan cadangan yang lain. Prinsip ini membantu memastikan bahwa data tetap terlindungi meskipun salah satu salinan hilang atau rusak.

f. *Menutup kamera bawaan laptop atau webcam saat tidak digunakan.*

Langkah ini mengurangi risiko jika terdapat *malware* yang mampu mengakses kamera bawaan laptop Anda. Beberapa aplikasi, termasuk yang berbasis *web*, meminta akses terhadap

kamera atau mikrofon laptop Anda. Periksa izin untuk setiap aplikasi sebelum memberikan akses kamera atau mikrofon.

g. *Pasang enkripsi pada laptop*<sup>11</sup>.

Dengan mengenkripsi laptop Anda, data-data di dalamnya tak bisa terbaca oleh orang yang tidak sah. Misalnya saat insiden laptop dalam penguasaan orang lain, orang tersebut tidak mudah membaca data/dokumen di dalamnya.

- Pada Windows, aktifkan Bitlocker untuk enkripsi seluruh isi *hard disk*. Untuk panduan lebih detail, bukalah tautan <https://t.ly/enkripsiwindows>
- Pada Mac, aktifkan FileVault. Untuk pengaturan, klik ikon apel > system preferences > security & privacy > FileVault > nyalakan jadi ON.
- Anda juga bisa menggunakan *software* gratis Veracrypt untuk mengenkripsi *hard drives* dan penyimpanan eksternal.
- Enkripsi membutuhkan password yang unik dan kuat agar tidak bisa ditembus oleh orang yang tidak berhak.

h. *Mengaktifkan firewall pada laptop*.

*Firewall* adalah perangkat jaringan yang memantau lalu lintas data masuk dan keluar hingga mengizinkan atau mencegah lalu lintas data yang tidak aman. Misalnya memblokir konten tertentu atau *e-mail* yang dianggap berbahaya.

- Pada Windows, klik Settings > Update and security > klik Firewall and protection untuk mengaktifkan *firewall*.
- Pada Mac, ketuk ikon apel > System Preference > security & privacy > aktifkan Firewall.

i. *Mematikan fitur lokasi pada laptop*.

- Dalam kondisi “on”, fitur lokasi membuat lokasi detail Anda mudah dibaca saat terhubung jaringan internet, misalnya oleh pengelola platform aplikasi *web*.
- Pada Windows masuklah menu *Setting > Privacy > Location*

---

11 Harlo Holmes, “Digital Security Fundamentals”, 2023, freedom.press

(matikan 'Pin to Start') untuk mematikan fitur lokasi.

- Pada Mac OS, masuklah *System Preference > security & privacy >* matikan *location* untuk mematikan fitur lokasi.
- j. *Ganti nama perangkat.*

Setiap laptop memiliki nama bawaan masing-masing. Masuklah menu. Setting dan gantilah nama itu dengan nama unik agar orang lain. Ini setidaknya membuat orang lain tidak mudah mengenali saat laptop Anda terhubung dengan jaringan publik.

## B. PERLINDUNGAN DATA ONLINE

Pada Selasa, 25 Juni 2024, sebuah akun X dengan nama greschinov yang aktif mengunggah isu konflik di Gaza membuat unggahan yang menyertakan berita berjudul "*Impor RI dari Israel Makin Menyala, Kenaikannya Tembus 1.204%*". Dia juga mengunggah nama lengkap jurnalis dan media yang menerbitkan artikel itu (*Bisnis.com*)<sup>12</sup>.

Akun greschinov kemudian menuliskan beberapa keraguannya tentang berita yang terbit pada Kamis, 20 Juni 2024 itu, menyertakan data perbandingan, dan pada akhirnya menuding berita itu hoaks. Berita itu ditulis jurnalis *Bisnis.com* itu berdasarkan data BPS tentang impor dari Israel pada April-Mei 2024. Sedangkan greschinov meyakini data resmi di *website* BPS baru keluar sampai periode April 2024.

"Dia tahu darimana data Mei 2024 itu. Klaimnya fantastis sampai 1200%! Ada apa ini?" tanya greschinov. "Lucunya berita ini langsung digembar gemborkan, kaum zionis pesek, seakan akan menjadi kabar gembira," imbuhnya.

Selain menuding berita tersebut hoaks, akun greschinov juga menyertakan profil jurnalis yang tertulis pada akun LinkedIn. "Ini akun linkedin si penulis berita. Tolong kau keluar dan buat klarifikasi, data darimana yang kau ambil? Jika terbukti manipulasi, orang ini harus siap dipecat, atau mengundurkan diri dari pekerjaannya, karena sengaja membuat data palsu mengatasnamakan BPS!"

Seperti jurnalis, pembuat konten yang kritis rentan menjadi target serangan yang memanfaatkan data pribadi yang tersebar di berbagai platform digital.

---

12 Aliansi Jurnalis Independen, "Jurnalis Bisnis Indonesia jadi Korban Doxing", 2024, <https://advokasi.aji.or.id/id/read/data-kekerasan/18889.html>

Data pribadi bisa dimanfaatkan untuk mengancam. Lihat kembali bagaimana profil dan data personal Anda tersebar di internet, lalu pikirkan ulang apakah data perlu dipublikasikan atau sebaliknya perlu dihapus.

### **1. Cek Data Anda yang Tersebar Online**

- a. Bukalah mesin pencari yang umum digunakan (Google, Duckduckgo, dan Bing).
- b. Ketik nama Anda pada mesin pencari dan lihat hasilnya.
- c. Ketik data Anda lainnya misalnya alamat, nomor telepon/HP, tanggal lahir, atau nomor KTP (NIK) pada mesin pencari.
- d. Gunakan pengaturan *private window* atau mode *incognito* (tersembunyi) untuk mendapatkan hasil pencarian yang lebih luas.
- e. Gunakan pencarian lanjutan (*advanced search*) pada mesin pencari atau teknik Boolean *searches* untuk mendapatkan hasil lebih akurat.
- f. Selain mencari identitas dalam bentuk teks (nama, nomor HP, tanggal lahir, alamat, dan NIK), carilah foto Anda pada mesin pencari. Caranya, gunakan fitur *reverse image search* (misalnya pada Google versi desktop atau Google Lens pada Android) untuk melihat di mana saja foto Anda menyebar.
- g. Carilah nama Anda di situs-situs pengarsipan seperti Wayback Machine.
- h. Cek data-data serupa milik anggota keluarga Anda untuk memastikan ada-tidaknya data mereka yang tersebar.
- i. Jika Anda menemukan data-data itu, hapuslah jika memang tidak diperlukan atau batasi akses terhadapnya (Anda punya akses terhadap data tersebut).
- j. Jika Anda tidak punya akses menghapusnya, hubungi admin situs web atau pemilik akun yang mengunggah data Anda. Mintalah mereka menghapus data tersebut.
- k. Jika Anda menemukan data sensitif tentang Anda di Wayback Machine, ajukan permohonan penghapusan data dengan

mengirim *e-mail* ke [info@archive.org](mailto:info@archive.org) dengan judul (*subject*) “Request for Exclusion from web.archive.org”. Pada badan surat (*body text*), sebutkan tautan (URL) informasi yang ingin Anda hapus, periode penghapusan, dan informasi lain<sup>13</sup>. Permohonan tersebut akan diulas oleh tim Wayback Machine dan tidak ada jaminan data yang dimaksud akan dihapus.

## 2. Cek Kebocoran Data

- Periksa apakah akun *e-mail* Anda pernah menjadi korban kebocoran data atau tidak.
- Untuk memeriksa kebocoran email, gunakan [www.haveibeenpwned.com](http://www.haveibeenpwned.com) atau <https://monitor.firefox.com/> atau [periksadata.com](http://periksadata.com).
- Masukkan alamat *e-mail* Anda. Situs tersebut akan memberikan hasil analisis, apakah *e-mail* Anda pernah bocor atau tidak.
- Jika *e-mail* Anda pernah bocor di layanan tertentu, segera ganti kata sandinya di layanan tersebut.

## 3. Hapus atau Batasi Akses

- a. Pastikan data-data yang Anda publikasikan di media sosial bukan data sensitif tentang Anda dan tidak mengancam privasi Anda, seperti alamat rumah, NIK, nomor HP/kontak Whatsapp pribadi, nomor rekening, dan sebagainya.
- b. Batasi akses terhadap informasi tentang Anda di media sosial (bagi akun pribadi yang tidak dipakai untuk kepentingan kampanye/penyebaran konten).
- c. Review secara berkala pengaturan privasi (*privacy setting*) akun media sosial untuk memastikan data Anda yang tersebar ke publik tidak berpotensi mengganggu Anda.
- d. Pastikan keluarga, teman, atau orang dekat juga tidak mempublikasikan data-data sensitif mereka di media sosial/platform digital lain. Ini penting untuk mencegah mereka menjadi sasaran serangan.

---

<sup>13</sup> Wayback Machine, “How do I request to remove something from archive.org?”, archive.org

- e. Untuk lebih menjaga privasi, Anda bisa meminta Google membuat kabur (*blur*) tampilan rumah Anda pada Google Street View. Caranya sebagai berikut:
- Masuk ke Street View, klik gambar rumah Anda.
  - Klik tanda tiga titik pada sudut kanan-atas, pilih “Report a problem”.
  - Seret kotak merah pada bagian gambar yang hendak dikaburkan.
  - Pilih “Request blurring” (“A face”, “My home”, “My vehicle / a license plate”, atau “A different object”).
  - Isi kolom berikutnya dan klik “Submit”.



### C. PENGAMANAN AKUN

Laporan riset PR2Media dan AJI tentang Keamanan Digital Pembuat Konten di Indonesia menunjukkan pembuat konten memiliki risiko serangan digital yang tidak jauh berbeda dengan jurnalis. Terutama pembuat konten yang menyuarakan isu-isu kepentingan publik. Bahkan risiko pembuat konten lebih besar karena tidak mendapat perlindungan Undang-Undang Pers seperti jurnalis.

Sebagai contoh, salah satu peneliti Indonesia Corruption Watch (ICW) menjadi korban doxing yang dilakukan akun Instagram @volt\_anonym.<sup>14</sup> Doxing tersebut disebar pada 3 Januari 2025 setelah peneliti ICW menyampaikan pandangannya terkait penominasian Joko Widodo dengan kategori “Kejahatan Terorganisasi dan Korupsi 2024” oleh Organized Crime and Corruption Reporting Project (OCCRP) di sejumlah media massa sejak 1 Januari 2025.

<sup>14</sup> <https://antikorupsi.org/id/jokowi-masuk-nominasi-pemimpin-terkorup-icw-kena-doxing-dan-kami-tidak-takut>

Doxing tersebut berupa pengungkapan sejumlah data pribadi mulai dari nomor telepon, nomor Kartu Tanda Kependudukan (KTP), alamat tinggal, spesifikasi device telepon yang digunakan, hingga titik koordinat lokasi terakhir peneliti dalam bentuk tautan google maps. Dalam unggahannya di instagram, @volt\_anonym menuliskan caption bernada ancaman dengan insinuasii kuat yang membahayakan keamanan diri peneliti. ICW kemudian melaporkan kasus ini ke Bareskrim Polri.

Riset PR2Media dan AJI juga mengungkap serangan yang dialami pengelola akun Aksi Kamisan Bandung. Mereka menyampaikan hampir setiap unggahan di media sosial terkait aksi mereka diserang oleh akun-akun pendengung (buzzer). Serangan berupa pernyataan negatif di kolom komentar itu muncul saat akun Instagram Aksi Kamisan Bandung mengunggah konten yang membahas isu Papua atau diskriminasi gender.

Selain itu, pengelola akun Aksi Kamisan Bandung mengalami berbagai percobaan peretasan akun setiap kali mereka mengunggah konten berisi ajakan aksi demonstrasi. Serangan ini juga tidak berdiri sendiri, melainkan disertai dengan ancaman akan mencari atau mengungkap admin akun Aksi Kamisan Bandung.

Kedua contoh di atas membuktikan bahwa pembuat konten rentan menjadi korban serangan digital. Karena itu, pembuat konten juga perlu melakukan upaya mitigasi untuk mencegah serangan terhadap akun digital. Berikut sejumlah hal fundamental yang dapat dilakukan pembuat konten dalam mengamankan akun digital.

### **1. Memperkuat Sandi**

Langkah paling mendasar untuk mengamankan akun adalah menggunakan sandi yang aman sehingga tidak gampang ditembus.

#### *a. Gunakan frasa kunci (passphrase), bukan kata kunci (password).*

- Periksa ulang seberapa tinggi tingkat keamanan kata sandi yang kita gunakan. Buka [www.howsecuremypassword.com](http://www.howsecuremypassword.com) atau [passwordmonster.com](http://passwordmonster.com). Masukkan sandi yang Anda pakai untuk salah satu akun (tuliskan saja pola kata sandinya, bukan kata sandi yang sebenarnya, untuk menghindari perekaman di situs itu) dan lihat seberapa mudah sandi Anda ditebak.
- Untuk memperkuat sandi, cobalah mengkombinasikan kata

sandi antara huruf kapital, angka, dan karakter lain. Misalnya “K!l1m4nj4r0”. Cek lagi di dua situs di atas untuk mengukur seberapa lama sandi Anda bisa dijebol.

- Berikutnya, gunakan spasi dan simbol untuk membuat *passphrase* yang lebih kuat, misalnya: “6unun6 K!!!m4nj4r0”.
- Perkuat keamanan kata sandi dengan menggunakan kombinasi antara huruf, angka, simbol, dan besar kecilnya huruf.
- Buatlah kata sandi berupa kalimat yang mudah diingat, tetapi tidak terkait dengan identitas kita yang diketahui publik (misalnya tanggal lahir, kota domisili, nama anak, dan lainnya).

#### *b. Gunakan Password Manager*

- Jangan gunakan satu sandi untuk beberapa akun. Bobolnya akun Mark Zuckerberg pada 2016 disebabkan penggunaan *password* yang sama untuk beberapa akun media sosialnya.
- Gunakan aplikasi penyimpan atau pengelola kata sandi (*password manager*) untuk memudahkan pengelolaan kata sandi berbeda-beda untuk semua identitas digital. Anda tidak perlu menghafal puluhan sandi yang berbeda, cukup dengan satu sandi yang kuat untuk *password manager*.
- Ganti kata sandi secara berkala, misalnya setahun sekali, untuk mengantisipasi jika kata sandi tersebut sudah bocor.

## **2. Pengamanan 2 Lapis**

### *a. Autentikasi dua langkah (2FA)*

- Aktifkan autentikasi dua langkah (2FA) pada setiap akun yang menyediakan fitur tersebut. 2FA adalah pintu kedua setelah sandi utama. Seandainya sandi kita dibobol, 2FA menjadi penghalang kedua terhadap peretas.
- Pengaturan 2FA tiap akun berbeda-beda. Pada dasarnya 2FA menggunakan kata sandi satu kali pakai, biasanya dalam bentuk angka yang harus dimasukkan setelah memasukkan *password* atau sandi utama.

- Penggunaan 2FA bisa menggunakan aplikasi tertentu, misalnya Google Authenticator atau aplikasi sejenis.
  - Tidak disarankan memasang 2FA yang menggunakan *short message service* (SMS) karena SMS rentan disadap dan tidak terenkripsi.
- b. *Pertimbangkan menggunakan kunci fisik (physical key)*
- Salah satu pengamanan 2 lapis yang dinilai paling aman saat ini adalah penggunaan kunci fisik, misalnya [YubiKey](#) atau [Google Titan](#).



*YubiKey (kiri) dan Google Titan.*

- Penggunaan kunci fisik mencegah siapa pun memasuki sebuah akun tanpa kunci fisik tersebut.
  - Kelemahannya, jika kunci fisik hilang dan tanpa backup metode 2FA lain, kita bisa kehilangan akses terhadap akun tersebut selamanya. Berhati-hatilah menyimpannya dan jangan sampai hilang/jatuh ke tangan orang lain.
- ### 3. Mengatur Privasi Akun
- a. Periksa pengaturan privasi di platform digital yang Anda gunakan.
  - b. Periksa informasi pribadi apa yang direkam oleh platform.
    - 1) Pengaturan di Google misalnya, bisa dicek di tautan <https://policies.google.com/privacy>.
    - 2) Pengaturan privasi pada Google bisa dicek di <https://myaccount.google.com/intro/privacycheckup>.

- 3) Untuk informasi pribadi yang direkam oleh Facebook, bisa dicek melalui <https://www.facebook.com/about/privacy>.
- 4) Pengaturan privasi pada Facebook melalui tautan <https://www.facebook.com/about/basics/manage-your-privacy>.
- 5) Lakukan pemeriksaan serupa pada platform lain yang kita gunakan, seperti Twitter, Instagram, YouTube, dan lain-lain.

#### **4. Manajemen Penggunaan Akun**

Berbagi informasi atau data melalui akun digital mendatangkan konsekuensi bagi keamanan pemiliknya. Lihat kembali informasi apa yang tersimpan di setiap akun digital Anda dan konsekuensinya bagi diri sendiri, keluarga, teman, kolega, atau narasumber seandainya akun tersebut bocor, diretas, atau diserang.

Berikut prinsip yang perlu dipertimbangkan dalam manajemen akun digital:

- 1) Pisahkan akun untuk tujuan yang berbeda. Misalnya akun untuk pekerjaan (penyebarluasan konten), aktivisme (jika Anda terlibat kampanye tertentu), untuk kebutuhan pribadi, dan lainnya. Pemisahan akun bisa mengurangi risiko saat terjadi kebocoran atau peretasan, yakni membatasi data yang bocor hanya pada satu akun.
- 2) Cek pengaturan privasi (*privacy setting*) dan lihat informasi apa saja yang bisa dilihat publik (khususnya pada akun media sosial). Pastikan informasi yang bisa dilihat publik bukan data sensitif tentang Anda/keluarga/orang dekat atau yang berpotensi menjadi celah menyerang Anda.
- 3) Hapus informasi atau data sensitif yang masih bisa diakses oleh publik. Tetapi, sebelum menghapus, pastikan Anda memiliki *back up* atau salinan data tersebut seperti pesan pribadi (*direct messenger/DM*), e-mail, dan lainnya di tempat penyimpanan yang aman. Simpan di *backup* data di *hard drive* eksternal yang bisa dikunci.
- 4) Review seluruh akun Anda. Catat semua akun digital yang pernah Anda buat (e-mail, media sosial, e-banking, dan seluruh

- platform digital lain). Catat satu per satu akun tersebut terkait akun apa saja (misal akun Gmail terkait akun Facebook, X, dan Instagram), terkait nomor seluler yang mana, sandi, dan model 2FA apa yang terpasang.
- 5) Setelah selesai mendata seluruh akun digital Anda, lihat kembali akun mana yang sudah tidak Anda gunakan. Sebaiknya hapus akun-akun yang sudah tidak digunakan (bukan sekadar keluar/*logout*). Sebelum menghapus, buatlah *backup* data dari akun-akun tersebut dan simpan di *hard drive* yang aman.
  - 6) Cek kembali apakah sandi pada setiap akun benar-benar kuat. Jika Anda merasa sandi yang Anda pakai lemah, ubahlah dengan sandi yang kuat. Kembalilah ke bagian C.1. tentang Memperkuat Sandi untuk detail panduan.
  - 7) Cek kembali akun mana saja yang belum dipasang 2FA dan segera pasang metode 2FA yang paling aman.
  - 8) Cek aktivitas akun (*account activity*) pada setiap akun. Buka menu pengaturan (*setting*) dan carilah pengaturan terkait. Lihat perangkat apa saja yang log in ke akun Anda. Jika Anda menemukan ada perangkat yang tidak dikenal, segera hapus *log* atau akses perangkat asing tersebut dari akun Anda.
  - 9) Sebisa mungkin tidak mengakses akun dari perangkat komputer publik atau milik orang lain. Jika terpaksa, pastikan hapus (*clear*) *history* dan *cache* pada peramban tersebut setelah *log out* dari akun Anda. Hal ini untuk mencegah pengguna komputer yang sama melihat aktivitas Anda pada akun tersebut.

## IV. MEKANISME PENANGANAN

Ada beberapa langkah yang perlu dilakukan saat pembuat konten menjadi sasaran serangan digital atau menyadari sedang menjadi target serangan.

### 1. Jangan panik, tenangkan pikiran sebelum merespons serangan

Reaksi panik dapat memperburuk situasi dan mengarah pada keputusan yang terburu-buru, seperti memberikan informasi sensitif, mengklik tautan berbahaya, atau melakukan tindakan yang memperbesar kerugian. Dengan menjaga ketenangan, kita bisa lebih objektif dalam menilai ancaman, mengambil langkah yang lebih terencana untuk mengatasi serangan, seperti memutuskan koneksi internet, mengganti kata sandi, atau melaporkan insiden kepada pihak berwenang atau profesional. Mengendalikan emosi juga memungkinkan kita untuk bertindak dengan lebih efisien dalam mencegah atau memitigasi dampak dari serangan digital tersebut.

### 2. Lakukan langkah-langkah darurat untuk mengidentifikasi masalah

Langkah-langkah darurat untuk mengidentifikasi masalah serangan digital adalah sebagai berikut:

1. **Putuskan koneksi internet:** segera cabut atau nonaktifkan koneksi internet untuk mencegah penyebaran atau dampak lebih lanjut dari serangan.
2. **Periksa aktivitas yang mencurigakan:** tinjau aktivitas perangkat dan akun yang terlihat tidak biasa, seperti login yang tidak dikenali, perubahan pengaturan, atau file yang hilang atau muncul tiba-tiba.
3. **Jalankan pemindai keamanan (antivirus):** gunakan perangkat lunak antivirus atau pemindai keamanan yang diperbarui untuk mendeteksi *malware* atau virus yang ada pada perangkat.
4. **Ubah kata sandi:** ganti kata sandi pada akun yang terhubung dengan perangkat yang diserang dan pastikan untuk mengaktifkan verifikasi dua langkah (2FA).
5. **Periksa riwayat log dan aktivitas:** antuk akun atau aplikasi online, jika masih bisa diakses, cek riwayat login dan aktivitas untuk melihat jika ada akses yang tidak sah.
6. **Cadangkan data penting:** segera cadangkan data penting yang masih aman untuk mencegah kehilangan informasi yang lebih besar.
7. **Hubungi penyedia layanan atau profesional keamanan:** jika perlu, hubungi pihak yang memiliki kapasitas/profesional dalam keamanan siber atau

organisasi masyarakat sipil yang bisa menangani serangan siber (misalnya Tim Reaksi Cepat atau TRACE) untuk mendapatkan bantuan lebih lanjut dan memperbaiki kerusakan.

8. **Laporkan serangan:** laporkan serangan ke layanan penyedia aplikasi atau platform *online* untuk pemulihan akun atau polisi jika diperlukan.

### 3. Dokumentasikan kondisi yang terjadi pada akun Anda

Segera dokumentasikan isi pesan (*e-mail* atau *direct messenger*), notifikasi, atau tanda-tanda lain yang muncul.

Cara dokumentasi yang paling mudah adalah merekam tangkapan layar (*screenshot*) lalu simpan rekaman itu sebagai bukti.

### 4. Susun kronologi terjadinya serangan

Dalam kondisi panik, hal ini tidak begitu mudah. Maka itu tenangkan pikiran dengan cara bertanya pada diri sendiri, kapan pertanda awal kondisi digital yang tidak wajar, hilangnya akses, hingga upaya terakhir yang dilakukan untuk merespons serangan. Ambil alat pencatat, segera catat apa yang diingat berdasarkan kronologi waktu.

Berikut langkah darurat yang bisa dilakukan di awal untuk merespons serangan:

#### A. KEHILANGAN AKSES TERHADAP AKUN

Akun *email*, media sosial, dan platform percakapan menjadi medium vital bagi semua orang, termasuk pembuat konten. Apalagi pembuat konten dengan isu-isu yang sensitif. Karenanya, akun sangat mungkin menjadi target serangan.

Salah satu dampak serangan adalah hilangnya akses terhadap sebuah akun platform digital. Jika itu terjadi, pastikan Anda melakukan langkah berikut:

##### 1. Identifikasi masalah

- a. Pastikan username dan password yang Anda masukkan benar, tidak ada kesalahan tulis (*typo*) termasuk posisi *capslock*.
- b. Ingat kapan kali terakhir mengganti *password* dan masukkan password terakhir yang dibuat.
- c. Cek akses terakhir yang dilakukan admin (jika admin lebih dari 1 orang). Pastikan tidak ada admin yang menghapus akun. Jika akun dihapus (oleh admin maupun orang lain), maka akun tidak bisa dikembalikan.

- d. Cek apakah Anda masih bisa mengakses akun email terkait akun (email pemulihan) dan nomor ponsel terkait.
- e. Cek *inbox email* terkait akun, apakah ada notifikasi yang menunjukkan ada upaya masuk (login) dari perangkat yang tidak Anda kenal.
- f. Jika yang bermasalah adalah akun media sosial, lihat profil akun Anda (lewat akun lain atau mesin pencari), apakah ada yang berubah atau ada postingan yang tidak pernah Anda unggah.
- g. Jika ada yang postingan yang hilang, muncul postingan yang diunggah bukan oleh Anda, ada notifikasi akses dari perangkat asing, atau ada indikasi perubahan email/nomor pemulihan yang tidak Anda lakukan, berarti akun Anda diambil alih orang lain.
- h. Jika *username* dan *password* sudah dipastikan benar, hal yang mungkin terjadi adalah akun Anda diblok atau di-*suspend* oleh platform. Hal ini bisa terjadi karena akun Anda dilaporkan secara masif oleh akun-akun lain atau karena dianggap melanggar panduan komunitas (*community guidelines*).

## **2. Peretasan Whatsapp**

- a. Pastikan apakah akun Whatsapp benar-benar diretas. Jika akun Whatsapp Anda tiba-tiba keluar (*log out*) dari perangkat, itu adalah indikasi bahwa ada orang lain yang berusaha mengakses akun tersebut dari perangkat lain.
- b. Jika akun Whatsapp hanya keluar dari perangkat dan belum mengirim pesan ke nomor lain, kemungkinan besar pelaku belum berhasil menguasai nomor Anda karena harus memasukkan PIN (jika Anda mengaktifkan Two-Step Verification pada akun Whatsapp).
- c. Jika akun Whatsapp itu sudah mengirim pesan ke nomor lain, artinya pelaku sudah berhasil menguasai akun Anda dan menggunakannya dari perangkat lain. Situasi ini lebih susah ditangani, apalagi jika pelaku sudah mengaktifkan 2FA.
- d. Lakukan prosedur berikut:
  - Copot/*uninstall* Whatsapp dari ponsel Anda dan install kembali.

- Daftarkan nomor Anda dan tunggu kode verifikasi melalui SMS dan masukkan segera kode verifikasi 6 digit yang dikirim via SMS.
  - Jika Anda tidak menerima kode 6 digit melalui SMS, tunggu hingga proses selesai dan coba lagi. Waktu tunggu dapat berlangsung hingga 10 menit.
  - Jika waktu berakhir sebelum Anda menerima kode verifikasi, akan ada opsi meminta panggilan telepon. Pilih opsi “Panggil saya” untuk meminta panggilan telepon.
  - Ketika Anda menerima panggilan, mesin suara otomatis akan memberitahukan kode verifikasi 6 digit. Masukkan kode ini untuk memverifikasi akun Whatsapp Anda.
  - Saat akun Anda kembali, segera tambahkan PIN dan email agar akun Whatsapp Anda tidak dicuri kembali.
  - Apabila Anda masih sulit masuk dan diminta untuk memasukkan kode verifikasi dua langkah, peretas mungkin telah mengaktifkan PIN di Whatsapp tersebut. Anda harus menunggu 7 hari sebelum dapat masuk ke akun tanpa kode verifikasi dua langkah.
  - Laporkan bahwa akun Anda telah dicuri ke alamat *email*: [support@whatsapp.com](mailto:support@whatsapp.com) dengan subyek “Hilang/Dicuri: Silakan nonaktifkan akun saya” di badan *email*.
- e. Cari bantuan jika langkah pemulihan gagal
- Tenangkan pikiran, susun kronologi peretasan.
  - Dokumentasikan semua tanda peretasan (notifikasi, pemberitahuan pada *e-mail*, dan langkah-langkah pemulihan), misalnya dengan *screenshot* (tangkapan layar).
  - Hubungi kontak darurat untuk bantuan penanganan (*daftar kontak bantuan penanganan ada di bagian akhir panduan ini*).

### **3. Peretasan akun Gmail**

- a. Jika 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 <https://s.id/PemulihanGmail>. Anda akan diminta memasukkan akun *recovery* (pemulihan) dan ikuti petunjuk berikutnya untuk mendapatkan kembali akses login ke akun email Anda.
  - c. Selengkapnya mengenai peretasan dan pemulihan akun Gmail, bisa mengikuti langkah-langkah dalam tautan ini <https://support.google.com/accounts/answer/7682439?hl=id>.
  - d. Cari bantuan jika langkah pemulihan gagal
    - Tenangkan pikiran, susun kronologi peretasan.
    - Dokumentasikan semua tanda peretasan (notifikasi, pemberitahuan pada *e-mail*, dan langkah-langkah pemulihan), misalnya dengan *screenshot* (tangkapan layar).
    - Hubungi kontak darurat untuk bantuan penanganan (*daftar kontak bantuan penanganan ada di bagian akhir panduan ini*).

#### **4. Peretasan Yahoo Mail**

- a. Reset sandi atau *password* Anda dengan masuk ke tautan <https://help.yahoo.com/kb/SLN27051.html>.
- b. Masukkan alamat email akun Yahoo Mail Anda.
- c. Pilih metode reset yang diinginkan, melalui nomor HP atau email pemulihan yang sudah Anda daftarkan. Pemulihan melalui email lebih direkomendasikan daripada nomor HP.
- d. Selanjutnya, sebuah kode akan dikirimkan ke email pemulihan atau via SMS. Masukkan kode itu ke halaman Yahoo.
- e. Buat sandi baru yang lebih kuat dengan kombinasi angka, huruf dan spasi.
- f. Cari bantuan jika langkah pemulihan gagal
  - Tenangkan pikiran, susun kronologi peretasan.
  - Dokumentasikan semua tanda peretasan (notifikasi, pemberitahuan pada *e-mail*, dan langkah-langkah pemulihan), misalnya dengan *screenshot* (tangkapan layar).

- Hubungi kontak darurat untuk bantuan penanganan (*daftar kontak bantuan penanganan ada di bagian akhir panduan ini*).

## 5. Pengambilalihan Akun Facebook

- a. Untuk mengetahui apakah ada orang lain yang mengakses akun Anda secara diam-diam, cek Pengaturan (setting)  Keamanan dan Info Login. Lalu periksa “Tempat Anda Login” untuk mengecek daftar perangkat (laptop atau ponsel) yang mengakses akun Anda.
- b. Jika menemukan perangkat yang bukan milik Anda, klik tiga titik di sebelah kanan, lalu pilih keluar. Ganti password Anda dengan yang lebih kuat.
- c. Saat akun Anda telah diretas dan password diubah, Facebook akan mengirimkan notifikasi melalui email yang Anda daftarkan. Cek apakah ada notifikasi tersebut!
- d. 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.
- e. Untuk melaporkan peretasan, klik tautan <https://www.facebook.com/hacked>.
- f. Cari bantuan jika langkah pemulihan gagal
  - Tenangkan pikiran, susun kronologi peretasan.
  - Dokumentasikan semua tanda peretasan (notifikasi, pemberitahuan pada *e-mail*, dan langkah-langkah pemulihan), misalnya dengan *screenshot* (tangkapan layar).
  - Hubungi kontak darurat untuk bantuan penanganan (*daftar kontak bantuan penanganan ada di bagian akhir panduan ini*).

## 6. Pengambilalihan Akun Instagram

- a. Jika menggunakan laptop, Anda bisa mengetahui apakah ada orang lain yang mengakses akun Anda secara diam-diam dengan

- mengecek Pengaturan (setting) > Login activity. Anda akan dibawa pada sebuah halaman yang berisi informasi tentang jenis perangkat dan lokasi login.
- b. Apabila Anda menemukan adanya perangkat yang tidak Anda gunakan, klik tanda panah di sebelah kanan, lalu klik logout.
  - c. Apabila Anda sudah tidak bisa masuk ke akun Instagram, cek pemberitahuan (*notice*) di alamat *e-mail* yang Anda daftarkan. Instagram akan mengirimkan pemberitahuan pada setiap perubahan yang terjadi pada akun Instagram Anda, seperti login dari perangkat berbeda atau perubahan password.
  - d. Klik fitur Secure Your Account Here dan Anda akan dibawa pada halaman untuk mengubah sandi. Masukkan sandi baru yang lebih kuat dan unik.
  - e. Jika akun sulit dipulihkan, laporkan ke Instagram dengan cara:
    - Pada layar login, ketuk “dapatkan bantuan untuk login” di bawah fitur Login (pada ponsel Android) atau “lupa kata sandi?” pada ponsel IOS.
    - Masukkan nama pengguna, email, atau nomor telepon
    - Anda, lalu ketuk “Berikutnya”.
    - 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.
  - f. Cari bantuan jika langkah pemulihan gagal
    - Tenangkan pikiran, susun kronologi peretasan.
    - Dokumentasikan semua tanda peretasan (notifikasi, pemberitahuan pada *e-mail*, dan langkah-langkah pemulihan), misalnya dengan *screenshot* (tangkapan layar).
    - Hubungi kontak darurat untuk bantuan penanganan (*daftar kontak bantuan penanganan ada di bagian akhir panduan ini*).

## **7. Pengambilalihan Akun Tiktok**

- a. Jika Anda mengalami hal-hal berikut pada akun Tiktok Anda,

bisa jadi itu adalah tanda peretasan:

- Sandi/*password* akun dan nomor telepon yang terhubung telah berubah.
  - *Username* akun atau *nickname* (nama akun) berubah.
  - Video-video yang pernah Anda unggah terhapus atau ada video yang terunggah tanpa izin Anda.
  - Akun Anda mengirim pesan tanpa disadari.
- b. Laman resmi Tiktok tidak memberitahukan detail prosedur jika pengguna kehilangan akun. Namun, berikut cara yang bisa dilakukan berdasarkan fitur pengamanan yang tersedia pada Tiktok.
- Buka aplikasi Tiktok pada ponsel, pilih “forgot password” atau “lupa password”.
  - Anda akan diminta memasukkan kontak yang terhubung dengan akun (nomor telepon atau *e-mail*, tergantung metode pemulihan akun yang pernah dipilih saat pembuatan akun).
  - Pilih tombol “reset” untuk mendapatkan kode pemulihan. Kode pemulihan akan dikirim nomor telepon (via SMS) atau *e-mail*.
  - Masukkan kode tersebut pada menu pemulihan atau “lupa password”. Jika semua berjalan normal, Anda bisa mengganti sandi dengan yang baru dan lebih kuat.
  - Jika tidak ada masalah, setidaknya peretas tidak dapat mengetahui sandi yang baru. Segera perkuat keamanan akun dengan 2FA yang lebih kuat, misalnya dengan *passkey* fisik jika ada.
- c. Hapus perangkat mencurigakan yang terhubung<sup>15</sup>
- Cek apakah ada yang *login* akun Tiktok Anda pada perangkat lain.
  - Buka menu “setting and privacy” (“pengaturan dan privasi”), lalu pilih “security” (“keamanan”). Klik “select your devices” (“pilih perangkat”).

---

<sup>15</sup> Tiktok, “My account has been hacked”, <https://support.tiktok.com/en/log-in-troubleshoot/log-in/my-account-has-been-hacked>

- Hapus semua perangkat lain yang mencurigakan.
  - Penguatan akun dan langkah penghapusan perangkat bisa diakses pada laman [\*My account has been hacked\*](#) pada situs web resmi Tiktok.
- d. Laporkan peretasan ke penyelenggara platform. Langkah-langkah pelaporan masalah ke Tiktok bisa dilihat pada laman Report a problem di laman [support.tiktok.com](https://support.tiktok.com) atau <https://support.tiktok.com/en/log-in-troubleshoot/troubleshooting/report-a-problem>.
- e. Cari bantuan jika langkah pemulihan gagal
- Tenangkan pikiran, susun kronologi peretasan.
  - Dokumentasikan semua tanda peretasan (notifikasi, pemberitahuan pada *e-mail*, dan langkah-langkah pemulihan), misalnya dengan *screenshot* (tangkapan layar).
  - Hubungi kontak darurat untuk bantuan penanganan (*daftar kontak bantuan penanganan ada di bagian akhir panduan ini*).

## **8. Pengambilalihan Akun Youtube**

Setiap akun Youtube terhubung dengan akun Google. Namun, ada kasus saat akun Youtube yang diretas belum bisa pulih kendati akun Gmail telah dipulihkan.

Pada 2022, sebuah akun Youtube milik kelompok aktivis gender minoritas diretas. Peretas mudah mengambil alih akun itu karena kata sandi yang sederhana (mudah ditebak) dan jarang diganti.

Upaya penanganan dilakukan dengan memaksa masuk ke akun Gmail yang terkait akun Youtube tersebut dan bisa kembali dikuasai. Meski demikian, akun Youtube tersebut belum bisa dipulihkan. Setelah melakukan upaya pemulihan berulang, akun Youtube tersebut sudah dihapus.

Muncul *e-mail* dari Youtube yang memberitahukan bahwa akun tersebut telah dihapus karena dianggap melanggar aturan. Mereka kemudian berulang kali mengajukan banding melalui tautan yang tersedia di *e-mail*, tetapi Youtube menyatakan akun tersebut tidak lagi terdaftar. Akun baru pulih setelah melaporkan kasus ini ke

Google dengan pendampingan dari lembaga yang biasa menangani serangan digital.

*a. Mengenali tanda peretasan*

- Muncul perubahan pada akun yang tidak Anda buat. Misalnya perubahan gambar profil, deskripsi, pengaturan *e-mail*, AdSense, atau ada pesan yang terkirim tanpa sepengetahuan Anda.
- Akun mengunggah video yang tidak pernah Anda buat. Ini berarti ada orang lain yang mengunggah video tersebut dengan akun Google Anda. Cek apakah ada *e-mail* notifikasi yang memperingatkan tentang unggahan video tidak dikenal itu atau adanya aktivitas *login* dari perangkat lain.

*b. Pemulihan akun<sup>16</sup>*

*1. Pemulihan akun Google/Gmail*

- Jika Anda masih bisa login ke akun Google, Segera ganti sandi (*password*) dengan sandi yang lebih kuat, pasang 2FA (dengan aplikasi *authenticator* atau *passkey* fisik).
- Jika Anda tidak bisa login ke akun Google, lakukan langkah pemulihan akun seperti pada poin 3 bagian ini.
- Lakukan langkah yang sama pada akun-akun Google lainnya.

*2. Jika akun Google bisa diamankan, semestinya akun Youtube bisa kembali dikuasai.*

*3. Detail langkah pemulihan akun bisa dilihat pada laman [Recover a hacked YouTube channel](https://support.google.com/youtube/answer/76187?hl=en).*

*c. Cari bantuan jika langkah pemulihan gagal*

- Tenangkan pikiran, susun kronologi peretasan.
- Dokumentasikan semua tanda peretasan (notifikasi, pemberitahuan pada *e-mail*, dan langkah-langkah pemulihan), misalnya dengan *screenshot* (tangkapan layar).

---

<sup>16</sup> Google, "Recover a hacked YouTube channel", <https://support.google.com/youtube/answer/76187?hl=en>

- Hubungi kontak darurat untuk bantuan penanganan (*daftar kontak bantuan penanganan ada di bagian akhir panduan ini*).
- d. *Kembalikan channel Youtube ke keadaan sebelum peretasan<sup>17</sup>.*
- Jika peretas sempat mengambil alih channel Youtube, biasanya mereka membuat beberapa perubahan pada channel tersebut dan akun Google yang terhubung.
- a. *Dokumentasikan semua jejak yang ditinggalkan peretas pada channel Youtube tersebut, termasuk pada akun e-mail yang terhubung. Salah satu caranya adalah dengan menyimpannya pada situs pengarsipan seperti <https://perma.cc/> atau <https://archive.is/>.*
  - a. *Hapus semua pengguna yang terhubung dengan channel Youtube tersebut.*
    - Jika menggunakan “channel permissions”, masuklah (sign in) ke YouTube Studio. Klik “Setting”, “Permissions”. Pilih username yang hendak dihapus. Klik “Remove access”.
    - Jika menggunakan “brand account”, masuklah ke bagian “Brand Accounts” pada pengaturan Google Account. Ikuti prosedur penghapusan yang serupa dengan yang di atas.
- e. *Mengembalikan channel ke pengaturan awal. Jika peretas mengubah nama channel, gambar profil, dan banner, lakukan perubahan ke status awal untuk menghindari penghapusan akun secara permanen.*
- f. *Hapus video-video yang diunggah oleh peretas secara permanen.*
- g. *Detail petunjuk upaya pemulihan akun hingga pengembalian pengaturan channel bisa dibaca pada laman [Clean up a hacked YouTube channel](#).*

---

<sup>17</sup> Google, “Clean up a hacked YouTube channel”, <https://support.google.com/youtube/answer/14849770#zippy=%2Cdelete-hacker-uploaded-videos-without-violations%2Crestore-your-channels-basic-info-and-branding%2Cremove-any-unknown-users-from-your-channel-or-account>

## B. SERANGAN PENDENGUNG (BUZZER)

Ada berbagai bentuk serangan yang dilakukan *buzzer*, seperti *trolling* (menciptakan kekacauan melalui komentar, argumen, atau informasi palsu untuk memancing reaksi negatif), *doxing* (pengungkapan identitas pribadi seseorang yang menjadi target), *impersonating* (peniruan/pemalsuan akun), hingga kekerasan berbasis gender *online* (KBGO).

Berikut beberapa langkah merespons serangan yang diadopsi dari Bab 6 *Panduan Keamanan Digital untuk Jurnalis 2022*<sup>18</sup>.

### a. Doxing

- Jika terjadi alamat rumah awak media diungkap, perusahaan media perlu mencari rumah aman sementara bagi korban dan keluarga hingga serangan mereda.
- Laporkan postingan yang mengandung *doxing* ke platform dan blokir akun pelaku.
- Jika pelaku mengungkap nomor telepon dan korban menerima banyak gangguan, telepon perlu dimatikan sementara waktu dan pertimbangkan mengganti nomor telepon di kemudian hari.
- Jika pelaku mengekspos nomor rekening bank, kartu kredit, atau informasi akun keuangan korban lainnya, segera hubungi semua lembaga keuangan yang terlibat dan laporkan pelanggarannya.
- Menutup sementara akun media sosial menjadi pilihan terbaik jika serangan meningkat.
- Laporkan ke polisi atas *doxing* dengan membawa hasil dokumentasi dan tautan.
- Arsipkan melalui <https://perma.cc/> atau <https://archive.is/>.

### b. Impersonating

- Buat pengumuman tentang pemalsuan akun agar publik (audiens dan *followers*) tidak tertipu.

<sup>18</sup> [https://aji.or.id/system/files/2024-07/layoutpanduankeamanandigitaluntukjurnalisfixcompressed\\_4.pdf](https://aji.or.id/system/files/2024-07/layoutpanduankeamanandigitaluntukjurnalisfixcompressed_4.pdf)

- Laporkan akun yang menggunakan identitas media atau awak media Anda ke penyedia platform agar akun palsu tersebut ditutup.
  1. Pelaporan akun palsu di Facebook: <https://s.id/akunpalsuFB>
  2. Pelaporan akun palsu di Twitter atau X : <https://help.x.com/en/forms/authenticity/impersonation>
  3. Pelaporan akun palsu di Instagram: <https://s.id/akunpalsuIG>
  4. Pelaporan akun palsu Gmail: <https://s.id/akunpalsuGmail>

### c. Pelecehan Online dan KGBO

- Laporkan/blokir akun, postingan atau komentar yang mengandung pelecehan termasuk KBGO ke platform.
- Minta dukungan dari organisasi masyarakat sipil yang fokus pada isu kebebasan berpendapat (misalnya Aliansi Jurnalis Independen/AJI kota terdekat atau Safenet).
- Minta dukungan dari lembaga penyedia layanan pendamping pelecehan/kekerasan seksual (misalnya LBH Apik atau lembaga perlindungan hak perempuan), dapatkan pendampingan hukum dan psikososial dari lembaga tersebut.
- Laporkan ke polisi atas kekerasan dan pelecehan yang diterima korban, baik melalui telepon, SMS, *chat*, atau di media sosial lainnya dengan menyertakan dokumentasi kekerasan/ pelecehan yang dialami.

## C. MENJADI TARGET PENANGKAPAN

- Jika Anda sedang berada dalam situasi rentan/berisiko menjadi target penangkapan/penahanan (misalnya karena konten Anda), pertimbangkan keluar (*log out*) dari akun-akun terkait dan akun yang menyimpan data/informasi sensitif.
- Hapus *history* pada *browser* (peramban) Anda. Pastikan semua data/informasi sensitif tersebut tersimpan aman pada *hard drive* yang terenkripsi (terkunci).
- Hubungi lembaga bantuan hukum (LBH), Lembaga Perlindungan Saksi dan Korban (LPSK), atau organisasi masyarakat sipil terdekat yang bisa memberikan bantuan dan perlindungan termasuk rumah aman (*safe house*).

## V. KONTAK DARURAT

### A. KONTAK BANTUAN PENANGANAN

Dalam situasi terjadi serangan atau saat media membutuhkan langkah-langkah mitigasi, berikut ini lembaga-lembaga yang bisa dikontak untuk memberikan bantuan.

**1. Aliansi Jurnalis Independen (AJI)**

Link pengaduan: <https://safetycorner.aji.or.id/node/6511>

**2. Tim Reaksi Cepat (TRACE)**

Link pengaduan: <https://lapor.trace.mu/>

**3. SAFEnet**

Link pengaduan: <https://aduan.safenet.or.id/>

**4. Access Now**

Link pengaduan: <https://www.accessnow.org/help/#contact-us>

## B. KONTAK BANTUAN HUKUM

### Wilayah Jabodetabek

| LEMBAGA                     | ALAMAT   | TELEPON/FAKSIMILI   | EMAIL                             |
|-----------------------------|--|---|-----------------------------------|
| <b>LBH Pers</b>             | Jl. Kalibata Timur IV G<br>No. 10 Kalibata,<br>Pancoran, Jakarta Selatan                   | Telp. 021-79183485,<br>0821-4688-8873                       | secretariat@lbhpers.org           |
| <b>YLBHI</b>                | Jl. Diponegoro No. 74,<br>Menteng, Jakarta Pusat 10320                                     | Telp. 021-3929840<br>Faks. 021 31930140                     | info@ylbhi.or.id                  |
| <b>LBH Jakarta</b>          | Jl. Pangeran Diponegoro No.74<br>, Menteng, Jakarta 10320                                  | Telp. 021-3145518<br>Faks. 021-3912377                      | lbhjakarta@bantuanhukum.<br>or.id |
| <b>PBHI</b>                 | Jl. Hayam Wuruk No.4, RT.9/<br>RW.5, Kb. Klp., Kec. Taman<br>Sari, Jakarta 10120           | Telp. 021-3859968   |                                   |
| <b>LBH Apik<br/>Jakarta</b> | Jl. Raya Tengah No. 31 RT 01<br>RW 09 Kampung<br>Tengah Kramat Jati Jakarta<br>Timur 13540 | Telp. 021-87797289,<br>0813-888226699<br>Faks. 021-87793300 | LBHAPIK@gmail.com                 |

### Wilayah Jawa Barat dan Banten

| LEMBAGA                    | ALAMAT   | TELEPON/FAKSIMILI                      | EMAIL                           |
|----------------------------|--|--|---------------------------------|
| <b>LBH<br/>Bandung</b>     | Jl Kalijati Indah Barat No 8,<br>Antapani Bandung                                  | Telp. 0821-2017-1321                   | konsultasi@lbhbandung.<br>or.id |
| <b>LBH Apik<br/>Jabar</b>  | Jalan Beringin No. 9 Kemiri<br>Muka, Beji, Kota Depok, Jawa<br>Barat               | Telp. 0813-8030-4852                   | lbhapikjawab arat@gmail.<br>com |
| <b>LBH Apik<br/>Banten</b> | Jln. Raya Pandeglang Km. 3,<br>Komp. Tembong Indah, Sempu,<br>Kota Serang – Banten | Telp. 0254-227969<br>Faks. 0254-227969 |                                 |

### Wilayah Jawa Tengah dan DIY

| LEMBAGA                      | ALAMAT  | TELEPON/FAKSIMILI                     | EMAIL                               |
|------------------------------|---|---------------------------------------|-------------------------------------|
| <b>LBH<br/>Semarang</b>      | Jl. Jomblangsari 4 No. 17,<br>Jomblang, Candisari, Kota<br>Semarang                                 | Telp. 024-86453054,<br>0882-2890-2001 | office.lbhsem arang@ylbhi.<br>or.id |
| <b>LBH Apik<br/>Semarang</b> | Jalan Poncowolo Timur Raya<br>No. 455 Semarang, Jawa<br>Tengah (masuk melalui jalan<br>Indraprasta) | Telp. 024-3510499                     | apiksemaran g@yahoo.com             |

| LEMBAGA                    | ALAMAT   | TELEPON/FAKSIMILI              | EMAIL                       |
|----------------------------|--|--------------------------------|-----------------------------|
| <b>LBH Yogyakarta</b>      | Jl. Benowo No.309, Winong, RT 12/RW 03, Prenggan, Kec. Kotagede, Kota Yogyakarta, Daerah Istimewa Yogyakarta 55172 | Telp. 0274-4351490             | kalabahulbhjo_gja@gmail.com |
| <b>LBH Apik Yogyakarta</b> | Jalan Nogodewo 12, Gowok, Sleman, Yogyakarta   | Telp. 0274-379614, 08179410624 | apik_jogja@yahoo.com        |

### Wilayah Jawa Timur

| LEMBAGA                        | ALAMAT   | TELEPON/FAKSIMILI   | EMAIL                      |
|--------------------------------|--|---------------------|----------------------------|
| <b>LBH Surabaya</b>            | Jl. Kidal No.6, Pacar Keling, Kec. Tambaksari, Kota SBY, Jawa Timur60131           | Telp. 031-5022273   | bantuanhuku_msby@gmail.com |
| <b>LBH Surabaya Pos Malang</b> | Jl. Teluk Perigi Rt 01, Rw 10 Tirtomoyo, Kec. Pakis, Kab. Malang, Jawa Timur 65154 | Telp. 081252226205  | lbhmalang@ylbhi.or.id      |
| <b>LBH APIK-Kota Batu</b>      | Jalan Kapten Ibnu, Ruko 8 RT03/RW13, Kel Sisir, Batu, Kota Batu, Jawa Timur        | Telp. 6281336554420 | lbhapikkotabatu@gmail.com  |

### Wilayah Bali dan Nusra

| LEMBAGA              | ALAMAT   | TELEPON/FAKSIMILI                    | EMAIL                  |
|----------------------|--|--------------------------------------|------------------------|
| <b>LBH Bali</b>      | Jalan Plawa No. 57, Denpasar Timur, Denpasar, Bali   | Telp. 0361-223010                    | lbhbali@indo.net.id    |
| <b>LBH APIK Bali</b> | Jalan Suli 119 – A3, Denpasar Timur  | Telp. 0361-9272245, 081337325896     | lbh.tentrem@gmail.com  |
| <b>LBH APIK NTT</b>  | Jalan Sam Ratulangi II no.33B Walikota Baru, Kel. Oesapa Barat, Kec. Kelapa Lima, Kota Baru, Kupang 85228. | Telp. 0380 823647                    | lbhapik.ntt@gmail.com  |
| <b>LBH APIK NTB</b>  | Jalan Angklung Raya no. 2 Karang Bedil, Mataram, Lombok, NTB   | Telp. 0817-5768-4 96, 0823-3959-3221 | lbhapikntb17@gmail.com |

### Wilayah Aceh dan Sumatera Utara

| LEMBAGA               | ALAMAT   | TELEPON/FAKSIMILI  | EMAIL                  |
|-----------------------|--|--------------------|------------------------|
| <b>LBH Banda Aceh</b> | Jalan Sakti Lorong LBH Banda Aceh No.1, Desa Pango Raya, Ulee Kareng, Banda Aceh 23119 | Telp. 0651-8057952 | lbh_aceh1995@yahoo.com |

| LEMBAGA               | ALAMAT   | TELEPON/FAKSIMILI                       | EMAIL                                       |
|-----------------------|--|---|---|
| <b>LBH APIK Aceh</b>  | Jalan Tengku Daud No. 147, Panggoi, Muara Dua, Kota Lhoksmeumawe, Aceh 24355 | Telp. 0645-43150                        | lbhapikaceh@gmail.com                       |
| <b>LBH Medan</b>      | Jalan Hindu No.12 Medan 20111, Sumatera Utara, Indonesia                     | Telp. 061-4515340<br>Faks. 061-4569749  | lbh_medan@yahoo.com,<br>kantor@lbhmedan.org |
| <b>LBH APIK Medan</b> | Jalan Jermal V No. 1C, Denai, Medan Denai                                    | Telp. 0821-5753-9308,<br>0282-115063359 | admlbhapikean@gmail.com                     |

### Wilayah Sumatera Barat dan Riau

| LEMBAGA              | ALAMAT  | TELEPON/FAKSIMILI              | EMAIL                   |
|----------------------|---|--------------------------------|-------------------------|
| <b>LBH Padang</b>    | Jalan Pekanbaru No 11A, Kota Padang, Sumatra Barat                                    | Telp. 0751-7056059             |                         |
| <b>LBH Pekanbaru</b> | Jl. Sapta Taruna No.51, Tengkerang Utara, Kec. Bukit Raya, Kota Pekanbaru, Riau 28289 | Telp. 0761-45832, 0811-765-832 | info@lbhpekanbaru.or.id |

### Wilayah Sumatera Selatan dan Lampung

| LEMBAGA                          | ALAMAT  | TELEPON/FAKSIMILI                     | EMAIL                         |
|----------------------------------|---|---------------------------------------|-------------------------------|
| <b>LBH Palembang</b>             | Jl. HBR Motik No.12A Rt.29 Rw.9 Kel.Karya Baru Kec. Alang-alang Lebar Kota Palembang                | Telp. 0711-5610122,<br>0813-6930-0442 | lbhpalembang@ylbhi.or.id      |
| <b>LBH APIK Sumatera Selatan</b> | Jalan Sekip Bendung Dalam No. 009 RT. 035 RW. 009, Kel. 8 Ilir, Kec. Ilir Timur III, Kota Palembang | Telp. 0821-7770-0069                  | yayasanlbhapiksusel@gmail.com |
| <b>LBH Bandar Lampung</b>        | Jalan Sam Ratulangi, Gg Mawar 1, Nomor 7, Gedong Air, Bandar Lampung 351117                         | Telp. 0721-5600425                    | bantuanhukumlampung@gmail.com |

### Wilayah Kalimantan

| LEMBAGA                     | ALAMAT   | TELEPON/FAKSIMILI       | EMAIL                 |
|-----------------------------|--|-------------------------|-----------------------|
| <b>LBH Kalimantan Barat</b> | Jl. Dr. Sutomo, Komplek Batara Indah 4 No. 16 D, Pontianak, Kalimantan Barat | Telp. +62 812-5880-6816 | lbhkalbar@ylbhi.or.id |
| <b>LBH APIK Pontianak</b>   | Jalan Aliyang No. 12A Pontianak, Kalimantan Barat 78116                      | Telp. 0561-766439       | apik_ptk@yahoo.com    |

| LEMBAGA                          | ALAMAT  | TELEPON/FAKSIMILI                                 | EMAIL  |
|----------------------------------|---|---|--|
| <b>LBH Samarinda</b>             | Jl Wijaya Kusuma II No 50, Air Putih, Samarinda Ulu Samarinda                           | Telp. 0821-5133-15537                             | lbhsamarinda @ylbhi.or.id, lbhsamarind@gmail.com |
| <b>LBH APIK Kalimantan Timur</b> | Jalan Sultan Sulaiman, Perum Citra Gading Blok B2 No. 9 Samarinda – Kalimantan Timur    | Telp. 0541-4106482, 0812-5822-7 15, 0812-5826-828 | ylbhapiikkaltim@gmail.com                        |
| <b>LBH Palangka Raya</b>         | Jl. Parawei, Perum Casadova blok B, No. 10, Kota Palangka Raya, Prov. Kalimantan Tengah | Telp. 0857-8696-8317                              | ylbhi.lbh.palangan karaya@gmail.com              |

### Wilayah Sulawesi dan Papua

| LEMBAGA           | ALAMAT   | TELEPON/FAKSIMILI                              | EMAIL                       |
|-------------------|--|--|-----------------------------|
| LBH Manado        | Jl.A Manonutu No. 29, Wanea, Kota Manado 95116   | Telp. 0431-8806473; 085256303949; 085240523068 | ylbhi.lbhmanado@gmail.com   |
| LBH APIK Manado   | Jalan Bethesda 6 No. 77, Ranotana ling II, Manado - 95116                                  | Telp. 0431-824132                              |                             |
| LBH Makassar      | Jl. Nikel 1 Blok A22 No.18 Kota Makassar, Kode Pos 90222                                   | Telp. 0411-4677699                             | lbhmks.ylbhi@gmail.com      |
| LBH APIK Makassar | Jalan Perintis Kemerdekaan, Perum Budidaya Permai Blok D no. 3, Makassar, Sulawesi Selatan |  | lbhapiksulsel.or.id         |
| LBH APIK Palu     | Jalan Teluk Tomini No. 8B, Kota Palu - 94221   | Telp. 0451-4015986, 0811-4540-1616             | lbhapik_sulsel@yahoo.com    |
| LBH Papua         | Jl. Gerilyawan No. 46 Jayapura, Papua 99532  | Telp. 0967-581710; 08124808635                 | lbh.papua@yahoo.co.id       |
| LBH APIK Jayapura | Jalan Raya Sentani, Padang Bulan, Abepura, Jayapura, Papua 99351                           | Telp. 0411-590147, 0812-9400-7696              | lbhapikjayapura17@gmail.com |

## C. KONTAK PENANGANAN PSIKOSOSIAL

### 1. Yayasan Pulih

Alamat : Jl. Teluk Peleng 63 A Komplek AL-Rawa Bambu Pasar Minggu, Jakarta 12520

Telepon : 021-788 42 580, 021- 982 86 39

E-mail : [pulihfoundation@gmail.com](mailto:pulihfoundation@gmail.com); [pulihcounseling@gmail.com](mailto:pulihcounseling@gmail.com)

### 2. Jaringan LBH Apik di berbagai kota

