# PANDUAN ANTI-RIBET

#NyamandiSosmed


KOMINFO

FACEBOOK

# Daftar isi

# Kata Pengantar

## Direktur Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika dalam Panduan Konsumen Facebook di Indonesia

Di era digital, hampir semua orang memiliki akun media sosial atau setidaknya pernah menggunakan internet untuk mengakses media sosial. Namun, kejahatan berbasis ruang digital seperti pencurian data, penipuan online dan pengambilalihan akun media sosial juga semakin sering terjadi dan menimbulkan kerugian bagi masyarakat. Sayangnya, sebagian besar masyarakat belum dibekali dengan informasi dan pengetahuan yang cukup tentang cara melindungi data pribadi dan akun media sosial mereka dari ancaman kejahatan berbasis ruang digital.

Saat ini, Pemerintah melalui Kementerian Komunikasi dan Informatika, bersama dengan DPR tengah membahas Rancangan Undang-Undang tentang Perlindungan Data Pribadi (RUU PDP), yang kami harapkan dapat segera diselesaikan dengan baik. RUU PDP akan menjadi rujukan perlindungan data pribadi di Indonesia serta dapat memberikan kepastian hukum dan perlindungan bagi masyarakat dan pengelola data pribadi.

Kementerian Komunikasi dan Informatika juga terus berupaya untuk mengedukasi masyarakat tentang pentingnya perlindungan data pribadi. Kendati demikian, upaya ini tidak dapat hanya dilakukan oleh pemerintah atau platform media sosial saja. Pemerintah tentu membutuhkan

dukungan dan partisipasi dari berbagai pemangku kepentingan lainnya seperti akademisi, komunitas, dan pelaku bisnis. Lebih dari itu, dibutuhkan juga kesadaran dan kecakapan digital masyarakat sebagai pengguna media sosial sekaligus pemilik data pribadi, dalam mendukung upaya edukasi ini.

Sehubungan dengan hal tersebut, Kementerian Komunikasi dan Informatika mengapresiasi upaya Facebook yang telah menerbitkan Panduan Konsumen 'Anti-Ribet #Nyamandisosmed'. Panduan Konsumen ini berisi langkah-langkah praktis yang mudah dipahami untuk meningkatkan perlindungan data pribadi dan akun media sosial di platform Facebook, WhatsApp dan Instagram. Harapannya, Panduan Konsumen ini dapat membantu masyarakat dalam meningkatkan perlindungan data pribadi dan akun media sosial mereka, dari upaya-upaya pencurian data pribadi dan pengambilalihan akun media sosial.

Panduan Konsumen ini hadir pada waktu yang sejalan dengan upaya pemerintah dalam menciptakan kerangka hukum terkait RUU Perlindungan Data Pribadi. Besar harapan kami bahwa upaya edukasi publik dan dukungan dari platform media sosial seperti ini dapat terus ditingkatkan, dan kolaborasi antara berbagai pemangku kepentingan dengan pemerintah dapat terus dilakukan melalui berbagai inisiatif yang kreatif dan inovatif.

Akhir kata, mari kita terus jaga optimisme dalam meningkatkan literasi digital masyarakat, untuk mewujudkan ekosistem digital yang aman, positif, beretika, dan berdaya saing.

Zaman sekarang, kayaknya hampir semua orang pasti punya sosmed. Bahkan, kalo enggak punya sosmed, bakal langsung dicap kudet alias kurang update. Lewat sosmed juga, hubungan dan silaturahmi dengan teman lama atau keluarga di luar kota maupun luar negeri bisa tetap terjalin.

Sayangnya, enggak semua orang paham dengan langkah-langkah yang harus dilakukan supaya bisa nyaman dan aman di sosmed. Padahal, ini penting banget, lho. Sebab, kalo enggak diperhatikan dengan seksama, ujung-ujungnya malah kita jadi korban aneka penipuan di sosmed.

Pasti sudah sering dengar atau baca tentang pengalaman orang-orang yang akun sosmednya di-*hack* atau diambil orang asing? Lalu, ujung-ujungnya, akun-akun itu digunakan untuk menipu para kenalan di daftar teman sosmednya.

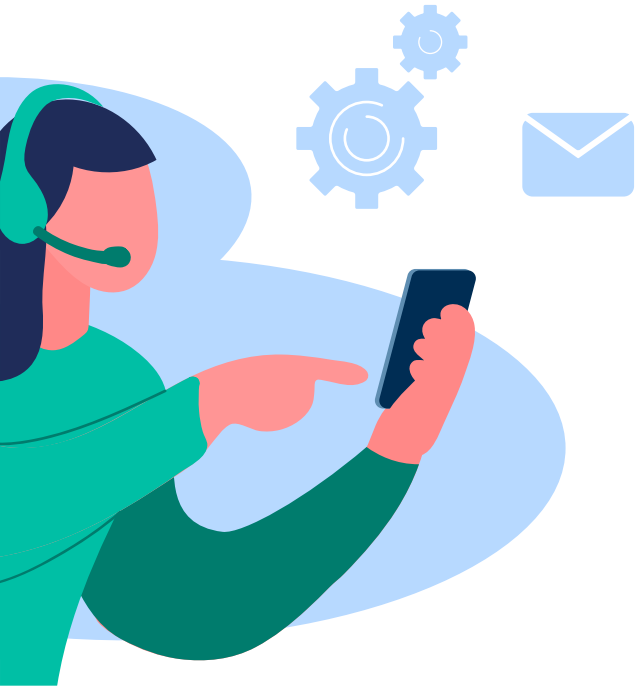
Contohnya, Anto kirim message ke teman-temannya di sosmed, mau pinjam uang atau minta tolong transfer. Padahal, itu bukanlah Anto, tapi penipu yang sudah nge-*hack* sosmed Anto. Karena si penipu mengirim message dengan menggunakan akun sosmed Anto, para korban pun rata-rata mau.

Untuk modus ini, korbannya sudah enggak kehitung saking banyaknya.

Atau kalo di Instagram nih, banyak *hacker* yang membajak akun dengan follower ratusan ribu atau bahkan jutaan. Tujuannya ya untuk dijual lagi atau memeras pemilik akun itu supaya mau mengembalikan akun Instagram mereka. Banyak lho selebriti kita yang pernah kena.

Modus *hacking* atau pembajakan sosmed pun beraneka ragam. Ada yang pura-pura jadi pusat servis Facebook, Instagram, atau WhatsApp lalu kirim link. Ada yang pura-pura jadi teman lama kita dan kirim link untuk dibuka. Intinya, para penipu ini ingin kita klik link yang mereka kirimkan dengan berpura-pura jadi orang lain. Begitu kita klik, langsung deh akun kita diambil alih.

**Nah gimana sih cara untuk bikin akun sosmed kita aman dan nyaman? Simak penjelasan berikut ya!**



# INGIN NYAMAN DI SOSMED TAPI ENGGAK PAHAM GIMANA CARA MENJAGA KEAMANAN SOSMED KITA? WAH BAHAYA BANGET. PADAHAL, BISA DIATUR TANPA PERLU RIBET, LHO.

## Mengontrol akses ke akun sosmed

Ini nih hal maha penting yang harus diperhatikan baik-baik. Sebab, kontrol atau kendali untuk akun sosmed seharusnya dipegang kita sendiri, bukan orang lain, apalagi orang asing. Begitu kontrol itu hilang, kita bakal jadi sasaran empuk bagi para *hacker* untuk membajak akun sosmed kita.

Untuk urusan keamanan, ada beberapa hal yang wajib diperhatikan supaya akun sosmed kita aman damai sentosa.

### Password

Urusan password enggak boleh dianggap enteng ya. Kita wajib banget membuat password yang enggak gampang ditebak, alias password yang rumit. Sebab, kalo password kita simple dan pasaran, ujung-ujungnya akun sosmed kita pun bakal gampang di-*hack* atau dibobol orang.

### Autentikasi Dua Langkah

Dari namanya, emang terkesan ribet. Padahal enggak juga kok, asalkan kita mau ikuti petunjuk yang ada di Facebook, Instagram, dan WhatsApp.

Autentikasi Dua Langkah ini kalo disederhanakan bisa dibilang dobel cek alias cek dan ricek.

Ibaratnya sih, seperti pasang gembok plus alarm di pagar rumah kita. Kalo pencuri bisa membobol gembok, dia enggak bakal bisa langsung masuk ke rumah kita karena alarm akan berbunyi. Supaya bisa membobol rumah, si pencuri masih harus mematikan alarm dulu.

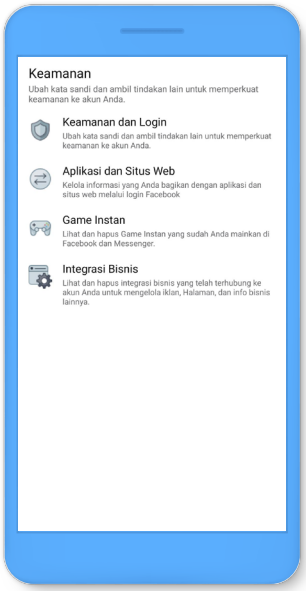
**Jadi dobel pengamanannya gitu kan.**

Tapi karena istilahnya asing, alhasil banyak yang malas mengaktifkan. Hasilnya, banyak akun sosmed yang kebobolan di-*hack*.

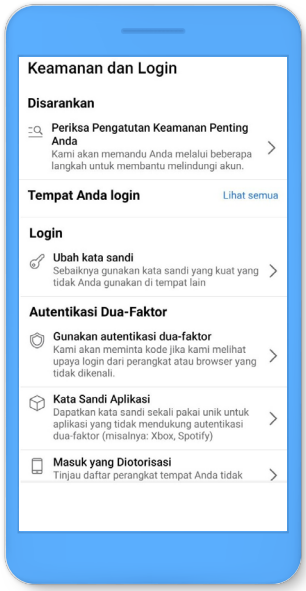
Padahal, kalo kita aktifkan fitur ini, akun sosmed kita bakal lebih aman lho. Sebab, orang lain enggak akan segampang itu membobol akun kita. Untuk bisa mengakses akun kita, mereka juga harus punya nomor telepon maupun kode PIN kita.

## Gimana sih cara aktifinnya?

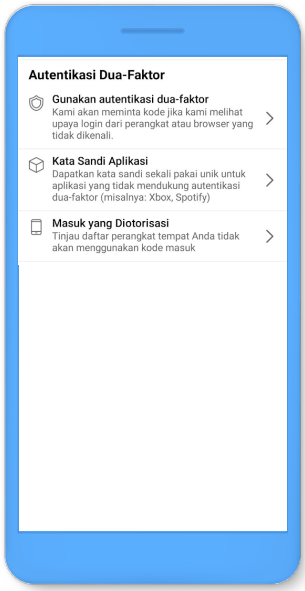
# FACEBOOK



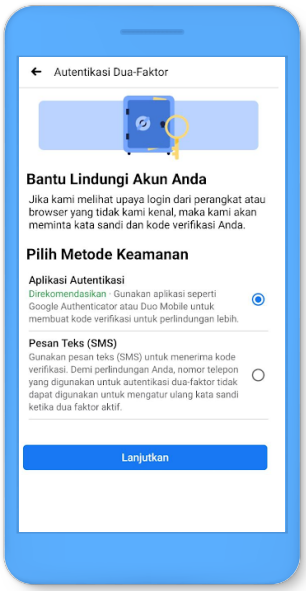

Buka Setting/ Pengaturan Keamanan dan Login.




Scroll turun ke Gunakan autentikasi dua langkah dan klik Edit.

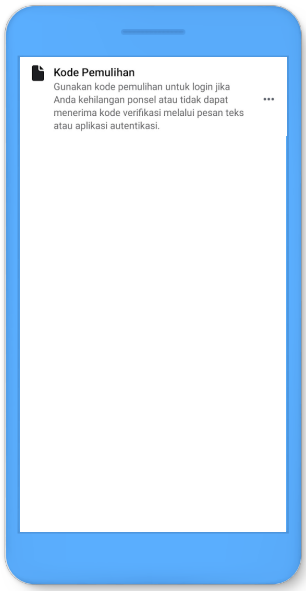



Pilih metode keamanan yang ingin ditambahkan dan ikuti petunjuk di layar.



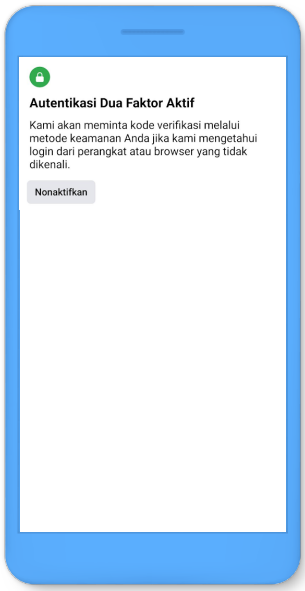

Pilih salah satu dari dua metode keamanan ini:

- Kode login dari aplikasi autentikasi pihak ketiga.
- Kode SMS dari ponsel kita.



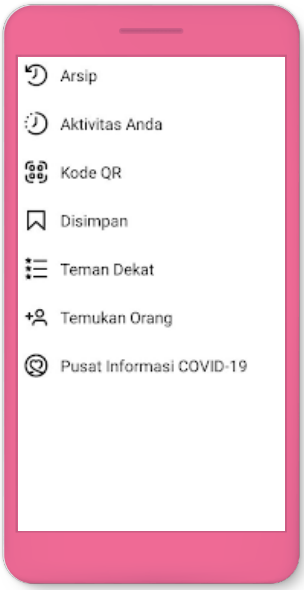

Kita juga bisa pilih metode ini:

- Menyetujui percobaan login dari gadget/ handphone yang dikenali Facebook.
- Menggunakan salah satu kode pemulihan yang kita pilih.
- Tap kunci keamanan kita di perangkat yang sesuai.

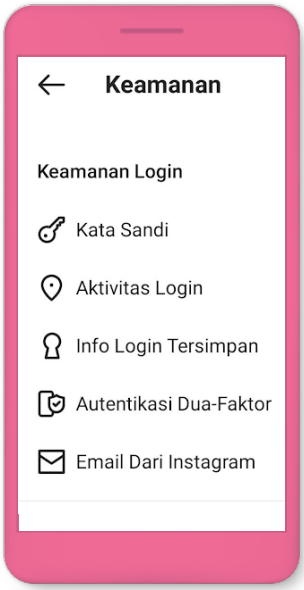



Setelah autentikasi dua langkah aktif, kita harus memasukkan kode yang dikirim Facebook kalo kita login di gadget atau perangkat yang beda dengan yang biasanya.

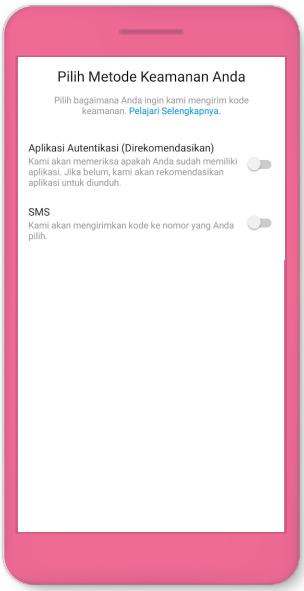
# INSTAGRAM




Masuk ke Profil dan klik Setting/Pengaturan.

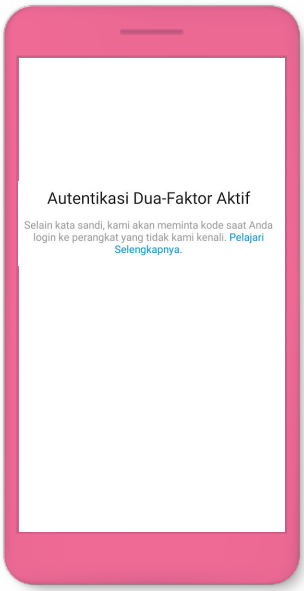



Klik Keamanan dan masuk ke autentikasi dua faktor.



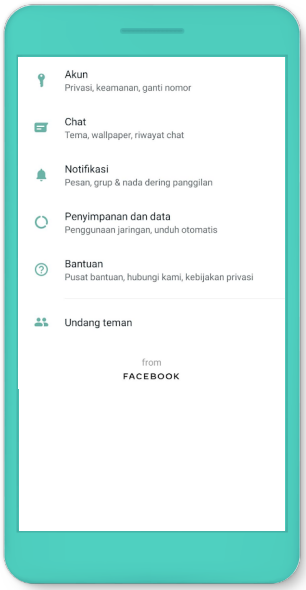

Pilih 2 metode ini:

- Kode SMS dari handphone kita.
- Kode login dari aplikasi autentikasi pihak ketiga (misalnya Duo Mobile atau Google Authenticator).

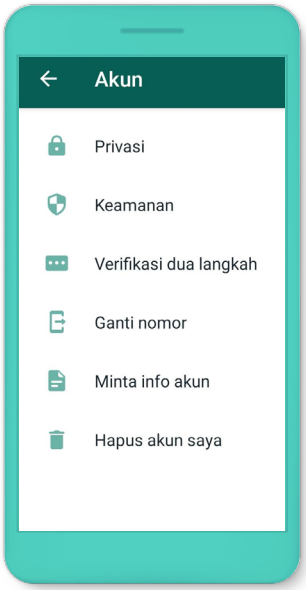



Setelah autentikasi dua faktor diaktifkan, kita harus memasukkan kode yang dikirim Instagram kalo kita login di gadget atau perangkat yang beda dengan yang biasanya.

## WHATSAPP

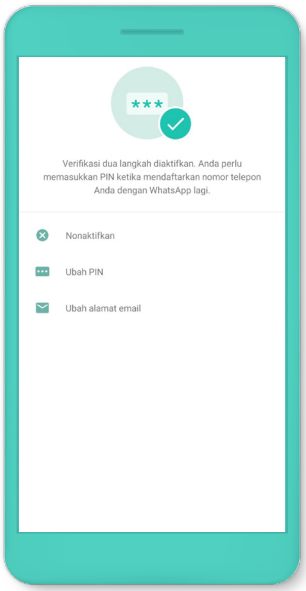



Masuk ke Profil dan klik Setting/Pengaturan.




Klik Akun dan pilih Verifikasi dua langkah.


Aktifkan verifikasi dua langkah dengan menggunakan kode PIN.

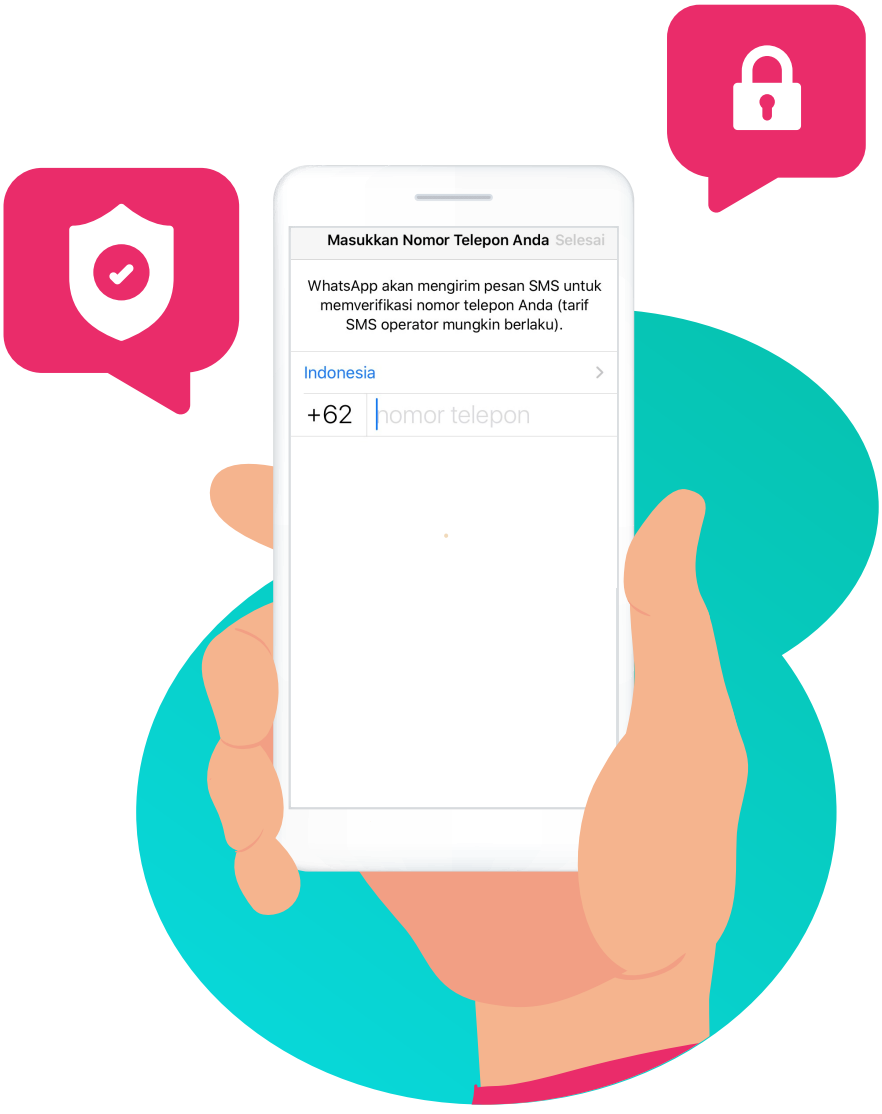



Setelah verifikasi dua langkah diaktifkan, kita harus memasukkan kode PIN yang kita buat sebelum login di gadget atau perangkat yang beda dengan yang biasanya.

## Verifikasi Nomor WhatsApp

Sebelum mengaktifkan WhatsApp kita wajib melakukan langkah ini ya supaya aman. Dan inget, ini syarat-syaratnya:

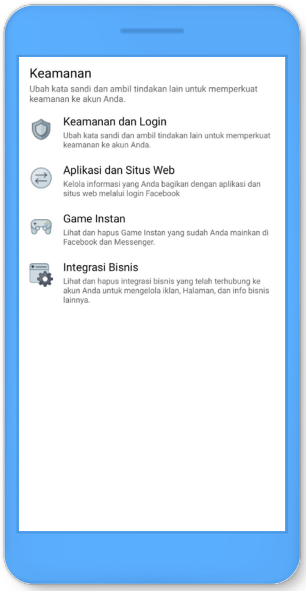
- Kita cuma bisa verifikasi nomor handphone milik kita sendiri, bukan orang lain.
- Kita harus bisa terima telepon dan SMS di nomor yang akan dipakai untuk WhatsApp.
- Kita harus mematikan pengaturan atau aplikasi yang nge-block telepon.
- Internet kita harus aktif supaya bisa verifikasi.



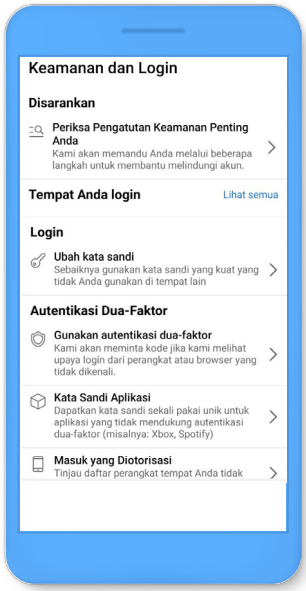
## Facebook Security Checkup

Alias tes keamanan di Facebook. Fitur ini enak banget nih buat kita yang gaptek tapi penasaran dan khawatir, apakah akun Facebook kita aman atau enggak.

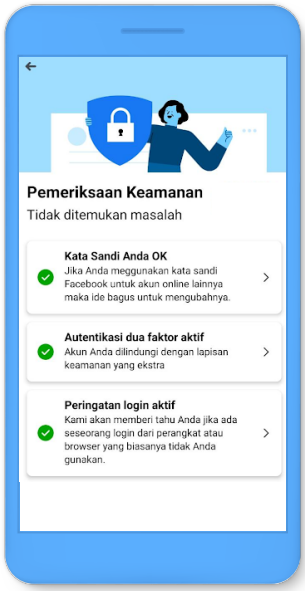
Tinggal klik dan ikuti petunjuk-petunjuk yang ada, termasuk **autentikasi dua langkah** yang tadi itu tuh. Yang penting, kita udah login ke akun Facebook, entah di komputer atau handphone.




Buka Setting atau Pengaturan Keamanan dan Login.

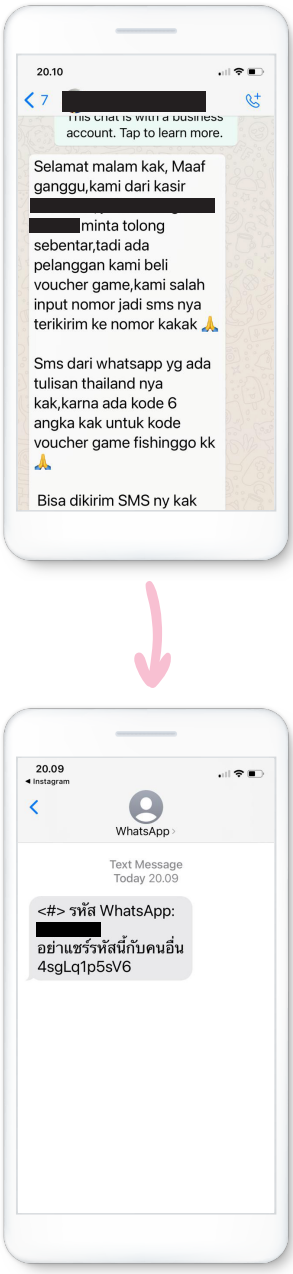



Pilih Periksa Pengaturan Keamanan Penting Anda.




Kamu bisa memilih opsi yang ingin kamu jelajahi, mulai dari mengubah kata sandi hingga kontrol peringatan.

## Aksi tipu-tipu dengan phishing dan scam

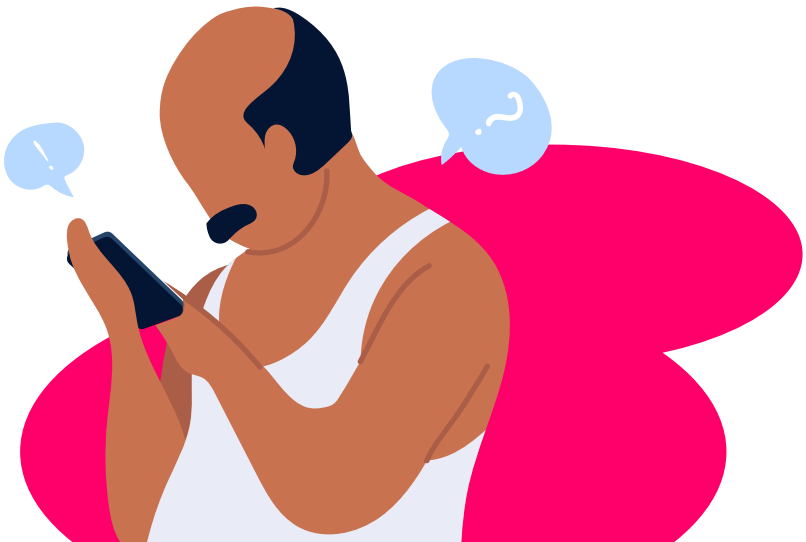



Dua istilah lagi nih selain **autentikasi dua langkah** yang bikin gatal telinga, ya kan? Soalnya, istilah-istilah ini terdengar asing dan njelimet banget. Padahal meski terdengar aneh, aksi tipu lewat *phishing* dan *scam* sering terjadi di kehidupan kita sehari-hari di sosmed.

Pernah dengar tentang orang-orang yang enggak bisa akses WhatsApp-nya setelah dapat chat dari kasir minimarket? Rame banget tuh kasusnya dan masih terus terjadi lho sampai sekarang.

Jadi ceritanya, banyak orang yang dapat chat di WhatsApp dari akun yang mengatasnamakan kasir minimarket dan pasang foto profil dengan seragam minimarket. Mbak "kasir" ini bilang bahwa ada pelanggan yang beli voucher game tapi dia salah input nomor teleponnya. Alhasil, kode voucher game-nya terkirim ke nomor telepon orang tersebut lewat SMS, bukan ke si pembeli voucher.

Mbak "kasir" pun minta orang itu kasih tau kode yang ada di SMS yang dikirim dalam bahasa Thailand. Nah, begitu orang itu kasih kodenya, langsung akan muncul notifikasi dari WhatsApp bahwa dia enggak bisa akses nomor WhatsApp-nya. Alasannya, nomor WhatsApp itu udah terdaftar di handphone lain. Atau dengan kata lain, nomor WhatsApp-nya dibajak.



**Nah saudara-saudara, inilah yang dinamakan *phishing*!**

Metode *phishing* ini bisa juga menggunakan aneka macam cara lainnya. Biasanya, taktik phishing mengincar sisi emosional kita dengan tujuan untuk membohongi. Bisa kasihan, senang, sedih, iba, wah macam-macam lah. Soalnya si penipu tahu, begitu emosi kita kepancing, logika pun susah diajak kerja sama. Kena deh ketipu.

Ada yang kasih info diskon menarik dengan minta kita klik web palsu. Ada yang pura-pura jadi teman atau saudara kita dan minta tolong untuk kirim uang. Ada yang bilang kita menang undian tapi harus bayar sejumlah uang untuk biaya. Ada juga yang kirim email atau message bahwa akun kita di-*hack* dan dia bisa membantu kita dengan sejumlah syarat.

Pokoknya, teknik *phishing* itu macam-macam. Yang pasti semuanya bikin kita enggak bisa lagi mengakses akun sosmed kita.

## Lalu gimana supaya enggak kena phishing?

**Jangan pernah memberikan detail login kita ke siapa pun.**
Apalagi, Facebook enggak pernah meminta password kita dalam bentuk email atau mengirim password dalam bentuk lampiran.

**Jangan pernah terima permintaan pertemanan dari orang tak dikenal.**
Penipu biasanya membuat akun palsu dan mencoba untuk menjadi teman kita. Kalo kita menerimanya, si penipu akan menyebarkan spam di timeline atau linimasa kita. Dan kemungkinan besar kita bisa terjebak mengkliknya.

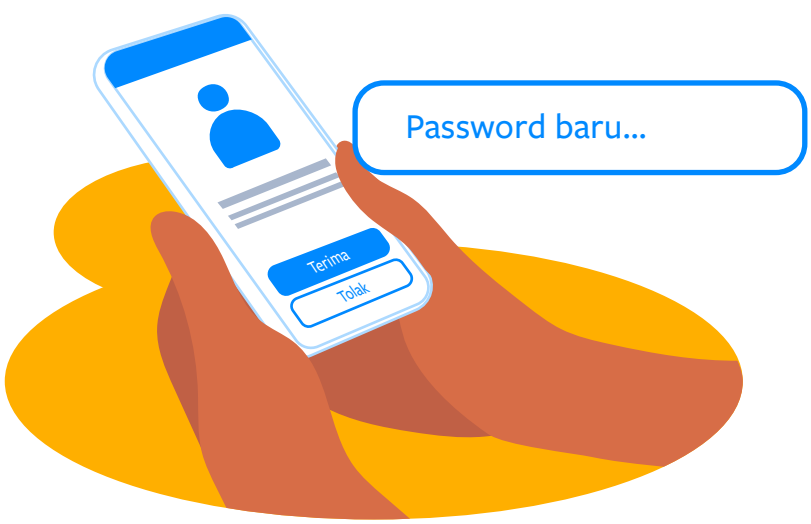
**Ganti password secara rutin.**
Ini akan mencegah akun kita dibajak oleh penipu yang akan menggu nakannya untuk menghubungi teman-teman kita di sosmed.

**Lihat aktivitas akun kita dan hapus spam.**
Kita bisa lho memeriksa riwayat login untuk melihat login yang mencurigakan dan juga memeriksa aplikasi yang di-*install* yang punya akses ke data kita.

**Kalo ada pesan yang aneh, jangan takut untuk melapor ke Facebook.**
Kalo tiba-tiba kita dapat email atau message aneh di messenger yang mengatasnamakan Facebook, jangan buka email atau lampirannya. Lebih baik langsung laporkan ke **phish@fb.com.**

**Kalo mau melaporkan percakapan, jangan lupa *screenshot* dulu sebelum dihapus.**

**Kalo ada teman yang jadi korban pembajakan, beritahukan mereka.**
Facebook akan membantu kita jika kita kena *hack*. Atau kunjungi Help Center di Facebook untuk bantuan.

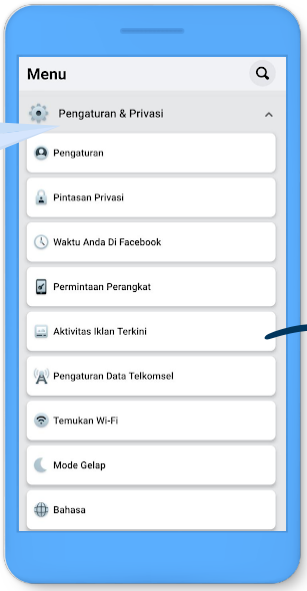




Belakangan ini, ada juga teknik *phishing* yang seolah-olah mengirimi kita email dari Facebook atau Instagram. Biasanya si penipu ini minta informasi pribadi kita dengan sejuta alasan. Misalnya, akun kita akan dihapus kalo enggak mau ikutin arahan mereka.

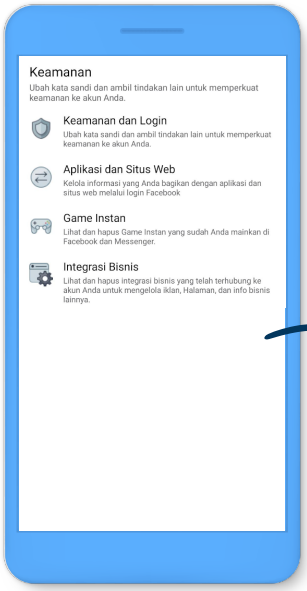
Sialnya, banyak juga yang tertipu. Apalagi si penipu mengirim email yang seolah-olah berasal dari Facebook atau Instagram dengan menyertakan logo. Jadi, banyak yang kurang ngeh apakah email itu asli atau palsu.

Nah, kalo terima email yang mengaku dari Facebook, kita bisa ngecek apakah benar email itu dari Facebook atau bukan.

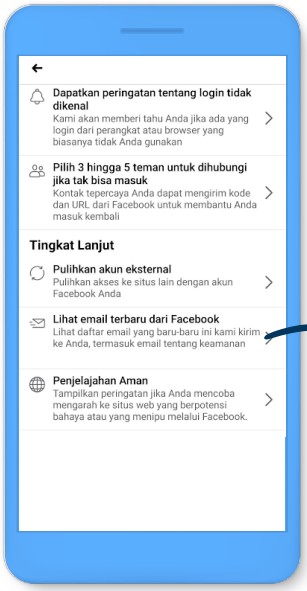
## Caranya:



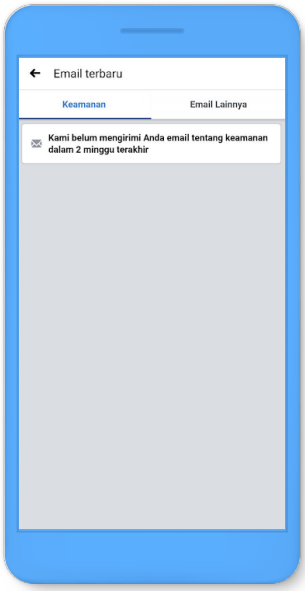

Buka Setting/Pengaturan Keamanan dan Login dengan mengklik di kanan atas Facebook.




Klik Pengaturan & Privasi, lalu klik Keamanan dan Login.




Scroll turun ke Lihat email terbaru dari Facebook, lalu klik Lihat.




Di sini kita bisa lihat email-email apa aja yang pernah dikirim oleh Facebook. Kalo email yang kita terima enggak ada di daftar itu, mending enggak usah ditanggapi deh.

## Tolong akun kita di-*hack*!

Beberapa waktu lalu, ada teman yang tiba-tiba enggak bisa buka akun sosmednya. Ternyata akunnya di-*hack*. Yang lebih menyebalkan, akun itu lalu kirim message ke semua teman-temannya di sosmed untuk minta transfer lah, ngemis bantuan lah, macam-macam deh. Bikin malu banget enggak sih?

Bagus kalo teman yang dikirimi message enggak percaya dengan permintaan seperti itu. Tapi kalo ada yang percaya, transfer, dan tertipu, kan bikin marah ya.

Terus, kalo kejadiannya kayak gini, kita harus ngapain? Tenang dan jangan panik dulu dong. Ternyata, ada beberapa cara yang bisa dilakukan untuk mengembalikan akun kita.

**Simak beberapa cara yang bisa dilakukan untuk mengembalikan akun kita.**

## Laporkan dan coba pulihkan akunnya.

# AKUN FACEBOOK KITA YANG DI-*HACK*?

**1 Laporkan!**
http://www.facebook.com/hacked
Lengkapi laporan dengan alamat email dan nomor hp yang kita pakai saat mendaftar akun.

**2 Gak ada akses ke akunnya?**
Tenang jangan panikk! Isi saja data-data yang diminta kayak email dan nomor hp yang baru.

**3 Terus ngapain lagi?**
Nanti Facebook akan hubungin kita buat proses verifikasi. Biasanya nih, kita bakalan dimintain foto identitas kayak KTP atau SIM.

**4 Udah, gitu aja dan tunggu deh akunnya balik.**

# ATAU AKUN INSTAGRAM DI-*HACK*?

**1 Laporkan!**
help.instagram.com
Pilih menu privasi dan keamanan - melaporkan sesuatu - sepertinya akun saya diretas.

**2 Lah kok akunnya malah hilang?**
Duh, jangan khawatir! Itu memang langkahnya Instagram untuk bisa mastiin kalau akun kita memang di-*hack*.

**3 Sering-sering cek email!**
Instagram hanya kirim informasi lebih lanjut lewat email terdaftar. Biasanya kita diminta isi formulir dan mengirimkan data diri kayak foto dan KTP kita.

**4 Tunggu deh!**
Biasanya proses berjalan 4-7 hari. Tungguin aja ya dengan sabar sampai Instagram ngimel kita lagi dan akun kita udah bisa ditemukan di kolom pencarian Instagram.

# KALAU WHATSAPP YANG DI-*HACK*?

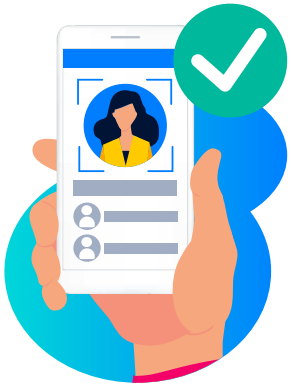
## Ganti akses keamanan.

Begitu akun kita sudah kembali di tangan, jangan pernah lupa untuk belajar dari pengalaman ya. Sekarang saatnya kita bikin akun kita lebih aman dengan mengganti password secara rutin atau menggunakan autentikasi dua langkah.

Facebook menyarankan supaya kita menghapus aplikasi yang mencurigakan atau berbahaya, yang memiliki akses terhadap data di akun Facebook kita. Ini semua bisa dilakukan di menu Pengaturan > Aplikasi dan Situs Web. Kita bisa secara khusus memeriksa daftar aplikasi yang sudah enggak dipakai, atau enggak kita kenali dan menghapusnya. Aplikasi yang biasanya di-*install* itu macam-macam, mulai dari games kayak Candy Crush sampe aplikasi lucu-lucu.

Facebook juga menyarankan kita untuk kasih tahu teman saat akun kita di-*hack*. Trus, kita sebaiknya minta mereka untuk enggak mengakses atau mengklik link dan post yang mencurigakan dari akun yang udah
di-*hack* itu.

Kita juga bisa mengatur pemberitahuan tentang login yang tidak dikenali dari menu Pengaturan > Login dan Keamanan di akun Facebook kita. Saat fitur ini diaktifkan, Facebook akan kasih tahu jika ada orang yang login ke akun kita dengan handphone atau perangkat yang enggak biasanya kita gunakan. Facebook juga akan kasih panduan cara gimana
mengamankan akun kita.



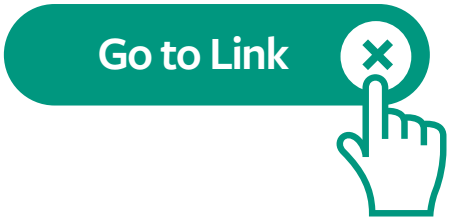
Saat ada orang dari alamat IP yang beda dengan IP kita mencoba login dengan nama dan password yang benar di waktu yang barengan dengan kita, Facebook bisa mengaktifkan fungsi Social Verification. Foto dari teman-teman dekat akan muncul dan orang yang melakukan login itu harus mengenali dan menjawab nama-nama orang di foto tersebut.

## Tips aman yang jitu dari Kominfo.


Gunakan kata sandi yang kuat dengan kombinasi huruf, angka, dan karakter.

Buat kata sandi yang berbeda di setiap akun kamu.

Jangan klik atau balas pesan yang meminta identitas pribadi.




Jangan buka link sembarang dari pesan yang kalian terima.

Berhati-hati menggunakan WiFi di tempat umum. Gunakan jaringan yang aman dan dikenali.

Pahami izin yang diminta oleh setiap aplikasi.

# PRIVASI ITU APA SIH? EITS, JANGAN DIANGGAP ENTENG LHO. PRIVASI INI PENTING BANGET DAN BISA KITA KENDALIKAN DI SOSMED.

## Ini nih data pribadi yang harus kamu jaga di sosmed.

Pertama nih yang penting banget! Sebisa mungkin gak perlu lah membagikan data pribadi di profil dan postingan sosmed biar terhindar dari keisengan orang-orang yang gak bertanggung jawab. Ya kan?

# Nah, apa aja sih data pribadi itu? Coba simak daftarnya dibawah ini:

**Nama dan lokasi tempat kerja.**

**Nama dan alamat sekolah.**

**Tanggal lahir.**

**Orientasi seksual.**

**Agama**

**Nomor telpon selular.**

**Data biometrik (sidik jari, retina, bentuk wajah)**

**Nama saudara kandung.**

**Nama kota tempat tinggal.**

**Nama kota asal.**

**Gender.**

**Bahasa.**

**Alamat dan foto rumah.**

**Preferensi politik.**

**Nama orang tua.**

**Status hubungan.**

## Siapa aja sih yang bisa lihat profil dan postingan kita?

Pernah enggak tiba-tiba dapat komen nyebelin di status yang kita tulis di Facebook dari orang yang enggak kita kenal? Atau, tau-tau ada  yang menyebarkan foto-foto pribadi yang kita posting di sosmed?

Rasanya pasti enggak enak ya. Bahkan lebih dari itu, ngeselin banget ih, asli! Apalagi kalo profil dan foto-foto kita dijadikan bahan gosipan orang yang sirik sama kita. Atau status sosmed kita malah jadi bahan julid ibu-ibu tetangga.

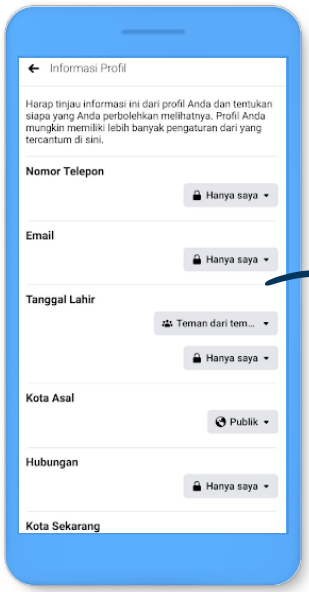
Padahal, kita tuh artis bukan, selebgram juga bukan. Lah kita kan cuma orang biasa.

Nah, sebenernya, ada cara dan fitur di sosmed yang bisa mengatur siapa aja yang bisa melihat profil dan postingan kita. Jadi, kita bisa posting foto dan update status, tanpa khawatir diintipin sama orang-orang yang julid dan nyebelin itu.

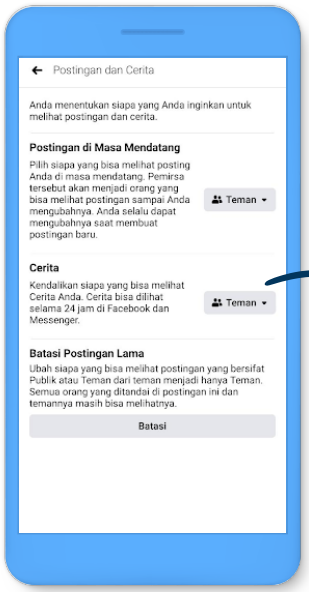
## Gimana caranya?

## FACEBOOK

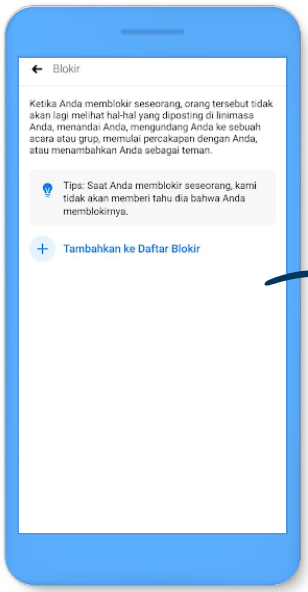
Pertama-tama, coba klik Facebook Privacy Checkup atau Pemeriksaan Privasi. Fitur ini ngebantu banget untuk ngecek siapa aja yang bisa melihat segala sesuatu yang kita posting di Facebook. Selain itu, kita juga bisa mengatur hal-hal lain seperti:



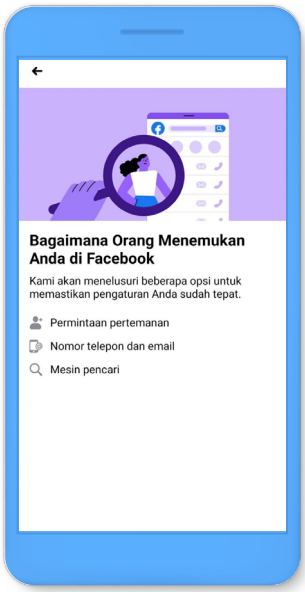

Mengetahui siapa yang bisa melihat nomor telepon, email, ulang tahun, dan status hubungan kita.



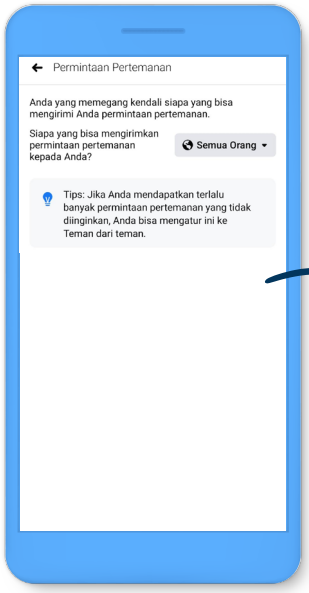

Mengatur siapa yang bisa melihat postingan lama dan postingan kita ke depan.



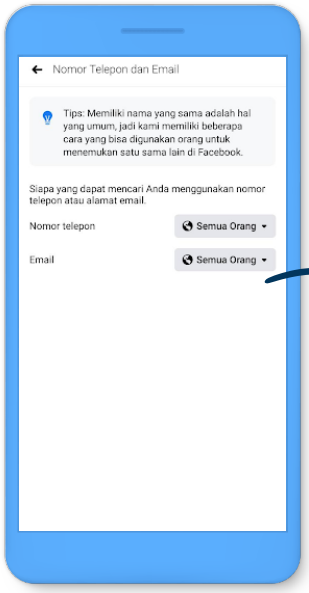

Mereview siapa aja yang kita blokir di Facebook.



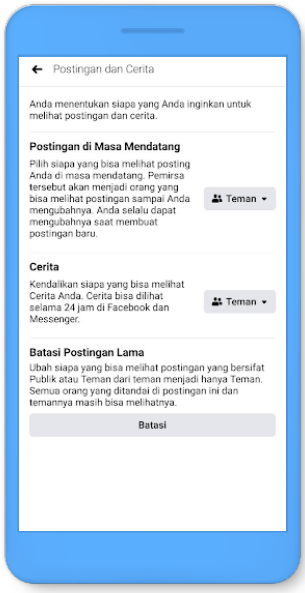

Mengetahui siapa aja bisa menemukan kita di Facebook.




Mengetahui siapa yang bisa kirim permintaan pertemanan di Facebook.



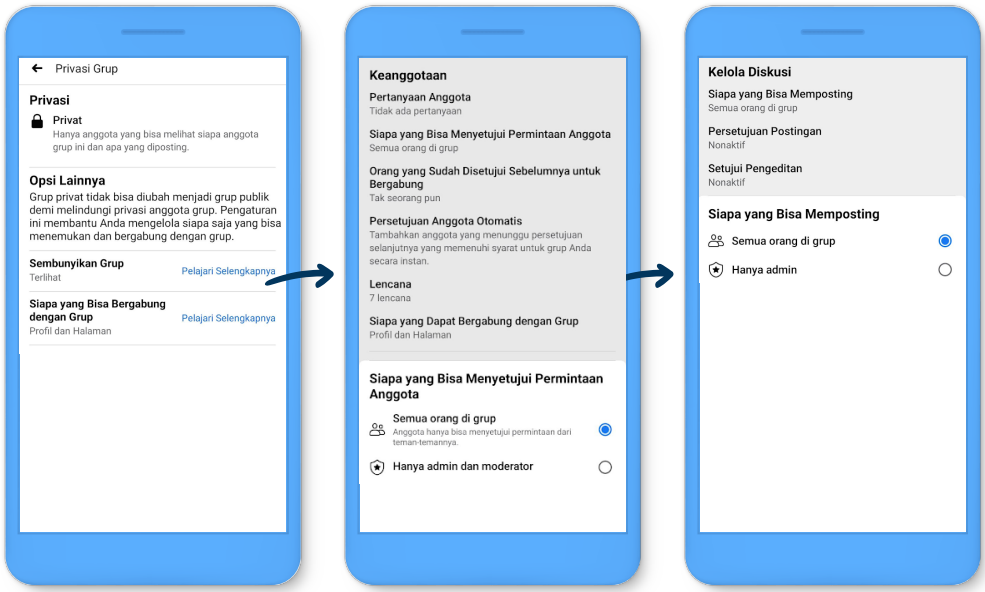

Membatasi gimana orang bisa mencari kita di Facebook dengan nomor telepon atau alamat email kita.




Mengontrol siapa aja yang bisa melihat postingan yang kita buat di Facebook.

## FACEBOOK GROUP

Nah kalau kita punya Facebook Group, ada juga nih caranya biar privasi Group kita dan aktivitasnya berjalan nyaman:



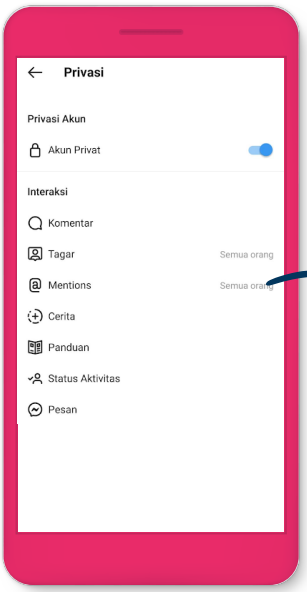

Mengetahui siapa yang bisa melihat nomor telepon, email, ulang tahun, dan status hubungan kita.

Mengatur siapa yang bisa melihat postingan lama dan postingan kita ke depan.

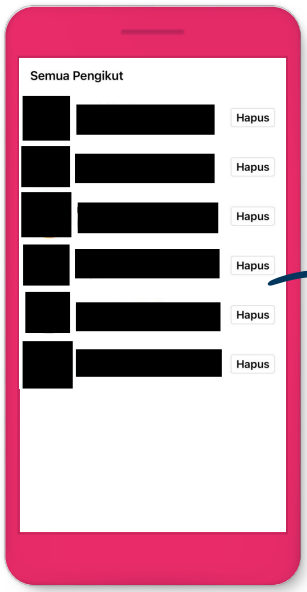
Mereview siapa aja yang kita blokir di Facebook.

## INSTAGRAM

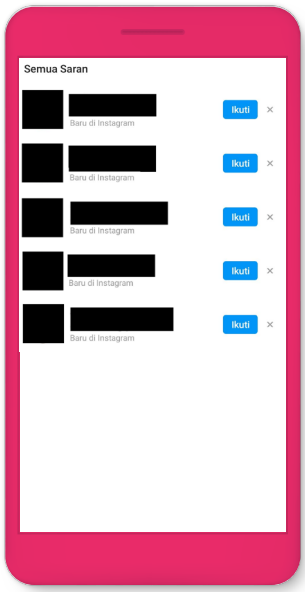
Di Instagram juga sama aja kayak di Facebook. Privacy setting atau pengaturan privasi perlu kalo kita enggak mau tiba-tiba punya *haters* macam artis dan selebgram. Hal yang kita bisa lakukan antara lain:



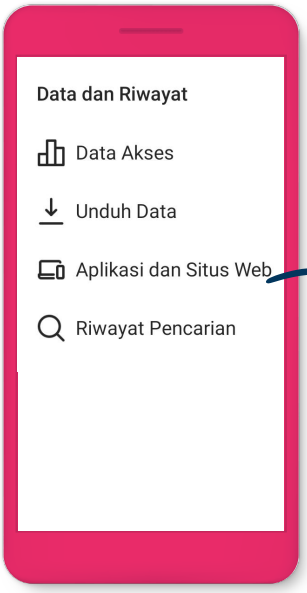

Mengunci akun Instagram kita jadi akun private. Jadi semua postingan kita cuma bisa dilihat oleh followers kita, bukan para netizen di dunia maya.



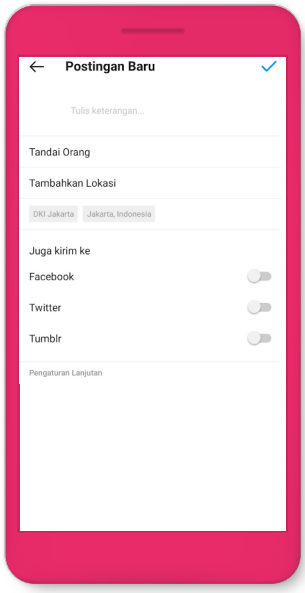

Menghapus followers di Instagram. Enak nih buat buang-buangin followers yang rese dan julid.




Mematikan rekomendasi teman yang harus di-follow.




Mengakses dan men-download data postingan kita di Instagram.




Mematikan lokasi foto atau video akan kita posting.

## WHATSAPP

Buibu Pakbapak pasti akrab ya sama WhatsApp status? Atau jangan-jangan suka kepoin status teman-teman sendiri di WhatsApp nih?

Nah, privasi status WhatsApp itu bisa diatur juga lho. Jadi kalo enggak mau status kita dilihat sama Ibu RT, Pak RW, atau tetangga depan, itu mah gampang lah. Semua bisa diatur.

Tinggal buka status, trus tekan titik tiga di atas dan klik Status Privacy/Privasi Status. Langsung deh atur sendiri siapa-siapa aja yang boleh dan enggak lihat status WhatsApp kita. Enggak ribet kok.

## Katanya Facebook itu suka nguping untuk kepoin kita ya?

Bener enggak sih Facebook itu hobi nguping obrolan kita untuk menyesuaikan dengan iklan yang muncul di akun kita?

Ternyata, Facebook enggak melakukan itu kok. Facebook itu hanya menunjukkan iklan berdasarkan ketertarikan orang-orang dan informasi yang mereka bagikan, bukan dari apa yang kita omongin langsung.

Facebook cuma mengakses mikrofon handphone kalo kita kasih izin dan kalo kita emang menggunakan fitur yang butuh audio. Misalnya, saat kita merekam video, tentu mikrofon harus aktif dan konek ya kan.

Lalu kenapa yang muncul di Feed Facebook kita dia lagi, dia lagi? Ternyata memang ada beberapa hal yang berpengaruh.
Di antaranya:

- Seberapa sering kita berinteraksi dengan postingan dari teman, grup, atau Page/Halaman. Oh ya, teman dan keluarga jadi prioritas Facebook untuk ditampilkan di Feed kita.
- Tergantung jenis postingan yang paling sering kita like dan komen. Misalnya, foto, video, atau link.
- Popularitas postingan teman, grup, dan Page/Halaman yang kita follow. Jadi, semakin banyak jumlah like, komentar, dan share yang didapatkan, postingan itu akan lebih sering muncul di Feed kita.
- Waktu postingan.
- Interaksi kita dengan postingan teman atau Page/Halaman. Misalnya kita sering like dan komen postingannya Bu RT, ya postingan dia akan sering muncul di Feed kita.
- Persamaan yang kita miliki, seperti teman bersama atau grup yang sama-sama kita ikuti.

## Apa aja sih informasi kita yang dikumpulin?

Suka penasaran enggak, apakah semua chat dan obrolan kita di WhatsApp itu benar-benar aman? Sebab, ada kan yang bilang bahwa obrolan, foto, video, dan sebagainya yang kita share di WhatsApp bakal dikumpulin kantor pusat WhatsApp untuk mengintai kita.

Ada juga yang bilang, chat dan info yang kita share di WhatsApp bakal dijual dan dijadiin duit.

Hmm... Gini ya gaes. Kalo lagi chat di WhatsApp pasti suka lihat ada tulisan *end to end encryption* kan? Nah itu artinya, mau kita chat apapun, ngobrol tentang apapun, enggak bakal ada orang lain yang ikut nimbrung baca dan dengerin. Obrolan, video, chat, apapun cuma bisa diketahui oleh kita dan teman yang kita ajak chat.

Ya bisa juga sih ketahuan orang, kalo handphone kita dicuri atau diintip, hehehe.

Istilah *end to end encryption* itu emang susah dijelaskan atau dicari padanannya dalam bahasa Indonesia. Tapi percaya deh, kalo lihat ada tulisan itu di WhatsApp, berarti semua chat kita terlindungi dan aman.

Oh ya di WhatsApp sekarang ada fitur untuk meminta informasi tentang akun kita. Fitur ini bisa membantu kita untuk men-*download* aneka informasi tentang akun kita sendiri.

Fitur bernama "Request Account Info" ini bisa membantu kita mendapatkan data berupa informasi akun, setting, dan foto profil, plus nama grup yang kita ikuti.

Tapi fitur ini enggak bisa dipakai untuk *download* semua chat yang pernah kita kirim dan terima di WhatsApp lho ya.

**TUH, CARA UNTUK #NYAMANDISOSMED ENGGAK RIBET KAN? YANG PENTING KITA TAHU TIPS DAN TRIK UNTUK MENGENDALIKAN KENYAMANAN DAN KEAMANAN DI SOSMED.**

Mudah-mudahan, apa yang di-share dan ditulis di buklet ini bisa membantu kita semua untuk bisa merasa aman dan nyaman di sosmed. Kalo kita sudah paham tips-tipsnya, sebenarnya enggak perlu khawatir kena aksi tipu-tipu ala Mbak "kasir" minimarket maupun *hacker* Turki yang ngetop banget karena hobi nge-*hack* akun Instagram selebriti.

Sebab, begitu tau kuncinya, mau ada aksi tipu-tipu, *hacker*, dan lainnya yang lebih canggih pun, dijamin kita lebih nyaman lah bersosmednya.

Begitu juga untuk urusan kenyamanan. Begitu paham dengan privasi, kita bisa bebas lah ya dari segala kejulidan netizen.

Untuk info lebih lanjut, silakan baca-baca langsung aja di:
**Facebook: facebook.com/help**
**Instagram: help.instagram.com**
**WhatsApp: faq.whatsapp.com**

Dadah!

**Untuk laporan akun bermasalah, bisa juga langsung lapor ke Kominfo nih di pengendalianaptika@kominfo.go.id**