
ICT watch!
ictwatch.id
YLBHI
Yayasan Lembaga Bantuan Hukum Indonesia
Luminate
DIGITAL AMAN,
AMAN BERGERAK
s.id/amanbergerak

DAFTAR ISI

Editor:
Donny B.U.

Penulis (urut abjad):
Bahruddin
Indriyatno Banyumurti
Lovandri Dwanda Putra
Selamet

BAB I

KEAMANAN DIGITAL PERSONAL

A. Prinsip Keamanan Digital

Seiring perkembangan teknologi, beragam masalah dalam kehidupan sehari-hari, idealnya menjadi semakin dimudahkan. Namun demikian, perkembangan teknologi digital juga memiliki risiko yang dapat menganggu kehidupan penggunanya. Seperti pisau yang bisa membantu proses memotong atau melukai orang lain. Kondisi serupa berlaku untuk kita yang memilih memanfaatkan teknologi digital seperti terkoneksi dengan internet, dengan beragam layanan yang tersedia di jaringan maya. Agar kita dapat meminimalisir risiko, ada baiknya memahami prinsip-prinsip dasar keamanan digital antara lain:

1. Tidak ada jaminan 100% aman

Saat Anda memilih berkegiatan di dunia maya, kita perlu menyadari prinsip sepenuhnya aman itu sebuah utopia. Tidak ada yang namanya 100 persen aman di dunia digital. Ilustrasi sederhana, saat menggunakan layanan Peduli Lindungi semasa pandemi, baik secara sadar atau tidak, Anda menyerahkan data-data pribadi kepada penyedia layanan. Namun jika diperhatikan dan dibaca benar ketentuan dari aplikasi tersebut, ada satu klausul yang menyatakan, penyedia layanan tidak bertanggungjawab jika terjadi kebocoran data. Saat Anda menyatakan setuju, biasanya orang tidak mau membaca ketentuan secara detil karena membutuhkan aplikasi itu untuk bepergian, maka Anda sudah menyetujui jika penyedia layanan tidak dapat dikenai tuntutan hukum saat terjadi kebocoran data. Semua karena Anda sepakat dengan satu klausul di atas tadi.

2. Makin nyaman, makin tidak aman

Prinsip lainnya adalah, untuk bisa aman, Anda harus merelakan ketidaknyamanan dalam mengakses telepon seluler, laptop, hingga beragam aplikasi atau layanan di internet. Coba refleksikan kebiasaan Anda mengakses telepon seluler. Apakah kuncinya bisa dibuka dengan hanya menempelkan satu dari 10 jari? Bagaimana saat Anda tertidur dan ada teman yang iseng mencoba menempelkan satu persatu jari Anda ke telepon seluler Anda. Perlahan namun pasti, rekan Anda bisa mengakses telepon itu tanpa Anda ketahui. Ilustrasi lainnya, penggunaan jaringan WIFI di tempat umum. Karena kita tidak mau bersusah payah mengeluarkan dana untuk paket data, maka kita memanfaatkan jaringan WIFI yang tidak kita ketahui tingkat keamanannya. Bisa saja, jaringan WIFI itu dibuat oleh peretas yang punya niat jahat mengambil data dari setiap orang yang mengaksesnya. Bukan perkara sulit membuat jaringan WIFI terdeteksi serupa dengan nama jaringan di tempat umum tersebut.

Sebagai realisasi dari dua prinsip tersebut di atas, Anda juga harus mengetahui dan memahami keamanan digital pada perangkat digital Anda diantaranya adalah:

a. Otentikasi Multifaktor

Otentikasi Multifaktor atau sering dikenal dengan *two-factor authentication* (2FA) adalah metode otentikasi elektronik di mana pengguna diberi akses ke situs web atau aplikasi. Jika suatu akun dilindungi dengan otentikasi multifaktor, penggunanya harus memberikan dua atau lebih bukti bahwa ia memang pemilik akun tersebut. Hanya dengan cara itulah seorang pengguna bisa mendapat akses masuk ke dalam sebuah akun.

beri akses ke situs web atau aplikasi. Jika suatu akun dilindungi dengan otentikasi multifaktor, penggunanya harus memberikan dua atau lebih bukti bahwa ia memang pemilik akun tersebut. Hanya dengan cara itulah seorang pengguna bisa mendapat akses masuk ke dalam sebuah akun.

Dengan perlindungan ekstra ini, kita bisa lebih tenang dan yakin bahwa akun kita tidak mudah dimasuki oleh orang lain dengan mudah. Saat ini, paling tidak *two-factor authentication* dibutuhkan untuk keamanan minimal.

b. Social Engineering

Social engineering atau rekayasa sosial, adalah sebuah teknik manipulasi yang memanfaatkan kesalahan manusia untuk mendapatkan akses pada informasi pribadi atau data-data berharga.

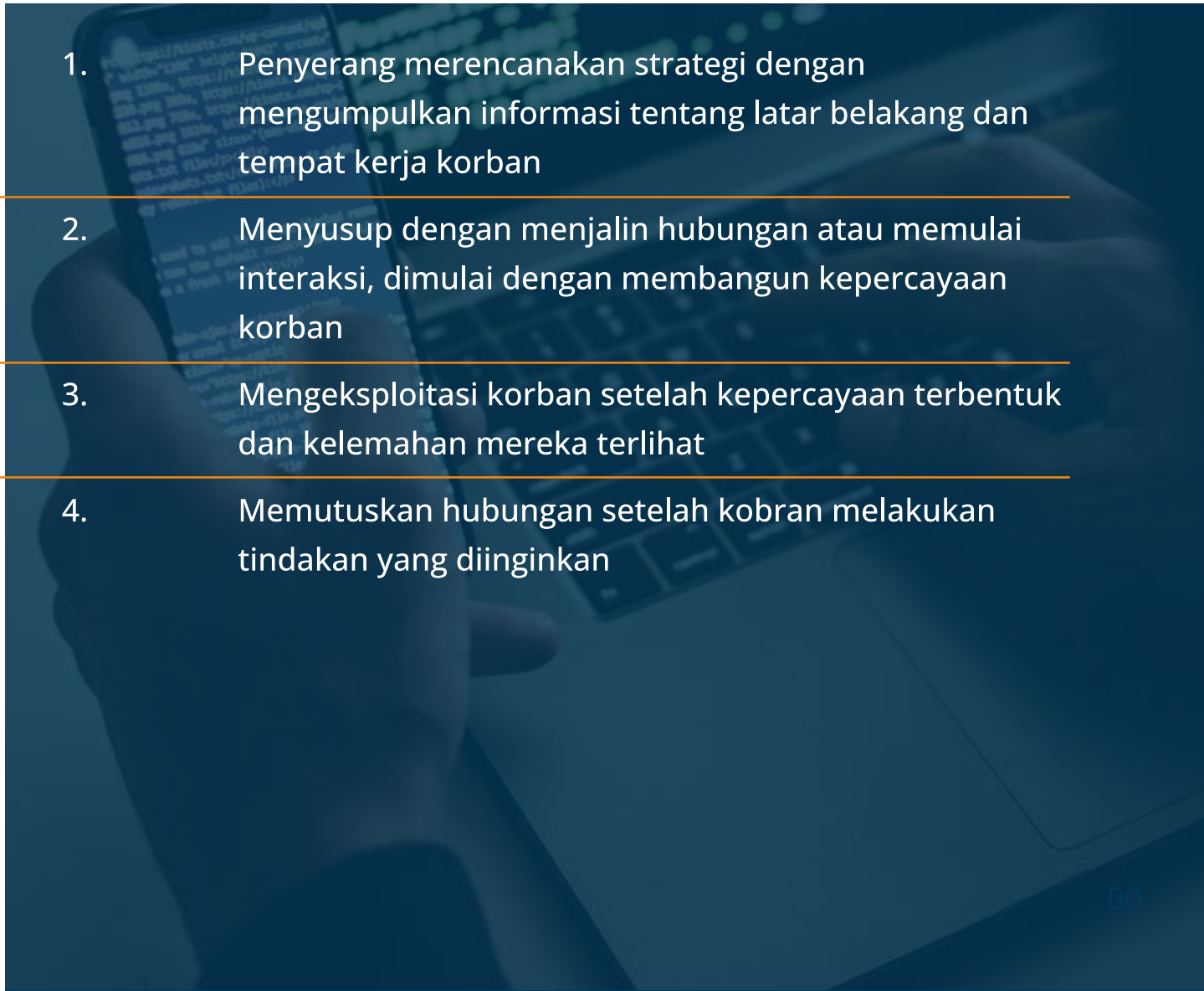
Dalam dunia *cybercrime,* jenis penipuan *human hacking* ini dapat memikat pengguna untuk tidak menaruh curiga. Pengguna dapat dengan mudah mengungkapkan data, menyebarkan infeksi *malware,* dan memberikan akses ke sistem yang terjaga. Serangan seperti ini dapat terjadi secara online, langsung, dan melalui interaksi lainnya yang sulit untuk diduga.

Umumnya, rekayasa sosial memiliki dua tujuan spesifik, yakni untuk menyabotase dan mencuri. Dikarenakan penipuan ini didasarkan pada manipulasi psikologis, strategi serangan akan dibangun berdasarkan cara korban berpikir dan bertindak. Dengan demikian, serangan manipulasi psikologis ini sangat berguna untuk mengelabui dan memengaruhi perilaku korban.

Setelah memahami apa yang memotivasi setiap tindakan korban, penyerang dapat menipu dan memanipulasi korban secara efektif dan tanpa beban. Selain itu, para penyerang juga dapat mengeksploitasi minimnya pengetahuan korban terkait dunia teknologi.

Calon korban juga mungkin tidak menyadari nilai penuh dari data pribadi, seperti nomor telepon dan informasi pada kartu identitas mereka. Akibatnya, korban kehilangan data pribadi karena tidak paham mengenai cara terbaik untuk melindungi diri mereka dari serangan-serangan tersebut.

Cara kerja serangan juga sangat terstruktur dan tidak berantakan. Menurut CSO Online, cara kerja *social engineering* adalah seperti berikut ini:



1. Penyerang merencanakan strategi dengan mengumpulkan informasi tentang latar belakang dan tempat kerja korban
2. Menyusup dengan menjalin hubungan atau memulai interaksi, dimulai dengan membangun kepercayaan korban
3. Mengeksploitasi korban setelah kepercayaan terbentuk dan kelemahan mereka terlihat
4. Memutuskan hubungan setelah kobran melakukan tindakan yang diinginkan

Proses ini dapat berlangsung dalam satu kali interaksi email atau selama berbulan-bulan dalam serangkaian obrolan di media sosial. Namun, pada akhirnya, serangan akan diakhiri setelah korban melakukan tindakan yang diharapkan penyerang. Hal itu seperti membagikan informasi pribadi atau memaparkan *malware* pada sistem *device* mereka.

Serangan *social engineering* juga datang dalam berbagai bentuk, dan dapat dilakukan di mana saja di mana interaksi manusia terlibat.

Menurut Imperva, berikut ini adalah lima bentuk serangan rekayasa sosial yang paling umum ditemukan.

1. Baiting

Baiting merupakan serangan *social engineering* yang paling sering ditemukan. Sesuai namanya, *baiting* menggunakan serangan umpan dalam bentuk janji palsu untuk memancing keserakahan atau keingintahuan korban. Penyerang akan memikat korban ke dalam perangkap, di mana nantinya mereka akan mencuri informasi pribadi atau menyebabkan sistem *device* korban untuk terkena *malware.*

2. Pretexting

Dalam serangan *pretexting,* seorang penyerang memperoleh informasi melalui serangkaian kebohongan yang dibuat dengan cerdik. Penipuan rekayasa sosial ini sering kali diprakarsai oleh pelaku yang berpura-pura membutuhkan informasi sensitif dari korban untuk melakukan tugas penting.

3. Phishing

Phishing merupakan jenis serangan *social engineering* yang paling berbahaya. Sering kali, bentuk penipuan ini hadir dalam kampanye *email* dan pesan teks yang bertujuan untuk menciptakan urgensi, keingintahuan, atau ketakutan pada korban. Kemudian, penyerang akan mendorong korban untuk mengungkapkan informasi sensitif, mengklik tautan ke situs web berbahaya, atau membuka lampiran yang berisi *malware*.

4. Spear phishing

Jenis serangan ini adalah versi penipuan *phishing* yang lebih terstruktur, di mana penyerang akan memilih individu atau perusahaan tertentu. Penyerang kemudian akan menyesuaikan pesan mereka berdasarkan karakteristik, posisi pekerjaan, dan kontak milik korban agar serangan mereka tidak terlalu mencolok. *Spear phishing* membutuhkan lebih banyak upaya, dan mungkin membutuhkan waktu berminggu-minggu hingga berbulan-bulan untuk melakukannya.

Cara mencegah *social engineering* sangat mudah, di mana pengguna *device* harus sadar akan bahaya yang mengancam data mereka. Berikut langkah-langkah jelasnya.

a. **Jangan mengklik tautan yang mencurigakan.**
b. **Periksa kembali sumber situs yang ingin dibuka.**
c. **Hindari percakapan dengan orang asing.**
d. **Hindari *download* dokumen yang tak dikenal.**
e. **Anggap saja bahwa seluruh tawaran hadiah itu palsu.**
f. **Tolak *request email* atau pesan dari orang yang tak dikenal.**
g. **Selalu ingat akan risiko kehilangan informasi penting.**

B. Praktik Keamanan Digital

Internet menjadi semakin kompleks seiring perkembangan teknologi informasi dan digital. Kini sebagai pengguna, tidak hanya memanfaatkan kelebihannya, namun kita juga harus memperhatikan aturan untuk melindungi data-data pribadi kita.

Data pribadi bisa dengan mudah kita serahkan atas persetujuan kita sendiri tanpa meneliti lebih jauh persyaratan yang ditawarkan. Selain itu penggunaan internet yang sembarangan dan tanpa pengamanan tambahan juga bisa tanpa sengaja membuat piranti kita diakses oleh pihak luar seperti penyadapan dan maupun kejahatan digital lainnya.

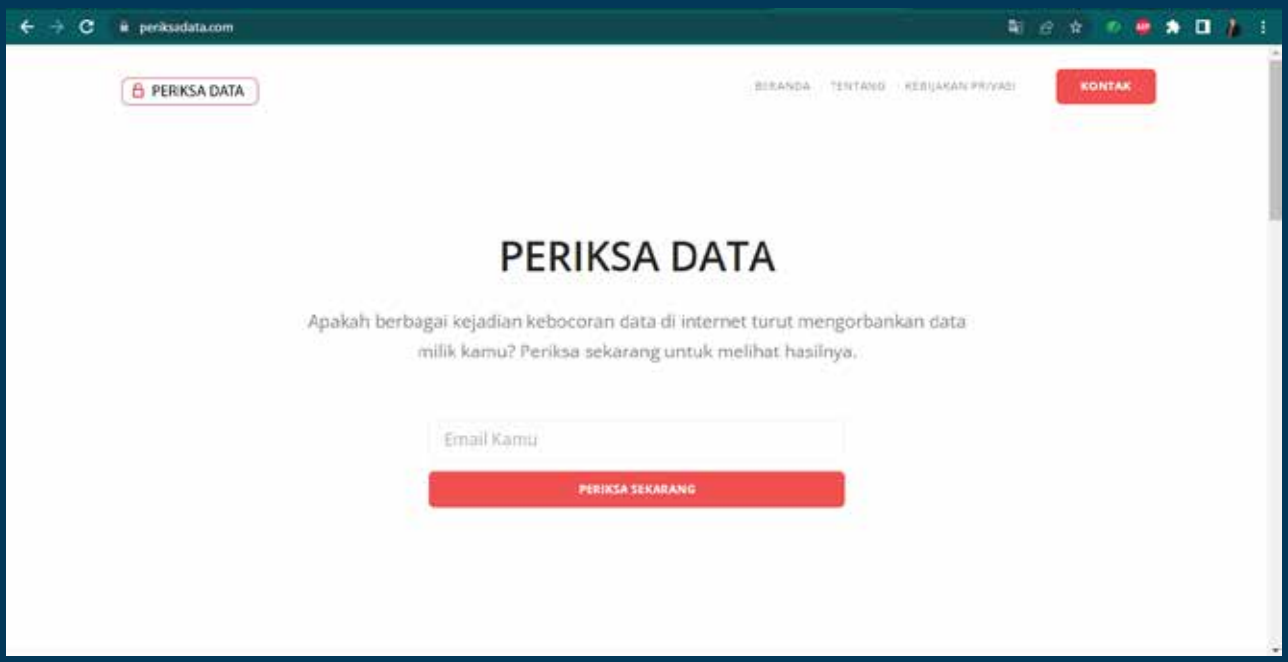
Ada aturan keamanan digital dasar yang mungkin sudah diterapkan banyak orang namun ada pula yang belum memperhatikan betapa pentingnya untuk mengetahui beberapa poin tertentu. Berikut aturan keamanan digital dasar untuk pengguna internet yang wajib diketahui:

1. Cek Risiko Kredensial e-Mail

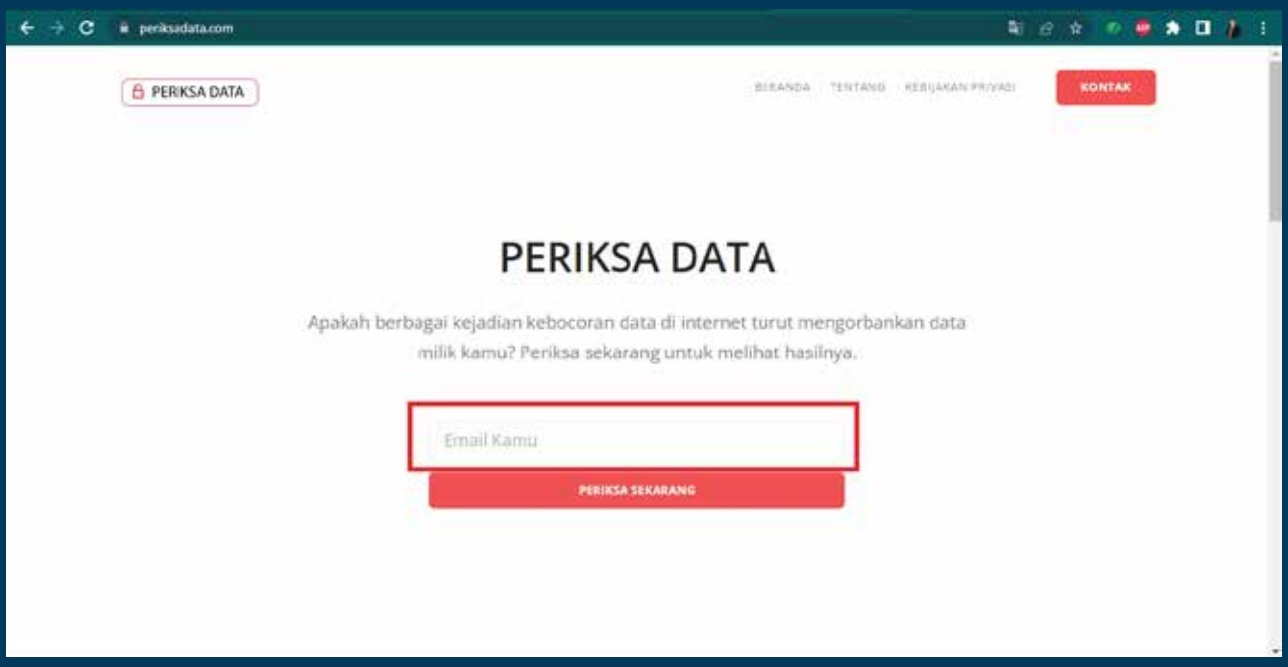
Di dunia yang semakin serba digital, ternyata tak hanya bisnis yang menjadi digital, tindak kriminal pun mengalami perubahan ke arah digital. Dalam beberapa tahun terakhir, makin sering rasanya kita mendengar kejahatan dengan modus pembajakan akun. Seluruh layanan berbasis akun tersebut memiliki persamaan, yaitu menggunakan kredensial untuk mengautentikasi identitas pemilik akun.

Berikut salah satu situs yang dapat membantu mengidentifikasi apakah email kita masuk dalam data email yang bocor di internet. Berikut cara memeriksa keamanan email:

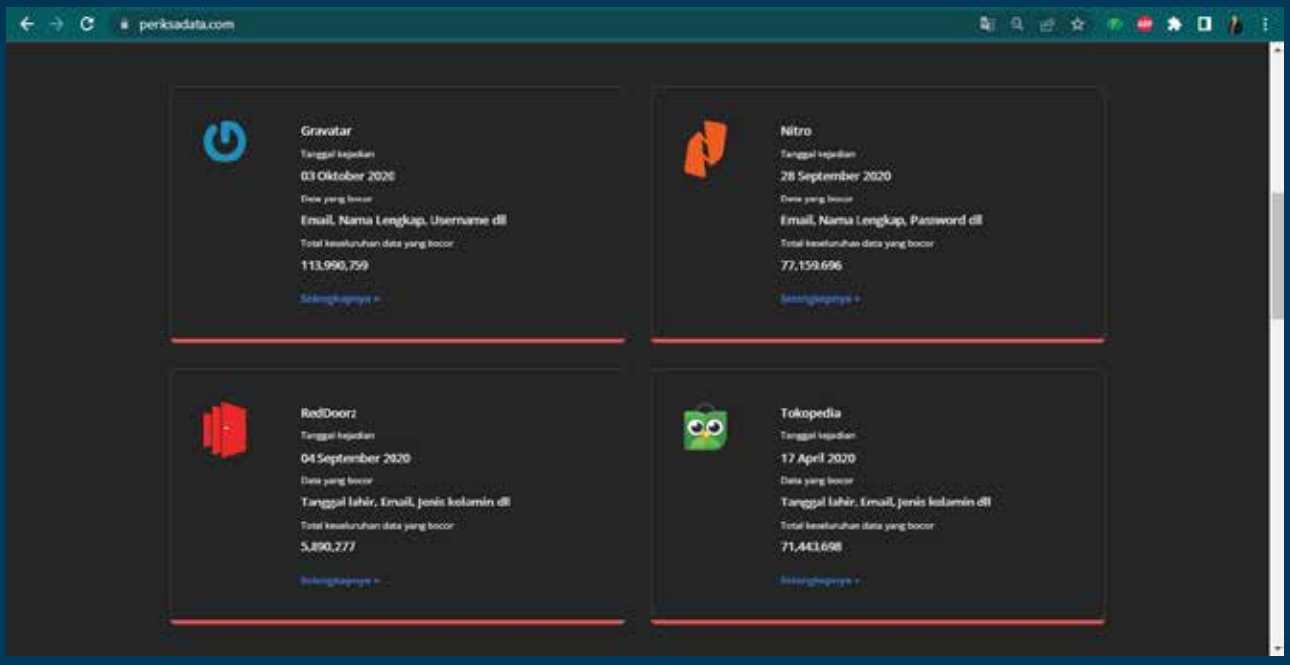
a. Buka link https://periksadata.com/
b. Akan muncul jendela periksadata.com



c. Pada bagian kotak merah isi dengan email yang ingin diperiksa, kemudian klik periksa sekarang



d. Periksa data (Ilustrasi)



Contoh Kebocoran Data (ilustrasi)

Tips jika data kamu bocor:

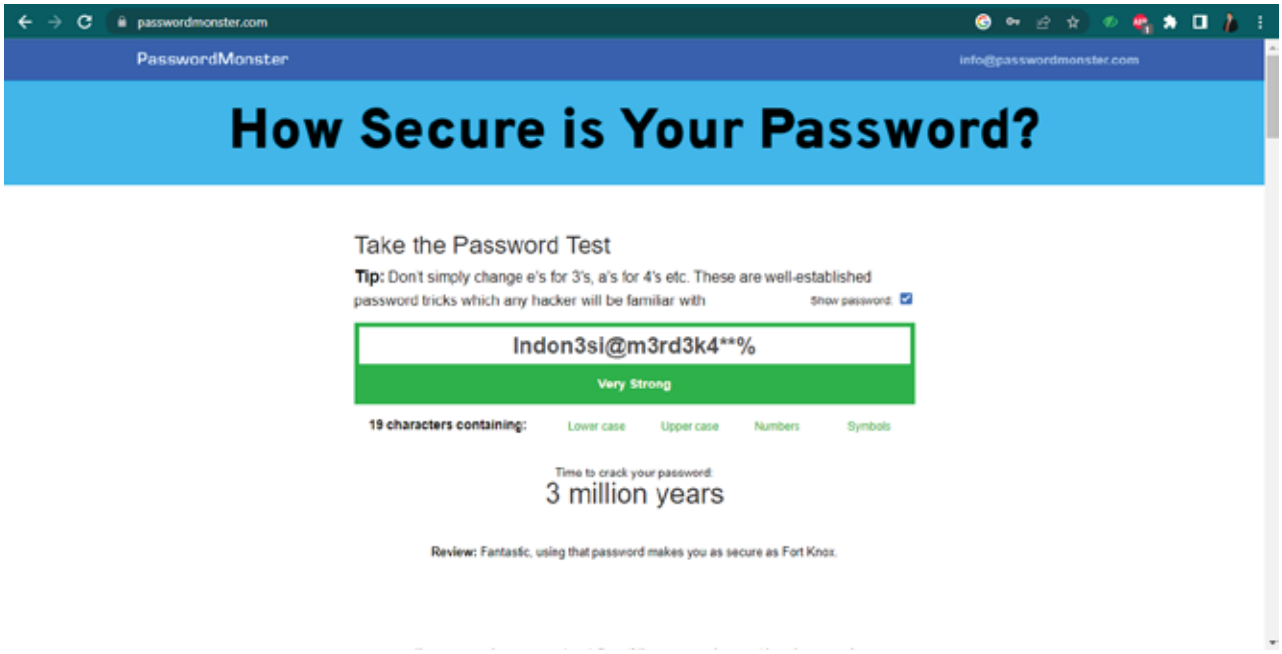
1. Segera ganti *password* yang kamu gunakan. Agar lebih aman, gunakan kombinasi huruf, angka dan *symbol* di *password* yang kamu gunakan.
2. Aktifkan verifikasi 2 langkah sekarang agar akun milik kamu menjadi lebih aman. disarankan untuk menggunakan *Authenticator App* dari pada sms.
3. Jika kamu merasa kesulitan untuk mengingat banyak *password,* kamu bisa menggunakan *password manager* untuk menyimpan banyak *password.*

2. Memperkuat Password

Pada asumsi ini, Anda mungkin bertanya-tanya mengapa saya membutuhkan *password* yang kuat ? Faktanya adalah meskipun mayoritas *website* sudah aman, namun selalu ada kemungkinan orang lain berniat jahat mencoba untuk mengakses atau mencuri informasi-informasi Anda. Tindakan seperti ini umumnya dikenal sebagai *hacking* (meretas). Kata sandi yang kuat adalah salah satu cara untuk mempertahankan akun dan informasi pribadi Anda dari *hacker.*

Berikut tips membuat password yang kuat:

a. Buka https://www.passwordmonster.com
b. Coba untuk membuat *password* minimal 15 karakter
c. Gunakan kombinasi angka, simbol, huruf kapital dan huruf kecil
d. Pada bagian kolom bertuliskan *Type a password,* tuliskan *password* kamu. Contoh ilustrasi *password* Indon3si@m3rd3k4**%



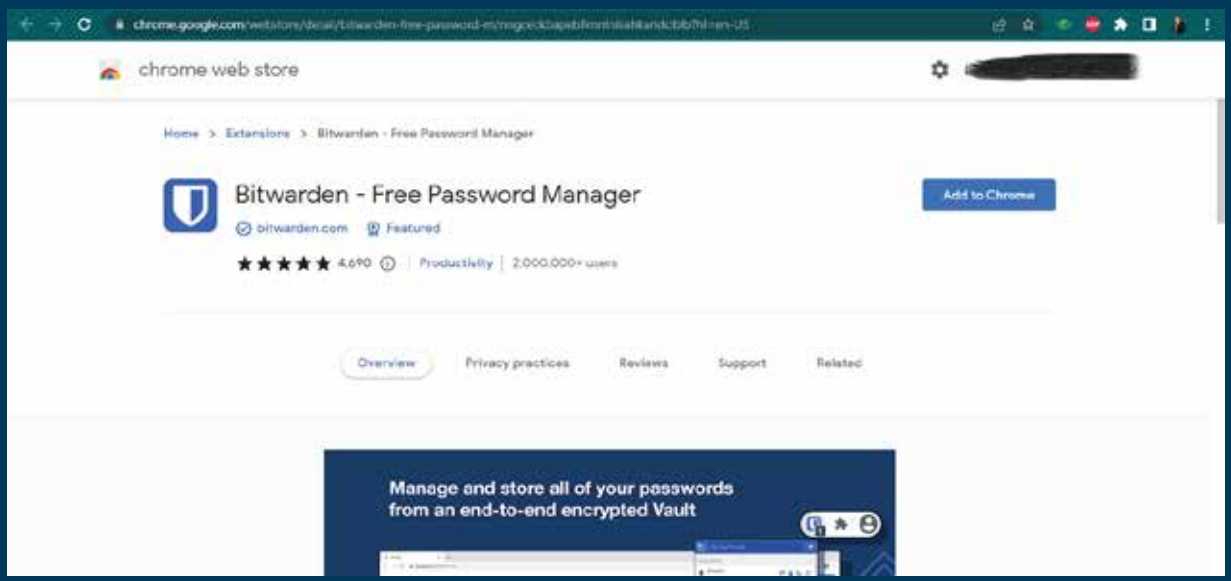
PasswordMonster (ilustrasi)

3. Optimasi Password Manager

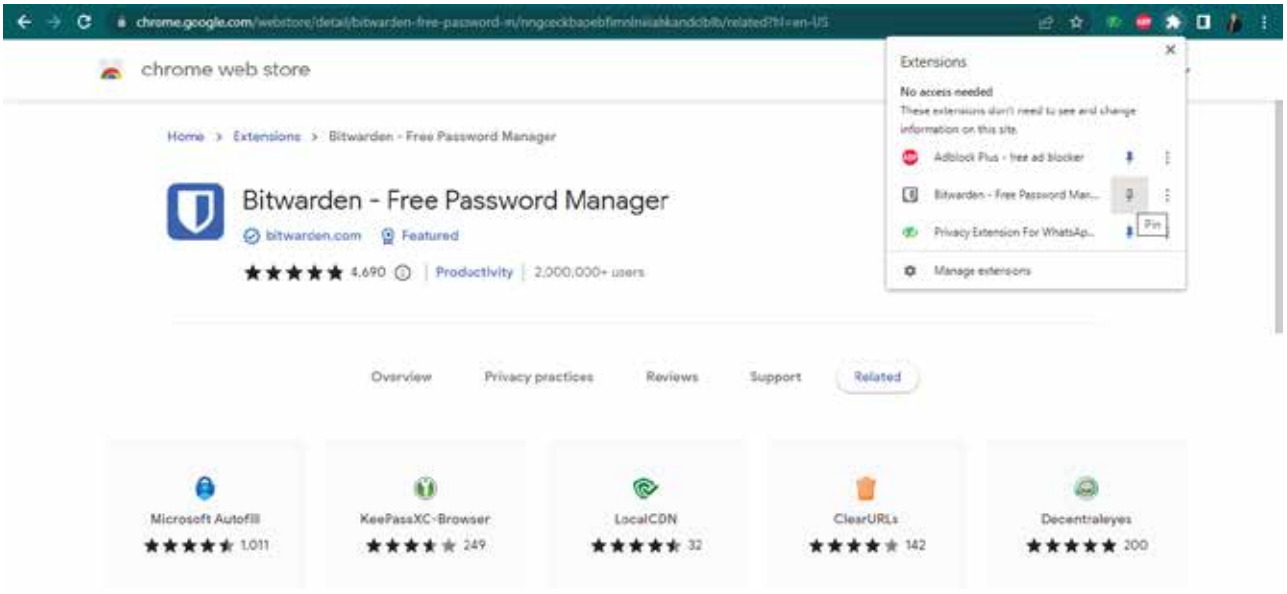
Di era serba digital, masyarakat dituntut memiliki akun untuk setiap layanan yang berbeda. Idealnya, setiap akun digital yang kita memiliki harus disertai kata sandi yang kuat dan berbeda-beda, terutama untuk akun-akun penting seperti email, perbankan, e-commerce, dan media sosial. Kebiasaan menggunakan satu kata sandi untuk semua akun digital dapat berbahaya. Apabila kata sandi itu bocor, maka semua akses akun digital bisa dikuasai. Namun, mengingat semua kombinasi kata sandi barisi huruf, simbol, dan angka untuk belasan bahkan puluhan akun digital tentu bukan pekerjaan mudah.

Berikut kami bagikan tips salah satu aplikasi password manager yaitu Bitwarden. Bitwarden memiliki fitur yang cukup lengkap dan gratis. Langsung saja, ini dia cara menggunakan Password Manager Bitwarden

a. Download Bitwarden di Browser



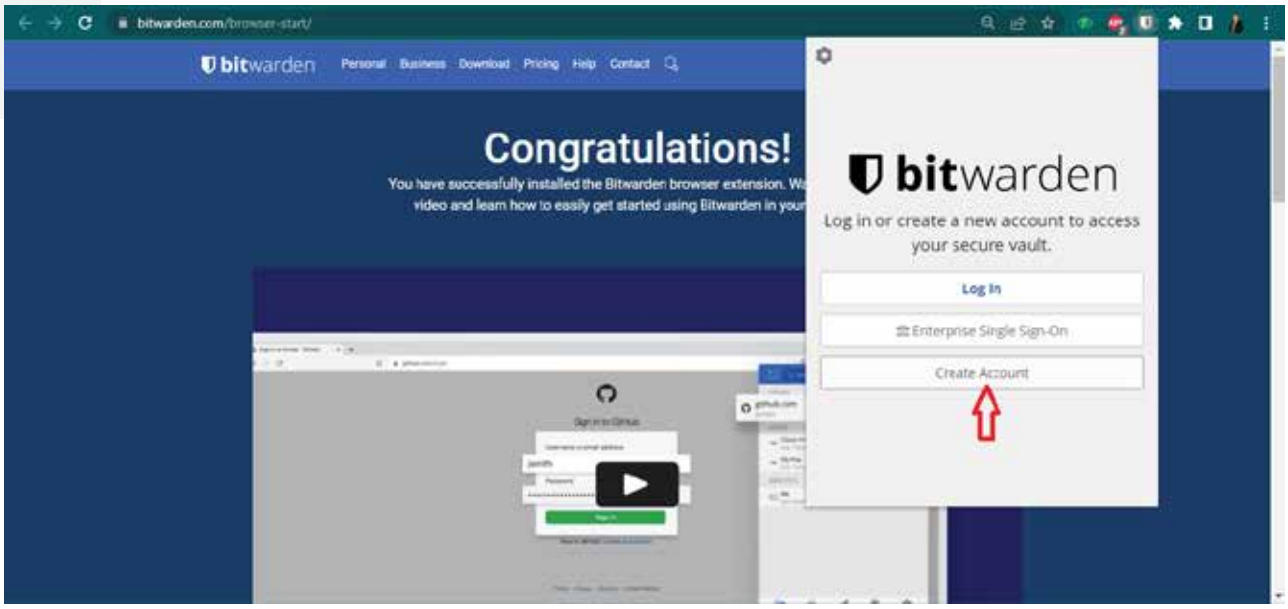
Bitwarden merupakan Password Manager berbasis online yang bisa di pasang di browser anda sebagai Extension atau Add-on. Disini, saya akan melakukan demonstrasi menggunakan browser Google Chrome. Dengan menggunakan Google Chrome, buka.link https://s.id/Bitwarden ini dan lakukan instalasi sama seperti Extension yang lain. Klik “Add to Chrome” dan klik “Add extension” untuk menambahkan. Tunggu beberapa saat hingga instalasi selesai.



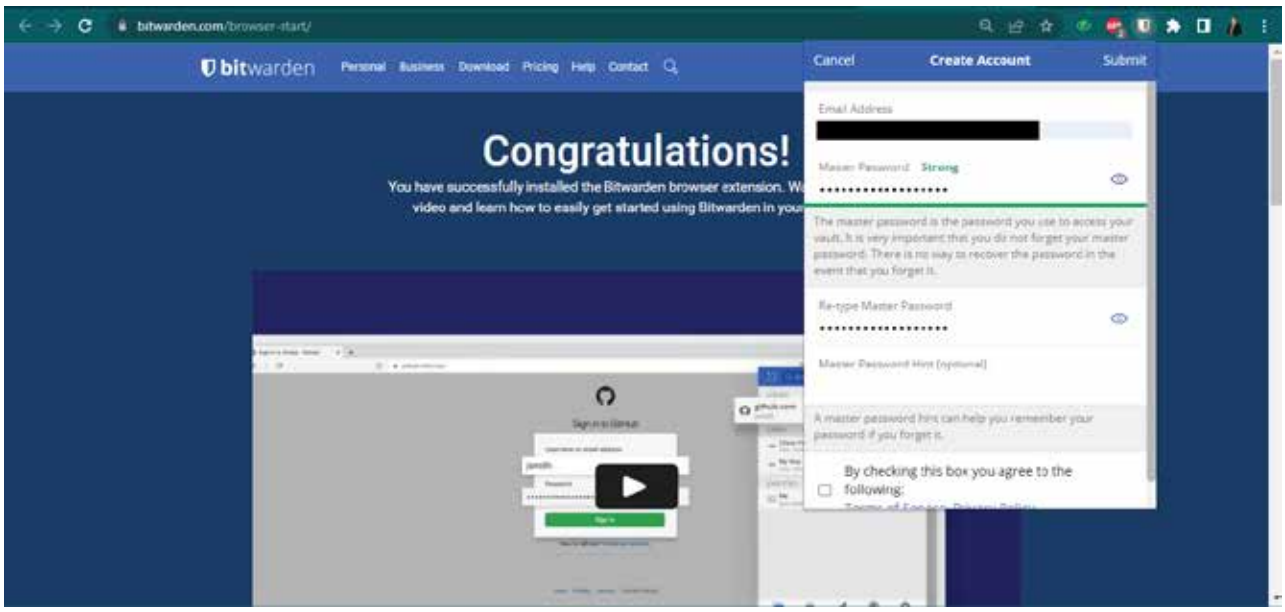
Untuk memudahkan akses, silahkan klik icon “Extension” dan klik icon “Pin” seperti gambar diatas.

b. Membuat akun Bitwarden

Langkah selanjutnya, anda harus membuat akun di Bitwarden. Fungsi akun ini adalah agar anda bisa menyimpannya secara online seluruh password yang anda buat. Dengan begitu, anda bisa mengaksesnya kapan saja dan otomatis akan sinkron di berbagai perangkat anda.



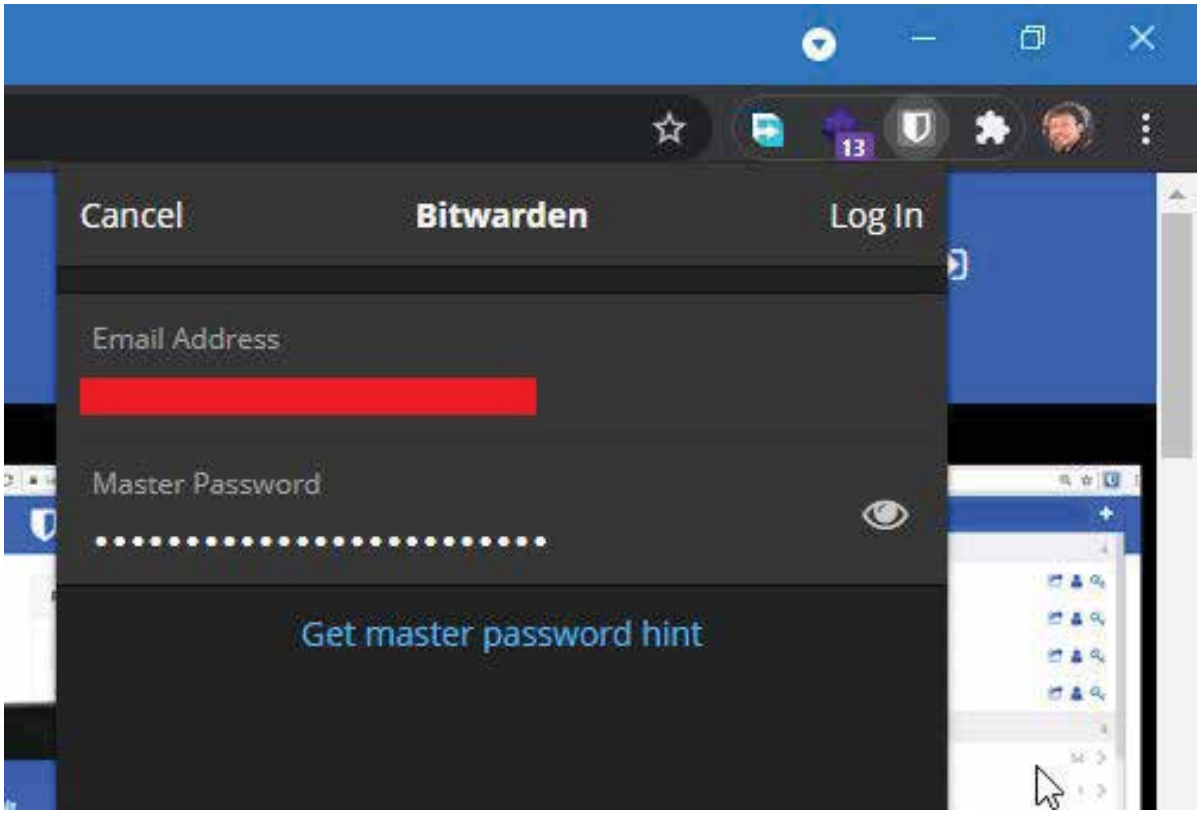
Klik saja extension Bitwarden pada Chrome anda. Kemudian klik **"Create Account"**



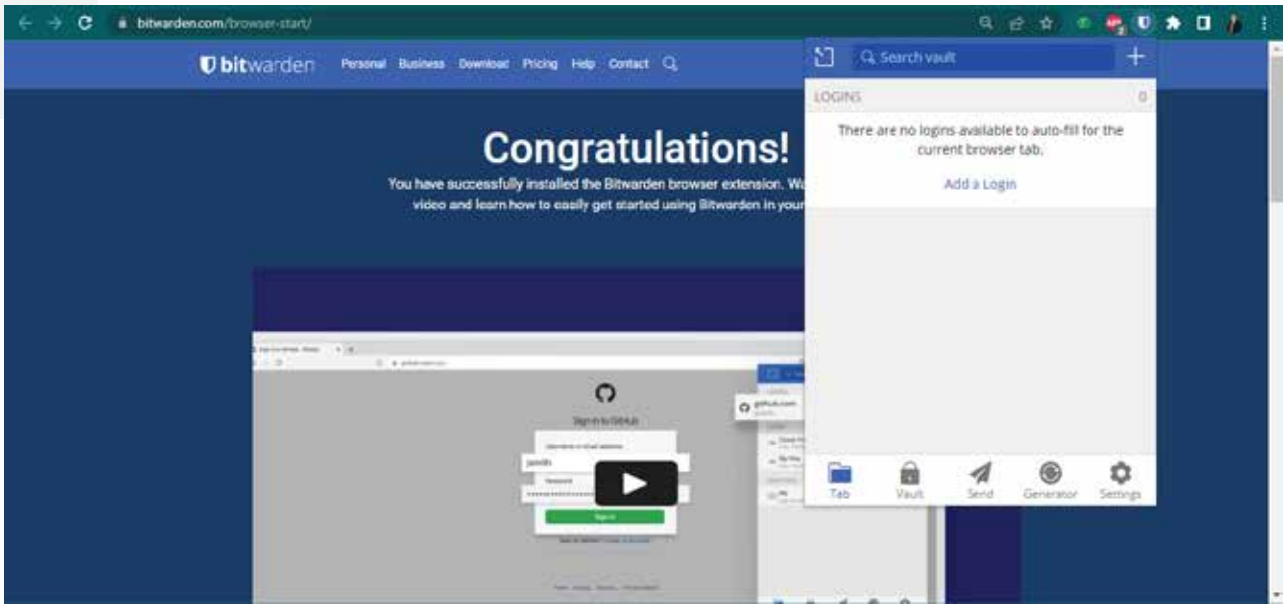
Kemudian, silahkan isi Email dan Master Password. Master Password ini adalah satu-satunya password yang harus anda ingat. Centang By Checking this box you agree to the following dan submit kemudian klik yes

c. Login ke Bitwarden

Langkah selanjutnya, anda harus membuat akun di Bitwarden. Fungsi akun ini adalah agar anda bisa menyimpannya secara online seluruh password yang anda buat. Dengan begitu, anda bisa mengaksesnya kapan saja dan otomatis akan sinkron di berbagai perangkat anda.



Akun anda saat ini telah dibuat. Langkah selanjutnya adalah silahkan Login dengan menggunakan Email dan Master Password yang telah anda buat seperti gambar diatas.



Setelah selesai, maka tampilannya adalah seperti gambar diatas. Untuk menambah daftar login cukup membuka alamat url yang akan ditambahkan, buka Bitwarden kemudian pilih add a login dan seterusnya.

Sumber : Bitwarden.com

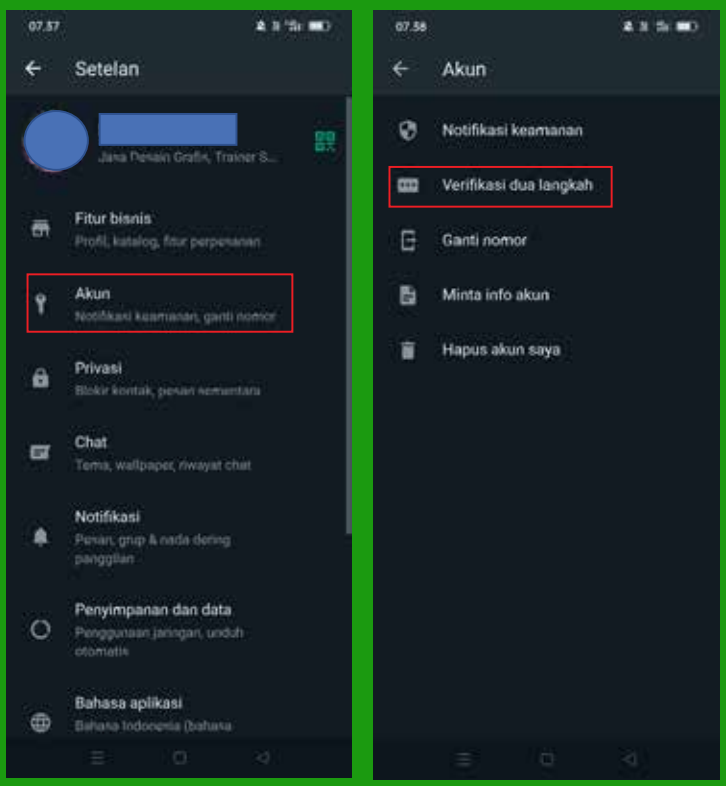
4. Aktivasi 2-Factor Authentication (2FA)

Akun WhatsApp dan media social kena *hack* atau peretasan itu sangat mungkin terjadi. Modus kejahatan peretasan akun Whatsapp atau media sosial yang umum dijumpai adalah menggunakan metode *social engineering* atau rekayasa sosial berupa pengelabuan, untuk mengamankan itu semua bisa mengaktifkan *Two Steps Verification.*

Berikut merupakan cara mengaktifkan Two Step Verification

a. WhatsApp

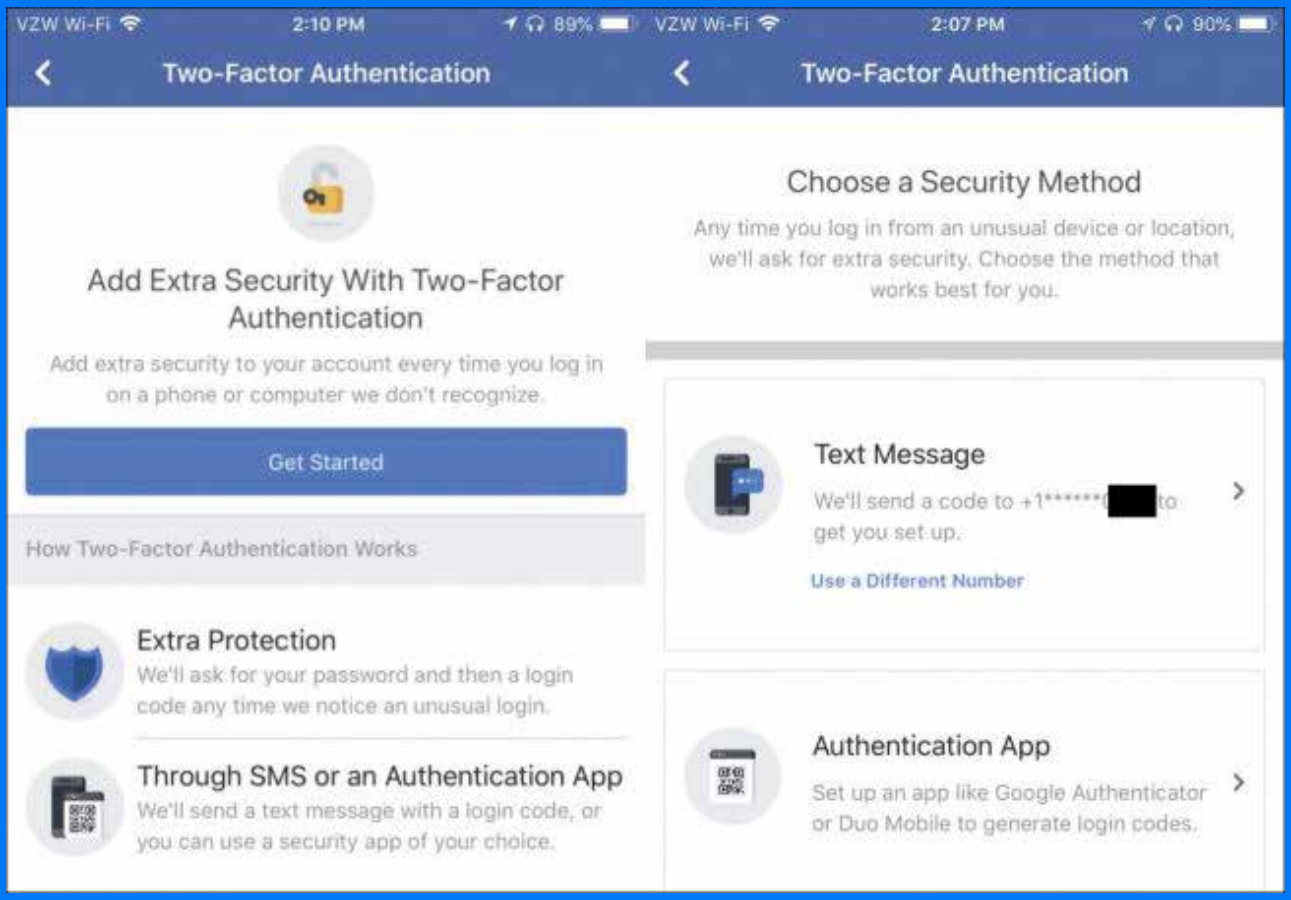
1. Buka WhatsApp, masuk ke Setelan / Pengaturan dengan mengklik “titik tiga” pada pojok kanan atas
2. Pilih opsi Akun, lalu pilih opsi Verifikasi Dua Langkah



3. Pilih Aktifkan
4. Kita akan diminta memasukkan PIN dan mengkonfirmasinya sekali lagi
5. Tambahkan alamat surel (email) saat proses aktivasi ini. Alamat ini akan digunakan sebagai alternatif untuk menerima tautan yang dapat menonaktifkan verifikasi dua langkah ini, seandainya kita lupa PIN

Sumber: http://s.id/2fa-whatsapp

b. Facebook



2FA Facebook (ilustrasi)

Cara aktivasi metode 2FA untuk Facebook dengan kode dikirimkan via SMS:

Saat sudah masuk ke akun, buka Pengaturan dan pilih opsi Keamanan dan Info Login

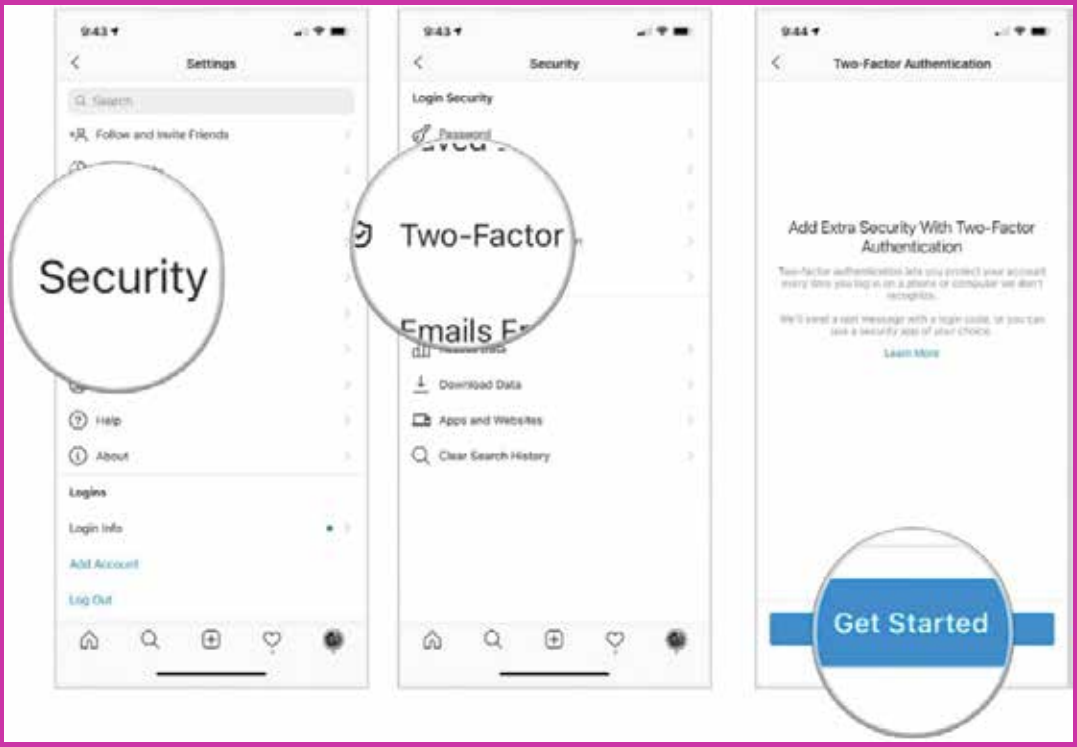
1. Cari opsi Menggunakan Autentikasi Dua Faktor Autentikasi, lalu klik Edit
2. Pilih metode autentikasi lalu ikuti instruksi yang muncul setelahnya
3. Setelah mengaktifkan metode autentikasi yang dipilih, klik Aktifkan

Setelah mengaktifkan 2FA, jika ada percobaan login dari perangkat yang tidak dikenal sebelumnya, maka ada beberapa opsi:

1. Notifikasi untuk persetujuan atas percobaan login dari perangkat tidak dikenal.
2. Dapat menggunakan kode pemulihan jika tidak memiliki ponsel yang sudah didaftarkan untuk metode 2FA.
3. Mengetuk kunci keamanan di perangkat lain. Kunci keamanan tersebut dapat ditambahkan dalam proses mengaktifkan 2FA.

Sumber: http://s.id/2fa-facebook

c. Instagram



2FA Instagram (ilustrasi)

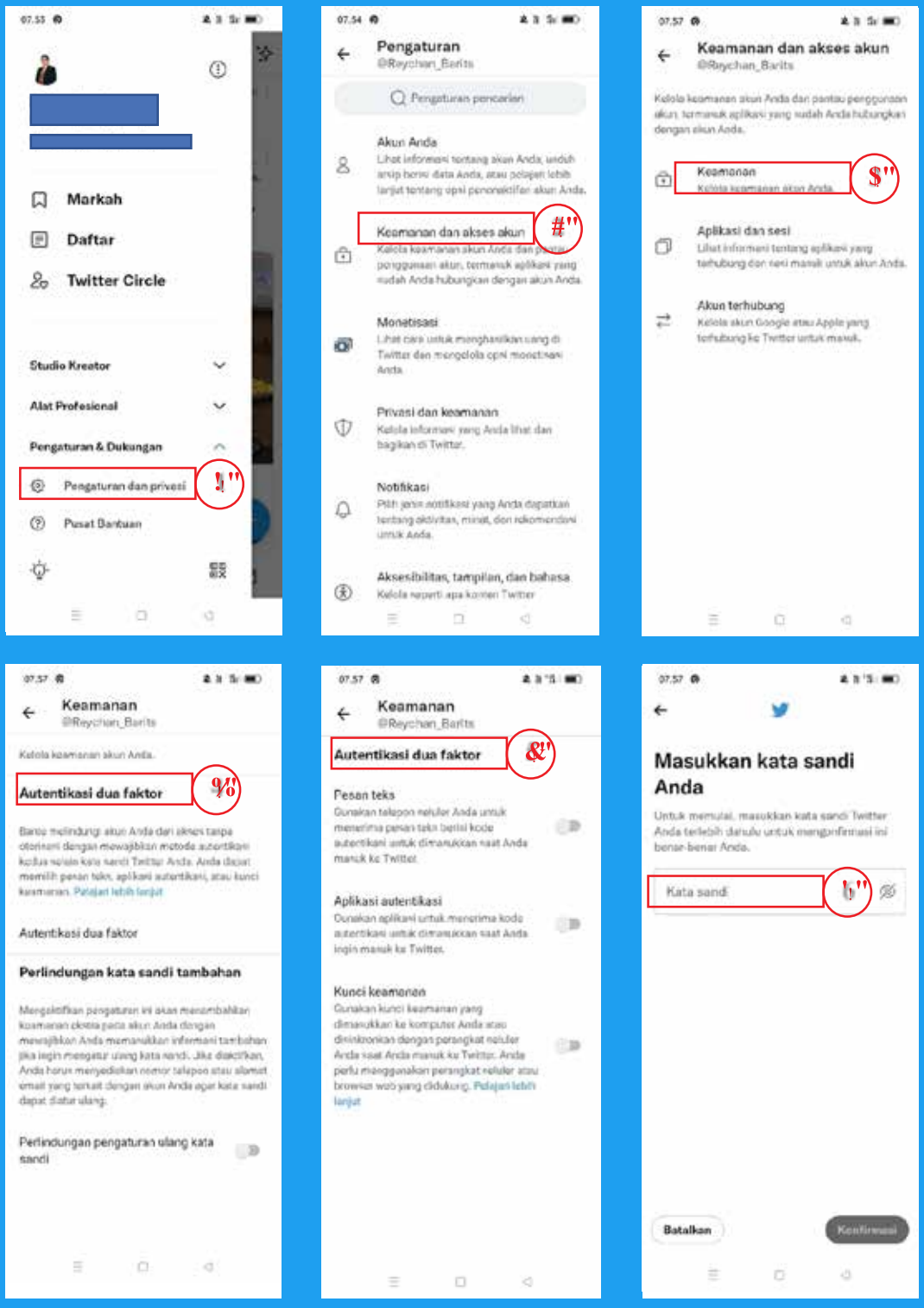
Cara aktivasi metode 2FA untuk Instagram dengan kode dikirimkan via SMS:

1. Masuk ke laman Profil dan klik ikon Menu pada pojok kanan atas
2. Pilih opsi Pengaturan
3. Pilih opsi Keamanan
4. Pilih opsi Autentikasi Dua-Faktor
5. Pilih opsi SMS
6. Jika sebelumnya tidak ada nomor telepon yang didaftarkan, maka kita akan diminta untuk mendaftarkan nomor telepon seluler
7. Setelah memasukkan nomor telepon, klik ikon Selanjutnya untuk menyelesaikan proses aktivasi autentikasi dua faktor.

Sumber: http://s.id/2fa-instagram

d. Twitter

Cara aktivasi metode 2FA untuk Twitter dengan kode dikirimkan via SMS:



2FA Twitter (ilustrasi)

1. Masuk ke laman Profil dan klik Pengaturan Privasi
2. Pilih opsi Keamanan dan Akses akun
3. Pilih opsi Keamanan
4. Pilih opsi Autentikasi Dua-Faktor
5. Pilih opsi Pesan Teks/SMS dan masukkan kata sandi/password lalu konfirmasi
6. Setelah membaca panduan aktivasi, klik Mulai
7. Masukan kata sandi dan klik Verifikasi
8. Klik Kirim kode
9. Masukan kode verifikasi yang sudah diterima di perangkat yang menggunakan nomor telepon tadi, lalu klik Selanjutnya untuk menyelesaikan proses aktivasi
10. Kita akan mendapatkan Kode Cadangan sekali pakai jika kamu tidak dapat mengakses metode autentikasi yang sudah dipilih karena berbagai macam sebab. Simpan kode cadangan di tempat aman
11. Setelah sukses mengaktivasi verifikasi login via SMS, tiap kali kita login ke akun Twitter, akan diminta memasukkan kode 6 angka yang dikirimkan melalui SMS ke nomor telepon kita

Sumber: http://s.id/2fa-twitterz

e. Tiktok

2fa Tiktok (ilustrasi)

https://samudranesia.id/

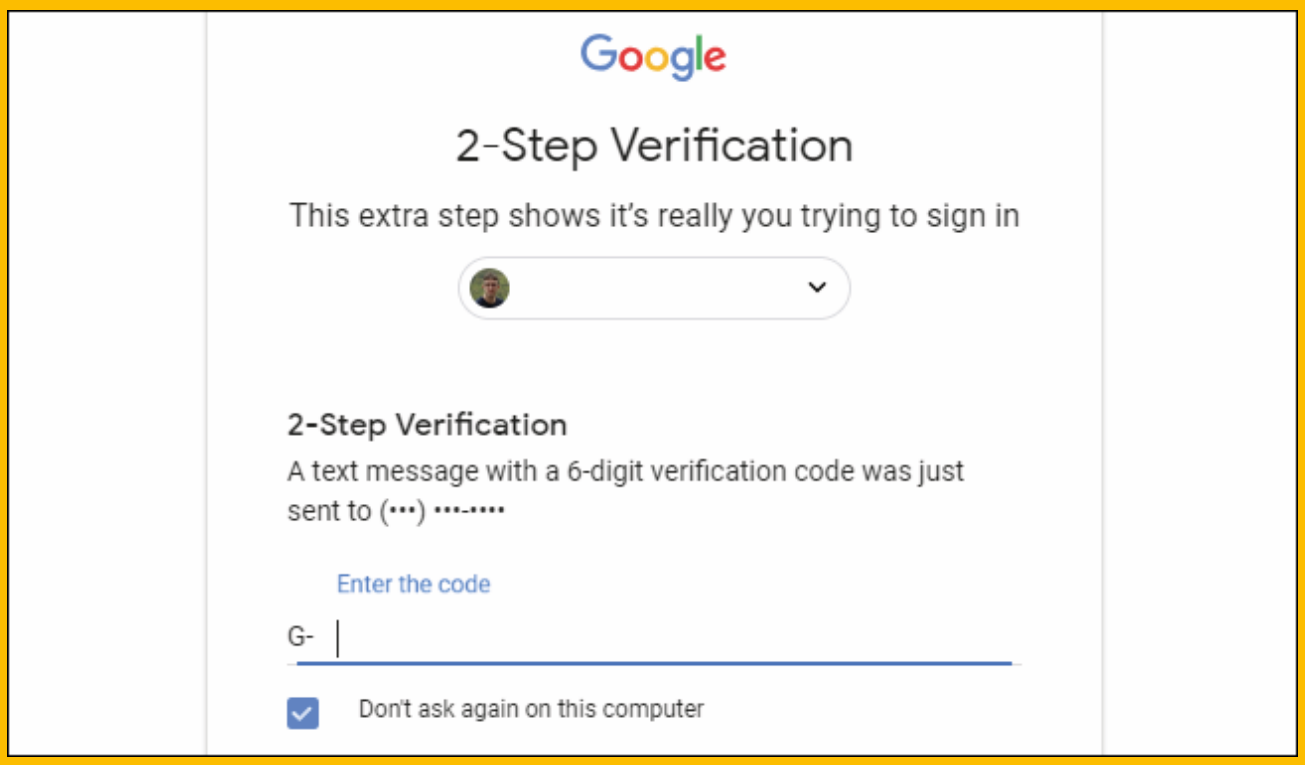
Verifikasi 2 langkah pada TikTok dapat menambahkan lapisan keamanan ekstra untuk akun Anda jikalau kata sandi Anda diretas.

Begini caranya:

1. Periksa apakah Anda telah mengunduh versi terbaru TikTok.
2. Ketuk Profil di kanan bawah.
3. Ketuk ikon 3-garis di kanan atas.
4. Ketuk Keamanan.
5. Ubah verifikasi 2 langkah dari tidak aktif menjadi aktif.
6. Pilih opsi SMS* atau Verifikasi email untuk kode verifikasi yang akan dikirim.

*dapat berlaku biaya SMS standar.

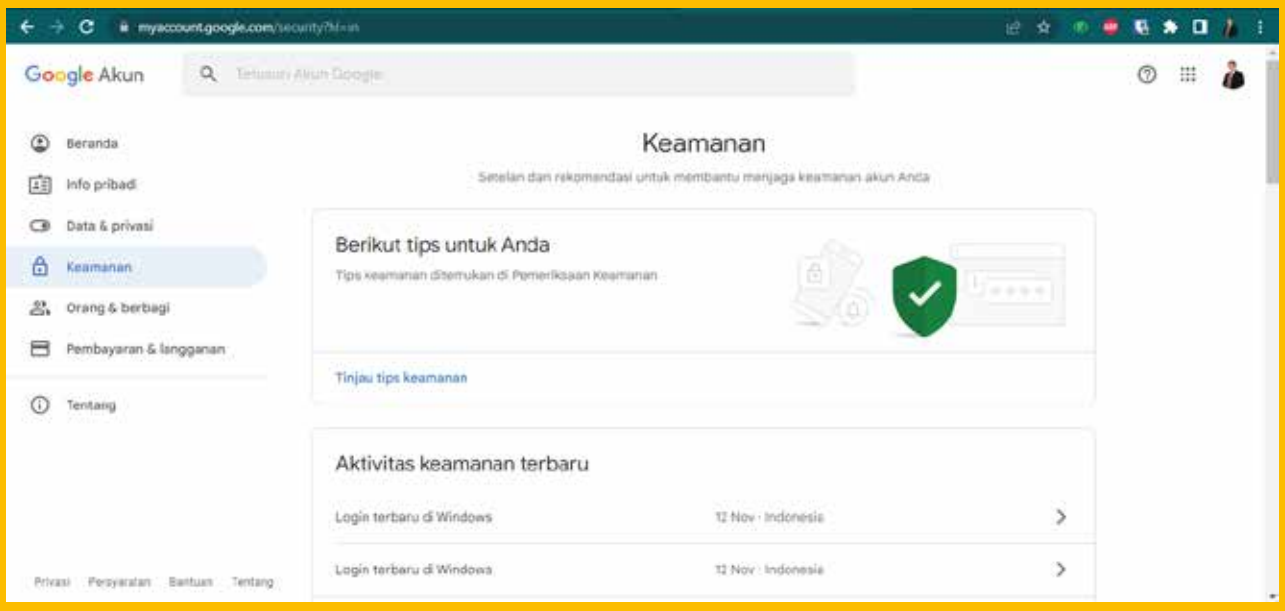
f. Gmail/Google



2FA Gmail / Google (ilustrasi)

Cara untuk mengaktifkannya:

1. Masuk ke Akun Google atau melalui https://myaccount.google.com
2. Di panel navigasi sebelah kiri, pilih Keamanan.



3. Pada bagian “Login ke Google”, pilih Verifikasi 2 Langkah, lalu Mulai dan ikuti petunjuk di layar dengan memilih metode SMS.
4. Kita akan diminta melakukan verifikasi nomor telepon yang dimasukkan. Kode 6 digit dikirimkan ke nomor yang kita berikan sebelumnya. Kode dapat dikirim melalui pesan teks (SMS) atau melalui panggilan suara, tergantung pada pengaturan yang Anda pilih.
5. Untuk memverifikasi diri Anda, masukkan kode di layar masuk.

Sumber: http://s.id/2fa-google

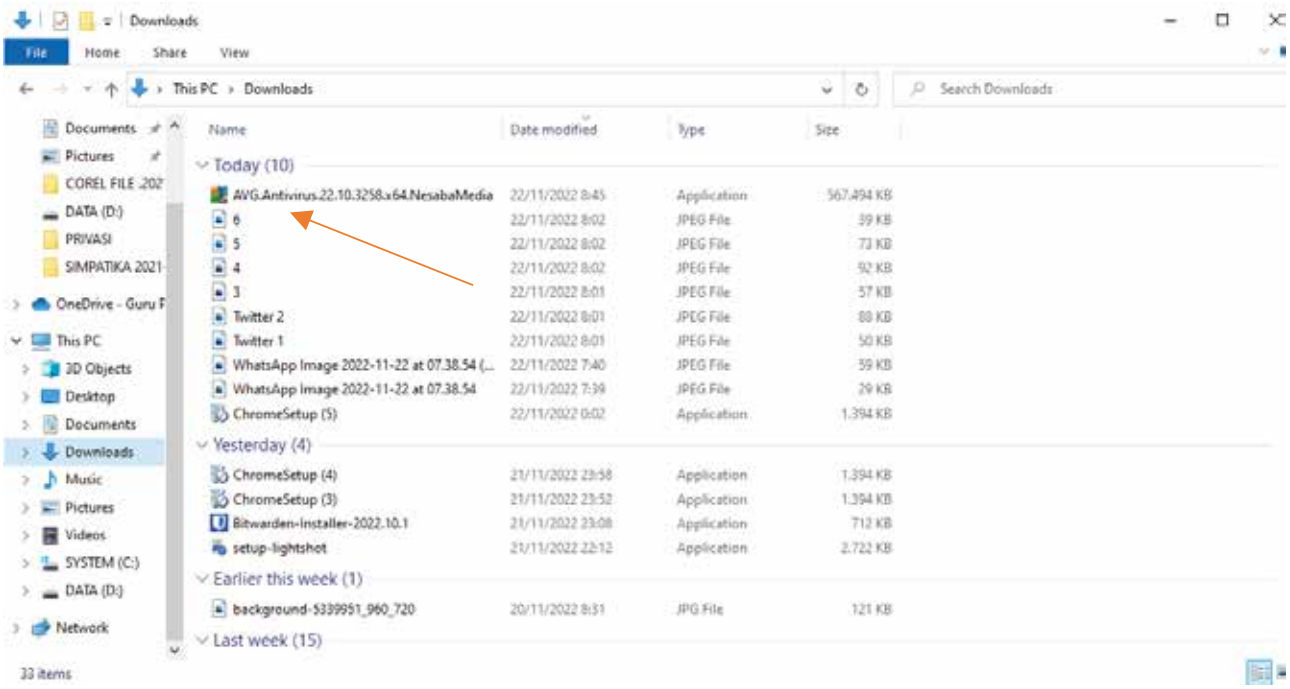
5. Antivirus

Salah satu cara untuk mendeteksi virus dengan baik adalah dengan memasang aplikasi antivirus yang terbaik seperti antivirus free AVG atau free Avast. Antivirus ini dapat melakukan scanning dengan sangat cepat, tidak memakan memory yang terlalu banyak, memiliki fitur Anti Rootkit, mempunyai perlindungan Firewall dan lain sebagainya. Dengan manfaat-manfaat tersebut kita dapat menjaga kesehatan komputer kita agar dilindungi dan terhindar dari virus yang berbahaya.

Kali ini akan jelaskan bagaimana cara menginstall antivirus AVG. Karena Antivirus ini sangat mampu untuk mendeteksi virus terkecil sekalipun. Berikut langkah-langkahnya.

a. Unduhlah terlebih dahulu installer antivirus AVG.

Pilih website resminya dan bebas virus. Sebagai contoh bisa di download di link Klik disini atau melalui link lain untuk mendownload installer AVG Antivirus. Jika proses download sudah selesai, maka klik dua kali pada installer Antivirus AVG tersebut.



b. Maka akan muncul aplikasi AVG.

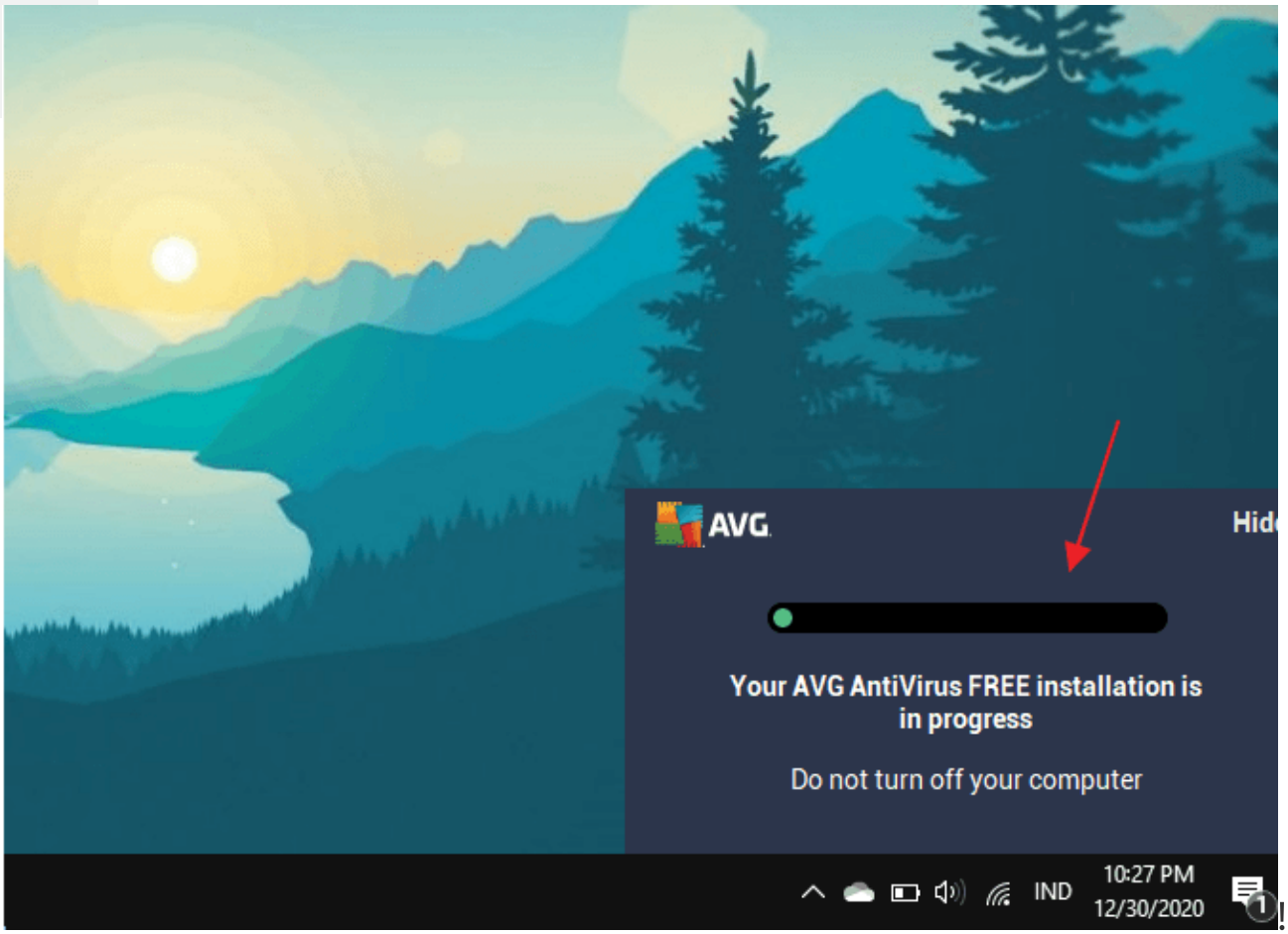
Disini Anda harus menunggu beberapa saat sampai proses loading selesai

c. Selanjutnya akan muncul jendela Setup dari AVG Antivirus.

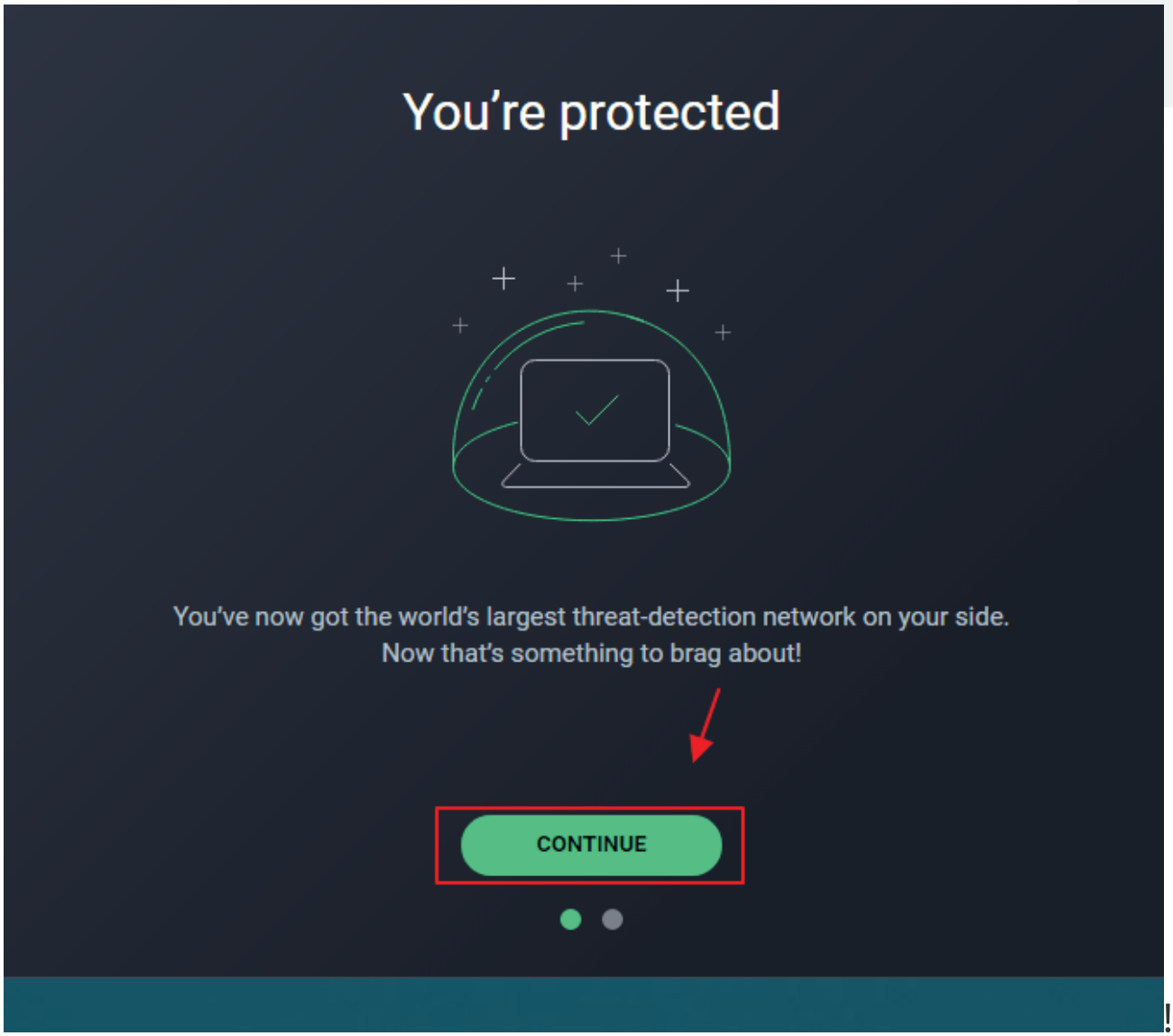
Untuk dapat melanjutkan proses pemasangan aplikasi AVG Antivirus, klik button Install yang berwarna hijau.

!

d. Kemudian proses installasi antivirus AVG akan muncul. Dan letak dari proses installasi antivirus AVG tersebut berada di sisi sudut kanan bawah. Selama Anda menginstall aplikasi Antivirus AVG ini, jangan mematikan komputer. Karena jika begitu, proses installasi akan terkendala. Tunggulah sampai proses installasi selesai. Proses ini juga memakan waktu yang sedikit lama. Anda dapat melakukan aktivitas apapun, tetapi jangan mematikan komputer Anda.



e. Apabila proses installasi antivirus AVG sudah selesai, maka akan muncul window AVG Antivirus. Dapat Anda lihat pada gambar dibawah ini, terdapat kata You’re Protected. Itu menandakan komputer Anda sudah dilindungi oleh AVG Antivirus. Klik Continue untuk melanjutkan.



f. Langkah selanjutnya yaitu Anda akan diminta untuk scanning komputer pertama kali. Dan ini harus Anda lakukan, agar komputer Anda bebas dari virus

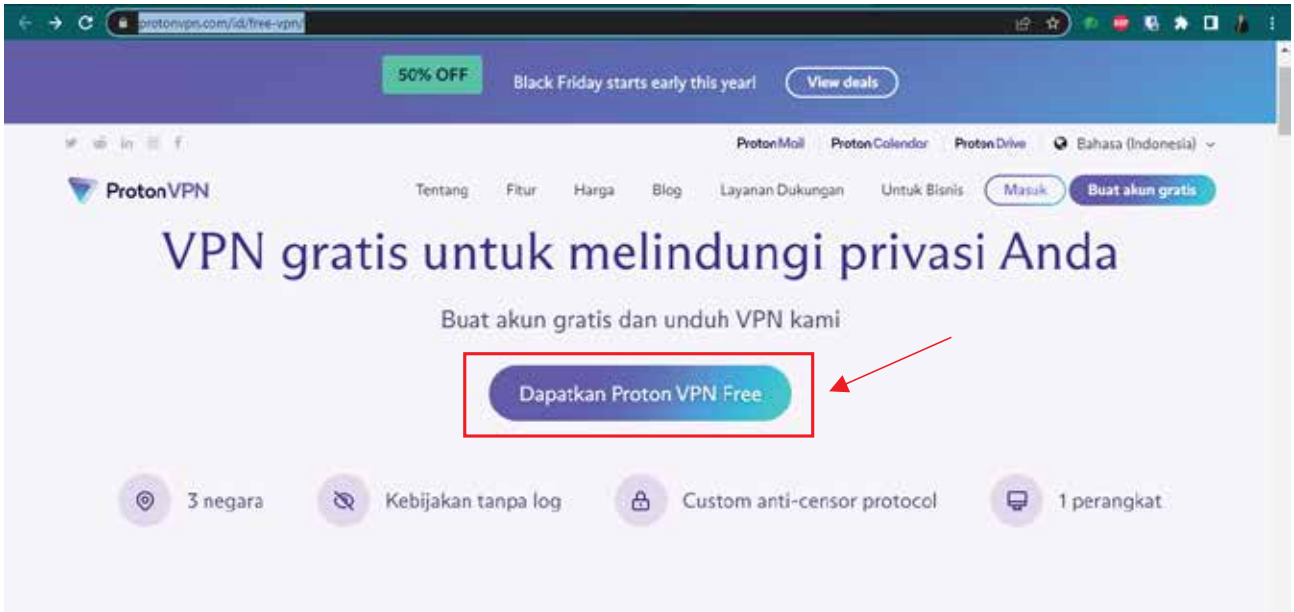
6. VPN (VIRTUAL PRIVATE NETWORK)

VPN memiliki kepanjangan yaitu Virtual Private Network. Perangkat lunak VPN mengenkripsi traffic internet Anda dan mengirim data Anda ke sebuah server eksternal via koneksi yang aman. Dari situ, datanya akan melalui internet. Selama perjalanan itu, alamat IP yang terlihat akan berubah. Ini artinya alamat IP yang terlihat saat online akan berbeda dari alamat IP di lokasi Anda. Alhasil, traffic internet Anda akan aman dan dianonimkan.

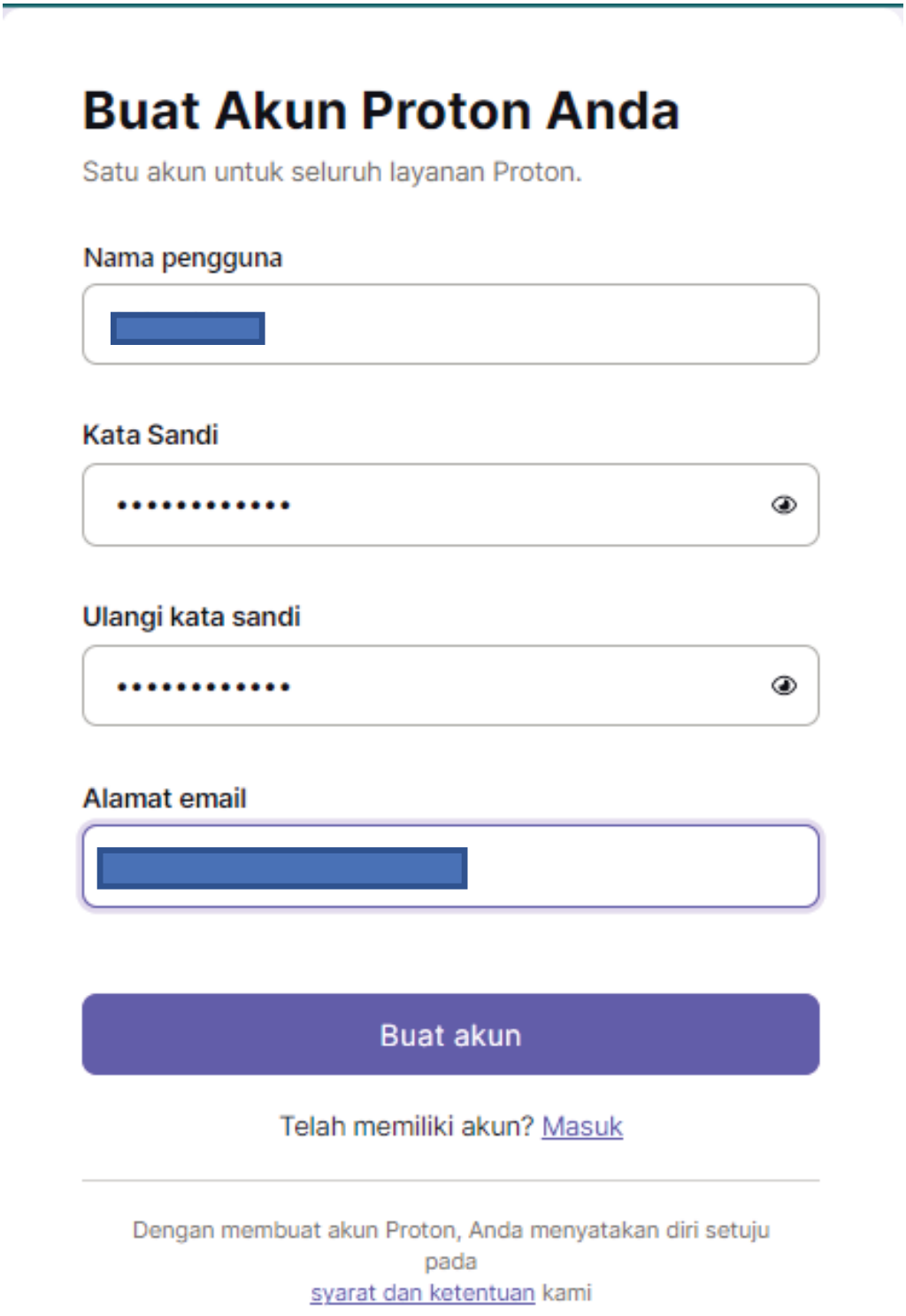
Apakah Anda tertarik untuk menggunakan internet secara lebih aman dan anonim? Apa Anda pernah berpikir untuk mengunduh sebuah VPN? Langkah pertama adalah dengan memilih sebuah penyedia VPN yang terpercaya. Dalam modul ini akan dibahas salah satu penyedia layanan VPN gratis yaitu Proton VPN

a. Buka alamat proton vpd free di link

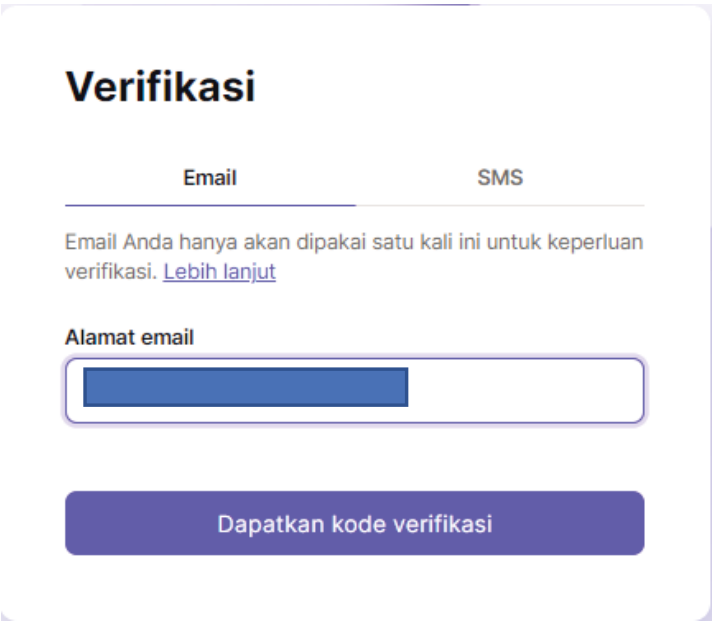
https://protonvpn.com/id/free-vpn/ dan klik pada menu
Dapatkan Proton VPN Free



b. Anda akan diarahkan untuk buat akun, isi nama pengguna, kata sandi dan surel (email) anda yang aktif. Isi semua kolom kemudian klik buat akun

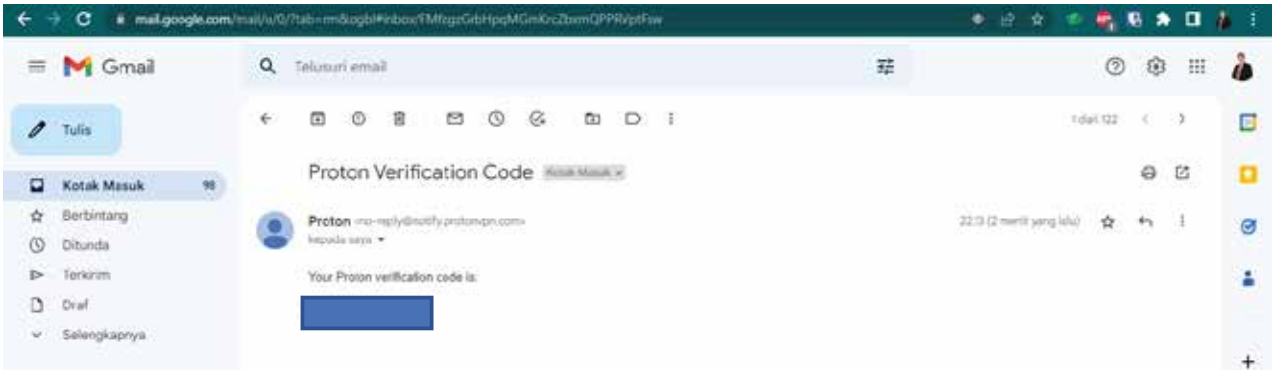


c. Muncul menu verifikasi. Nah, di sini Anda bisa memilih mode verifikasi melalui email atau sms. Sebagai contoh kami berikan mode verifikasi melalui email

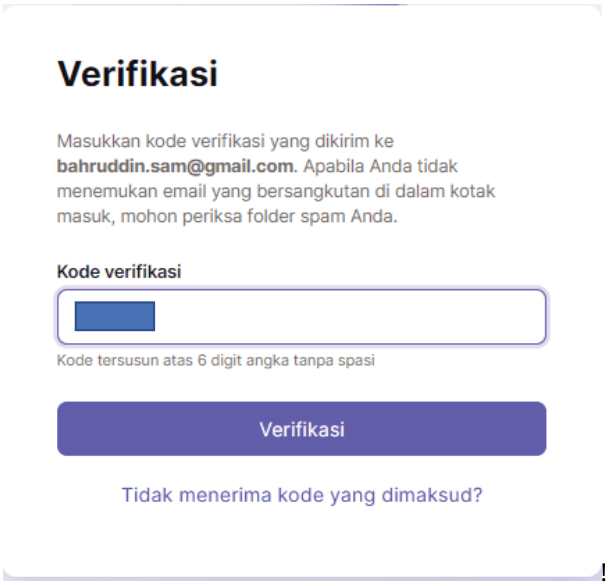


d. Setelah klik dapatkan kode verifikasi, silahkan buka email Anda. Di menu kotak masuk silahkan cari Proton kemudian buka.

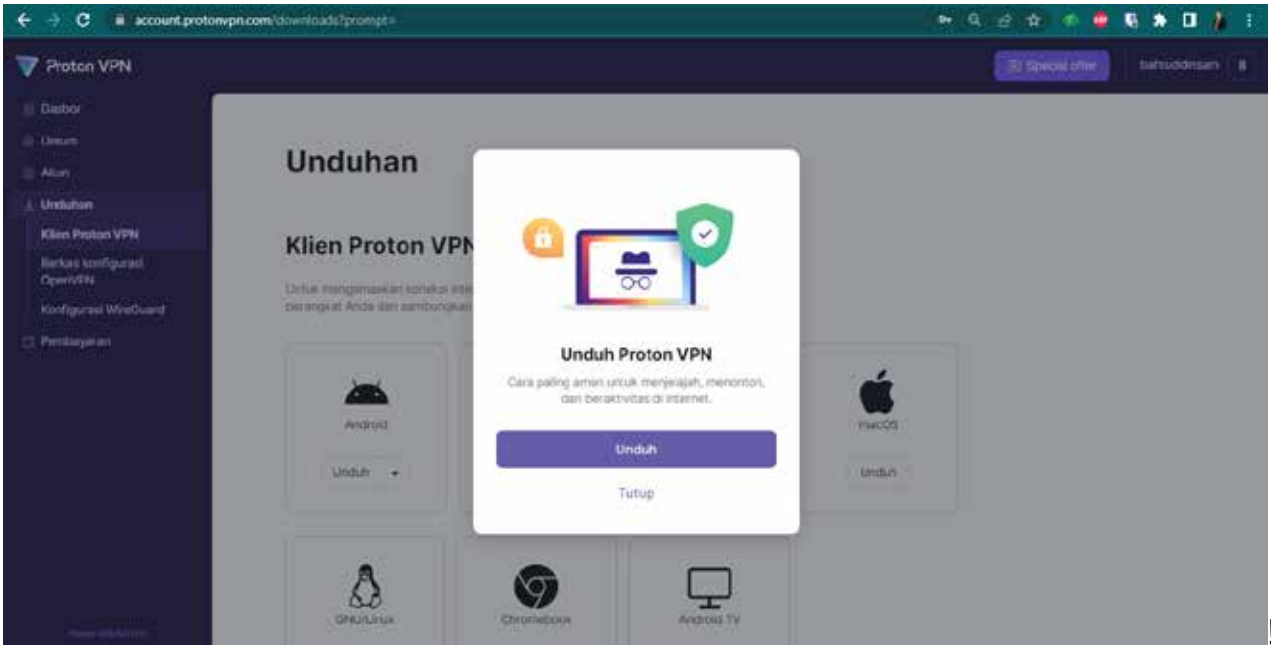
e. Maka akan muncul kode verifikasi yang terdiri dari 6 angka untuk selanjutnya di copy



f. Kemudian kembali ke laman Proton VPN da isi atau paste di kolom kode verifikasi dan klik verivikasi



g. Selamat akun Anda sudah dibuat, selanjutnya akan diarahkan ke beranda utama



h. Langkah selanjutnya silahkan disesuaikan penggunaan OS dan lain sebagainya menurut kebutuhan.

Sumber: http://s.id/2fa-google

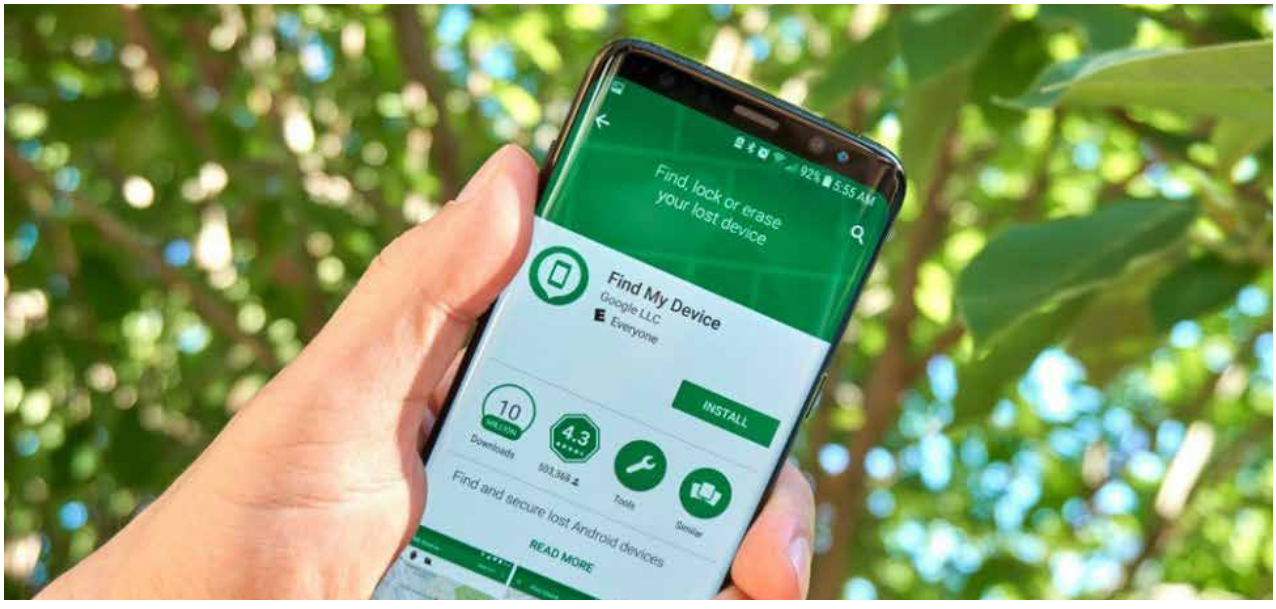
7. Find My Device for Android & Find My iPhone or IOS

Sebenarnya, setiap ponsel sudah menyediakan aplikasi khusus untuk lacak nomor HP jika terjadi hal yang tidak diinginkan, salah satunya adalah kehilangan ponsel. Aplikasi tersebut adalah Find My Device untuk Android dan Find My iPhone untuk iPhone.

Sebelum mengaktifkan *Find My Divice*, Anda perlu tahu dulu syarat untuk mengaktifkannya.

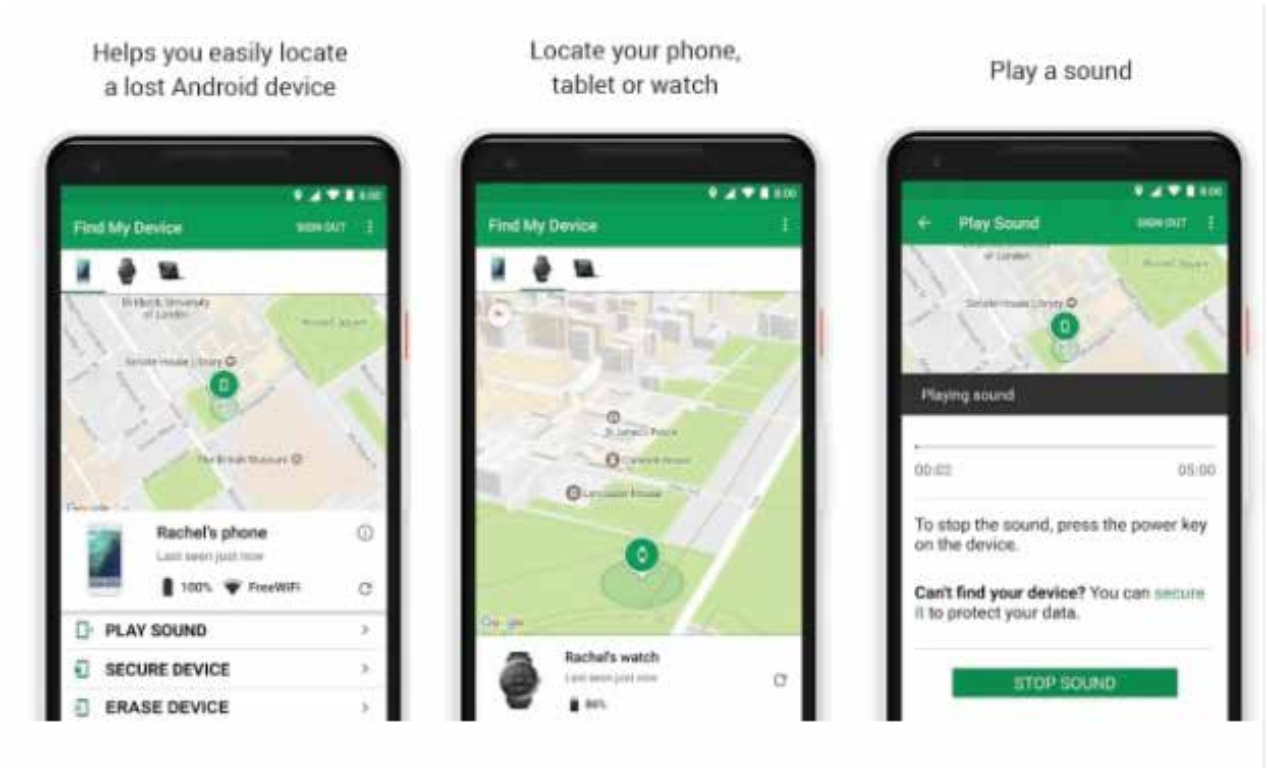
a. Perangkat dalam kondisi aktif dan terhubung dengan akun Google
b. Perangkat terhubung dengan data seluler atau Wi-Fi
c. Terlihat di Google Play
d. Fitur Location Service dalam kondisi aktif
e. Fitur Find My Device telah diaktifkan

Setelah pemilik smartphone dipastikan memenuhi persyaratan yang telah disebutkan, maka pemilik dapat memulai menggunakan fasilitas Find My Device secara gratis.



Cara Menggunakan Find My Device di Android

1. Buka Aplikasi Find My Device



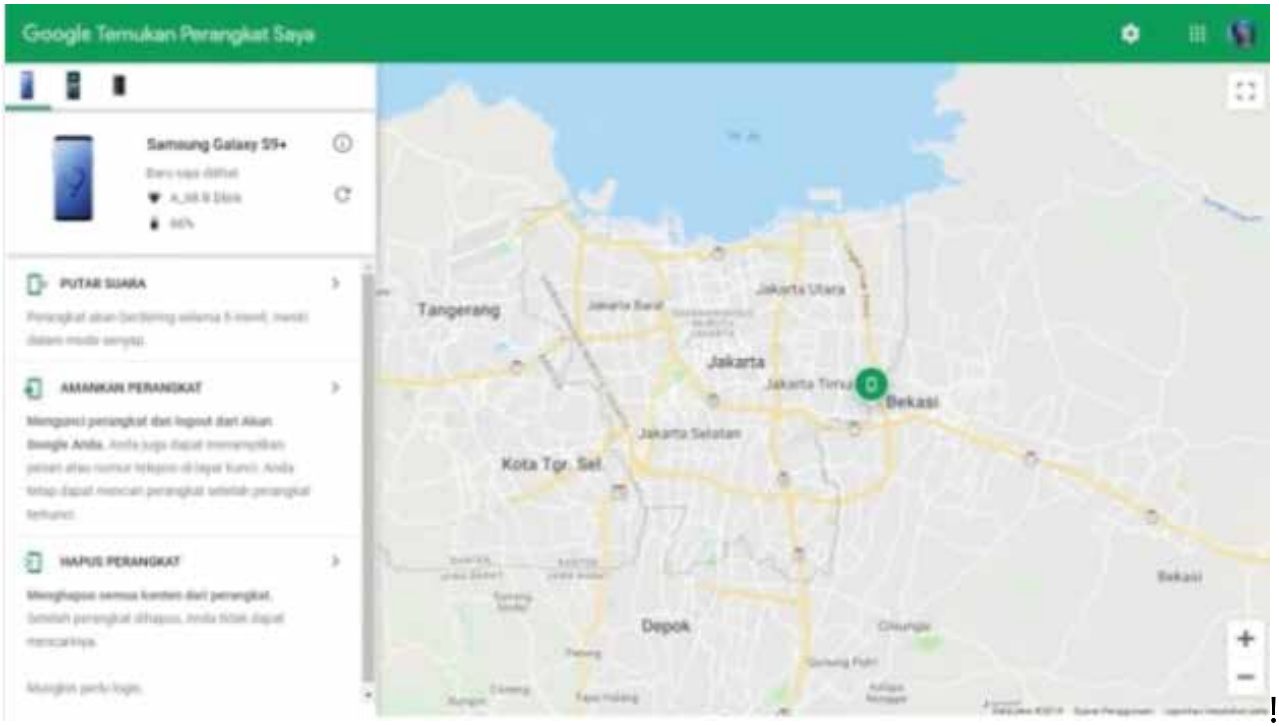
Buka browser lewat ponsel atau laptop. Lalu, kunjungi alamat https://www.google.com/android/find. Anda juga bisa menggunakan aplikasi Find My Device yang bisa diunduh melalui Google Play Store.
Selanjutnya, masuk ke akun Google yang terpasang di ponsel yang ingin dilacak. Jika terdapat dua akun Google atau lebih pada ponsel tersebut, gunakan Google utama. Jika akun Google digunakan pada banyak ponsel, semua tipe ponsel akan muncul dan pilih ponsel yang ingin dilacak

2. Peta akan Menunjukkan Lokasi Terkini

Setelah itu, peta akan menunjukkan lokasi ponsel terkini. Jika ponsel sudah dalam keadaan mati, maka lokasi yang ditunjukkan adalah lokasi terakhir saat ponsel masih nyala.

Anda bisa membunyikan ponsel menggunakan Find My Device untuk memudahkan pelacakan dengan klik 'Putar Suara'. Fitur ini masih bisa membunyikan ponsel meski sebelumnya Anda memasang mode silent.

3. Sisipkan Nomor Telepon Teman atau Keluarga



Segera gunakan opsi 'Amankan Perangkat' untuk mengunci ponsel dan memberi pesan di layar ponsel. Kamu bisa menyematkan nomor telepon teman atau keluarga untuk memudahkan orang yang menemukan ponsel menghubungimu.

Jika belum juga menemukan ponsel tersebut, maka bisa menghapus semua data di dalamnya agar tidak disalahgunakan dengan klik 'Hapus Perangkat'. Setelah itu, semua data di dalamnya akan terhapus secara permanen, termasuk akun Google yang menyebabkan kamu tidak lagi dapat melacak ponsel.

Cara Menggunakan Find My iPhone

Jika pada ponsel Android menggunakan Find My Device, maka Apple memiliki layanan lacak ponsel mereka sendiri, yaitu Find My iPhone. Berikut adalah cara menggunakan fitur Find My iPhone

1. Buka aplikasi Find My iPhone yang bisa diunduh lewat App Store atau buka situs icloud.com/find. Setelah itu, masukkan ID Apple ponsel yang ingin dilacak.
2. Klik 'Directions' untuk melihat lokasi ponsel.

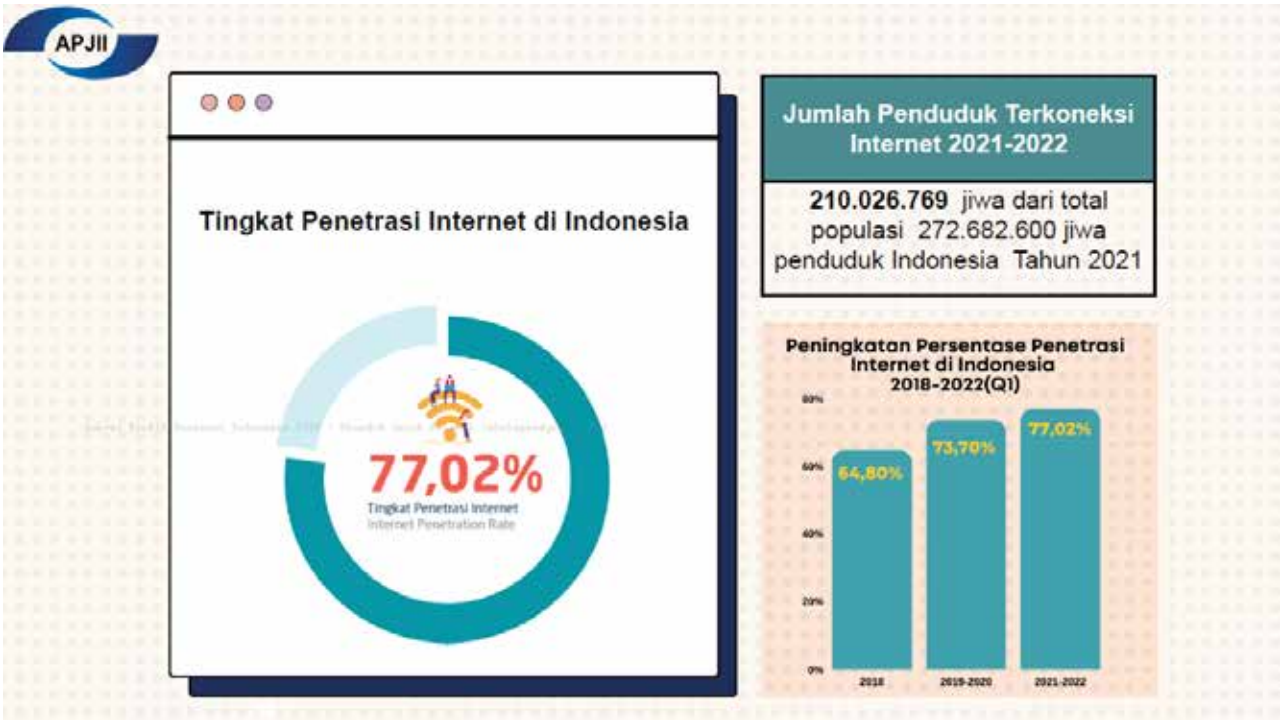
   Anda bisa menggunakan beberapa fitur Find My iPhone untuk memudahkan pelacakan iPhone, seperti 'Play Sound' untuk membunyikan iPhone.
3. Anda juga bisa menggunakan fitur 'Lost Mode' untuk menampilkan pesan yang akan muncul di layar ponsel. Masukkan juga nomor telepon teman atau keluarga agar orang yang menemukan ponsel dapat menghubungimu.
4. Klik 'Erase This Device' jika ponsel tidak ketemu dan ingin menghapus data di dalamnya untuk menghindari penyalahgunaan data pribadi.
5. Namun, jika ponsel Anda menggunakan AppleCare+ dengan perlindungan Pencurian dan Kehilangan, maka jangan pernah menggunakan fitur 'Erase This Device'. Segera ajukan klaim atas ponsel yang hilang tersebut.

Tampilan Find My iPhone. Foto: Apple

BAB II

KEAMANAN KOMUNIKASI DIGITAL

Berbicara tentang dunia digital tak lepas dari keamanan digital. Keamanan digital menjadi sangat penting dengan semakin bertambahnya pengguna internet di Indonesia. Data APJII Tahun 2022 menggambarkan bahwa pengguna internet di Indonesia selama 2021 – 2022 menunjukkan peningkatan luar biasa. Perhatikan gambar berikut.



Data APJII Tahun 2022 (Sumber: Survey APJII Tahun 2022)

Sebanyak 210.026.769 jiwa dari total populasi 272.682.600 jiwa Penduduk Indonesia sudah mengakses internet. Artinya 77,02 % Penduduk Indonesia sudah kenal dan aktif berselancar di dunia maya selain di dunia nyata. Keamanan menjadi hal penting yang harus diperhatikan dalam konteks kehidupan di dua dunia ini.

Keamanan digital, dikutip dari https://gudangssl.id adalah “sebuah perlindungan pribadi di media digital (online), termasuk aset digital dan identitas pribadi.”

Hal penting yang harus diperhatikan dalam keamanan digital ini meliputi perlindungan pribadi yang meliputi asset digital dan identitas pribadi. Perlindungan asset digital sangat erat kaitannya dengan akun – akun digital kita yang meliputi akun media sosial, akun belanja, akun toko digital dan akun – akun penting lainnya. Dan yang paling rentan terhadap kemanan digital ini yaitu terkait perlindungan data pribadi kita. Betapa pentingnya data pribadi sehingga pemerintah sudah menetapkan Rancangan Undang – Undang Perlindungan Data Pribadi (RDP) menjadi Undang – Undang Perlindungan Data Pribadi (UU PDP) pada tanggal 29 Oktober 2022.

Data Jumlah Serangan Siber Januari - Agustus 2019/2020 dari Pusat Operasi Keamanan Siber Nasional yang dirilis oleh Kompas Tekno 20 Oktober 2020 sebagai berikut:

Data Kejahatan Siber Tahun 2019 – 2020
(Sumber : https://tekno.kompas.com/image/2020/10/12/07020007/kejahatan-siber-di-indonesia-naik-4-kali-lipat-selama-pandemi?page=2)

Dari data tersebut dari tahun 2019 sampai dengan tahun 2020 menunjukkan tingginya serangan siber di Indonesia. Ini sangat penting bagi kita untuk mengamankan dunia kita di era digital.

Prinsip Keamanan Digital

Pentingnya menjaga kemanan digital tergantung dari salah satu komponen pendukung utama komputer yaitu Brainware (Manusia). Jika Hardware (perangkat keras) sudah ada, dan pendukung Software (Perangkat Lunak) sudah tersedia, peran selanjutnya tentang praktik keamanan digital ini bergantung pada manusianya (Brainware).

Ada dua hal yang perlu menjadi perhatian dalam berbicara tentang keamanan digital yaitu berbicara tentang Malware dan Phising.

MALWARE

Pengertian Malware dari Wikipedia menyebutkan bahwa “Malware (sebutan untuk perangkat lunak berbahaya) adalah perangkat lunak apa pun yang sengaja dirancang untuk menyebabkan kerusakan pada komputer, peladen/server, klien, atau jaringan komputer (Wikipedia)
Berbagai jenis malware antara lain virus komputer, worms, Trojan Horse, ransome ware, spyware, adware, dan scareware” (Wikipedia)
Berikut beberapa jenis malware yang umum berdasarkan ulasan dari *https://www.exabytes.co.id*

1. Virus

Merupakan *malware* yang pertama kali tercipta. Kemampuan dia adalah memanipulasi data, menggandakan diri serta menginfeksi, merubah bahkan bisa merusak suatu program. Dampak negatifnya adalah berkurangnya kinerja suatu computer sehingga tidak optimal dalam kinerjanya.

2. Worms

Sama seperti virus Worms ini bisa menggandakan diri dan dia menyebar melalui jaringan komputer yang mempunyai celah terbuka pada port kemananannya. Worms akan menyebar dengan tanpa campur tangan dari penggunanya sendiri dengan cepat melalui jaringan LAN, Internet dan WAN. Worms ini tidak masuk kategori sangat berbahaya, dampak pada komputer yaitu akan membuat kuota penyimpanan semakin cepat penuh dengan munculnya penggandaan file – file baru di dalam perangkat penyimpanan.

3. Spyware

Selanjutnya adalah Spyware, diambil dari kata Spy (mata-mata) dalam Bahasa inggris, program ini juga bertindak sebagai mata-mata atau penyusup ke perangkat komputer kamu untuk mengetahui kebiasaan kamu di komputer dan mencuri informasi penting kamu dan juga data penggunaan internet kamu. Sumber dari Spyware ini adalah mereka yang memasang iklan dengan tujuan untuk mempelajari semua data dan perilaku pengguna internet yang nantinya akan dikirim ke perusahaan data untuk dimanfaatkan sebagai keuntungan bagi para pengiklan. Data – data penting seperti Rekening Bank, Kartu kredit dan juga identitas pribadi menjadi sasaran dari aktivitas spyware ini. Parahnya, ada bebrapa jenis spyware yang mampu meninstall aplikasi lainnya dan merubah settingan utama pada komputer kita. Penting untuk mengamankan settingan dasar keamanan komputer kita.

4. Trojan

Bentuk dari Trojan adalah dia menyamar sebagai aplikasi yang seakan – akan terlihat legal dan sah padahal tujuannya untuk masuk ke komputer agar aplikasi lainnya dengan mudah menyusup ke komputer kita. Keunggulan dari Trojan ini sulit dilacak karena seakan – akan berbentuk aplikasi yang dibutuhkan untuk komputer. Bahayanya yaitu begitu aplikasi yang terinstall bisa masuk ke komputer, maka dia akan mengambil seluruh data aktivitas kita dan data penting kita yang sering dipakai selama menggunakan perangkat komputer.

5. AdWare

Program ini sama seperti melacak riwayat pencarian kamu dan juga yang kamu download, dengan tujuan untuk memprediksi produk atau layanan apa yang kamu sukai. Diambil dari kata Ads yang berarti iklan, Adware ini cara kerjanya juga dengan menampilkan iklan untuk produk atau layanan yang sering kamu cari atau yang terkait untuk menarik kamu untuk mengklik dan melakukan pembelian. Biasanya program ini sifatnya untuk tujuan promosi. Adware ini selain digunakan untuk tujuan marketing, adware juga dapat memperlambat komputer Anda.
Adware dimasukkan secara diam-diam oleh si pembuat program dengan kemampuan untuk download dan menampilkan iklan secara otomatis tanpa di ketahui oleh usernya. Adware sendiri yang sangat umum adalah yang berbentuk seperti iklan Pop-Up yang ada di suatu situs yang sedang kamu kunjungi.

6. RootKit

Rootkit ini juga salah satu bentuk malware lain yang cara kerjanya lumayan mirip dengan malware lain yang telah disebutkan sebelumnya, yaitu program yang menyusup kedalam sistem komputer, bersembunyi dengan menyamar sebagai bagian dari system, kemudian mengambil alih sistem, dan juga memantau kerja sistemnya. Rootkit ini dapat memberikan akses dan kontrol aktor jarak jauh ke komputer atau sistem lain. Rootkit ini dapat diinstal dalam beberapa cara, termasuk serangan phising yang digunakan untuk mengelabui pengguna agar memberikan izin rootkit untuk diinstal pada sistem komputer kita. Setelah diinstal, rootkit memberikan akses jarak jauh dan kontrol atas hampir setiap aspek sistem operasi (OS).

7. Bots

Bots adalah sebuah malware yang bekerja secara otomatis dengan berinteraksi pada jaringan lain. Bots ini memerlukan suatu perintah atau arahan dari pembuat bot ini sendiri agar melakukan apa yang diperintahkan, contohnya seperti mencuri informasi penting atau mengirimkan spam. Bots adalah software yang dibuat untuk melakukan suatu tujuan tertentu, banyak juga tujuan dibuatnya adalah untuk tujuan yang tidak berbahaya, seperti permainan video, kontes online dan hal ini sudah sangat umum. Bot ini tapi digunakan oleh pihak tidak bertanggung jawab untuk tujuan yang jahat seperti mencuri informasi penting seseorang. Namun, banyak juga situs web yang telah melindungi diri dari bot yang beredar di luar sana dengan tes CAPTCHA dan memverifikasi pengguna sebagai human.

8. Ransomware

Yang terakhir adalah ransomware, yang merupakan suatu jenis perangkat perusak yang dirancang untuk menghalangi akses kepada sistem komputer atau data. Nah, ransomware ini biasanya sih khusus menargetkan perusahaan/korporasi dengan mengkompromikan jaringan yang kemudian mencoba untuk mengenkripsi semua perangkatnya. Ia juga memblokir akses hingga tebusan dibayarkan. Metode pengiriman yang paling umum untuk ransomware adalah dengan mengklik tautan di dalam email atau membuka lampiran jahat. Ransomware biasanya menyebar seperti worms komputer normal berakhir di komputer melalui file yang diunduh atau melalui beberapa kerentanan lain dalam layanan jaringan.

PHISHING

Pengelabuan (Inggris: phishing) dalam istilah komputer adalah suatu bentuk penipuan yang dicirikan dengan percobaan untuk mendapatkan informasi yang sensitif, seperti kata sandi dan kartu kredit, dengan menyamar sebagai seseorang atau pebisnis tepercaya melalui komunikasi elektronik resmi, seperti surat elektronik atau pesan instan. (Wikipedia)

Istilah phishing dipublikasikan pertama kali oleh American Online Usernet Newgroup pada 2 Januari 1996 dan mulai dikenal tahun 2004. Istilah tersebut dalam bahasa Inggris berasal dari kata fishing (memancing), dalam hal ini berarti memancing informasi keuangan dan kata sandi pengguna. Salah satu penyebab utama aksi ini dapat terjadi adalah faktor kelalaian manusia berupa kurangnya ketelitian dan rendahnya pengetahuan mengenai teknologi keamanan. Metode itu sering digunakan karena mudah dilakukan dan cenderung lebih berhasil memancing para pengguna akun untuk memberikan informasi pribadinya. Dengan banyaknya kasus pengelabuan yang dilaporkan, metode tambahan atau perlindungan sangat dibutuhkan. Upaya-upaya itu termasuk pembuatan undang-undang, pelatihan pengguna, dan langkah-langkah teknis. (Wikipedia)

Jenis Phishing

Berdasarkan jenisnya, terdapat tiga macam phising, yaitu:

- Whaling adalah upaya phising yang menargetkan pelaku bisnis.
- Pharming adalah upaya phising yang menggunakan malware yang dipasang di komputer korban untuk megalihkan mereka ke situs perangkap.
- Voice phising atau vishing adalah upaya phishing dengan menggunakan video call atau telekonferensi

Ciri – Ciri Phishing:

Ada beberapa ciri-ciri aksi ini, yaitu:

- Pelaku akan berpura-pura menjadi seseorang, perusahaan, atau layanan yang dipercaya.
- Meminta target untuk membalas dengan nama pengguna atau surel yang disertai kata sandi.
- Email yang mengandung tautan untuk melihat atau mengunduh file dari seseorang yang tidak dikenal.
- Membujuk dengan diskon atau hadiah.
- Tautan dalam kolom komentar media sosial yang mengarah ke halaman masuk palsu atau halaman setel ulang kata sandi

Sumber: https://id.wikipedia.org/wiki/Pengelabuan

Praktik Kemanan Digital

Upaya – upaya yang dilakukan manusia untuk pengamanan digital dimulai dari edukasi kepada pengguna yang meliputi edukasi terhadap berbagai aset digital yang dimilikinya. Salah satu praktik keamanan digital dilakukan terhadap akun – akun aplikasi pertemuan daring yang marak digunakan oleh warganet selama pandemi covid-19.

Aplikasi – aplikasi tersebut banyak pengguna belum memahami praktik keamanan dalam penggunaan dan pemanfaatannya. Berikut beberapa contoh aplikasi yang banyak dipakai selama pandemi Covid-19 tahun 2020 sampai sekarang Tahun 2022.

Beberapa Aplikasi Pertemuan Daring yang banyak digunakan oleh Warganet (Koleksi penulis)

Praktik Keamanan Aplikasi Zoom Meeting

Aplikasi Zoom membantu banyak lembaga pendidikan, lembaga bisnis dan lembaga – lembaga lokal sampai internasional terhubung satu dengan lainnya melakukan pertemuan virtual, seminar dan kerja – kerja kolaborasi sehingga efisien waktu dan ruang. Aplikasi ini memberikan ruang – ruang pertemuan virtual secara produktif, nyaman dan aman. Selama pandemi COVID-19 Aplikasi ini banyak digunakan oleh masyarakat dalam mengatasi keterbatasan pertemuan fisik dan pembatasan kegiatan massal, Zoom Meeting solusinya.

Ada bebepara Praktik keamanan yang harus diperhatikan dalam aplikasi Zoom meeting. Mulai dari Pengaturan pertemuan sebelum acara dimulai, pada saat zoom meeting berlangsung dan resource tambahan untuk kemanan pertemuan secara virtual.

Tiga tingkatan pengguna Zoom:

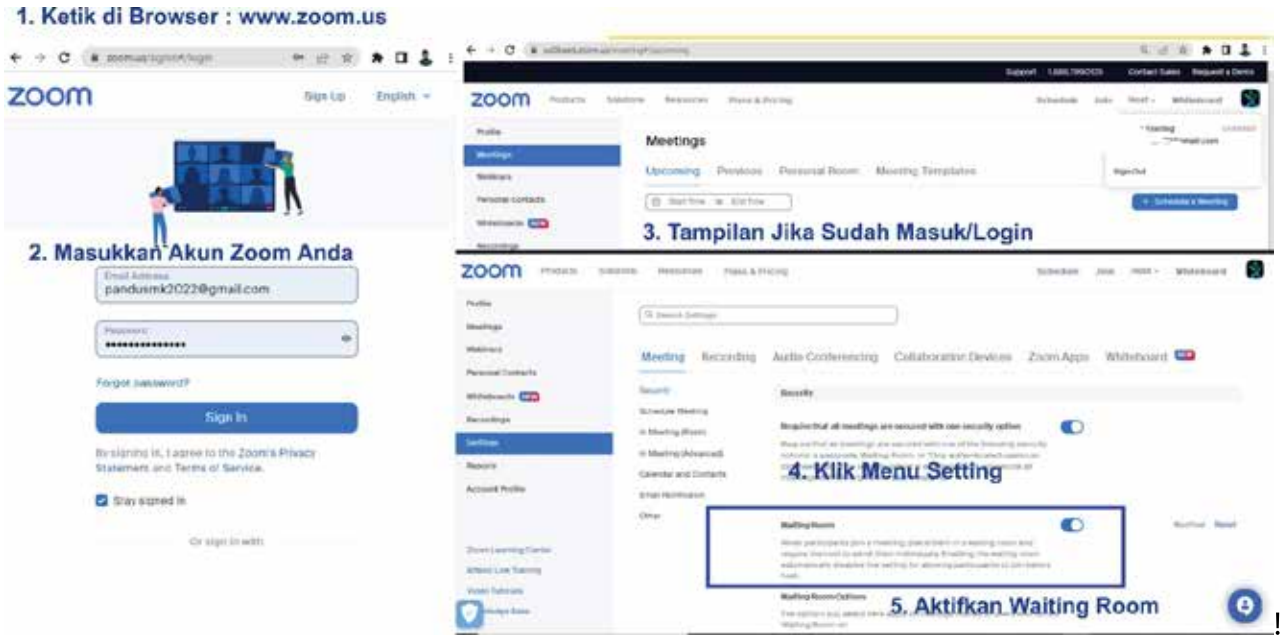
HOST : Orang yang memiliki akun zoom aktif terdaftar, menyiapkan pertemuan virtual dan mengatur jalannya pertemuan virtual dari awal sampai selesai.

Co-HOST : Orang yang tugasnya sama dengan HOST, Cuma dia dibatasi sebagai asisten HOST.

PARTICIPANT/AUDIENCE: Peserta yang tergabung dalam aplikasi pertemuan ini.

Pengaturan Keamanan Zoom Sebelum Acara (Pre-Acara)
Untuk menjaga kenyamanan dan keamanan dalam aplikasi virtual meeting ini sebaiknya ada pengaturan yang harus diperhatikan, Antara lain :

Aktifkan Ruang Tunggu (Waiting Room)



Cara mengaktifkan Waiting Room pada Zoom Aplication
(Sumber : Tangkapan layar penulis dengan editing)

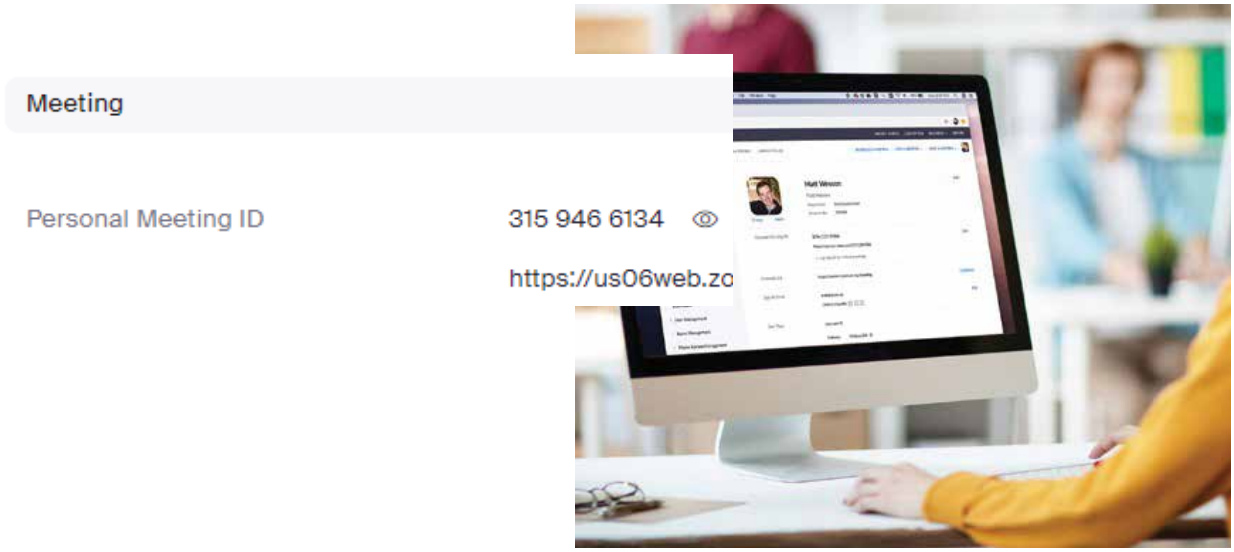
Waiting Room (ruang tunggu), berguna untuk peserta yang sudah masuk ke ruang meeting, akan tetapi Host belum mengijinkan masuk ke ruang utama. Sehingga keberadaan peserta bisa menunggu di ruang tunggu sambil menunggu Host mengijinkan masuk ke ruang utama.
Langkah Untuk Mengaktifkan Waiting Room adalah :

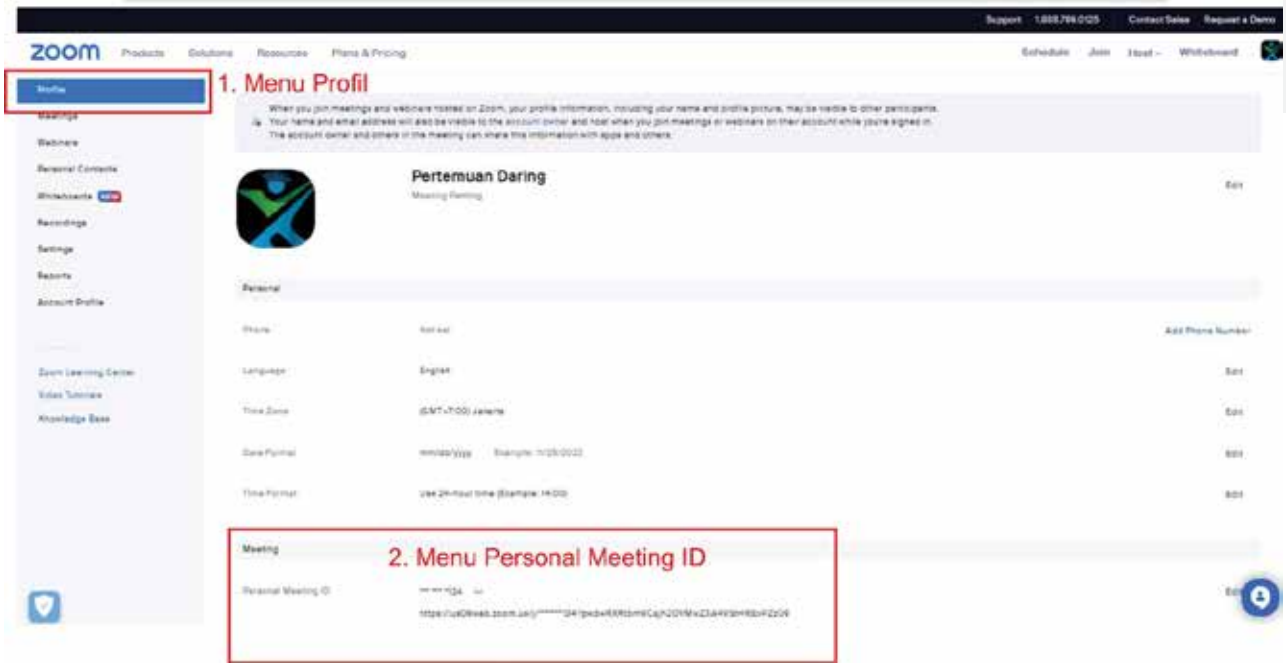
- Masuklah Ke Aplikasi Zoom dengan mengetik www.zoom.us
- Masukkan Akun Zoom Anda, Jika belum punya, silahkan daftarkan terlebih dahulu
- Pastikan Anda sudah bisa login/masuk ke menu utama.
- Masuk ke menu Setting.
- Selanjutnya cari menu Waiting Room, pastikan aktif dengan menggeser slider ke tombol aktif

Untuk detailnya silahkan perhatikan pada menu di atas.

Jangan Gunakan PMI (Personal Meeting ID)

Ketika mengadakan pertemuan Publik





Menu Personal Meeting ID pada Zoom

Untuk Mengetahui Personal Meeting ID (PMI) pada zoom terdapat pada menu Profil dan carilah menu PMI di deretan menu Zoom. Seperti tampak pada Gambar 2.5 di atas

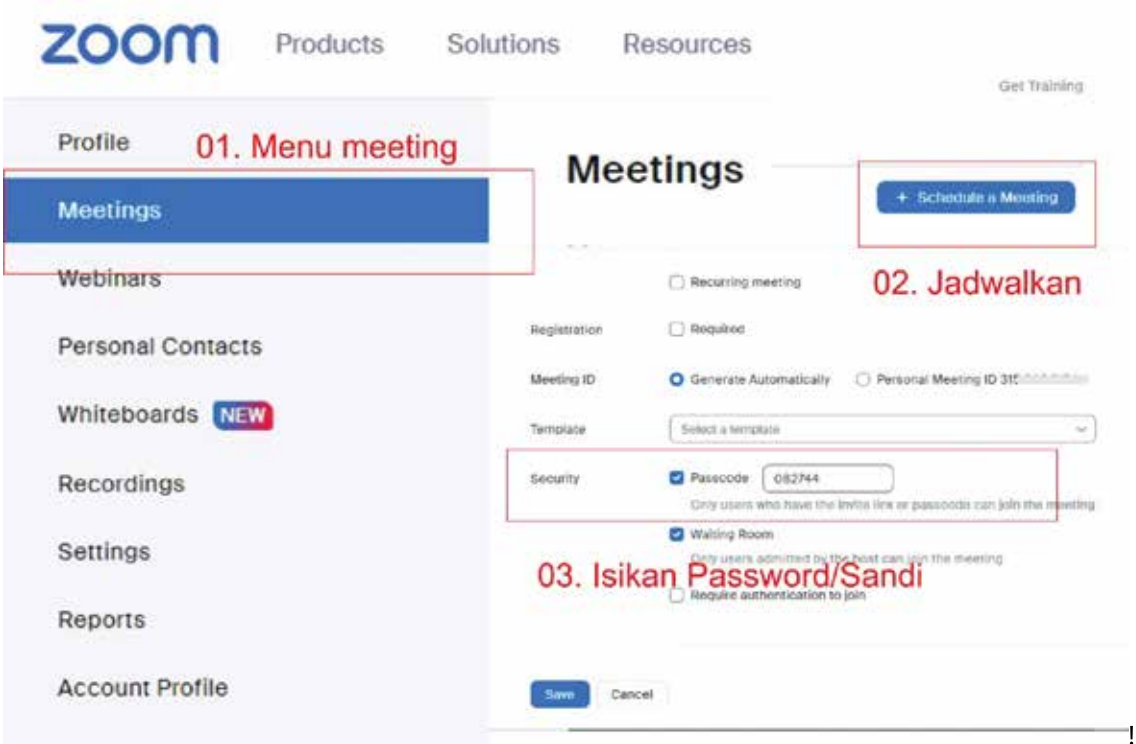
Host disarankan untuk membuat jadwal meeting menggunakan fitur 'Generated Autimatically' untuk keamanan meeting bagi semua audience/peserta yang diundang. Karena dengan menampilkan identitas PMI pada zoom itu sama saja dengan kita menggunakan meeting ID dan mengundang siapapun yang memiliki PMI untuk masuk ke pertemuan – pertemuan kita.

Jika ID PMI zoom ditampilkan kepada calon Audience maka ID PMI tersebut akan permanen dipakai selama akun zoom ini masih aktif. Peserta yang diundang atau siapapun yang memiliki akun PMI tersebut sewaktu – waktu bisa bergabung pada agenda meeting kita di jadwal lainnya. Oleh Karena itu hindari, menjadwalkan meeting pada zoom menggunakan akun Personal Meeting ID agar pertemuan virtual kita, agar tidak serta merta peserta umum bisa masuk. Perhatikan cara setting pada gambar 2.6 di bawah.

!

Aktifkan Password untuk Join Meeting

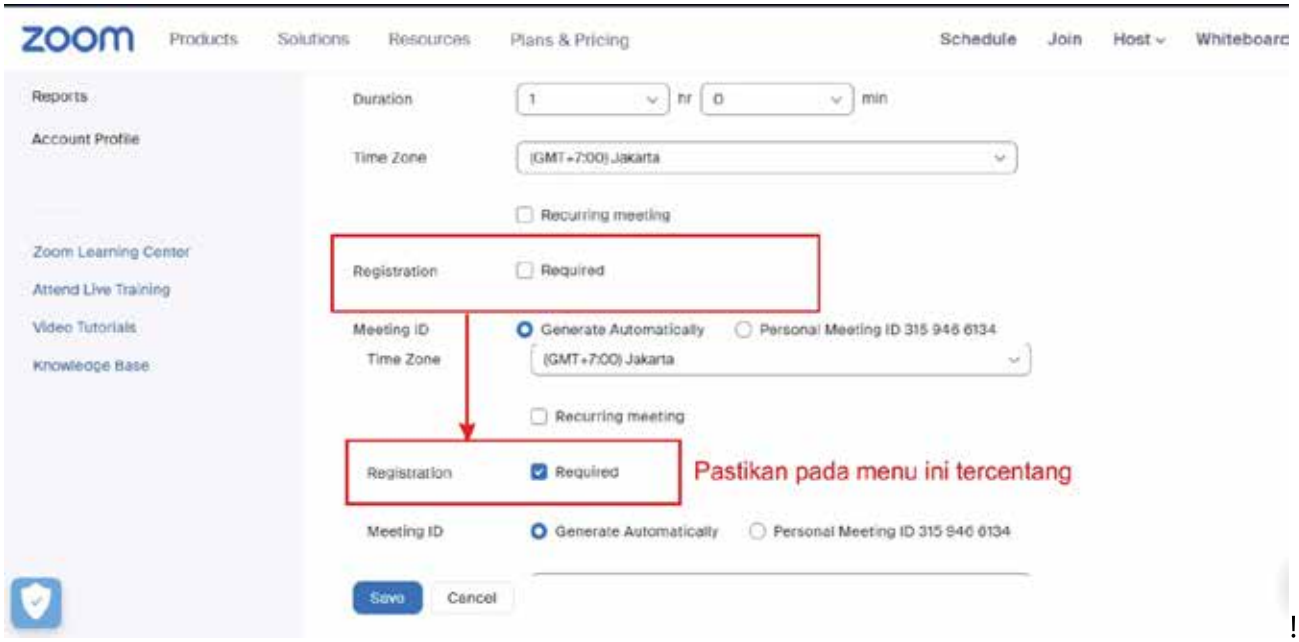
Pada fitur ini Audience/peserta akan bisa bergabung dengan pertemuan virtual kita, ketika mereka mempunyai password pertemuan yang disiapkan oleh Host pertemuan. Untuk membuat password perhatikan gambar 2.7 Berikut.



!

Cara membuat Password/Sandi di Zoom

Hanya Peserta yang terdaftar yang bisa bergabung



Menu Peserta yang terdaftar yang bisa bergabung pertemuan

Pada Gambar 2.8 di atas, ketika kita aktifkan menu Registration, dengan mencentang pada pilihan Registration, maka hanya peserta yang sudah mengisi form registrasi/pendaftaran saja yang diizinnkan masuk pada menu zoom.

Pengaturan Keamanan Zoom Saat Meeting Berlangsung

Perhatikan menu utama keamanan saat pertemuan zoom sedang berlangsung berikut.

Menu Utama Fitur kemanan Zoom

Keterangan Menu Utama Keamanan

1. Kunci Pertemuan
   Ketika fitur ini diaktifkan (dicentang) maka setiap peserta yang mau masuk ke Ruang meeting tidak akan bisa masuk selama fitur ini tidak di-NON AKTIFKAN (dibuang centangnya).
2. Aktifkan Ruang Tunggu
   Menu ini berfungsi untuk membuat peserta masuk ke Ruang Tunggu sebelum mereka diizinkan masuk ke ruang utama pertemuan.
3. Sembunyikan Gambar Profil
   Jika Fitur ini dicentang (Aktif), semua gambar profil peserta akan disembunyikan dari tampilan menu utama rapat virtual, hal ini biasanya digunakan untuk peserta yang sengaja menampilkan gambar profilnya yang niatnya untuk jualan, branding dan menghindari menampilkan gambar yang melanggar aturan dalam bertransaksi elektronik.
4. Ijinkan Berbagi Layar
   Jika fitur ini diaktifkan maka semua peserta yang dijadikan Co-Host didalam pengaturan utama zoom, maka dia bisa melakukan berbagi layar untuk presentasi.
5. Ijinkan Chat
   Fitur ini jika diijinkan untuk aktif, maka peserta bisa melakukan percakapan melalui aplikasi chat pada zoom sesuai ijin yang diberikan oleh HOST.
6. Ijinkan Merubah Nama Sendiri
   Jika Fitur ini diaktifkan maka semua peserta yang tergabung dalam pertemuan, bisa merubah nama profil yang tampak pada ruang pertemuan sesuai dengan keinginannya. Maka dalam hal ini perlu disampaikan tentang aturan main dalam pertemuan virtual.

7. Ijinkan Tidak Senyapkan diri sendiri
Mute (senyap), Unmute (tidak senyap). Unmute Themselves (Tidak senyap dirinya sendiri), artinya jika menu ini diaktifkan, maka semua peserta yang ikut pertemuan bisa dengan leluasa mebuka mic pada aplikasi zoom untuk berbicara kepada seluruh yang ada dalam pertemuan ini. Maka dalam hal ini perlu disampaikan tentang aturan main dalam pertemuan virtual tentang kapan diijinkan menghidupkan/mengaktifkan mic untuk berbicara.

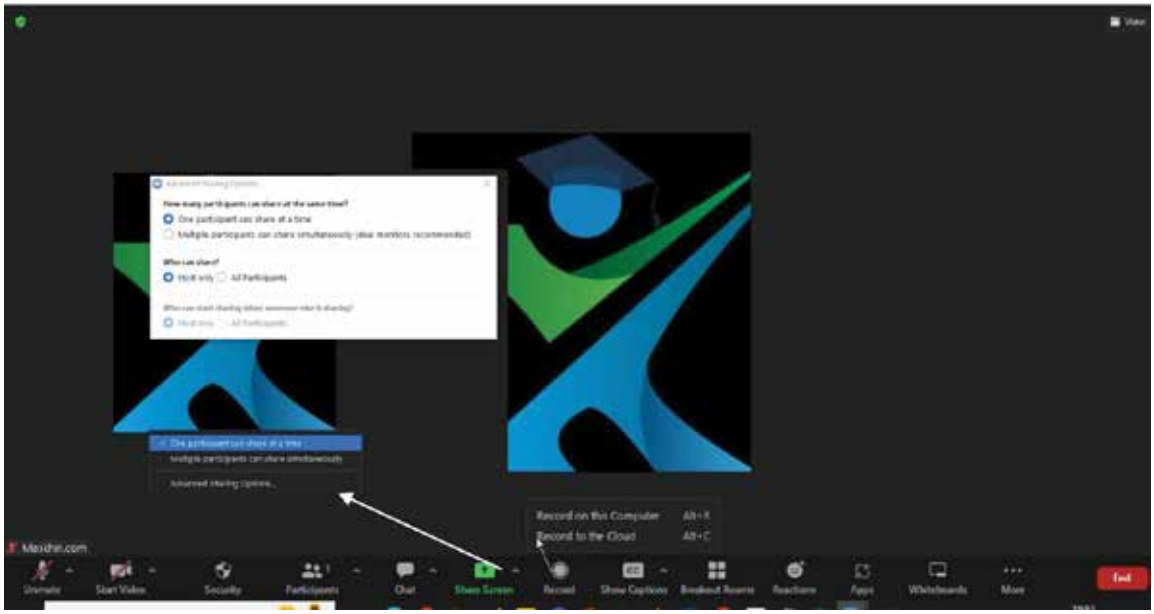
8. Ijinkan Memulai Video
Jika Fitur ini diaktifkan maka, semua peserta bisa leluasa mengaktifkan camera saat pertemuan. Dan Sebaliknya, peserta juga leluasa untuk mematikan camera saat pertemuan.

9. Ijinkan Berbagi Papan Tulis
Jika fitur ini diaktifkan maka semua peserta bisa memanfaatkan papan tulis (whiteboard) yang terdapat pada fitur aplikasi zoom.

10. Menghentikan Peserta dari Ruang Meeting
Pada menu tersebut tercetak/tertulis warna merah, artinya sangat berhati-hati ketika memanfaatkan fitur tersebut. Begitu salah satu peserta di-'suspend', artinya peserta tersebut secara dipaksa untuk keluar dari ruang meeting, dan tidak bisa masuk kembali ke dalam ruang meeting tersebut, sesuai yang dilakukan oleh HOST ketika mengeluarkannya.

Pengaturan Fitur Tambahan sebagai Fasilitas Utama dalam pertemuan Zoom.

Fitur – fitur Tambahan ini seperti Ijin Live Chat, Streaming dan Ijin Merekam saat pertemuan berlangsung. Perhatikan contok fitur tambahan pada Gambar 2.11 di Bawah.



Beberapa Fitur Tambahan Zoom

Praktik Pengaturan Privasi dan Keamanan pada Aplikasi WhatsApp (WA)

Tampilan Aplikasi WhatsApp di berbagai Perangkat
(Sumber : https://faq.whatsapp.com/)

WhatsApp secara default mengatur pengaturan privasi Anda untuk memungkinkan:

- Setiap pengguna dapat melihat terakhir dilihat dan online, foto profil, info, dan laporan dibaca Anda
- Kontak dapat melihat pembaruan status Anda
- Setiap pengguna dapat menambahkan Anda ke grup

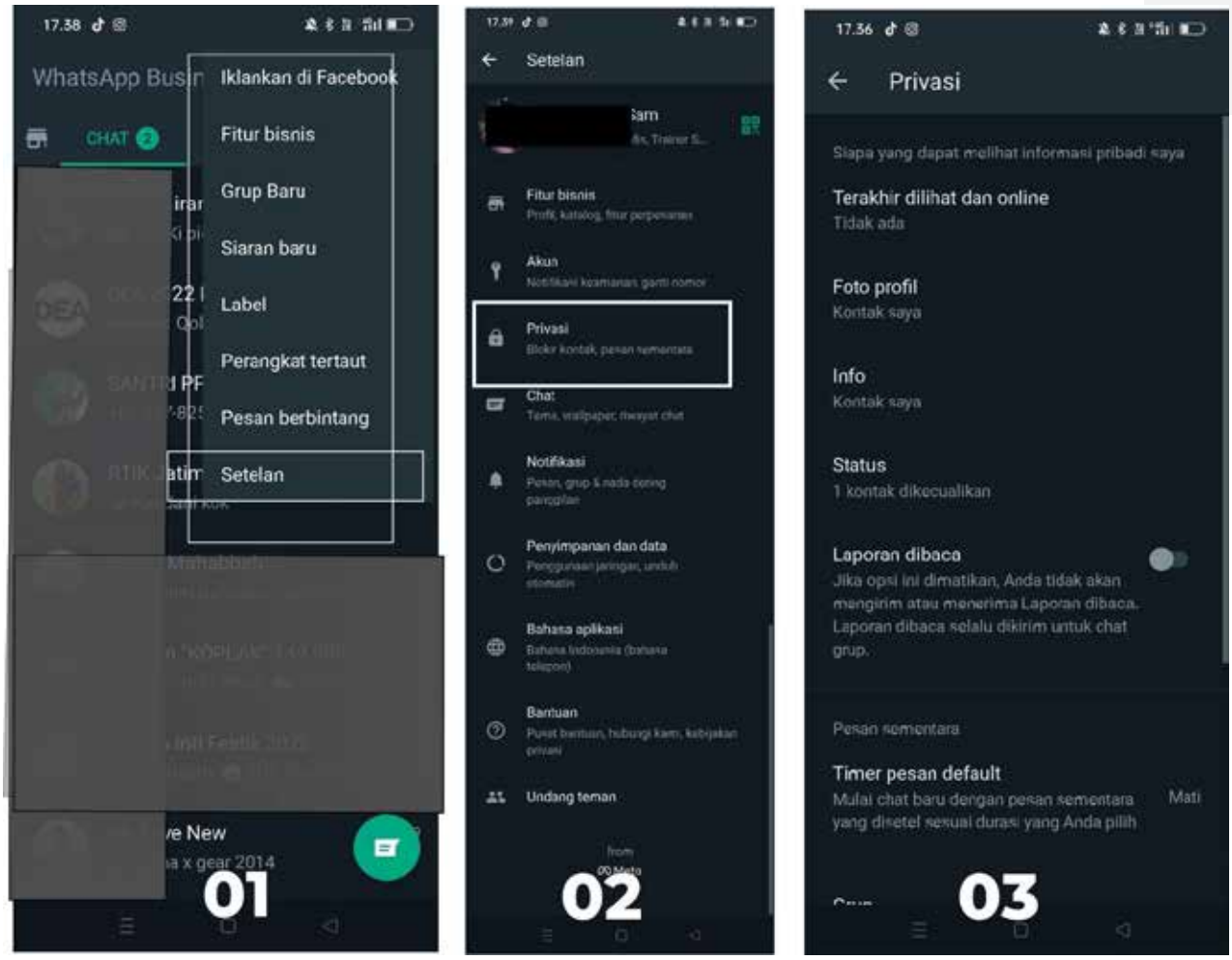
Mengubah pengaturan privasi WA

1. Di :

- Android: Ketuk Opsi lainnya > Setelan > Privasi.
- iPhone: Ketuk Pengaturan > Privasi.
- KaiOS: Tekan Opsi > Setelan > Akun > Privasi.
- Desktop: Klik Menu > Setelan > Privasi.

2. Anda dapat mengubah siapa yang dapat:

- Melihat Terakhir Dilihat dan Online Anda
- Melihat Foto profil Anda
- Melihat Info Anda
- Melihat pembaruan Status Anda
- Melihat Laporan dibaca
- Menambahkan Anda ke Grup

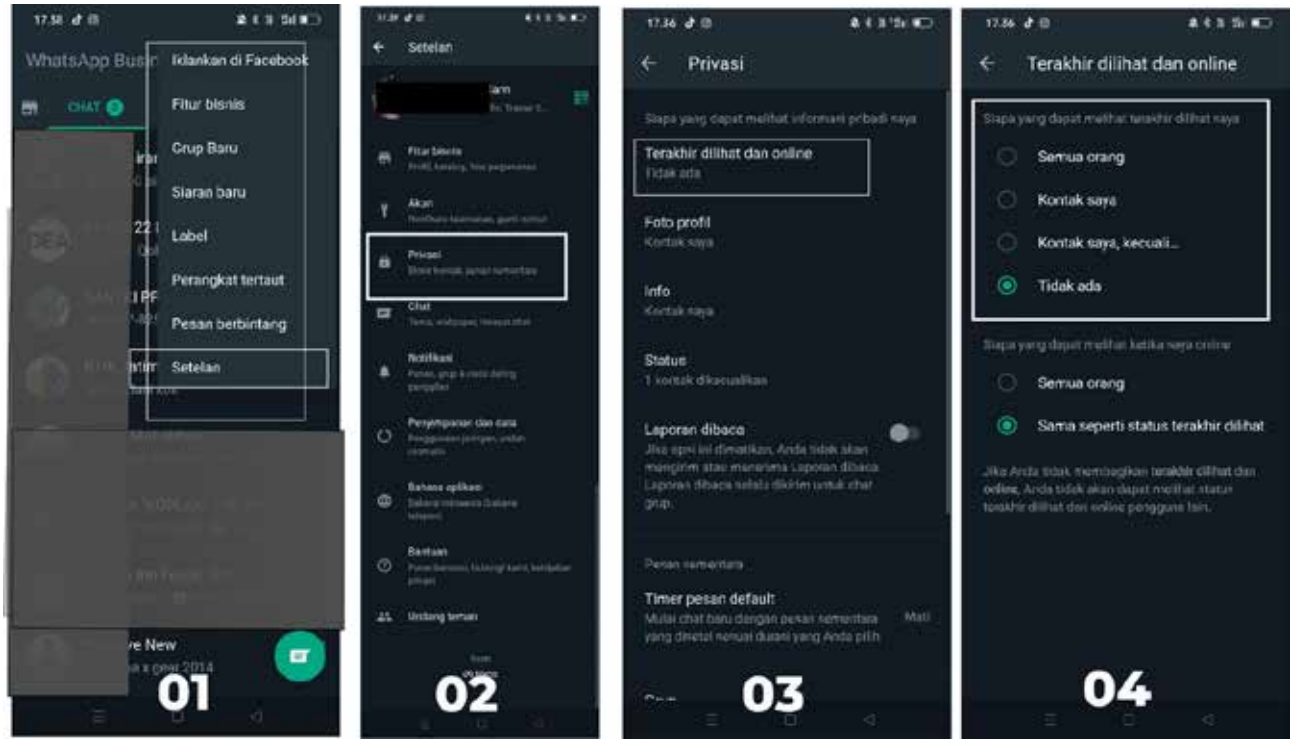


Setting Menu Privasi di WhatsApp (Hasil Tangkapan Layar Penulis)

Catatan:

- Jika Anda tidak membagikan status terakhir dilihat atau online, Anda tidak akan dapat melihat terakhir dilihat atau online pengguna lain.
- Jika Anda mematikan laporan dibaca, Anda tidak akan dapat melihat laporan dibaca pengguna lain. Laporan dibaca selalu dikirim untuk chat grup.
- Jika seorang kontak telah mematikan laporan dibaca, Anda tidak akan dapat melihat apakah kontak tersebut telah melihat pembaruan status Anda.
- Pengguna yang online di utas chat dengan Anda dapat melihat saat Anda mengetik.

Pengaturan Privasi WA: Terakhir dilihat dan Online



Pengaturan Terakhir dilihat dan Online

Terakhir dilihat dan online menunjukkan status kapan terakhir kali kontak Anda menggunakan WhatsApp atau apakah mereka sedang online.

Jika kontak sedang online, berarti kontak tersebut sedang membuka WhatsApp di perangkatnya dan terhubung ke Internet. Namun, bukan berarti kontak telah membaca pesan Anda.

Terakhir dilihat menunjukkan kapan terakhir kali kontak Anda menggunakan WhatsApp. Melalui setelan privasi WA, Anda memiliki opsi untuk mengontrol siapa yang dapat melihat informasi terakhir dilihat dan online Anda. Anda mungkin tidak dapat melihat informasi terakhir dilihat atau online orang lain kecuali mereka telah menyimpan nomor telepon Anda atau sebelumnya pernah mengirimi Anda pesan.

Siapa yang melihat terakhir dilihat saya, Ada 4 Pilihan:

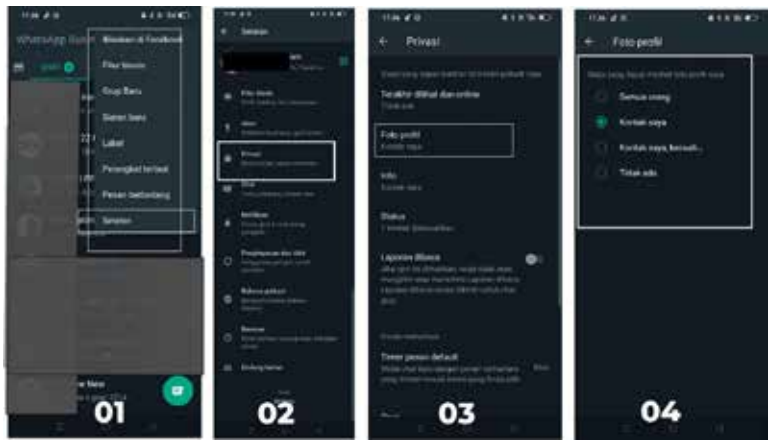
- Semua Orang : Semua orang yg memiliki nomer saya
- Kontak Saya : semua orang yang masuk di kontak saya
- Kontak Saya, Kecuali... : Semua daftar kontak, kecuali seseorang yang tidak boleh lihat.
- Tidak Ada : Semuanya dilarang melihat status terlihat terakhir

Pengaturan Privasi WA: Foto Profil

Pengaturan Privasi Foto Profil menunjukkan siapa saja yang menggunakan WhatsApp yang dapat melihat foto profil kita. Pengaturannya kurang lebih seperti yang tampak pada Gambar 2.15 di bawah:

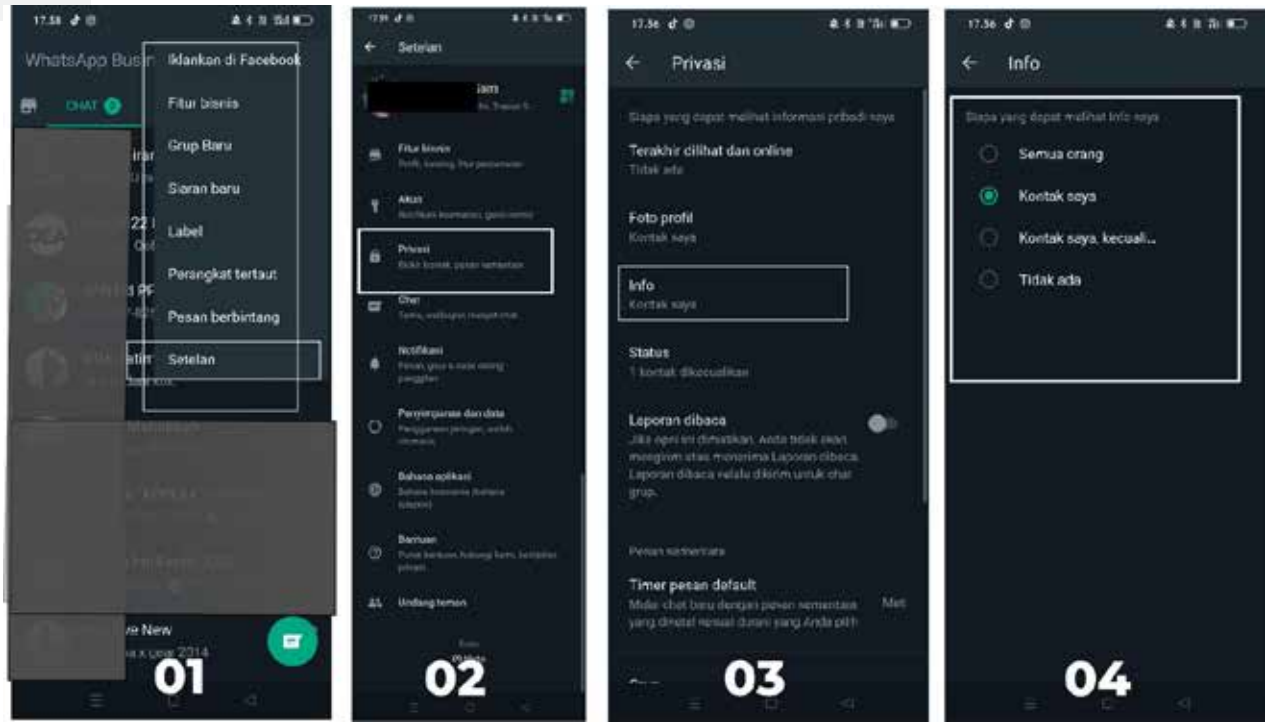
Siapa yang melihat Foto Profil saya, Ada 4 Pilihan:

- Semua Orang : Semua orang yg memiliki nomer saya
- Kontak Saya : semua orang yang masuk di kontak saya
- Kontak Saya, Kecuali... : Semua daftar kontak, kecuali seseorang yang tidak boleh lihat.
- Tidak Ada : Semuanya dilarang melihat Foto profil saya.



Pengaturan Privasi Foto Profil WA

Pengaturan Privasi WA: Informasi WA



Pengaturan Privasi Info WA

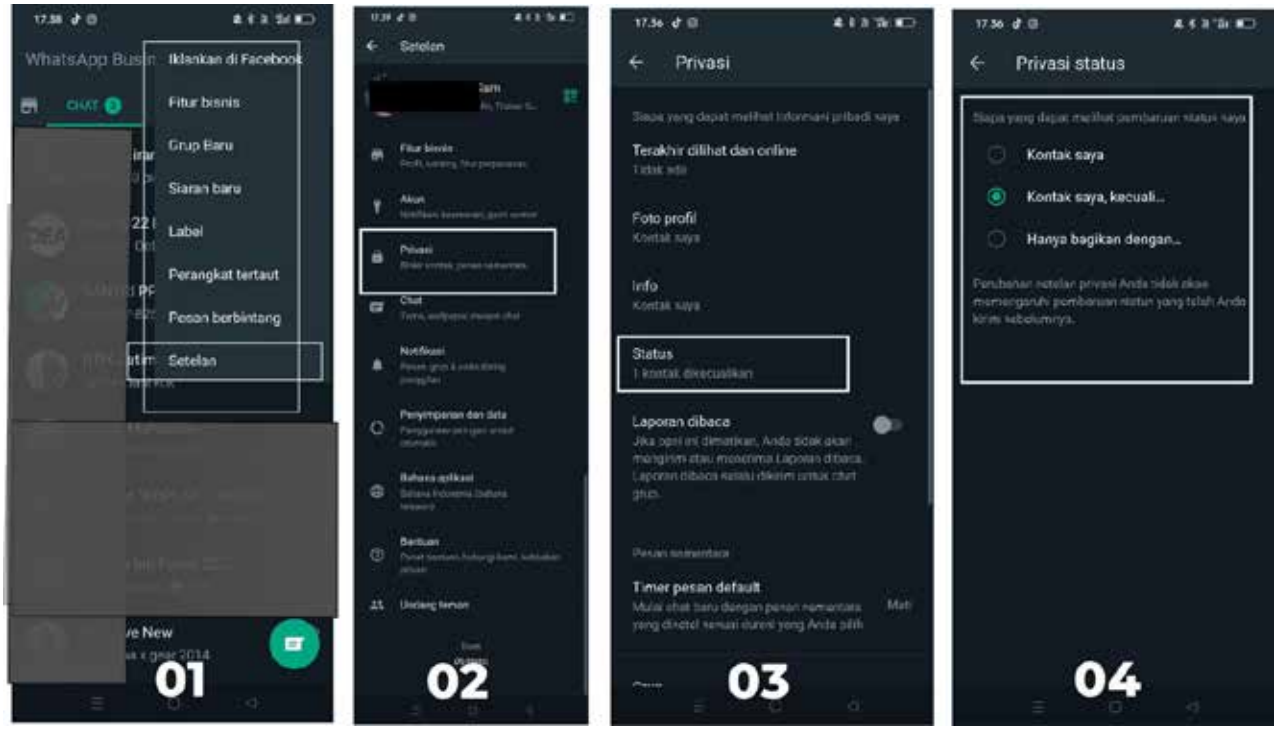
Pengaturan Privasi Informasi WA menunjukkan siapa saja yang menggunakan WhatsApp yang dapat melihat info biografi kita yang kita tuliskan pada WhatsApp kita. Pengaturannya kurang lebih seperti yang tampak pada Gambar 2.16 di atas:

Siapa yang melihat Info saya, Ada 4 Pilihan:

- Semua Orang : Semua orang yg memiliki nomer saya
- Kontak Saya : semua orang yang masuk di kontak saya
- Kontak Saya, Kecuali... : Semua daftar kontak, kecuali seseorang yang tidak boleh lihat.
- Tidak Ada : Semuanya dilarang melihat info biodata saya.

Pengaturan Privasi WA: Status WA

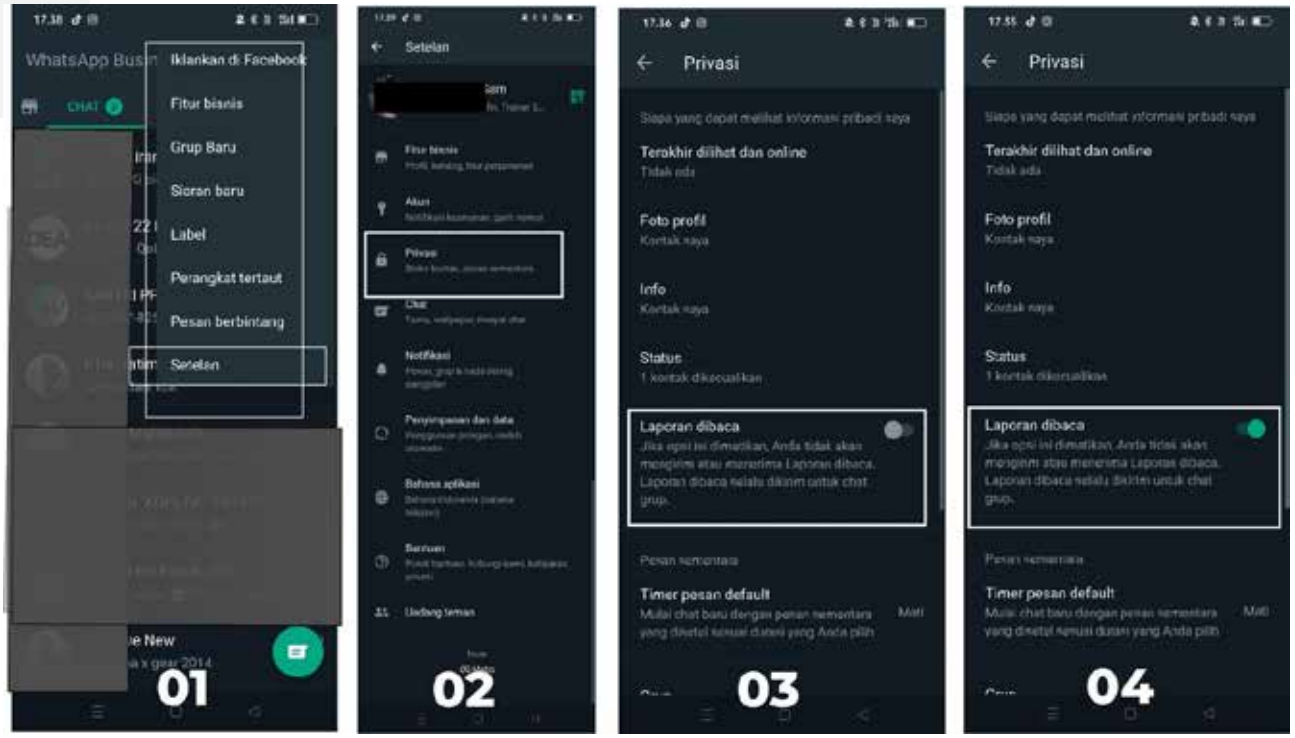
Jika Anda tidak membagikan status terakhir dilihat atau online, Anda tidak akan dapat melihat terakhir dilihat atau online pengguna lain. Pengaturannya kurang lebih sebagai berikut:



Pengaturan Privasi pada Status Saya

Pengaturan Privasi WA: Laporan dibaca

Jika Anda mematikan laporan dibaca, Anda tidak akan dapat melihat laporan dibaca pengguna lain. Laporan dibaca selalu dikirim untuk chat grup. Pengaturannya sebagai berikut.

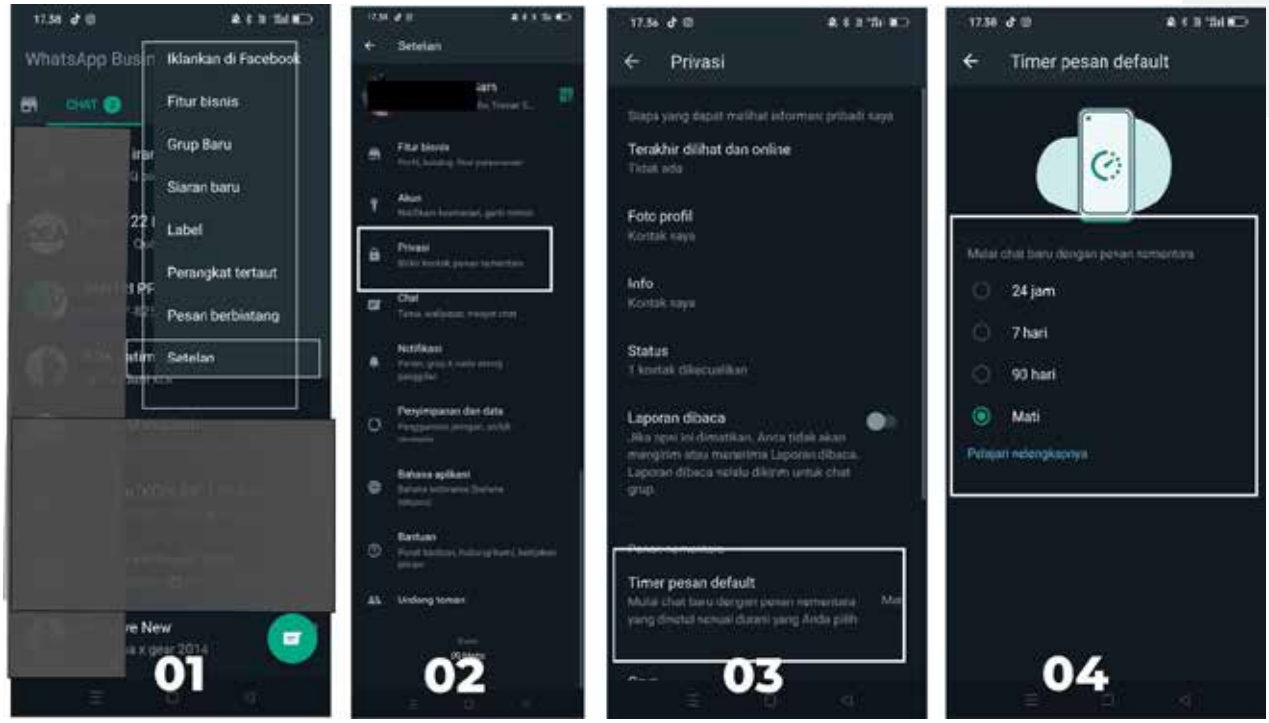


Pengaturan Privasi WA Laporan dibaca

Pengaturan Privasi & Kemanan WA: Timer Pesan Default

Di WhatsApp, Anda dapat mengirim pesan yang akan hilang secara otomatis dengan menyalakan fitur pesan sementara. Anda dapat memilih opsi pesan sementara yang akan hilang setelah 24 jam, 7 hari, atau 90 hari. Anda dapat menyalakan fitur pesan sementara untuk beberapa chat yang sudah ada, dan pesan baru yang dikirim di chat tersebut akan hilang setelah durasi yang dipilih. Setelan yang terbaru akan mengendalikan pesan baru di chat. Pesan yang dikirim atau diterima sebelum fitur pesan sementara dinyalakan tidak akan terpengaruh.

Pengaturannya sebagai berikut:



Setting Pengaturan Timer Pesan Default WA

Menyalakan fitur pesan sementara (Timer Pesan Default) seperti tampak pada gambar 2.19 di atas.

Di chat individual, masing-masing pihak dapat menyalakan fitur pesan sementara. Setelah dinyalakan, pesan baru yang dikirim di chat akan hilang setelah durasi yang dipilih.

1. Buka chat WhatsApp.
2. Ketuk nama kontak.
3. Ketuk Pesan sementara.
4. Jika diminta, ketuk LANJUTKAN.
5. Pilih 24 jam, 7 hari, atau 90 hari.
6. Pilih di chat mana Anda ingin menyalakan fitur ini.
7. Ketuk ✓
8. Ketuk SELESAI.

Pengaturan Privasi & Kemanan WA: Menambahkan ke Group WhatsApp WhatsApp selalu mengizinkan semua pengguna yang memiliki nomor telepon Anda untuk mengirimi Anda pesan atau menambahkan Anda ke grup. Ini serupa dengan bagaimana seseorang dapat mengirimi Anda pesan SMS atau email jika mereka memiliki informasi kontak Anda.

Secara default, setelan privasi grup Anda disetel ke Semua orang agar Anda dapat terhubung secara mudah dengan teman dan keluarga, meskipun mereka tidak ada dalam daftar kontak Anda.

Untuk memberikan privasi tambahan, kami juga telah menambahkan fitur untuk mengendalikan siapa yang dapat menambahkan Anda ke grup dengan menyesuaikan Setelan WhatsApp.

Catatan:

Mengubah setelan privasi grup tidak dapat dilakukan di WhatsApp Web atau Desktop, tetapi setelan dari telepon akan disinkronkan dengan WhatsApp Web dan Desktop.

Cara Mengubah setelan privasi grup:

1. Buka Setelan WhatsApp:
- Android: Ketuk Opsi lainnya > Setelan > Privasi > Grup.
- iPhone: Ketuk Pengaturan > Privasi > Grup.
- KaiOS: Tekan Opsi > Setelan > Akun > Privasi > Grup.

2. Pilih salah satu dari opsi berikut ini:
- Semua orang: Semua orang, termasuk mereka yang tidak terdapat di buku alamat telepon, dapat menambahkan Anda ke grup tanpa meminta persetujuan Anda.

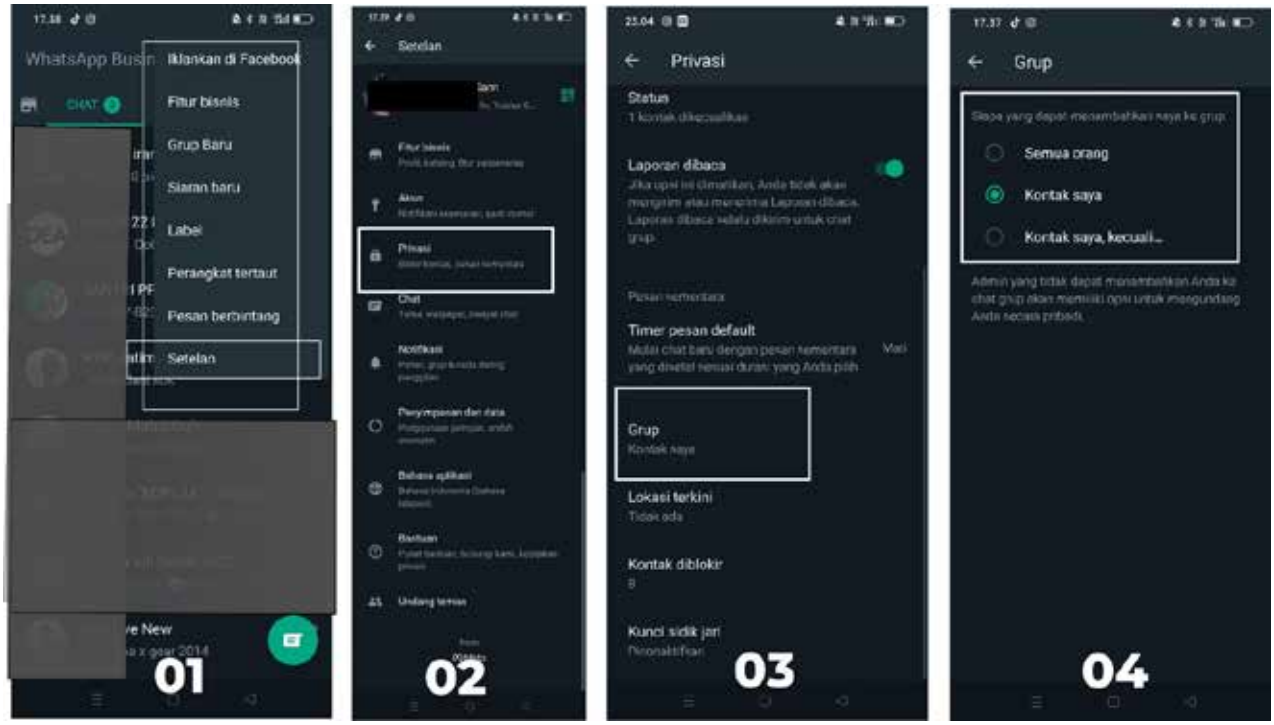
• Kontak saya: Hanya kontak yang terdapat di buku alamat telepon yang dapat menambahkan Anda ke grup tanpa meminta persetujuan Anda. Jika admin grup tidak terdapat di buku alamat telepon dan mencoba menambahkan Anda ke grup, mereka akan mendapat pesan pop-up yang menyatakan mereka tidak dapat menambahkan Anda. Mereka akan memiliki opsi untuk mengundang Anda secara pribadi melalui chat individual dengan mengetuk Undang ke grup atau menekan Lanjut, yang diikuti oleh tombol kirim. Anda akan memiliki waktu tiga hari untuk menerimanya sebelum undangan kadaluwarsa.

• Kontak saya, kecuali...: Selain mereka yang Anda kecualikan, hanya kontak yang terdapat di buku alamat telepon yang dapat menambahkan Anda ke grup tanpa meminta persetujuan Anda. Setelah memilih Kontak saya, kecuali..., Anda dapat mencari atau memilih kontak yang ingin dikecualikan. Jika admin grup yang telah Anda kecualikan mencoba menambahkan Anda ke grup, mereka akan mendapat pesan pop-up yang menyatakan mereka tidak dapat menambahkan Anda. Mereka akan memiliki opsi untuk mengundang Anda secara pribadi melalui chat individual dengan mengetuk Undang ke grup yang diikuti oleh tombol kirim. Anda akan memiliki waktu tiga hari untuk menerimanya sebelum undangan kedaluwarsa.

Image Source: https://www.freepik.com

3. Jika diminta, ketuk SELESAI atau tekan OKE.

Langkah pengaturannya tampak pada Gambar 2.20 Berikut:



Setting Privasi dan Keamanan menambahkan seseorang di Group WhatsApp

Pengenalan tools alternatif Keamanan Data Digital Proton Mail

Layanan Keamanan Digital Proton Mail

Proton Mail adalah layanan surel(email) terenkripsi ujung ke ujung yang didirikan pada tahun 2013 di Jenewa, Swiss oleh para ilmuwan yang bertemu di fasilitas penelitian CERN. Proton Mail menggunakan enkripsi sisi klien untuk melindungi isi surel dan data pengguna sebelum dikirimkan ke peladen Proton Mail, tidak seperti penyedia surel lain seperti Gmail dan Outlook.com. Layanan ini dapat diakses melalui klien webmail, jaringan Tor, atau aplikasi iOS dan Android. (https://id.wikipedia.org/wiki/ProtonMail)

ProtonMail ini juga memiliki beberapa fitur yang menguntungkan dan berguna pagi penggunanya. Misalnya saja dari sistem keamanan yang dirancang untuk menjaga kerahasiaan email dan identitas pengguna.
Dengan menggunakan dan memanfaatkan layanan proton mail, pengguna akan terjamin keamanan dalam penggunaan media email, karena dikutip dari Kompas Tekno mengatakan bahwa fiturnya sudah dilengkapi dengan layanan end to end dan akses nol untuk mengamankan emailnya. Sehingga mereka tidak dapat mendekripsi dan membaca isi surel penggunannya.

JitSi Meet Solusi Alternatif lain selain Zoom

Aplikasi JitSi Meeting ini adalah alternative lain sebagai aplikasi yang digunakan untuk melakukan pertemuan virtual selain zoom, Google Meet, Microsoft Teams. Aplikasi ini sudah dilengkapi dengan Video Conference yang mendukung kebutuhan anda melakukan pertemuan virtual.

Dikutip dari https://www.icescrum.com/documentation/jitsi/ bahwa prinsipnya Aplikasi ini sifatnya AMAN, Mendukung Video Conference dan yang jelas Gratis karena dibangun dari Aplikasi sumber terbuka (open source).

Jadi, aplikasi ini bisa dijadikan alternative lain selain aplikasi pertemuan yang umumnya dipakai di negara kita. Berikut tampilan aplikasi JitSi Meeting.

Tampilan Aplikasi JitSi Meeting
(Sumber Gambar: https://www.icescrum.com/documentation/jitsi/)

Berkolaborasi Digital melalui Aplikasi Wire

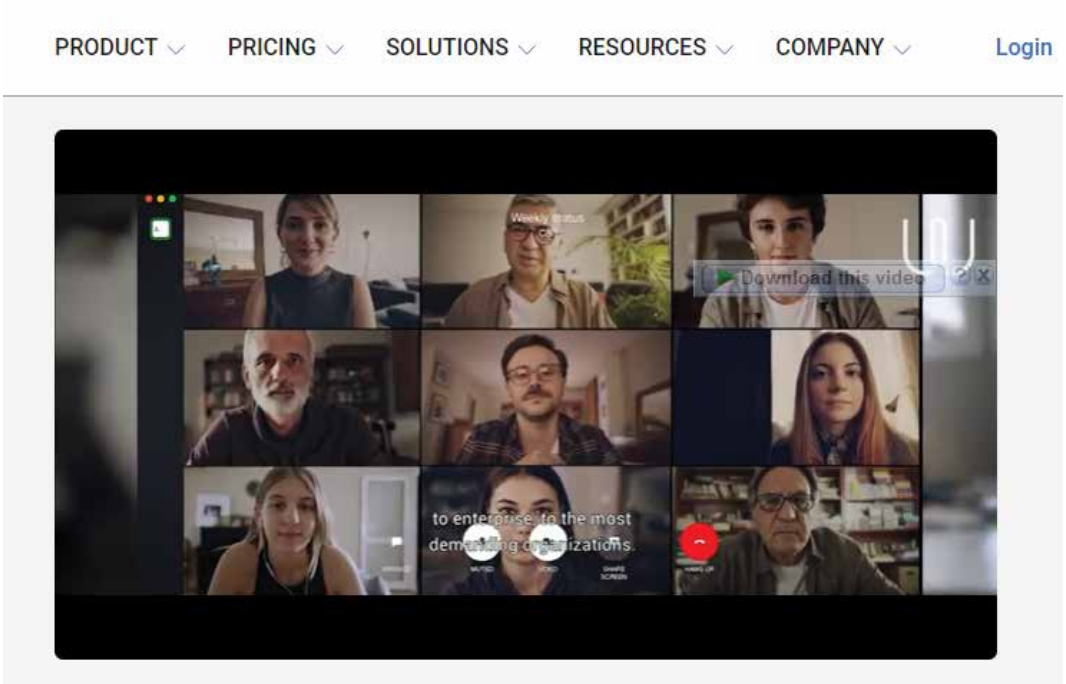
Wire merupakan aplikasi perpesanan dan telepon terbaru yang mampu berjalan di atas platform Android, iOS dan OS X. Aplikasi ini sepertinya fokus dalam desain yang sederhana, berpenampilan minimalis dan memiliki interface yang interaktif untuk memudahkan navigasi. User Interface-nya pun luas, memiliki huruf yang enak untuk dibaca. (https://www.blackxperience.com/)

Berikut Tampilan dan Fitur Aplikasi Wire.

Tampilan dan Fitur Utama Aplikasi Wire (Gambar diolah oleh penulis)

Dari gambar di atas tampak bahwa aplikasi ini sebagai pilihan alternative untuk melakukan kerja – kerja kolaborasi mulai dari chat, telepon, Fitur Group Chat, Voice & Video Conference, Fitur berbagi file secara aman dan dijamin aman sesuai dengan tampilan di website utamanya.

Dibawah ini merupakan fitur tampilan Aplikasi Wire saat Video Conference.

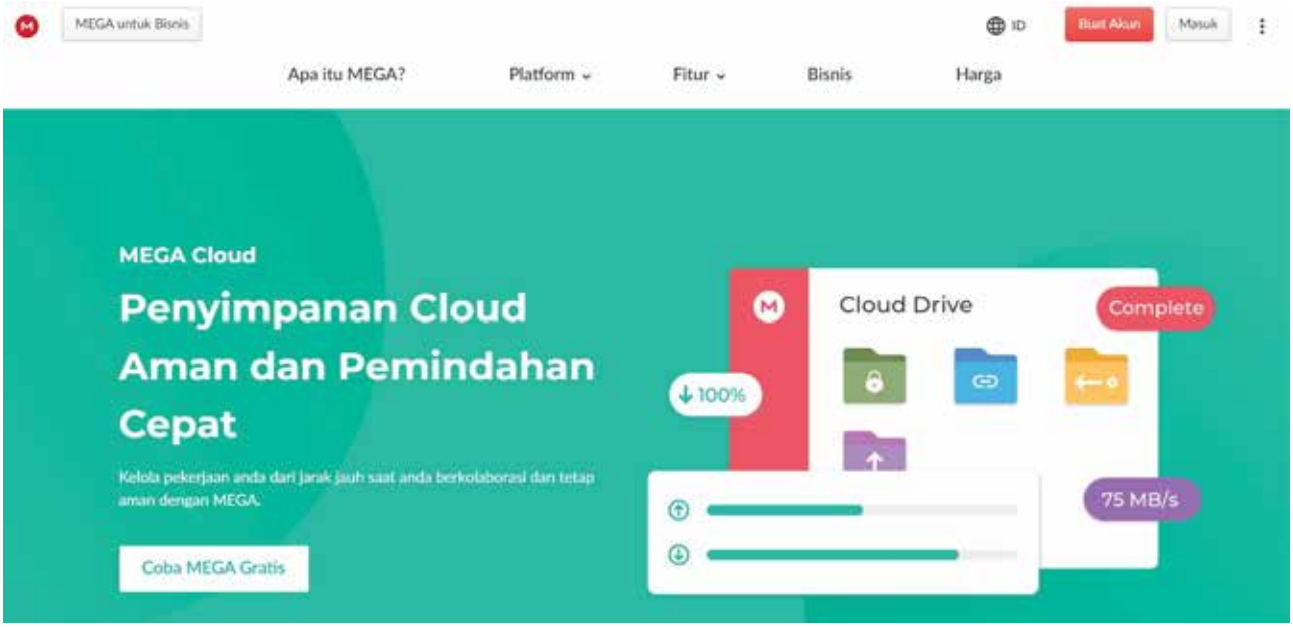


Tampilan Video Confereence Aplikasi Wire
(Sumber : Hasil Tangkap Layar dari website Wire)

Penyimpanan ‘CLOUD’ Mega.io

Sesuai dengan slogan di halaman website utamanya https://mega.io dalam bahasa indonesia disebutkan bahwa Mega Cloud adalah penyimpanan cloud aman dan pemindahan secara Cepat. Diperkuat lagi dengan narasi kelola pekerjaan anda dari jarak jauh saat anda berkolaborasi dan tetap aman dengan MEGA.

Platform ini merupakan platform untuk penyimpanan data secara virtual dalam bentuk awan (cloud) dengan dilengkapi fitur keamanan agar bekerja secara berkolaborasi secara aman dan nyaman. Perhatikan gambar berikut:



Halaman Utama Website Mega.io Bahasa Indonesia

Demikian beberapa pengetahuan dasar tentang kemanan digital beserta praktik secara aman dalam memanfaatkan serta menyelamatkan aset digital kita. Mari terus tingkatkan Literasi Digital agar kita bisa bekerja secara nyaman, aman dan optimal untuk mendukung kehidupan yang sehat, cerdas, kreatif dan produktif di dunia maya dan dunia nyata.

BAB III

DIGITAL AMAN SAAT UNJUK RASA

Teknologi digital dan perangkat elektronik merupakan beberapa komponen penting dalam melakukakan aktivitas saat ini, tidak hanya dalam kehidupan sehari-hari saja, bahkan dalam aksi protes atau unjuk rasa yang pernah dilakukan, teknologi digital menjadi pemicu, membuat aksi semakin meluas dan aksi bisa mendapatkan perhatian di media-media mainstream. Sebagai contoh, aksi protes yang dilakukan di hongkong pada Juni 2019, teknologi bahkan menjadi salah satu penyebab mobilisasi dan memiliki representasi yang menyedihkan sebagai mekanisme penindasan, melalui kampanye pemerintah terhadap pengunjuk rasa, aksi ini semakin meluas dan didengar oleh aktivis-aktivis lain didalam hongkong dan diluar hongkong berkat masifnya pemberitaan aksi di berrbagai sosial media.

Dalam Melakukan aksi protes, seorang atau kelompok aktivis sangat mungkin menjadi sasaran pelacakan digital oleh penegak hukum pada perangkat elektronik mereka. Berbagai sumber menunjukkan Peningkatan penggunaan alat pelacakan digital oleh lembaga penegak hukum; memo khusus dikeluarkan ketika polisi amerika serikat melakukan pengawasan aksi protes masyrakat amerika sebagai buntut tewasnya George Floyd oleh salah satu anggota kepolisian AS ketika melakukan penangkapan. Memo internal yang diperoleh BuzzFeed News menunjukkan DEA (Drugs Enforcement Agency) mulai memata-matai pemrotes pada saat aksi protes dilakukan.

Mereka yang terlibat dalam aksi atau protes damai dapat menjadi sasaran penggeledahan atau penangkapan, gerakan dan asosiasi mereka dipetakan, atau menjadi target pengawasan dan penindasan. Penting bahwa dalam demokrasi, warga negara menggunakan hak mereka untuk berkumpul secara damai, dan para demonstran harus menyadari beberapa tindakan pencegahan yang dapat mereka ambil untuk menjaga diri mereka sendiri dan data mereka tetap aman.

Saat ini, penting sekali memiliki praktik yang baik dalam hal keamanan digital, karena saat ini informasi adalah salah satu aset yang paling berharga. Data atau informasi yang ada pada anda, baik di ponsel maupun di perangkat elektronik lainnya harus di berikan perlindungan, banyak terjadi serangan-serangan digital pada aktivis pada saat mereka melakukan aksinya, Serangan digital adalah segala bentuk gangguan secara tidak sah terhadap aset dan atau identitas digital target, baik secara kasar maupun halus, dengan cara menguasai, mencuri, menyadap, atau menyebarluaskan data-data pribadi target.

Hasil riset dari safenet menunjukkan serangan digital relatif naik pada saat ada momentum tertentu. Empat tahun terakhir, misalnya, puncak serangan itu terjadi ketika ada gerakan nasional menolak revisi UU KPK (2019), pengesahan UU Cipta Kerja (2020), pelaksanaan Tes Wawasan Kebangsaan (TWK) pada staf KPK (2021), dan wacana perpanjangan periode jabatan Presiden Joko Widodo (2022)

Secara sederhana, bentuk serangan digital bisa dibagi menjadi dua berdasarkan metode dan tujuannya, yaitu serangan kasar (hard attack) atau serangan secara teknis (technical attack) dan serangan halus (soft attack) atau serangan secara psikologis (psychological attack)

Meskipun demikian, satu serangan juga kadang bisa memenuhi dua kriteria sekaligus, yaitu serangan secara kasar dan halus. Misalnya Zoom Bombing yang dilakukan dengan cara masuk ke dalam sebuah kegiatan pertemuan Zoom, di mana dia menggunakan identitas palsu untuk masuk dan kemudian mengganggu jalannya kegiatan.

Berikut macam-macam serangan digital yang harus kita ketahui:

1. Serangan kasar (hard attack)

Memerlukan kemampuan teknis dan teknologi relatif tinggi. Serangan dalam metode ini memerlukan perangkat dan aplikasi yang sering kali secara khusus memang didesain untuk melakukan serangan. Baik pelaku maupun korban serangan harus terhubung peralatan dan komunikasi agar serangan itu terjadi.

Berikut beberapa contoh serangan kasar yang biasanya terjadi:

(a) Peretasan (hacking) yaitu upaya memasuki sistem korban secara ilegal untuk tujuan mengambil alih, merusak, atau hanya sekadar melihat sistem dan aset milik korban.

(b) Penyadapan (intercepting) yaitu mengakses komunikasi korban dari jarak jauh untuk mendengar atau mengetahui materi komunikasi tanpa sepengetahuan korban.

(c) Pengawasan (surveillance) yaitu memata-matai aktivitas korban terutama untuk hal-hal yang dianggap mencurigakan.

(d) Pemancingan (phishing) yaitu mengirimkan tautan kepada korban dengan tujuan agar korban membuka tautan yang sebenarnya berisi perangkat lunak jahat (malware)

(e) Distributed denial-of-service (DDoS) Attack yaitu membanjiri peladen target dengan lalu lintas yang sangat banyak sehingga peladen tersebut tidak bisa diakses.

(f) Selain itu ada pula beberapa istilah lain dalam serangan kasar termasuk mengganti tampilan depan situs web (deface), man-in-the-middle (MiTM) attack, dan lain-lain.

1) Hapus fitur biometrik dari ponsel Anda

Jika Anda menggunakan sidik jari untuk membuka kunci posel Anda, kami sarankan untuk ganti fitur keamanan ponsel anda ini dengan metode pin atau passwor. Gunakan password atau pin dengan kombinasi yang sulit tetapi anda bisa mengingatnya, jangan sekali-sekali menggunakan urutan tanggal lahir atau tanggal yang berhubungan erat dengan anda. Meskipun pemindaian sidik jari nyaman dan praktis, pemindaian ini dapat digunakan untuk melawan anda balik. Jika Anda mengambil bagian dalam suatu aksi atau unjukrasa, polisi dapat memaksa Anda untuk membuka kunci ponsel dengan sidik jari Anda. Namun, polisi tidak dapat memaksa Anda untuk memberikan kata sandi telepon jika mereka tidak memiliki surat perintah.

Image Source: https://yourtechdiet.com/

Ingatlah bahwa perangkat digital sangat berharga tidak hanya karena nilai ekonominya, tetapi juga untuk nilai informasi yang dikandungnya. Perlu diingat bahwa Polisi tidak dapat menggeledah ponsel atau prangkat elektronik lainnya tanpa surat perintah. Pengenalan wajah menimbulkan masalah keamanan yang serupa. Polisi bisa saja meminta Anda menggunakan pengenalan wajah untuk membuka kunci ponsel Anda selama protes. Mereka mungkin juga dapat membuka kunci perangkat Anda secara paksa bertentangan dengan keinginan Anda.

2) Gunakan VPN

Image Source: https://www.telkomsel.com/

Alat ini akan mengaburkan aktivitas online Anda, sehingga Anda tidak dapat dilacak.

Upaya Pelacakan aktivitas online dengan Ip addres pernah dilakukan Pada Agustus 2017, pemerintah AS mencoba membuka kedok semua orang yang mengunjungi situs web anti-Trump, yaitu www.disruptj20.org. Situs web disruptj20.org berada dihosting di DreamHost DreamHost didekati oleh agen federal untuk mendapatkan alamat IP dan detail lain dari pengunjungnya. Namun, DreamHost menentang surat perintah yang dikeluarkan oleh pemerintah untuk mendapatkan semua detail pengguna, yang berpotensi menciptakan kegemparan publik. Jika mereka menyerahkan rinciannya kepada pemerintah, rincian ratusan orang akan jatuh ke tangan lembaga pengawasan, alamat IP pengujung situs dapat dilacak kembali ke lokasinya dan aktivitasnya dapat dipantau semua.

Jika Anda ingin tetap aman, yang terbaik adalah menyembunyikan alamat IP Anda. Anda dapat bersembunyi di balik alamat IP lain dengan bantuan VPN. Jaringan pribadi virtual akan memberi Anda IP yang berbeda saat Anda menjelajah internet. Anda dapat memeriksa alamat IP Anda menggunakan website ini; https://www.vpnmentor.com/

Perusahaan hosting dan bahkan ISP (Internet Service Provider) atau Penyelenggara Jasa Internet (PIJI) tidak dapat mendeteksi IP asli di balik IP palsu yang disediakan oleh VPN. Menggunakan VPN juga akan membuat Anda tetap aman dari peretas.

3) Enkripsi penyimpanan ponsel Anda

Image Source: https://blog.hitechcomputer.co.id/

Enkripsi melindungi data di ponsel Anda dan perangkat lain. Anda bisa mendapatkan enkripsi disk penuh untuk memastikan bahwa setiap file di penyimpanan Anda diamankan. Saat Anda menggunakan VPN, data yang dikirim dan diterima oleh komputer Anda dienkripsi. Dengan enkripsi penyimpanan, Anda dapat mengenkripsi data yang disimpan di perangkat Anda. Saat Anda mengenkripsi disk, semua foto, video, pesan teks, dan kata sandi browser Anda akan dienkripsi.

Jika polisi menyita ponsel terenkripsi Anda, mereka tidak akan dapat membaca file pribadi Anda dan melihat foto Anda. Selain itu, ada kemungkinan kehilangan ponsel Anda dalam melakukan aksi. Ini berarti bahwa semua data Anda bisa berakhir di tangan yang salah. Untungnya, semua perangkat Android yang menjalankan Lollipop dan di atasnya dan semua Iphone mulai seri 5s keatas dapat dienkripsi.

Bahkan jika Anda telah mengenkripsi perangkat Anda, pastikan untuk menggunakan kata sandi yang kuat sekitar 10-12 karakter acak. Anda dapat membuat kata sandi yang sangat aman menggunakan platform ini; https://www.vpnmentor.com/tools/secure-password-generator/

4) Ambil foto dan video tanpa membuka kunci perangkat Anda

Image Source: https://heresthethingblog.com/

Mengambil foto ataupun video dalam sebuah aksi bisa menjadi data dan rekaman moment sejarah dalam aksi anda, Jika Anda telah memilih kata sandi yang kuat, memasukkannya ke dalam perangkat membutuhkan waktu yang lumayan lama atau tidak praktis, dan Anda bisa kehilangan moment berharga dalam aksi anda karna hal tersebut, Untungnya, versi iOS dan Android yang lebih baru memungkinkan Anda mengambil foto dan video tanpa membuka kunci perangkat, memberi Anda waktu lebih cepat untuk mengabadikan momen.

Dengan perangkat Android, anda bisa melakukan settingan pengambilan foto dan video pada saata layer terkunci dengan menekan dua kali tombol daya. Di layar kunci iOS, Anda dapat menggesek ke kiri.

5) Cadangkan data Anda

Image Source: Ist/Net

Mencadangkan data Anda secara teratur dan menyimpan cadangan itu di tempat yang aman dapat membuat anda merasa sedikit aman ketika hanphone anda hilang saat melakukan aksi. Anda bisa mencadangkan data anda dilayanan backup data cloud yang ada

6) Bawa ponsel kosong

Image Source: https://www.xataka.com/

Jika ponsel Anda disita oleh polisi, mereka dapat memindai teks, foto, video, dan aplikasi Anda.Untuk memastikan data Anda aman bahkan jika perangkat Anda disita, gunakan ponsel yang tidak terdapat informasi atau data-data penting anda didalamnya,atau anda bisa gunakan hanphone baru yang memang tidak akan digunakan dalam waktu yang lama (burner phone). Sebaiknya beli ponsel pay-as-you-go atau ponsel sekali pakai yang murah dan bayar waktu isi ulang dengan uang tunai. Tinggalkan smartphone anda di rumah selama aksi Anda.

7) Nyalakan mode pesawat

Image Source: https://img.okezone.com

Setelah Anda berkoordinasi dengan teman-teman Anda dan bertemu satu sama lain, Anda mungkin tidak perlu mengirim pesan kepada mereka. Tentukan tempat di mana Anda dapat bertemu jika teman-teman Anda terpisah. Saat Anda semua bersama-sama, letakkan ponsel dalam mode pesawat. Dengan cara ini, perangkat Anda akan berhenti mentransmisikan saat Anda melakukan aksi.

8) Jangan membawa ponsel

Jika Anda ingin bertemu teman-teman Anda pada saat aksi, Anda dapat mendiskusikan dan menyepakati tempat pertemuan dengan teman-teman Anda sejak dini dan berkumpul di sana. Mungkin hal ini merupakan cara komunikasi yang kurangg nyaman saat ini, tetapi cara ini sangat ampuh menghindari anda dari serangan digital. “Lahh, wong gak bawa HP”

Image Source: https://www.freepik.com

9) Tinggalkan media sosial mainstream

Jika Anda berencana terlibat dalam aksi atau unjuk rasa, ada baiknya Anda sementara tidak terlibat aktif dalam sosial media seperti Facebook dan Twitter. Meskipun platform media sosial ini akan memberi Anda banyak eksposur seperti like, dukungan dan komentar media sosial ini juga memiliki risikonya sendiri. Lembaga penegak hukum dapat dengan mudah melihat halaman yang anda sukai, acara yang akan anda ikuti, bahkan melacak dan memeriksa semua orang dekat atau yang intens berkomunikasi dengan anda.

Image Source: https://www.freepik.com

10) Pertimbangkan untuk menggunakan kendaraan umum, bersepeda atau berjalan ketika ikut aksi

Image Source: ANTARA FOTO/Aprillio Akbar/pras.

Saat ini jalan-jalan umum dan beberapa titik favorit dalam melakukan aksi menggunakan Automated License Plate Reader Systems (ALPR) alat ini secara otomatis merekam pelat nomor mobil atau motor yang melewati suatu area secara realtime , tanggal, dan lokasinya. Teknologi ini sering digunakan oleh penegak hukum, atau digunakan oleh perusahaan swasta yang kemudian berbagi data plat nomor dengan penegak hukum dan entitas lain. Dikumpulkan dalam database besar, data ini disimpan untuk jangka waktu yang tidak diketahui dan dapat digunakan melacak anda apabila anda menjadi target operasi penegak hukum

BAB IV

JAGA JEJAK DIGITAL DAN LAWAN HOAKS

Merawat jejak digital adalah proses mengontrol dan mengelola informasi yang diterbitkan di internet tentang diri kita. Hal ini penting karena informasi yang diterbitkan di internet dapat digunakan oleh berbagai pihak, seperti perusahaan, kampanye politik, atau bahkan penipu. Dengan merawat jejak digital, kita dapat memastikan bahwa informasi yang diterbitkan di internet tentang diri kita akurat, profesional, dan mencerminkan identitas kita yang sebenarnya.

Selain itu, melawan hoaks adalah hal yang penting untuk dilakukan dalam era digital saat ini. Hoaks adalah informasi yang tidak benar atau tidak sah yang disebarluaskan melalui internet, yang dapat menimbulkan kerugian bagi individu atau masyarakat. Melawan hoaks dapat dilakukan dengan mengecek keabsahan informasi sebelum menyebarluaskannya, serta menyebarkan informasi yang akurat dan terpercaya.

Kedua hal ini sangat penting untuk dilakukan agar kita dapat menjaga reputasi kita di dunia maya dan menghindari kerugian yang mungkin timbul dari penyebaran informasi yang tidak benar. Selain itu, merawat jejak digital dan melawan hoaks juga dapat membantu dalam membangun masyarakat yang lebih baik dan lebih memiliki kemampuan berpikir kritis dengan peendekatan literasi digital

A. MERAWAT JEJAK DIGITAL

Jejak digital merupakan segala informasi atau rekam jejak data maupun aktivitas seseorang saat mengakses internet. Jejak digital terbagi menjadi 2, yakni jejak digital pasif dan jejak digital aktif.

- **Jejak Digital Pasif :** Data atau informasi yang ditinggalkan tanpa disadari, seperti rute pada Google Maps, riwayat pencarian, situs yang dikunjungi, transaksi belanja, riwayat telepon, dll

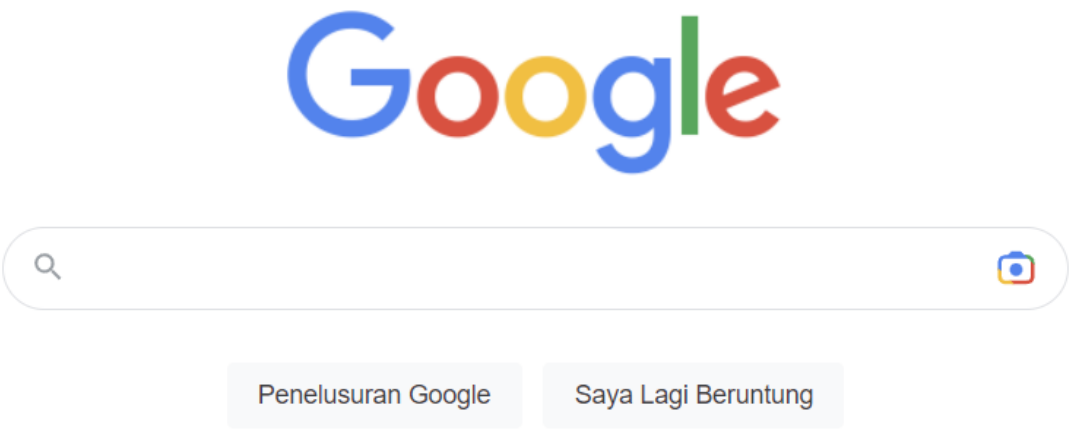
- **Jejak Digital Aktif :** Data atau informasi yang ditinggalkan dengan sengaja, seperti unggahan foto/video, status di media sosial, testimoni produk/jasa, percakapan di aplikasi perpesanan, dll

Bahaya Jejak Digital

1. **Pencurian identitas** seperti nama, nomor telepon, hingga kartu kredit tanpa izin untuk melakukan penipuan atau kejahatan lainnya.
2. Penyebaran informasi seseorang baik individu maupun kelompok kepada publik **(Doxing)** sehingga menimbulkan perspektif **(Framing)** yang salah terhadap pemilik data.
3. **Akses ilegal terkait data pribadi** yang tersimpan di internet.
4. **Pencemaran nama baik** atau penghinaan

Tips Mengelola Jejak Digital

1. Telusuri diri sendiri. Coba untuk menelusuri nama Anda di Google untuk melihat informasi apa yang akan muncul dan terekam di internet.



5. Kelola Akun Google. Dengan Akun Google, Anda dapat mengelola informasi seperti biodata, detail kontak, dan informasi lain tentang Anda yang dapat orang lain lihat di layanan Google.

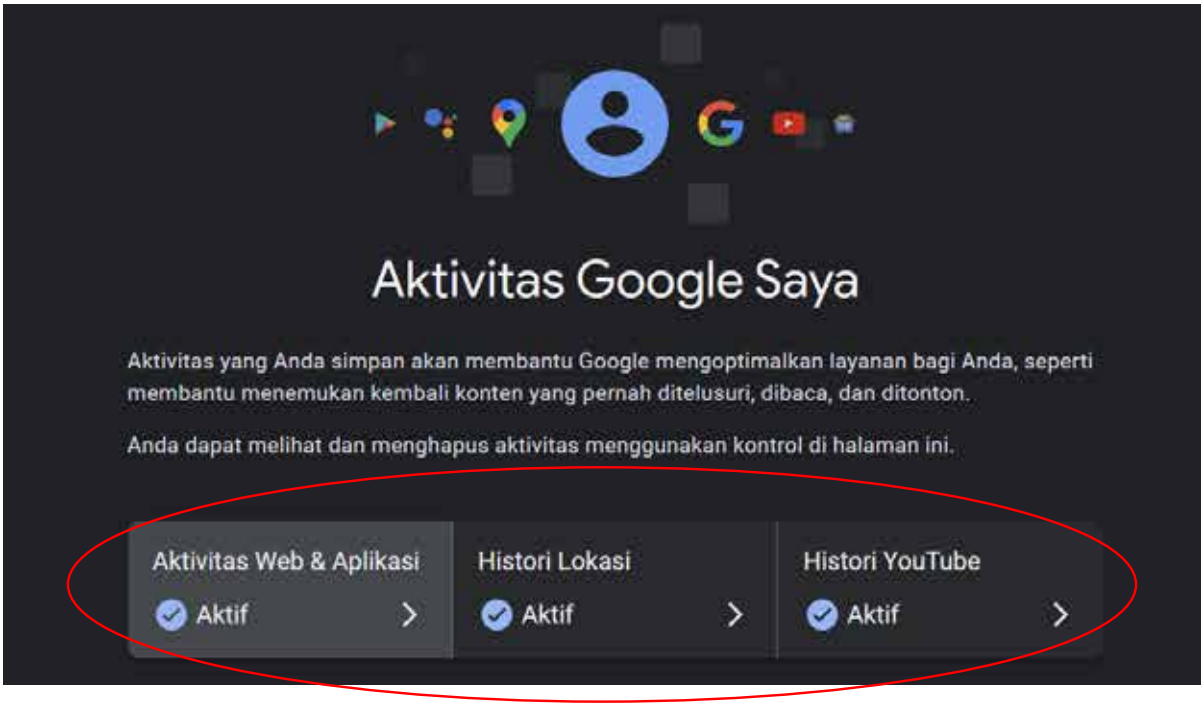
6. Hapus konten dan hasil penelusuran terkait yang tidak diinginkan. Jika Anda menemukan konten online seperti, nomor telepon atau foto Anda yang memalukan yang tidak ingin dimunculkan secara online, tentukan terlebih dahulu apakah Anda atau orang lain mengontrol konten tersebut.

4. Jika konten yang tidak diinginkan berada pada situs atau halaman yang tidak Anda kontrol, Anda dapat meminta Google untuk menghapus informasi pribadi dari Google dengan mengisi formulir Permintaan Penghapusan yang ada pada s.id/hapusdarigoogle

Adapun fitur ini dapat membantu Anda untuk:

- Menghapus gambar pribadi non-konsensual yang vulgar atau intim dari Google
- Menghapus pornografi palsu yang disebarluaskan tanpa izin dari Google
- Menghapus konten tentang Anda pada situs yang menerapkan praktik penghapusan eksploitatif dari Google
- Menghapus informasi identitas pribadi (PII) atau konten penyebaran informasi pribadi tertentu dari Google Penelusuran
- Menghapus gambar anak di bawah umur dari hasil penelusuran Google
- Menghapus pornografi yang tidak relevan dari hasil penelusuran Google untuk nama Anda

5. Anda dapat menonaktifkan histori penelusuran dengan mengontrol aktivitas pada Google dengan melalui tautan https://myactivity.google.com/

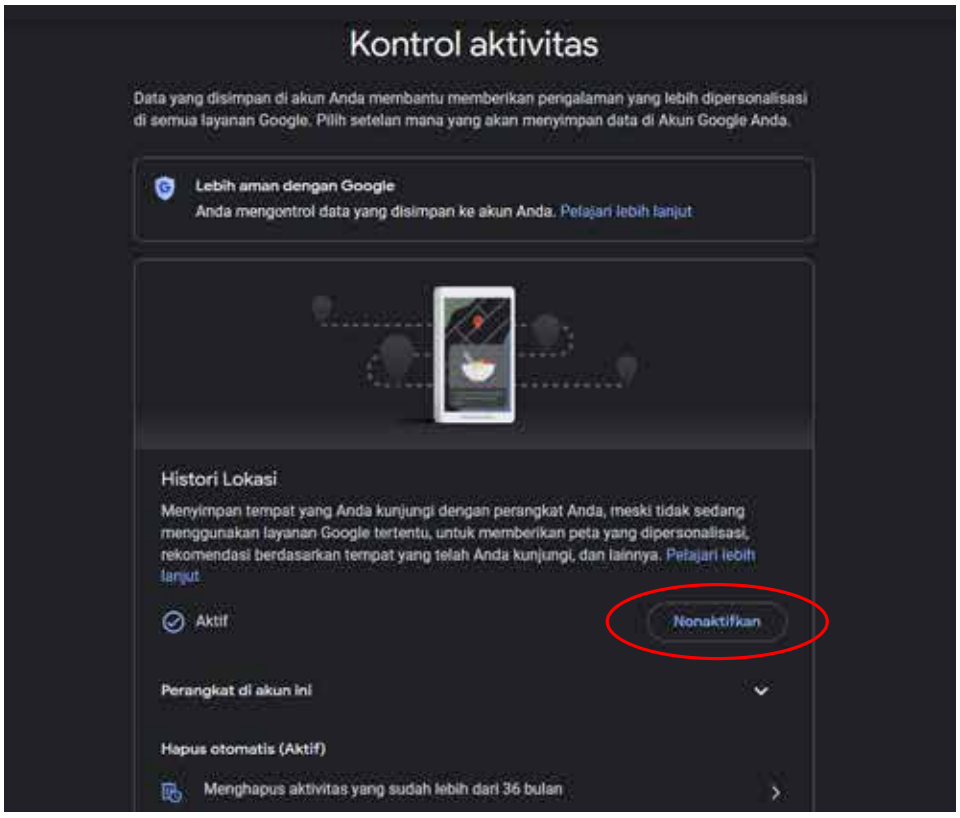


z• Mengontrol aktivitas pada web dan aplikasi

Pilih bagian Aktivitas Web & Aplikasi – kemudian klik tombol Nonaktifkan

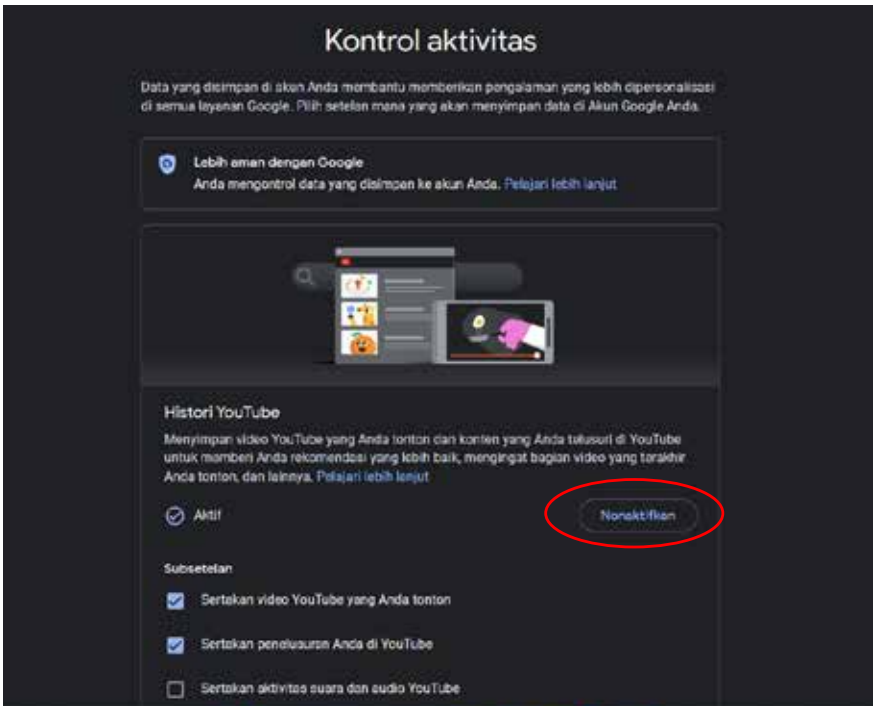
• Mengontrol histori lokasi

Pilih bagian Histori Lokasi – kemudian klik tombol Nonaktifkan



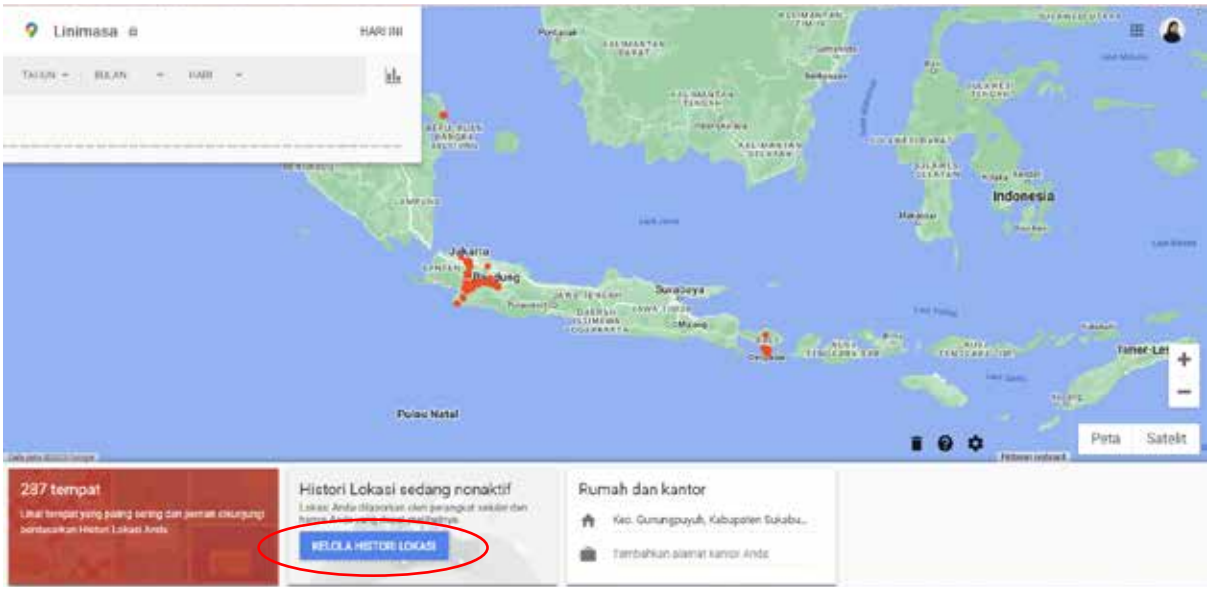
• Mengontrol histori di YouTube

Pilih bagian Histori YouTube – kemudian klik tombol Nonaktifkan



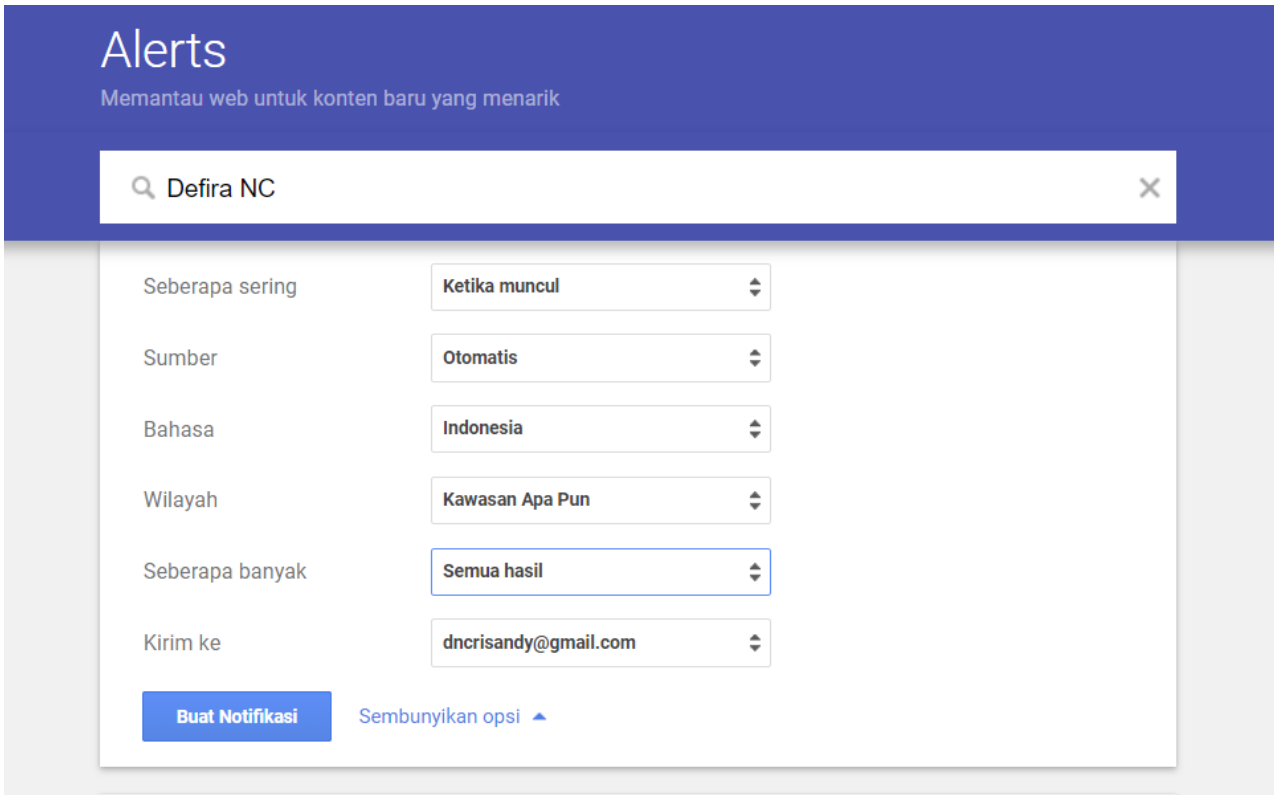
6. Mengelola linimasa/histori lokasi

Anda dapat menonaktifkan histori lokasi melalui tautan https://google.com/maps/timeline



7. Periksa jejak digital Anda melalui https://alerts.google.com

Google Alerts dapat memberi tahu Anda jika terdapat berita baru tentang Anda di internet melalui surel (email). Anda cukup mengisi kolom pencarian dengan menulis nama Anda sendiri dan pilih “Buat Notifikasi”



B. MELAWAN HOAKS

“Eh, kamu tau gak sih....”

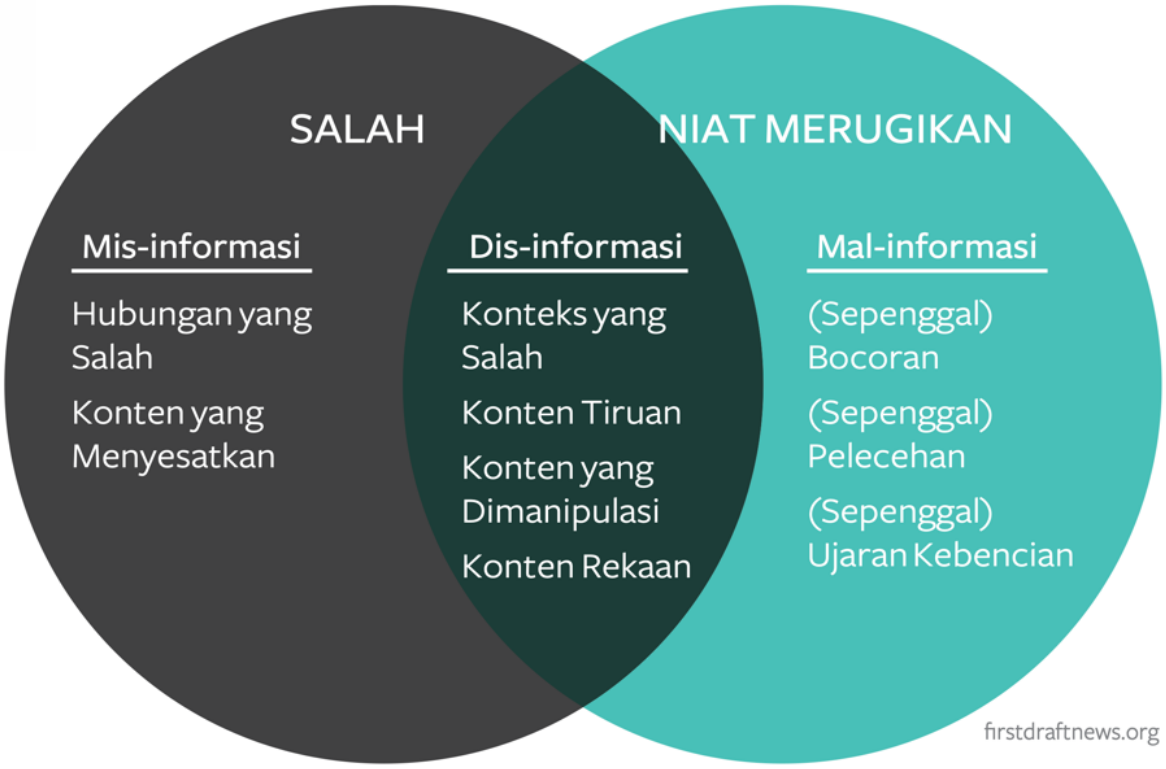
“Ih gak nyangka yah, ternyata dia...”

“Kemarin ya saya dengar, katanya...”

Hoaks menyebar begitu cepat, dimulai dari “katanya” dan terdistribusi secara masif dari mulut ke mulut atau saat ini dari jari ke jari (melalui media social). Sebenarnya apa yang dimaksud dengan hoaks? Secara umum hoaks dapat didefinisikan sebagai **suatu informasi yang tidak benar yang dibuat seolah-olah benar sehingga dapat dipercaya oleh orang lain.** Kata hoaks sendiri diduga pertama kali mulai populer digunakan pada pertengahan hingga akhir abad ke-18, berasal dari frasa hocus pocus yang merupakan istilah dalam dunia sulap menyulap.

UNESCO (2019) menerbitkan buku “Jurnalisme, “berita palsu”, & disinformasi: buku pegangan untuk pendidikan dan pelatihan jurnalisme”[1], yang membagi hoaks dalam tiga kategori: misinformasi, disinformasi dan mal-informasi. **Misinformasi** adalah informasi salah yang disebarkan oleh orang yang mempercayainya sebagai hal yang benar. Sementara, disinformasi adalah informasi salah yang disebarkan oleh orang yang tahu bahwa informasi itu salah. **Disinformasi** adalah kebohongan yang disengaja dan berkenaan dengan orang-orang yang disesatkan secara aktif oleh aktor jahat. Kategori ketiga bisa disebut **mal-informasi,** yaitu informasi yang berdasarkan realitas, tapi digunakan untuk merugikan orang, organisasi, atau negara lain. Biasanya dengan menggunakan informasi yang dipenggal.

[1] Jurnalisme, “berita palsu”, & disinformasi: buku pegangan untuk pendidikan dan pelatihan jurnalisme; https://unesdoc.unesco.org/ark:/48223/pf0000368022



Selain itu "kekacauan informasi" *(information disorder)* ini juga dapat dikelompokkan menjadi 7 jenis:

1. Satire atau Parodi

Informasi yang dibuat untuk menyatakan sindiran terhadap suatu keadaan atau seseorang, biasanya disampaikan dalam bentuk ironi, sarkasme, atau parodi. Satir umumnya dibuat tanpa maksud untuk mengelabui orang yang melihatnya karena hanya bersifat sindiran. Namun, bagi yang tidak memahami gaya bahasa ini dapat terkecoh dan menganggap informasi yang dilihatnya sebagai Sebuah kebenaran, terutama ketika yang menyampaikannya tidak secara jelas menyatakan bahwa informasi tersebut satir.

2. Konten yang Menyesatkan

Penggunaan informasi yang sesat untuk membingkai sebuah isu. Biasanya informasi ditampilkan dengan menghilangkan konteksnya untuk menggiring persepsi publik agar sesuai dengan keinginan pembuat informasi tersebut.

3. Konten Tiruan

Informasi yang dibuat mirip dengan aslinya dengan tujuan untuk mengelabui publik, seperti situs web yang dipalsukan agar pengunjungnya tertipu dan menganggap situs tersebut adalah situs aslinya

4. Konten Palsu

Konten baru yang 100% salah, sengaja dirancang dan dibuat untuk mengelabui pembacanya. Pembuatan konten palsu ini dapat dilatarbelakangi oleh berbagai tujuan, baik keuntungan finansial, propaganda, maupun kepentingan politik, sehingga berpotensi menyesatkan dan bahkan membahayakan masyarakat.

5. Koneksi yang salah

Ketika judul, gambar atau keterangan tidak mendukung konten yang sebenarnya. Salah satu contohnya adalah metoda click bait, membuat judul atau gambar yang mengundang orang untuk mengklik tautan yang tersedia dengan bentuk yang provokatif, menarik dan sensasional, padahal kontennya sendiri tidak “seheboh” judulnya.

6. Kontels yang salah

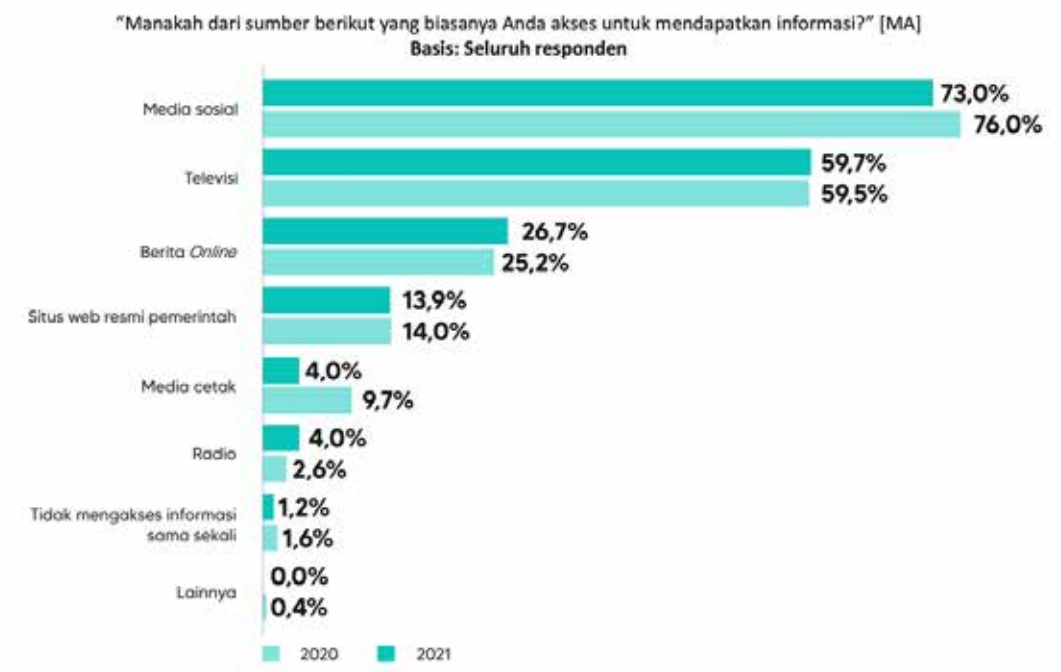
Ketikan konten yang asli disampaikan dalam konteks yang salah, dimana sebuah informasi (tulisan, gambar atau video) yang benar ditempatkan dalam konteks yang tidak sesuai aslinya.

7. Konten yang dimanipulasi

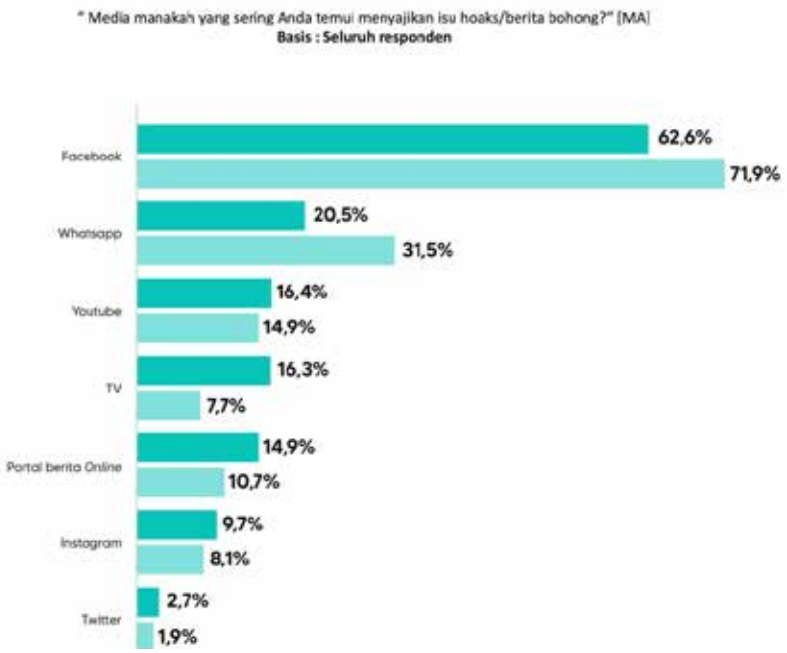
Informasi yang asli dimanipulasi dengan tujuan menipu. Bisa jadi hanya sekedar iseng, tetapi bisa juga bertujuan untuk memprovokasi, menyebarkan propaganda, maupun untuk kepentingan politik.

BAGAIMANA HOAKS MENYEBAR

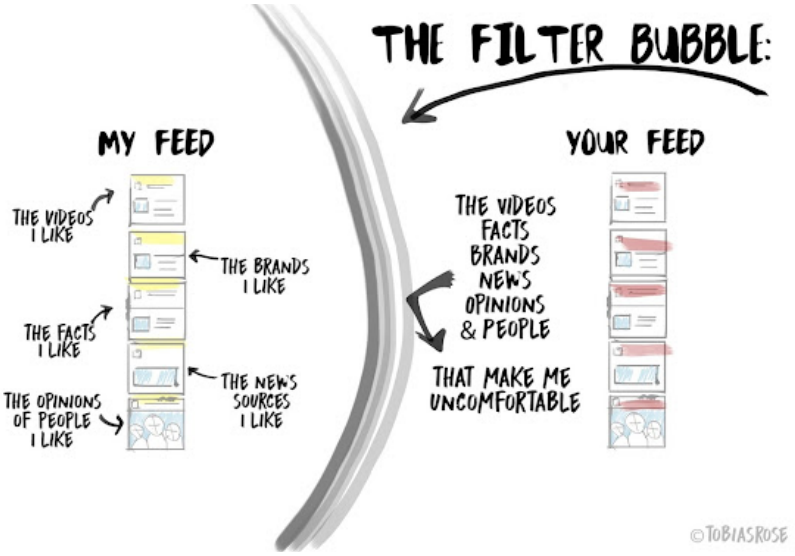
Dalam studi Status Literasi Digital di Indonesia 2021, yang disusun oleh Katadata Insight Center dan Kementerian Komunikasi dan Informatika, disebutkan bahwa pengguna internet di Indonesia sebagian besar (70%) memilih media sosial sebagai sumber untuk mendapatkan informasi.



Akan tetapi, di satu sisi media sosial juga dianggap sebagai media dimana hoaks sering ditemukan.



Media sosial menjadi katalisator dalam penyebaran hoaks. Jumlah pengguna media sosial yang besar memungkinkan penyebaran informasi dengan cepat dan masif. Selain itu media sosial memiliki algoritma yang membuat penggunanya dibuat betah berlama-lama tinggal di platformnya, sebab merasa menjumpai banyak kawan yang, misalnya, memiliki hobi serupa atau memiliki pandangan yang sama. Namun diam-diam, algoritma membuat pengguna media sosial terkotak-kotak.



Algoritma Media Sosial[2]

Jika terus-menerus disuguhi informasi dari satu sudut pandang yang kita sukai saja, maka dikhawatirkan dapat menumbuhkan sikap tertutup untuk dapat menerima sudut pandang lain yang berbeda atau berseberangan dengan keyakinan kita. Akhirnya, pengguna media sosial seolah hidup di dalam ruang bergema (echo chamber) yang senantiasa meyakinkan pandangannya sebagai yang paling benar.

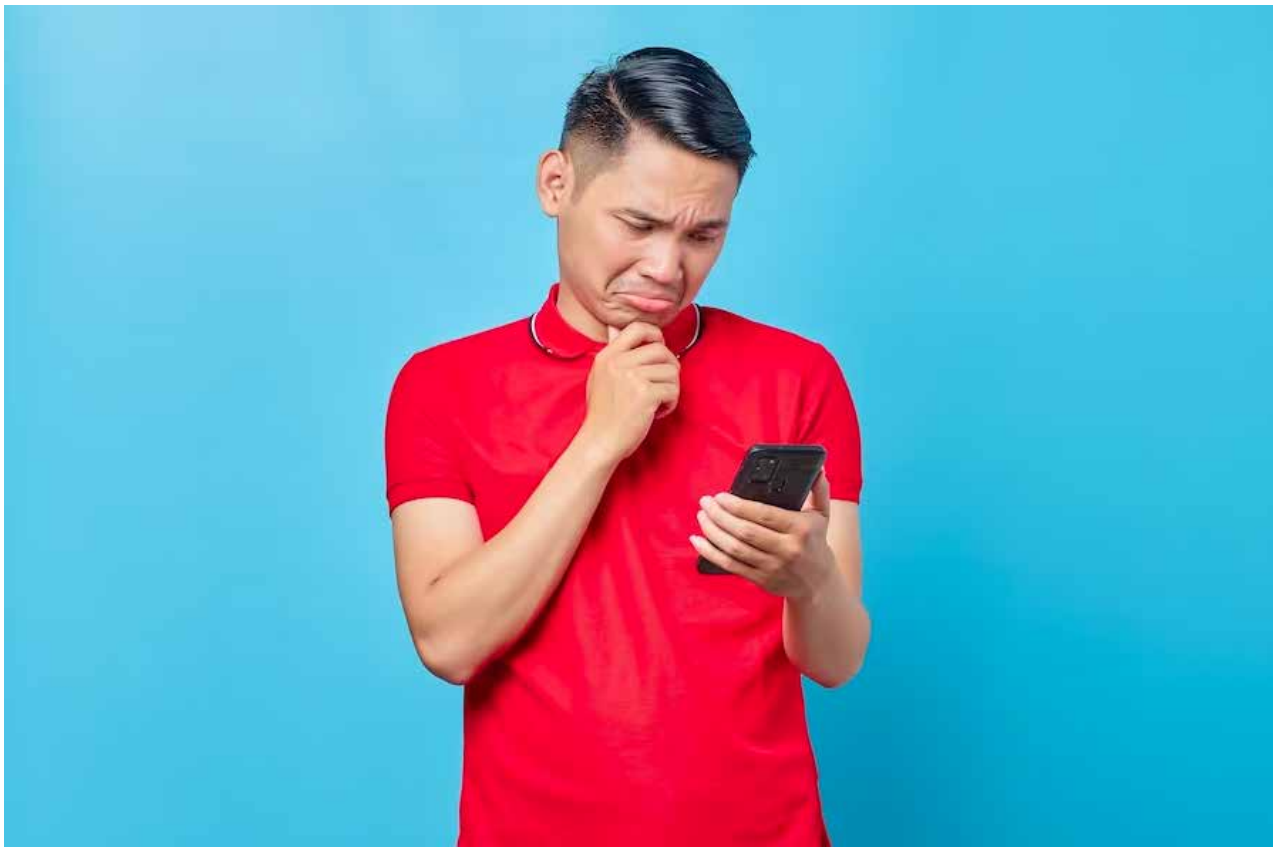
Kepungan echo chamber dikhawatirkan dapat menggerus daya pikir kritis pengguna media sosial. Semua informasi yang dianggap mendukung pendapatnya bakal diyakini sebagai kebenaran. Sebaliknya, informasi yang bertentangan dengan pendapatnya bakal diabaikan dan bahkan dapat

[2] *How We Broke Democracy:*
https://medium.com/@tobiasrose/empathy-to-democracy-b7f04ab57eee

dilabeli sebagai sebuah kebohongan. Maka tidaklah mengherankan apabila hoaks semakin mudah ditemui, tersebar, dan menjadi konsumsi sehari-hari.

Banyak hal yang membuat kita menjadi mudah percaya akan hoaks, berikut beberapa penyebabnya:

- Bisik-bisik tetangga, saudara, kawan
- Mengambil kesimpulan hanya dari judul
- Tidak mencari tahu sumber lain
- Pas dengan perasaan / keyakinan kita
- Sering muncul di WA atau media sosial
- Tergiur iming-iming pahala
- Mudah percaya pada sumbernya

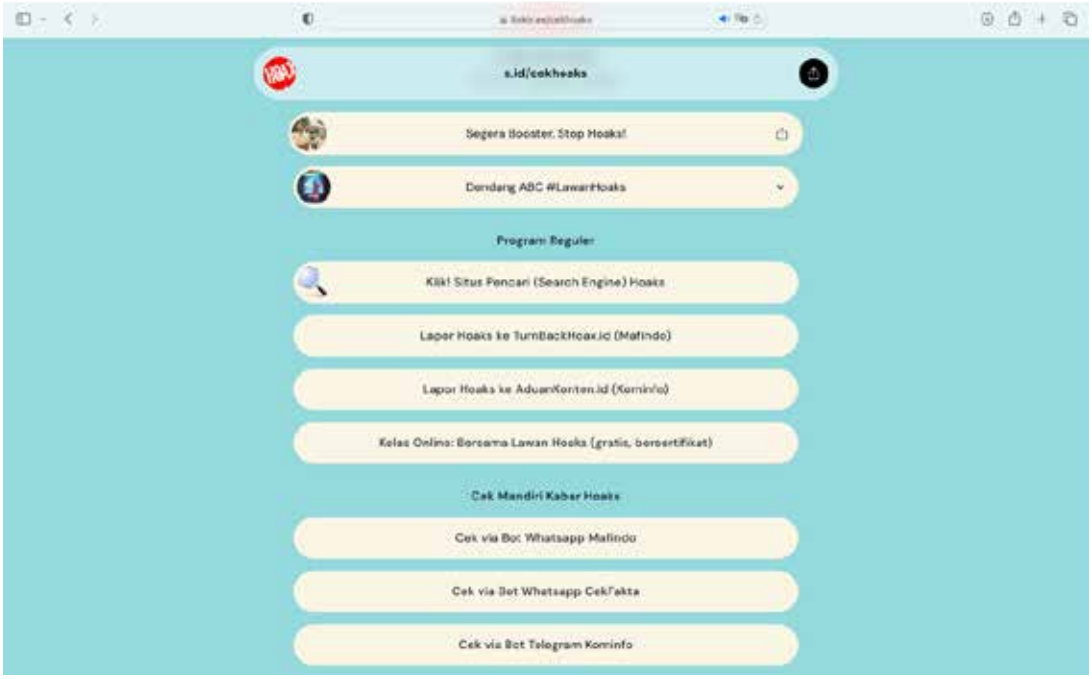


VERIFIKASI HOAKS

Jika ada sebuah informasi yang kita ragukan kebenarannya, maka kita perlu melakukan pemeriksaan terlebih dahulu untuk mengetahui apakah informasinya benar atau hoaks. Walau tidak selalu, akan tetapi beberapa hoaks yang tersebar memiliki ciri-ciri sebagai berikut:

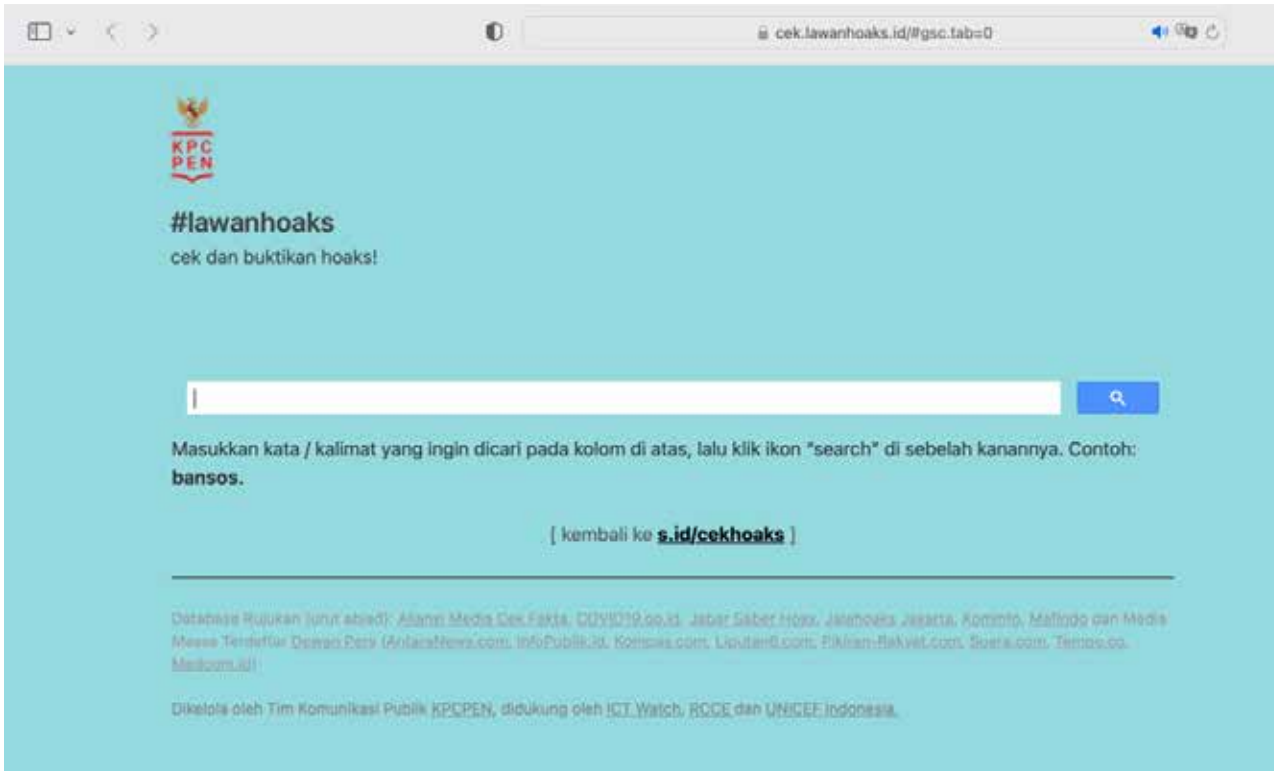
- Kontennya mengaduk emosi: membuat kita sangat gembira, sangat sedih atau marah
- Minta diviralkan: pesan berantai yang biasanya diakhiri dengan perintah untuk menyebarkan
- Tidak jelas sumbernya: tidak memiliki sumber yang jelas, atau laman situs yang tidak jelas pengelolanya
- Mencatut nama orang atau Lembaga terkenal
- Tidak logis: informasinya tidak dapat diterima dengan akal sehat
- Tata Bahasa yang buruk: banyak kesalahan ketik, susunan kalimat yang tidak beraturan, terkadang banyak menggunakan huruf kapital

Banyak tools yang bisa kita manfaatkan untuk melakukan verifikasi hoaks secara mandiri, mulai dari situs web sampai WhatsApp Chatbot. Semua itu bisa kita akses melalui laman https://lawanhoaks.id



Beberapa alat bantu yang bisa kita gunakan di situs ini adalah sebagai berikut:

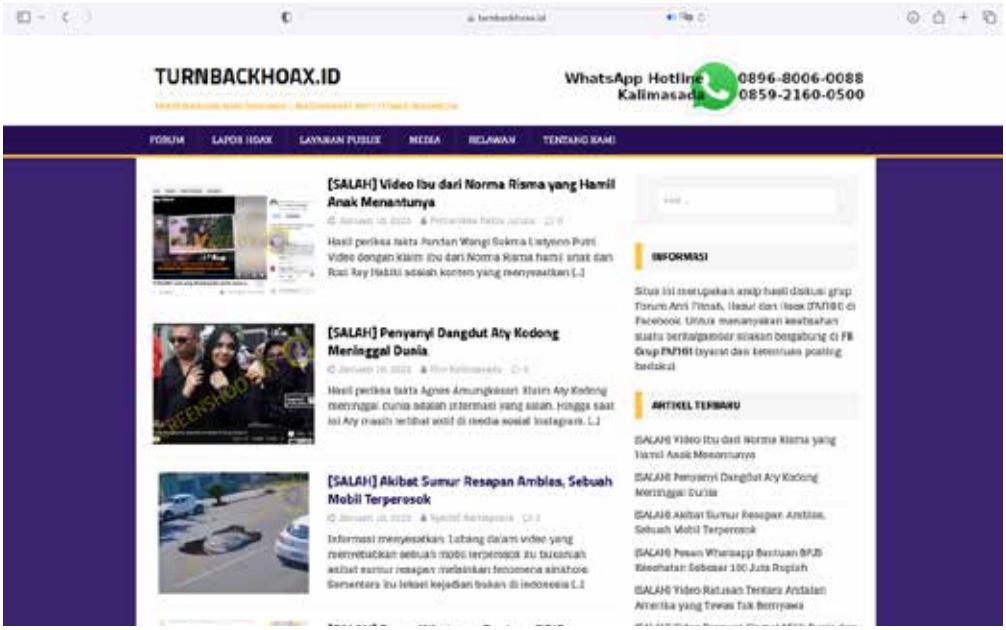
• Situs Pencari (Search Engine) Hoaks



Melalui situs ini kita bisa memasukkan kata kunci dari informasi yang kita cari kebenarannya, kemudian situs ini akan mencari informasi hoaks yang sudah diverifikasi oleh lembaga/media fact checker seperti Mafindo, Kominfo atau media cek fakta (seperti Tempo, Liputan6, Antara, Suara.com, Tirto.id dan sebagainya)

• Situs Turnbackhoax.id

Ini adalah situs yang mengumpulkan hasil debunk yang dilakukan oleh Masyarakat Anti Fitnah Indonesia (MAFINDO) akan hoaks yang beredar di internet. Kita tinggal masukkan kata kunci dibagian pencarian, maka akan diberikan hasil debunking hoaks yang sesuai dengan kata kunci yang diberikan



• Situs komin.fo/inihoaks

Serupa dengan situs turnbackhoax.id, akan tetapi situs ini dikelola oleh tim dari Kementerian KOMINFO.

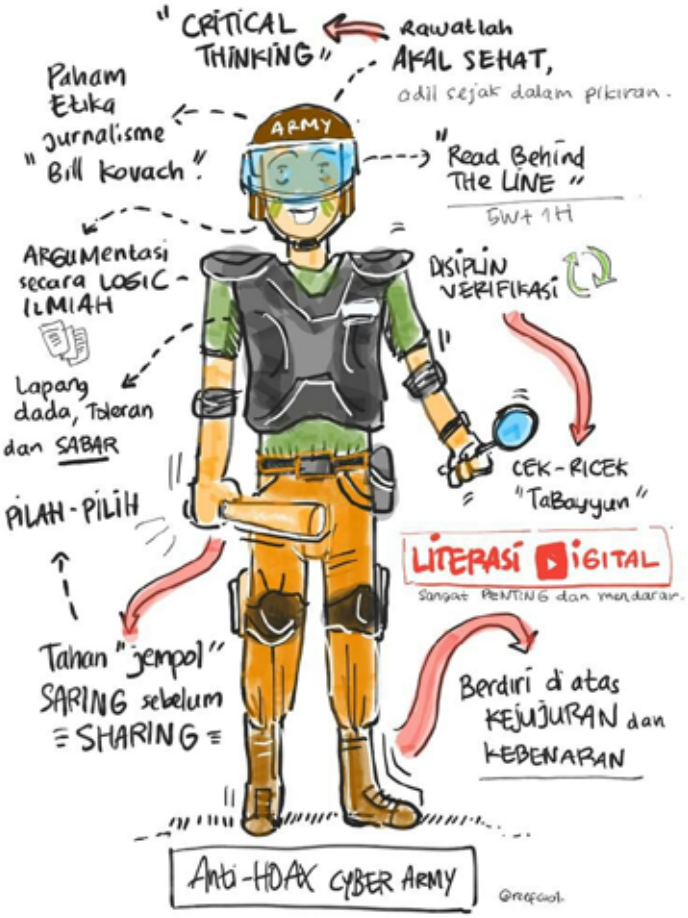
- **WhatsApp ChatBot Kalimasada di 085921600500**

Untuk pengguna WhatsApp, cukup kirimkan pesan WA ke Chatbot Mafindo ini. Masukkan kata kunci terkait info hoaks yang mau diperiksa, maka akan dikirimkan beberapa tautan informasi klarifikasi hoaks yang sudah diverifikasi oleh MAFINDO

- **WhatsApp ChatBot Cekfakta Liputan6 di 08119787670**

Serupa dengan WhatsApp Chatbot Kalimasada, kita juga bisa memeriksa apakah sebuah informasi itu benar atau hoaks dengan mengirimkan pesan ke ChatBot CekFakta dari Liputan6 ini.

MENJADI WARGANET KEBAL HOAKS



(Sumber: Instagram @refcool)

Pada prinsipnya, penting untuk menjadi warganet yang ***"kebal hoaks".*** Dan untuk menjadi warganet seperti itu terdapat beberapa tips, diantaranya:

- Baca! Setiap informasi yang tersaji di depan kita perlu dibaca secara utuh. Jangan mengambil kesimpulan hanya dari judul berita saja
- Mampu berpikir kritis, rawatlah akal sehat ketika membaca sebuah informasi
- *Tabayyun,* cek dan ricek kembali setiap informasi yang kita terima
- Gunakan pikiran logis dan ilmiah dalam menilai suatu berita, jangan *baper*, membawa perasaan ketika menelaah informasi

- Tahan Jempol, *Saring sebelum Sharing.* Pilihlah informasi yang memang mau disebarkan.
- Lapang dada, toleran dan sabar adalah perilaku yang perlu kita kedepankan ketika menerima suatu berita
- Dan penting bagi kita untuk berdiri di atas kejujuran dan kebenaran agar hoaks tidak mudah menyebar


ICT watch!
YLBHI
Luminate
DIGITAL AMAN,
AMAN BERGERAK
s.id/amanbergerak