PAHAMIN DULU · E-BOOK GRATIS



Aman di Dunia Digital

Panduan keamanan digital untuk keluarga Indonesia:
10 langkah melindungi akun, data, dan uang Anda.

Sebelum percaya, sebelum daftar, sebelum bagikan.

pahamindulu.id · Edisi November 2026

PENGANTAR

Tentang e-book ini

Sepuluh panduan keamanan digital dari **pahamindulu.id**, dirangkum dalam satu buku saku. Setiap bab berdiri sendiri, jadi Anda bisa langsung membuka bagian yang paling dibutuhkan.

Isinya disusun dari sumber resmi dan media tepercaya yang dicantumkan di akhir setiap bab. Informasi berlaku per **November 2026**. Tampilan aplikasi dan aturan bisa berubah, jadi periksa kembali sumber aslinya bila ada yang berbeda.

Cara memakai

1. Mulai dari **Daftar periksa cepat** dan centang yang sudah Anda lakukan.
2. Buka bab untuk poin yang belum dicentang. Setiap bab punya langkah praktis.
3. Bagikan ke keluarga, terutama orang tua yang baru memakai HP.

10	38	Gratis
BAB PANDUAN	POIN PERIKSA	BOLEH DIBAGIKAN

Boleh disimpan, dicetak, dan dibagikan gratis selama tidak diubah dan tidak dijual.
Menemukan kekeliruan? Kirim koreksi lewat pahamindulu.id/kontak.

ISI BUKU

Daftar isi

✓ **Daftar periksa cepat** 4
Ringkasan semua bab, bisa dicentang

01 **Kata sandi yang kuat** 7
Kata Sandi 123456 Sudah Tidak Zaman, Begini Cara Membuat yang Kuat

02 **Kunci akun WhatsApp** 10
Akun WhatsApp Dibajak Bisa Dicegah, Aktifkan Fitur Ini Sekarang

03 **Tolak grup WhatsApp asing** 13
Sering Dimasukkan ke Grup WhatsApp Asing? Begini Cara Membatasinya

04 **Cek email yang bocor** 17
Email Anda Ikut Bocor? Cara Mengecek dan Langkah Setelahnya

05 **Kenali link phishing** 21
Link Hadiah dan Ancaman Blokir Akun: Cara Mengenali Phishing

06 **Jangan pasang file APK** 24
Awas APK Berkedok Undangan dan Surat Tilang, Rekening Bisa Terkuras

07 **Waspadai video call palsu** 27
Wajah dan Suaranya Mirip, Tapi Palsu: Kenali Penipuan Berbasis AI

08 **Cek rekening sebelum transfer** 31
Sebelum Transfer ke Orang Asing, Cek Dulu Rekeningnya di Sini

09 **Saring hoaks sebelum membagikan** 35
Sebelum Klik Bagikan: 6 Cara Sederhana Mengenali Hoaks

10 **Kalau sudah terlanjur tertipu** 38
Jadi Korban Penipuan Online? Lakukan 6 Langkah Ini Secepatnya

RINGKASAN

Daftar periksa cepat

Poin terpenting dari setiap bab. Centang yang sudah Anda lakukan.

1 Kata sandi yang kuat

- [ ] Panjang lebih penting daripada rumit: minimal 12 karakter.
- [ ] Satu akun, satu kata sandi. Jangan dipakai ulang.
- [ ] Gunakan kalimat sandi (passphrase) agar mudah diingat.
- [ ] Aktifkan verifikasi dua langkah di akun penting.

2 Kunci akun WhatsApp

- [ ] Kode 6 digit dari SMS WhatsApp TIDAK BOLEH diberikan ke siapa pun.
- [ ] Verifikasi dua langkah menambah PIN pribadi yang tidak dikirim lewat SMS.
- [ ] Tambahkan email agar PIN bisa dipulihkan bila lupa.

3 Tolak grup WhatsApp asing

- [ ] Atur privasi Grup ke "Kontak Saya" atau "Kontak Saya, kecuali...".
- [ ] Orang di luar pilihan itu harus mengirim undangan, bukan langsung memasukkan Anda.
- [ ] Keluar, laporkan, dan blokir bila terlanjur dimasukkan ke grup mencurigakan.

4 Cek email yang bocor

- [ ] Cek email Anda di situs **haveibeenpwned.com**.
- [ ] Ganti kata sandi akun yang terdampak, terutama bila sandinya dipakai di tempat lain.
- [ ] Aktifkan verifikasi dua langkah di email dan akun penting.
- [ ] Waspadai email atau pesan "resmi" setelah kebocoran, karena sering berupa phishing.

5 Kenali link phishing

- [ ] Phishing memakai situs palsu yang meniru tampilan resmi.
- [ ] Cek alamat situs dengan teliti, bukan hanya tampilannya.
- [ ] Bank dan instansi resmi tidak meminta PIN, OTP, atau kata sandi.
- [ ] Masuk ke layanan lewat aplikasi resmi, bukan lewat link di chat.

6 Jangan pasang file APK

- [ ] Undangan, foto, atau resi asli TIDAK berbentuk file .apk.
- [ ] APK berbahaya bisa membaca SMS, termasuk kode OTP bank.
- [ ] Jangan pernah memasang aplikasi dari luar Play Store/App Store.
- [ ] Bila terlanjur memasang: putuskan internet, hubungi bank, laporkan.

7 Waspadai video call palsu

- [ ] IASC menerima 1.379 aduan penipuan yang diduga memakai AI hingga akhir Juni 2026.
- [ ] Suara, wajah, dan video yang diterima secara digital bisa dipalsukan.
- [ ] Selalu verifikasi lewat jalur lain sebelum mentransfer uang.
- [ ] Sepakati "kata kunci keluarga" untuk keadaan darurat.

8 Cek rekening sebelum transfer

- [ ] Cek nomor rekening atau e-wallet di **cekrekening.id**.
- [ ] Hasil "tidak ditemukan" bukan jaminan aman.
- [ ] Utamakan pembayaran lewat fitur resmi marketplace.
- [ ] Bila tertipu, segera hubungi bank dan lapor ke IASC.

9 Saring hoaks sebelum membagikan

- [ ] Judul yang memancing emosi adalah tanda bahaya pertama.
- [ ] Cek sumbernya: media resmi atau akun tak jelas?
- [ ] Gunakan situs cek fakta sebelum percaya.
- [ ] Kalau ragu, jangan dibagikan.

10 Kalau sudah terlanjur tertipu

- [ ] Laporkan secepat mungkin, idealnya dalam hitungan jam.
- [ ] Hubungi bank Anda dan lapor ke IASC: **iasc.ojk.go.id**.
- [ ] Simpan semua bukti, jangan hapus chat dengan pelaku.
- [ ] Waspadai "jasa pemulihan dana" yang meminta biaya. Itu penipuan lanjutan.

01

BAB 1 · KATA SANDI YANG KUAT

Kata Sandi 123456 Sudah Tidak Zaman, Begini Cara Membuat yang Kuat

Kata sandi ibarat kunci rumah digital kita: email, media sosial, marketplace, sampai dompet digital. Sayangnya, banyak orang masih memakai sandi yang mudah ditebak, misalnya tanggal lahir, nama anak, atau "123456". Lebih berbahaya lagi kalau sandi yang sama dipakai di semua akun.

POIN PENTING

- Panjang lebih penting daripada rumit: minimal 12 karakter.
- Satu akun, satu kata sandi. Jangan dipakai ulang.
- Gunakan kalimat sandi (passphrase) agar mudah diingat.
- Aktifkan verifikasi dua langkah di akun penting.

Kenapa satu sandi untuk semua akun itu berbahaya?

Kebocoran data di satu situs bisa membuat email dan kata sandi Anda tersebar. Penjahat siber lalu mencoba kombinasi yang sama di akun lain: email, media sosial, bahkan aplikasi belanja. Kalau sandinya sama, semua akun bisa terbuka sekaligus. Inilah alasan **setiap akun penting wajib punya sandi berbeda**.

Cara membuat sandi yang kuat dan mudah diingat

Gunakan **kalimat sandi**: gabungan beberapa kata acak yang hanya bermakna bagi Anda, ditambah angka atau simbol.

Contoh pola (jangan dipakai persis):

- `Kopi-Pagi-Hujan-Sungai-27`
- `NasiUduk!DiTeras#2026Pagi`

Kalimat seperti ini panjang sehingga sulit ditebak mesin, tetapi tetap mudah diingat karena berupa gambaran di kepala.

Hindari:

- Tanggal lahir, nomor HP, nama sendiri atau keluarga.
- Kata umum seperti "password", "admin", "qwerty".
- Pola keyboard seperti "asdfgh" atau "1qaz2wsx".

Gunakan pengelola kata sandi (password manager)

Mengingat puluhan sandi berbeda memang sulit. Solusinya adalah **pengelola kata sandi**, aplikasi yang menyimpan semua sandi dalam brankas terenkripsi. Anda cukup mengingat satu sandi utama yang kuat.

- Bawaan HP: **Google Password Manager** (Android/Chrome) dan **Kata Sandi/iCloud Keychain** (iPhone).
- Aplikasi khusus juga tersedia dari penyedia tepercaya. Pilih yang reputasinya jelas dan unduh dari toko aplikasi resmi.

Fitur ini juga bisa **membuatkan sandi acak** dan memperingatkan bila sandi Anda pernah bocor.

Kunci tambahan: verifikasi dua langkah

Aktifkan verifikasi dua langkah (2FA) di email, media sosial, dan aplikasi keuangan. Dengan 2FA, pelaku tetap butuh kode tambahan meski sandi bocor. Bila tersedia, pilih aplikasi autentikator atau **kunci sandi (passkey)** yang memakai sidik jari atau wajah, karena lebih aman daripada SMS.

Kebiasaan aman sehari-hari

1. Jangan pernah memberikan sandi atau kode OTP kepada siapa pun, termasuk yang mengaku petugas bank.
2. Jangan menyimpan sandi di catatan HP biasa atau foto galeri.
3. Segera ganti sandi bila mendapat notifikasi login mencurigakan.
4. Keluar (logout) dari akun saat memakai komputer umum.

SUMBER BAB INI

- Disusun redaksi Pahamin Dulu dari praktik umum keamanan akun yang dianjurkan penyedia layanan digital (panjang sandi, sandi unik per akun, pengelola sandi, verifikasi dua langkah).

02

BAB 2 · KUNCI AKUN WHATSAPP

Akun WhatsApp Dibajak Bisa Dicegah, Aktifkan Fitur Ini Sekarang

Modus pembajakan WhatsApp masih sering terjadi. Pelaku biasanya mengaku kurir, petugas, atau bahkan teman, lalu meminta "kode 6 digit yang baru saja masuk". Begitu kode diberikan, akun berpindah ke tangan pelaku. Setelah itu pelaku memakai akun korban untuk meminjam uang ke semua kontak.

Ada satu fitur bawaan yang membuat pembajakan seperti ini jauh lebih sulit: **verifikasi dua langkah**.

POIN PENTING

- Kode 6 digit dari SMS WhatsApp TIDAK BOLEH diberikan ke siapa pun.
- Verifikasi dua langkah menambah PIN pribadi yang tidak dikirim lewat SMS.
- Tambahkan email agar PIN bisa dipulihkan bila lupa.

Apa itu verifikasi dua langkah?

Saat seseorang mencoba memasang WhatsApp Anda di HP lain, biasanya cukup memasukkan kode SMS. Dengan verifikasi dua langkah, ia juga harus memasukkan **PIN 6 digit buatan Anda sendiri**. Jadi meski kode SMS bocor, akun tetap aman selama PIN tidak ikut diberikan.

Cara mengaktifkannya

1. Buka WhatsApp, ketuk **Setelan** (iPhone) atau ikon titik tiga lalu **Setelan** (Android).
2. Pilih **Akun**.
3. Ketuk **Verifikasi dua langkah**, lalu **Aktifkan**.
4. Buat PIN 6 digit yang mudah Anda ingat tetapi sulit ditebak orang lain. Hindari tanggal lahir atau 123456.
5. Masukkan alamat email untuk pemulihan PIN, lalu konfirmasi email tersebut.
6. Selesai. Sesekali WhatsApp akan meminta PIN ini agar Anda tidak lupa.

Tambahan pengamanan yang disarankan

- **Kunci aplikasi:** aktifkan kunci sidik jari atau wajah di menu Privasi.
- **Kunci sandi (passkey):** bila tersedia di HP Anda, fitur ini memungkinkan masuk dengan sidik jari atau wajah.
- **Periksa perangkat tertaut:** di menu **Perangkat tertaut**, keluarkan perangkat yang tidak Anda kenali, misalnya WhatsApp Web di komputer orang lain.

Tanda-tanda akun Anda sedang diincar

- Tiba-tiba ada SMS kode WhatsApp padahal Anda tidak sedang masuk.
- Ada telepon atau chat yang meminta kode tersebut dengan berbagai alasan.
- Muncul notifikasi permintaan mengubah PIN.

Jika ini terjadi, **jangan berikan kode apa pun**. Pastikan verifikasi dua langkah aktif.

Kalau akun sudah terlanjur dibajak

1. Masuk ulang ke WhatsApp dengan nomor Anda dan masukkan kode SMS yang baru. Pelaku akan otomatis terkeluarkan.
2. Bila diminta PIN yang tidak Anda buat (pelaku sudah memasangnya), jangan menebak-nebak. Ikuti opsi atur ulang PIN di layar. Bila tidak bisa, tunggu sampai batas waktu yang ditampilkan aplikasi selesai, lalu daftarkan ulang nomor Anda.
3. Kabari keluarga dan teman lewat jalur lain agar tidak mentransfer uang ke "Anda".
4. Laporkan ke WhatsApp melalui menu bantuan atau email dukungan resmi yang tercantum di aplikasi.

SUMBER BAB INI

- Disusun redaksi Pahamin Dulu dari fitur keamanan resmi WhatsApp (verifikasi dua langkah, kunci aplikasi, perangkat tertaut). Nama menu bisa sedikit berbeda tergantung versi aplikasi.

03

BAB 3 · TOLAK GRUP WHATSAPP ASING

Sering Dimasukkan ke Grup WhatsApp Asing? Begini Cara Membatasinya

Tiba-tiba Anda menjadi anggota grup "Investasi Cuan Harian" atau "Kerja Paruh Waktu Dibayar Per Tugas" yang tidak pernah Anda ikuti. Grup seperti ini sering menjadi pintu masuk penipuan. Kabar baiknya, WhatsApp menyediakan pengaturan untuk membatasi siapa yang boleh memasukkan Anda ke grup.

POIN PENTING

- Atur privasi Grup ke "Kontak Saya" atau "Kontak Saya, kecuali...".
- Orang di luar pilihan itu harus mengirim undangan, bukan langsung memasukkan Anda.
- Keluar, laporkan, dan blokir bila terlanjur dimasukkan ke grup mencurigakan.

Cara mengatur siapa yang bisa memasukkan Anda ke grup

1. Buka WhatsApp, lalu masuk ke **Setelan** (iPhone) atau ketuk ikon titik tiga lalu **Setelan** (Android).

2. Pilih **Privasi**.
3. Ketuk **Grup**.
4. Pilih salah satu:
   - **Semua orang:** siapa pun bisa memasukkan Anda ke grup. Ini yang paling berisiko.
   - **Kontak Saya:** hanya orang yang tersimpan di kontak Anda.
   - **Kontak Saya, kecuali...:** seperti Kontak Saya, tetapi Anda bisa mengecualikan kontak tertentu.
5. Simpan pilihan Anda.

Setelah diatur, orang yang tidak diizinkan hanya bisa mengirim **undangan pribadi** untuk bergabung. Anda bebas menerima atau mengabaikannya.

Kalau terlanjur dimasukkan ke grup mencurigakan

1. **Jangan klik tautan** apa pun yang dibagikan di grup, dan jangan mengirim data pribadi.
2. Buka info grup, lalu pilih **Laporkan grup**. Anda bisa sekaligus keluar dari grup.
3. **Blokir** nomor admin yang memasukkan Anda, terutama bila nomornya berawalan kode negara asing yang tidak Anda kenal.

Tambahan pengaturan yang membantu

- **Bisukan panggilan dari nomor tak dikenal:** di **Privasi > Panggilan**, aktifkan **Bisukan penelepon tak dikenal**.
- **Batasi siapa yang melihat foto profil dan info "terakhir dilihat"** di menu Privasi, agar data Anda tidak mudah dikumpulkan orang asing.

- **Aktifkan verifikasi dua langkah** di **Setelan > Akun** untuk mencegah pembajakan akun.

Undangan lewat tautan grup

Selain dimasukkan langsung, Anda juga bisa diajak bergabung lewat **tautan undangan grup** yang dibagikan di media sosial atau pesan pribadi. Sebelum menekan tautan seperti ini, cek dulu siapa yang membagikannya dan apa tujuan grupnya. Pengaturan privasi di atas tidak bisa mencegah Anda bergabung sendiri lewat tautan, jadi kehati-hatian tetap diperlukan.

Bantu orang tua mengaturnya

Orang tua dan kerabat yang baru memakai WhatsApp sering menjadi sasaran grup penipuan. Luangkan waktu lima menit untuk:

1. Mengubah pengaturan **Privasi > Grup** di HP mereka menjadi **Kontak Saya**.
2. Mengaktifkan **Bisukan penelepon tak dikenal**.
3. Menjelaskan bahwa ajakan "kerja mudah dibayar per tugas" dan "investasi untung pasti" adalah tanda bahaya.
4. Menyimpan nomor Anda sebagai tempat bertanya bila mereka ragu.

Kenali ciri grup penipuan

- Menjanjikan keuntungan tetap atau komisi besar untuk tugas mudah.
- Banyak anggota yang terlihat "sukses" dan memamerkan bukti transfer.
- Admin meminta deposit atau transfer untuk "naik level".
- Diarahkan pindah ke aplikasi lain, misalnya Telegram, untuk "tugas lanjutan".

Modus kerja paruh waktu berbasis deposit dan investasi dengan janji untung tinggi termasuk yang disorot menjelang akhir 2026. Bila sudah mentransfer uang, segera hubungi bank dan laporkan ke **iasc.ojk.go.id**.

SUMBER BAB INI

- Disusun redaksi Pahamin Dulu dari pengaturan privasi resmi WhatsApp. Nama menu bisa sedikit berbeda tergantung versi aplikasi.
- Katadata — https://katadata.co.id/lifestyle/varia/6ad7321d98974/modus-penipuan-terbaru-menjelang-akhir-tahun-2026-waspadai-investasi-bodong

04

BAB 4 · CEK EMAIL YANG BOCOR

Email Anda Ikut Bocor? Cara Mengecek dan Langkah Setelahnya

Kabar kebocoran data dari aplikasi atau situs tertentu muncul hampir setiap bulan. Pertanyaannya: apakah email Anda ikut bocor? Ada cara sederhana untuk mengeceknya, dan yang lebih penting, ada langkah jelas untuk mengamankan akun setelah itu.

POIN PENTING

- Cek email Anda di situs **haveibeenpwned.com**.
- Ganti kata sandi akun yang terdampak, terutama bila sandinya dipakai di tempat lain.
- Aktifkan verifikasi dua langkah di email dan akun penting.
- Waspadai email atau pesan "resmi" setelah kebocoran, karena sering berupa phishing.

Cara mengecek

1. Buka **haveibeenpwned.com** di browser. Situs ini dikelola peneliti keamanan dan sudah lama dipakai untuk mengecek kebocoran data.
2. Ketik alamat email Anda, lalu klik tombol pencarian.

3. Bila muncul tulisan berwarna hijau, email Anda tidak ditemukan di kebocoran yang tercatat.
4. Bila muncul tulisan berwarna merah, situs akan menampilkan daftar kebocoran yang memuat email Anda, lengkap dengan jenis data yang ikut bocor (misalnya kata sandi, nomor telepon, atau alamat).

Anda juga bisa mendaftarkan email untuk mendapat **pemberitahuan** bila email muncul di kebocoran baru.

Hasil "aman" bukan jaminan mutlak, karena tidak semua kebocoran tercatat. Kebiasaan keamanan di bawah tetap penting.

Kalau email Anda muncul di kebocoran

1. Ganti kata sandi akun yang terdampak. Mulai dari layanan yang disebut dalam daftar kebocoran.

2. Ganti juga di akun lain yang memakai sandi yang sama. Penjahat siber biasa mencoba pasangan email dan sandi yang bocor di banyak layanan sekaligus. Satu akun, satu sandi.

3. Aktifkan verifikasi dua langkah di email utama, media sosial, marketplace, dan aplikasi keuangan. Dengan cara ini, sandi yang bocor saja tidak cukup untuk masuk.

4. Periksa aktivitas login. Di akun Google, buka **Kelola Akun Google > Keamanan > Perangkat Anda**. Keluarkan perangkat yang tidak Anda kenali.

5. Gunakan pengelola kata sandi bawaan HP atau browser untuk membuat dan menyimpan sandi acak yang panjang.

Dari mana kebocoran biasanya terjadi?

Kebocoran tidak selalu karena kesalahan Anda. Data bisa bocor ketika sebuah situs atau aplikasi diretas, ketika basis data tersimpan tanpa pengamanan memadai, atau ketika karyawan pihak ketiga menyalahgunakan akses. Yang bisa Anda kendalikan adalah dampaknya: sandi berbeda di setiap akun dan verifikasi dua langkah membuat data yang bocor jauh lebih sulit disalahgunakan.

Pertimbangkan kunci sandi (passkey)

Semakin banyak layanan, termasuk akun Google dan Apple, mendukung **kunci sandi (passkey)**: masuk dengan sidik jari, wajah, atau PIN perangkat, tanpa mengetik kata sandi. Passkey tidak bisa dicuri lewat kebocoran sandi atau situs phishing, sehingga lebih aman. Aktifkan bila tersedia di pengaturan keamanan akun Anda.

Waspada penipuan lanjutan

Setelah kebocoran, pelaku sering mengirim pesan yang terlihat resmi: "Akun Anda bermasalah, verifikasi di sini." Jangan klik tautan di pesan seperti itu. Buka aplikasi atau situs resmi layanan secara langsung bila ingin mengecek akun.

Bila nomor HP Anda ikut bocor, waspadai telepon atau chat dari pihak yang mengaku petugas dan meminta kode OTP. Bank, OJK, dan instansi resmi tidak pernah meminta OTP.

Bila data bocor dipakai untuk penipuan keuangan

Hubungi call center resmi bank Anda dan laporkan ke **Indonesia Anti-Scam Centre (IASC)** di **iasc.ojk.go.id**.

SUMBER BAB INI

- Disusun redaksi Pahamin Dulu. Layanan pengecekan: Have I Been Pwned — https://haveibeenpwned.com

05

BAB 5 · KENALI LINK PHISHING

Link Hadiah dan Ancaman Blokir Akun: Cara Mengenali Phishing

"Selamat! Anda mendapat hadiah Rp5 juta, klaim di sini." Atau sebaliknya: "Akun Anda akan diblokir dalam 24 jam, segera verifikasi." Dua pesan ini terlihat berbeda, tetapi tujuannya sama: membuat Anda mengklik tautan dan memasukkan data. Inilah yang disebut **phishing**.

POIN PENTING

- Phishing memakai situs palsu yang meniru tampilan resmi.
- Cek alamat situs dengan teliti, bukan hanya tampilannya.
- Bank dan instansi resmi tidak meminta PIN, OTP, atau kata sandi.
- Masuk ke layanan lewat aplikasi resmi, bukan lewat link di chat.

Apa itu phishing?

Phishing (dibaca "fising") berasal dari kata *fishing*, memancing. Pelaku "memancing" korban dengan umpan berupa hadiah, ancaman pemblokiran, atau tawaran menarik. Tautan di pesan itu membawa ke **situs palsu** yang tampilannya mirip sekali dengan bank, marketplace, atau instansi pemerintah. Data yang diketik di situ langsung jatuh ke tangan pelaku.

Ciri-ciri pesan phishing

1. **Mendesak dan menakut-nakuti:** "dalam 1x24 jam", "terakhir hari ini".
2. **Terlalu indah:** hadiah, undian, atau cashback besar yang tidak pernah Anda ikuti.
3. **Meminta data rahasia:** PIN, OTP, kata sandi, nomor kartu, atau foto KTP sambil memegang kartu.
4. **Pengirim tidak resmi:** nomor pribadi, email gratisan, atau akun tanpa centang resmi.
5. **Bahasa janggal:** salah ketik atau tata bahasa aneh, meski kini pelaku makin rapi.

Cara mengecek alamat situs

Perhatikan alamat di bilah browser, bukan tampilan halamannya:

- Situs palsu sering mengganti satu huruf (misalnya huruf "l" diganti angka "1"), menambah kata ("-promo", "-verifikasi"), atau memakai akhiran domain aneh.
- Situs instansi pemerintah Indonesia berakhiran **.go.id**.
- Ikon gembok (HTTPS) **bukan jaminan aman**. Situs palsu pun kini bisa memasangnya.
- Tautan pendek (bit.ly dan sejenisnya) menyembunyikan alamat aslinya. Waspadai bila datang dari pengirim tak dikenal.

Kebiasaan yang paling ampuh

Jangan masuk ke akun lewat link di chat, SMS, atau email. Buka aplikasi resminya langsung, atau ketik sendiri alamat situsnya. Kalau memang ada masalah dengan akun Anda, informasinya akan muncul di aplikasi resmi.

Ingat juga: bank, OJK, dan instansi pemerintah tidak pernah meminta PIN, OTP, atau kata sandi melalui telepon maupun chat.

Kalau terlanjur memasukkan data

1. **Segera ganti kata sandi** akun yang bersangkutan dari aplikasi atau situs resmi.
2. Bila data bank yang bocor, **hubungi call center resmi bank** dan minta pemblokiran.
3. Keluarkan semua perangkat yang tertaut di pengaturan akun.
4. Bila ada kerugian dana, **laporkan ke Indonesia Anti-Scam Centre (IASC) melalui iasc.ojk.go.id** atau lewat bank Anda. Untuk informasi, Layanan Konsumen OJK dapat dihubungi di **157**.
5. Laporkan situs atau akun penipu ke **aduankonten.id**.

SUMBER BAB INI

- OJK — https://www.ojk.go.id/id/berita-dan-kegiatan/info-terkini/Documents/Pages/Tingkatkan-Pelindungan-Konsumen-Satgas-Pasti-Lakukan-Soft-Launching-IASC/SP%20Satgas%20Pasti%20Soft%20Launching%20IASC.pdf

06

BAB 6 · JANGAN PASANG FILE APK

Awas APK Berkedok Undangan dan Surat Tilang, Rekening Bisa Terkuras

Pesan masuk dari nomor tak dikenal: "Assalamualaikum, mohon kehadirannya di acara pernikahan kami", lengkap dengan lampiran berakhiran **.apk**. Ada juga versi lain: "Ini foto resi paket Anda", "Surat tilang elektronik", atau "Tagihan BPJS". Modus ini sudah lama ada dan terus berganti kedok. Dalam rangkuman Katadata (20 Oktober 2026), penipuan lewat aplikasi palsu termasuk modus yang perlu diwaspadai menjelang akhir tahun.

POIN PENTING

- Undangan, foto, atau resi asli TIDAK berbentuk file .apk.
- APK berbahaya bisa membaca SMS, termasuk kode OTP bank.
- Jangan pernah memasang aplikasi dari luar Play Store/App Store.
- Bila terlanjur memasang: putuskan internet, hubungi bank, laporkan.

Kenapa file APK berbahaya?

APK adalah format file pemasang aplikasi Android. Saat dipasang, aplikasi jahat biasanya meminta izin membaca SMS, notifikasi, atau mengendalikan layar. Dengan izin itu, pelaku dapat mencuri kode OTP dan data akun, lalu menguras rekening atau mengambil alih akun media sosial korban.

Ciri-ciri pesan penipuan APK

- Dikirim dari nomor tidak dikenal, kadang memakai foto profil instansi atau kurir.
- Lampiran berakhiran **.apk**, padahal disebut "foto", "PDF", atau "undangan".
- Ada desakan: "segera cek", "tagihan jatuh tempo hari ini", "paket akan dikembalikan".
- Meminta mengaktifkan "instal dari sumber tidak dikenal".

Cara melindungi diri

1. **Jangan buka file .apk dari chat**, siapa pun pengirimnya. Akun teman pun bisa saja sudah dibajak.
2. Pasang aplikasi hanya dari **Google Play Store** atau **App Store**.
3. Biarkan pengaturan **"Instal aplikasi tidak dikenal"** tetap nonaktif.
4. Aktifkan **Google Play Protect** di Play Store (ketuk foto profil, lalu Play Protect).
5. Cek kebenaran tagihan atau tilang langsung ke aplikasi atau situs resmi instansinya, bukan lewat tautan di chat.

Kalau terlanjur memasang: lakukan segera

1. **Matikan data seluler dan Wi-Fi** untuk memutus koneksi aplikasi jahat.
2. **Hubungi call center resmi bank** (nomor di balik kartu ATM atau situs resmi bank) dan minta blokir sementara akun atau kartu.
3. Hapus aplikasi mencurigakan dari menu Pengaturan > Aplikasi. Bila tidak bisa dihapus, bawa HP ke service center dan pertimbangkan reset pabrik setelah data penting dicadangkan.
4. Ganti kata sandi email, media sosial, dan mobile banking dari **perangkat lain yang aman**.
5. Bila sudah ada dana yang berpindah, **laporkan secepatnya ke Indonesia Anti-Scam Centre (IASC) di iasc.ojk.go.id** atau melalui bank Anda. OJK menegaskan bahwa kecepatan melapor memengaruhi besar dana yang masih bisa diselamatkan.

Kesimpulan

Satu klik pada file yang salah bisa berakibat besar. Ingat aturan sederhananya: **undangan dan foto tidak pernah berbentuk APK**. Kalau ragu, tanyakan langsung ke pengirim lewat telepon, jangan lewat chat yang sama.

SUMBER BAB INI

- Katadata — https://katadata.co.id/lifestyle/varia/6ad7321d98974/modus-penipuan-terbaru-menjelang-akhir-tahun-2026-waspadai-investasi-bodong
- OJK — https://www.ojk.go.id/id/berita-dan-kegiatan/info-terkini/Documents/Pages/Tingkatkan-Pelindungan-Konsumen-Satgas-Pasti-Lakukan-Soft-Launching-IASC/SP%20Satgas%20Pasti%20Soft%20Launching%20IASC.pdf

07

BAB 7 · WASPADAI VIDEO CALL PALSU

Wajah dan Suaranya Mirip, Tapi Palsu: Kenali Penipuan Berbasis AI

"Ma, ini Adi. HP-ku rusak, pakai nomor teman dulu. Tolong transfer sekarang ya, darurat." Suaranya persis seperti anak sendiri. Atau video seorang tokoh terkenal yang tampak meyakinkan sedang mempromosikan investasi. Dengan teknologi kecerdasan buatan (AI), wajah dan suara kini bisa ditiru, dan penipu sudah memanfaatkannya.

POIN PENTING

- IASC menerima 1.379 aduan penipuan yang diduga memakai AI hingga akhir Juni 2026.
- Suara, wajah, dan video yang diterima secara digital bisa dipalsukan.
- Selalu verifikasi lewat jalur lain sebelum mentransfer uang.
- Sepakati "kata kunci keluarga" untuk keadaan darurat.

Seberapa sering terjadi?

Otoritas Jasa Keuangan (OJK) mencatat, Indonesia Anti-Scam Centre (IASC) menerima **1.379 laporan** penipuan keuangan yang diduga memanfaatkan AI, terhitung sejak IASC beroperasi pada 22 November 2024 hingga akhir Juni 2026. Jumlahnya naik dari 13 laporan pada akhir 2024 menjadi 1.366 laporan sepanjang 2025 hingga Juni 2026.

Enam modus yang dicatat OJK

1. **Deepfake tokoh publik:** video atau foto palsu artis, pejabat, atau tokoh terkenal yang seolah mempromosikan investasi.
2. **Robot trading "AI":** program yang diklaim memakai AI dan pasti untung.
3. **Aplikasi belanja berlabel AI palsu** yang sebenarnya bertujuan mencuri uang atau data.
4. **Suara tiruan (voice cloning):** meniru suara orang yang dikenal korban untuk meminta uang atau data.
5. **Wajah atau video palsu:** video buatan AI agar seseorang tampak nyata, termasuk saat panggilan video.
6. **Pemalsuan identitas digital:** foto, suara, nomor telepon, nomor rekening, atau dokumen yang dipalsukan agar terlihat asli.

Tanda-tanda yang perlu dicurigai

- **Permintaan mendesak** untuk transfer uang, dengan alasan darurat atau rahasia.
- **Nomor baru** atau akun berbeda dari yang biasa dipakai orang tersebut.
- Pada video: **gerak bibir tidak pas** dengan suara, kedipan mata janggal, wajah tampak kabur di tepi, atau pencahayaan aneh.

- Penelepon **menghindari pertanyaan pribadi** atau mengakhiri panggilan saat diminta melakukan sesuatu, misalnya menoleh ke samping.
- **Janji keuntungan pasti** dari "tokoh terkenal".

Cara melindungi diri dan keluarga

1. **Verifikasi lewat jalur lain.** Tutup telepon, lalu hubungi orang itu di nomor lama yang sudah Anda simpan, atau tanyakan ke anggota keluarga lain.
2. **Sepakati kata kunci keluarga**, misalnya satu kata yang hanya diketahui keluarga, untuk memastikan permintaan darurat benar-benar dari mereka.
3. **Jangan percaya nama, foto, suara, atau video** yang diterima secara digital sebagai bukti tunggal. Ini juga anjuran OJK.
4. **Jangan memberikan PIN, kata sandi, atau OTP** kepada siapa pun.
5. **Batasi rekaman suara dan video pribadi** yang diunggah ke publik, karena bisa dipakai sebagai bahan tiruan.
6. **Cek legalitas investasi** di situs atau kontak resmi OJK (157) sebelum menanam uang, meskipun dipromosikan tokoh terkenal.

Lindungi orang tua dan kerabat

Orang tua sering menjadi sasaran suara tiruan yang mengaku anak atau cucu. Bicarakan modus ini dengan mereka, sepakati kata kunci keluarga, dan tegaskan bahwa permintaan uang mendadak lewat telepon harus selalu dicek ulang ke anggota keluarga lain. Simpan nomor penting keluarga di HP mereka dengan nama yang jelas, supaya mereka mudah menelepon balik ke nomor yang benar.

Bila sudah terlanjur mentransfer

Segera hubungi bank atau penyedia pembayaran untuk menunda atau memblokir transaksi, lalu laporkan ke **iasc.ojk.go.id** dan kepolisian.

SUMBER BAB INI

- Katadata — https://katadata.co.id/finansial/keuangan/6a71e479d5349/ojk-ungkap-6-modus-penipuan-keuangan-berbasis-ai-sudah-ada-1379-kasus

08

BAB 8 · CEK REKENING SEBELUM TRANSFER

Sebelum Transfer ke Orang Asing, Cek Dulu Rekeningnya di Sini

Membeli barang dari penjual di media sosial atau marketplace di luar fitur pembayaran resmi memang praktis, tetapi berisiko. Sebelum mentransfer uang ke rekening orang yang belum pernah Anda temui, luangkan satu menit untuk mengecek apakah rekening itu pernah dilaporkan terkait penipuan.

POIN PENTING

- Cek nomor rekening atau e-wallet di **cekrekening.id**.
- Hasil "tidak ditemukan" bukan jaminan aman.
- Utamakan pembayaran lewat fitur resmi marketplace.
- Bila tertipu, segera hubungi bank dan lapor ke IASC.

Cara mengecek di cekrekening.id

cekrekening.id adalah situs pemerintah untuk mengecek rekening yang pernah dilaporkan terkait tindak penipuan.

1. Buka **cekrekening.id** di browser.
2. Pilih menu **Periksa Rekening**.
3. Pilih jenis: **bank** atau **e-wallet**.

4. Pilih nama bank atau penyedia, lalu masukkan nomor rekening atau nomor akun.
5. Klik **Periksa**.

Bila rekening pernah dilaporkan, hasil pencarian akan menampilkan keterangan laporan. Bila tidak ditemukan, artinya belum ada laporan yang tercatat. **Itu belum tentu berarti aman**, karena pelaku sering berganti rekening.

Tanda bahaya sebelum transfer

- **Harga jauh di bawah pasaran**, apalagi untuk barang elektronik atau tiket konser.
- **Penjual mendesak** agar segera transfer dengan alasan stok terbatas.
- **Nama pemilik rekening berbeda** dengan nama penjual atau nama toko.
- **Menolak COD atau pembayaran lewat fitur marketplace**, dan meminta transfer langsung.
- **Akun baru**, sedikit unggahan, atau kolom komentar ditutup.
- **Mengirim bukti transfer** atau bukti pengiriman yang terlihat janggal. Bukti seperti ini kini mudah dipalsukan dengan aplikasi edit dan AI.

Cara mengenali bukti transfer palsu

Penipu kadang berbalik peran: berpura-pura menjadi pembeli dan mengirim "bukti transfer" agar Anda mengirim barang. Sebelum mengirim barang:

1. **Cek mutasi rekening** di aplikasi bank Anda sendiri. Jangan hanya percaya tangkapan layar.
2. **Perhatikan detailnya**: format tanggal, jam, logo, dan nomor referensi yang janggal.

3. **Waspadai alasan "dana tertahan"** atau "transfer antarbank masih diproses" yang disertai desakan agar barang segera dikirim.
4. **Jangan pernah mengembalikan dana "salah transfer"** ke rekening lain atas permintaan orang tak dikenal. Arahkan mereka untuk mengurusnya melalui bank.

Cara bertransaksi lebih aman

1. Gunakan **fitur pembayaran resmi** di marketplace, karena dana baru diteruskan ke penjual setelah barang diterima.
2. Untuk transaksi langsung, utamakan **COD** atau bertemu di tempat ramai.
3. Cari nama penjual, nomor HP, dan nomor rekening di mesin pencari. Kadang sudah ada keluhan korban lain.
4. Jangan pernah mengirim **kode OTP** kepada penjual dengan alasan apa pun.

Kalau sudah terlanjur tertipu

1. **Telepon call center resmi bank** Anda dan minta pemblokiran atau penundaan transaksi.
2. **Laporkan ke Indonesia Anti-Scam Centre (IASC)** di **iasc.ojk.go.id**. Semakin cepat dilaporkan, semakin besar peluang dana masih bisa ditahan.
3. Simpan semua bukti percakapan dan transfer, lalu buat laporan ke kepolisian.

SUMBER BAB INI

- CNN Indonesia — https://www.cnnindonesia.com/edukasi/20251027112051-561-1288791/cara-cek-rekening-aman-atau-tidak-agar-bebas-dari-penipuan

- OJK — https://www.ojk.go.id/id/berita-dan-kegiatan/info-terkini/Documents/Pages/Tingkatkan-Pelindungan-Konsumen-Satgas-Pasti-Lakukan-Soft-Launching-IASC/SP%20Satgas%20Pasti%20Soft%20Launching%20IASC.pdf

09

BAB 9 · SARING HOAKS SEBELUM MEMBAGIKAN

Sebelum Klik Bagikan: 6 Cara Sederhana Mengenali Hoaks

Pesan berantai di grup keluarga, video potongan di media sosial, atau tangkapan layar "surat edaran" sering menyebar lebih cepat dari klarifikasinya. Sekali dibagikan, hoaks sulit ditarik kembali. Karena itu, kebiasaan paling penting di era digital sederhana saja: **pahamin dulu, baru bagikan**.

POIN PENTING

- Judul yang memancing emosi adalah tanda bahaya pertama.
- Cek sumbernya: media resmi atau akun tak jelas?
- Gunakan situs cek fakta sebelum percaya.
- Kalau ragu, jangan dibagikan.

1. Waspadai judul yang memancing emosi

Kalimat seperti "SEBARKAN SEBELUM DIHAPUS!", "Viral! Pemerintah diam-diam...", atau penuh huruf kapital dan tanda seru adalah ciri khas hoaks. Tujuannya membuat kita panik atau marah sehingga langsung membagikan tanpa berpikir.

2. Cek sumber aslinya

Tanyakan: siapa yang pertama kali menyampaikan? Kabar resmi dari pemerintah biasanya juga dimuat di situs resmi instansi (berakhiran **.go.id**) atau akun media sosial resmi bercentang. Kalau kabar besar hanya beredar di grup WhatsApp tanpa satu pun media kredibel yang memberitakan, patut dicurigai.

3. Perhatikan alamat situs

Hoaks sering memakai situs yang namanya mirip media terkenal, dengan sedikit perbedaan huruf atau akhiran domain yang aneh. Baca alamatnya pelan-pelan sebelum percaya.

4. Periksa tanggal dan konteks

Banyak "kabar baru" ternyata berita lama yang diedarkan ulang. Foto bencana dari negara lain atau dari tahun lalu juga sering diberi keterangan seolah terjadi hari ini. Cari tanggal aslinya.

5. Cek foto dan video

Gunakan pencarian gambar terbalik (*reverse image search*) di Google Lens: tekan lama gambar, lalu pilih cari dengan Google Lens. Dari sini sering ketahuan bahwa foto itu sudah beredar bertahun-tahun dengan cerita berbeda. Waspadai juga video atau suara hasil rekayasa AI yang meniru tokoh terkenal.

6. Gunakan situs cek fakta

Beberapa kanal yang bisa dipakai untuk mengecek kebenaran kabar:

- **cekfakta.com**: kolaborasi sejumlah media dan pemeriksa fakta di Indonesia.
- **turnbackhoax.id**: dikelola Masyarakat Antifitnah Indonesia (Mafindo).

- Situs dan akun resmi instansi terkait (kementerian, pemerintah daerah, kepolisian).

Untuk melaporkan konten negatif di internet, gunakan kanal aduan resmi Kementerian Komunikasi dan Digital di **aduankonten.id**.

Kalau sudah terlanjur membagikan

Tidak apa-apa, semua orang bisa keliru. Hapus pesannya bila masih bisa, lalu kirim klarifikasi ke grup yang sama. Langkah kecil ini membantu memutus rantai hoaks.

Kesimpulan

Kita tidak harus jadi ahli untuk melawan hoaks. Cukup berhenti sejenak sebelum menekan tombol bagikan, lalu tanyakan: dari mana sumbernya, kapan kejadiannya, dan apakah media tepercaya juga memberitakannya.

SUMBER BAB INI

- Disusun redaksi Pahamin Dulu. Kanal rujukan: cekfakta.com, turnbackhoax.id (Mafindo), aduankonten.id (Komdigi).

10

BAB 10 · KALAU SUDAH TERLANJUR TERTIPU

Jadi Korban Penipuan Online? Lakukan 6 Langkah Ini Secepatnya

Tertipu belanja online, "investasi" palsu, atau kerja paruh waktu berkedok tugas memang menyakitkan. Tapi jangan larut dalam panik atau malu. Dalam kasus penipuan transfer, **waktu sangat menentukan**. Semakin cepat dilaporkan, semakin besar peluang dana masih bisa ditahan sebelum dipindahkan pelaku.

Sejak 22 November 2024, Indonesia punya **Indonesia Anti-Scam Centre (IASC)**, pusat penanganan penipuan yang dikoordinasikan OJK bersama bank dan penyedia jasa keuangan. Menurut OJK, hingga 30 September 2026 IASC telah menerima 702.342 laporan. Dana korban yang berhasil diblokir mencapai Rp811,1 miliar, dan Rp207,16 miliar di antaranya sudah dikembalikan kepada korban.

POIN PENTING

- Laporkan secepat mungkin, idealnya dalam hitungan jam.
- Hubungi bank Anda dan lapor ke IASC: **iasc.ojk.go.id**.
- Simpan semua bukti, jangan hapus chat dengan pelaku.
- Waspadai "jasa pemulihan dana" yang meminta biaya. Itu penipuan lanjutan.

Langkah 1: Hubungi bank atau e-wallet Anda

Telepon **call center resmi** bank atau dompet digital yang Anda gunakan. Nomornya ada di balik kartu ATM atau di aplikasi resmi. Jelaskan bahwa Anda korban penipuan, sebutkan nomor rekening tujuan, nominal, dan waktu transfer. Minta laporan diteruskan ke IASC.

Langkah 2: Laporkan ke IASC

Buka **iasc.ojk.go.id** dari HP, isi data kejadian, dan unggah bukti. Laporan ini dikoordinasikan dengan bank-bank anggota IASC untuk menunda transaksi dan memblokir rekening yang terkait penipuan. Informasi lebih lanjut: **Layanan Konsumen OJK 157** atau email **iasc@ojk.go.id**.

Langkah 3: Kumpulkan dan simpan bukti

- Tangkapan layar percakapan dengan pelaku (nama, nomor, akun).
- Bukti transfer: tanggal, jam, nominal, rekening tujuan.
- Tautan situs, iklan, atau akun media sosial pelaku.
- Nomor telepon yang dipakai pelaku.

Jangan hapus chat dan jangan memblokir pelaku sebelum bukti tersimpan lengkap.

Langkah 4: Lapor ke kepolisian

Buat laporan di kantor polisi terdekat atau lewat kanal resmi Polri. Bawa bukti yang sudah dikumpulkan. Laporan polisi juga sering dibutuhkan untuk proses lanjutan di bank.

Langkah 5: Amankan akun-akun Anda

Bila Anda sempat memberikan kode OTP, PIN, atau memasang aplikasi dari pelaku, segera ganti kata sandi akun penting dari perangkat yang aman, keluarkan perangkat asing dari akun, dan minta bank memblokir kartu atau akses mobile banking sementara.

Langkah 6: Peringatkan orang terdekat

Ceritakan kejadian Anda kepada keluarga dan teman. Bila akun media sosial atau WhatsApp Anda dipakai pelaku, kabari kontak Anda lewat jalur lain agar tidak ikut tertipu.

Hati-hati penipuan lanjutan

Setelah menjadi korban, banyak orang dihubungi pihak yang mengaku bisa "mengembalikan dana" dengan imbalan biaya di muka. **Ini hampir selalu penipuan kedua.** Pelaporan ke bank dan IASC tidak dipungut biaya.

Modus yang sedang marak

Katadata (20 Oktober 2026) merangkum sejumlah modus yang patut diwaspadai menjelang akhir 2026: diskon belanja online yang tidak masuk akal, kerja paruh waktu dengan sistem deposit, investasi dengan janji untung tinggi, aplikasi palsu, pemalsuan identitas disertai ancaman menyebarkan data, pinjol ilegal, serta transfer "salah kirim" yang diminta dikembalikan.

SUMBER BAB INI

- Kontan — https://keuangan.kontan.co.id/news/iasc-terima-702342-laporan-kasus-penipuan-hingga-september-2026
- OJK — https://www.ojk.go.id/id/berita-dan-kegiatan/info-terkini/Documents/Pages/Tingkatkan-Pelindungan-Konsumen-Satgas-Pasti-Lakukan-Soft-Launching-IASC/SP%20Satgas%20Pasti%20Soft%20Launching%20IASC.pdf

- Katadata — https://katadata.co.id/lifestyle/varia/6ad7321d98974/modus-penipuan-terbaru-menjelang-akhir-tahun-2026-waspadai-investasi-bodong



Pahamin dulu, baru bertindak.

Sebelum percaya, sebelum daftar, sebelum bagikan.

Panduan lain tentang layanan publik, teknologi, lowongan kerja, beasiswa, dan resep tersedia gratis.

pahamindulu.id

© 2026 Pahamin Dulu · Boleh dibagikan gratis tanpa diubah dan tidak untuk dijual.