

KELUARGA AMAN DIGITAL:

MELINDUNGI IBU DAN ANAK
DI RUANG SIBER





ZOOM
MEETING

GAME
ONLINE

ONLINE SHOP



PROMO!



LIHAT KABAR DARI
TEMAN-TEMAN SEWAKTU
MUDA DULU



YouTube

Penetrasi Internet di Indonesia

Dalam satu dekade terakhir, penetrasi internet di Indonesia meningkat signifikan.
Pada 2024, sekitar **4 dari 5 penduduk** Indonesia telah terhubung ke internet.

TINGKAT PENETRASI INTERNET INDONESIA DARI TAHUN KE TAHUN

(Persentase dari total populasi)



PER 2024



281,6 juta jiwa

Total populasi Indonesia 2024*
(Proyeksi penduduk pertengahan tahun/Juni 2024)



79,5%

Penetrasi internet 2024**
Dari total populasi Indonesia telah menggunakan internet



221,56 juta orang

Pengguna internet di Indonesia 2024**
≈ 4 dari 5 penduduk Indonesia telah terhubung ke internet

PETERANGAN:

* Sumber: Badan Pusat Statistik (BPS) – Proyeksi Penduduk Indonesia 2020–2050 hasil Sensus Penduduk 2020 (pertengahan tahun/Juni 2024)

** Sumber: APJII, dikutip dalam Laporan Kinerja Kementerian Komdigi 2024, Gambar 3.4

“Ruang digital telah berubah dari ruang tambahan menjadi bagian integral kehidupan masyarakat Indonesia.

PRE-BOOMERS
≥ 79 tahun



POST GEN Z
< 12 tahun



BABY BOOMERS
60 – 78 tahun



GEN X
44 – 59 tahun

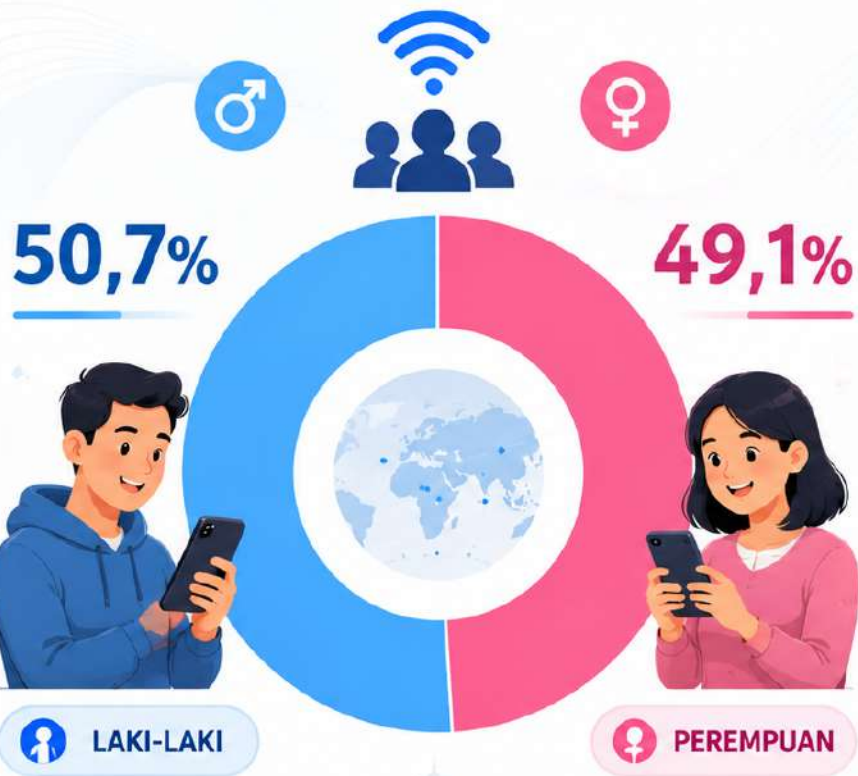


GEN Z
12 – 27 tahun



MILENIAL
28 – 43 tahun







8 dari 10
Ibu Rumah Tangga
di Indonesia
telah Menggunakan
Internet
(84,76%)
Sumber: Survei APJII 2024



NEGARA YANG PALING SERING DIKAITKAN DENGAN ONLINE SCAM CENTRES / SCAM COMPOUNDS DI ASIA TENGGARA

SCAM CENTRE
TARGET 100 / DAY

HOTSPOT UTAMA



MYANMAR

Banyak scam compounds di wilayah perbatasan (Myawaddy, Shwe Kokko, Kokang, dll)



KAMBOJA

Lokasi utama scam compounds (Sihanoukville, Poipet, Bavet, dll)



LAOS

Golden Triangle Special Economic Zone (GTSEZ)



LOKASI OPERASI LAIN



FILIPINA

Operasi POGO dan offshore scam centres di berbagai wilayah



MALAYSIA

Lokasi perekrutan, fasilitas dan operasi scam centres

HUB / TRANSIT PERDAGANGAN ORANG



THAILAND

Semakin berperan sebagai hub perdagangan orang dan jalur transit / pemulangan korban

TRAFFICKING HOTSPOT



VIETNAM

Wilayah rawan rekrutmen dan perdagangan orang

!
ONLINE SCAMMER

PENIPUAN ONLINE DI INDONESIA

Data resmi Indonesia Anti-Scam Centre (IASC) & Otoritas Jasa Keuangan (OJK)

 Periode: 22 November 2024 – 28 Desember 2025



411.055

LAPORAN SCAM

Laporan yang diterima IASC melalui bank/penyedia pembayaran dan langsung ke IASC.



Rp9 TRILIUN

KERUGIAN DILAPORKAN

Total nilai kerugian yang dilaporkan masyarakat kepada IASC.



127.047

REKENING DIBLOKIR

Rekening yang berhasil diblokir untuk mencegah kerugian lebih lanjut.



681.890

REKENING DILAPORKAN

Rekening dilaporkan terkait aktivitas penipuan online.

 Sumber: Indonesia Anti-Scam Centre (IASC) & Otoritas Jasa Keuangan (OJK)

 IASC adalah inisiatif kolaboratif OJK, Bank Indonesia, Kementerian Kominfo, dan industri jasa keuangan untuk menampung laporan penipuan (scam) dan menindaklanjutinya secara cepat.



Ancaman Siber yang Sering Mengintai Ibu Rumah Tangga

Penipuan Marketplace



Penipuan Perbankan



Pencurian Data Pribadi



Pembajakan akun



Disinformasi





PENIPUAN MARKETPLACE DENGAN TARGET KAUM IBU

Pelaku memanfaatkan aktivitas belanja online yang semakin populer di kalangan ibu rumah tangga untuk mendapatkan uang dan data pribadi secara tidak sah.

1 TUJUAN / SASARAN PELAKU



Uang korban



Data pribadi



Kredensial akun



Akses ke akun



2 TEKNIK / MODUS YANG DIGUNAKAN



Toko / penjual palsu



Harga / promo tidak wajar



Social engineering



Phishing / Smishing



Tautan pembayaran palsu



Mengaku sebagai admin marketplace



WASPADA SELALU!

Belanja aman, keluarga nyaman.
Jangan sampai tertipu di ruang siber.



PENIPUAN PERBANKAN DENGAN TARGET KAUM IBU

Modus penipuan perbankan memanfaatkan kepercayaan dan kepedulian ibu untuk memperoleh akses ke rekening, uang, atau data pribadi korban.

1 APA ITU PENIPUAN PERBANKAN?



Tindakan kejahatan yang dilakukan untuk mengelabui korban agar memberikan akses ke rekening, uang, atau data pribadi korban.



Pelaku berpura-pura sebagai pihak bank atau lembaga resmi untuk meminta kode OTP, PIN, atau data pribadi lainnya.

2 TUJUAN / SASARAN PELAKU



Mengambil uang korban melalui transfer, tarik tunai, atau pembayaran.



Menguasai data pribadi korban untuk digunakan dalam kejahatan lain.



Mengambil alih akses akun perbankan atau dompet digital korban.



Melakukan transaksi tanpa sepengetahuan korban untuk keuntungan pribadi.

3 TEKNIK YANG DILAKUKAN PELAKU



Panggilan telepon / spoofing

Pelaku berpura-pura sebagai petugas bank menggunakan nomor palsu.



SMS / WhatsApp palsu

Mengirim pesan berisi link mencurigakan yang mengarahkan ke situs palsu.



Phishing (tautan palsu)

Korban diminta mengisi data login, PIN, atau kode OTP di situs palsu.



Iming-iming hadiah / promo

Menawarkan hadiah atau promo palsu dengan syarat memberikan data pribadi.



Social engineering

Pelaku membujuk korban agar percaya dan mengikuti instruksi mereka.



Pelaku penipuan semakin cerdas dan bisa menasar siapa saja, termasuk kaum ibu.
Kenali modusnya, pahami tujuannya, dan waspadai dampaknya!



PEMBAJAKAN AKUN DENGAN TARGET KAUM IBU

Pembajakan akun adalah tindakan pelaku untuk mengambil alih sebuah akun milik orang lain tanpa izin, sehingga pelaku dapat menggunakan akun tersebut seolah-olah miliknya sendiri.

CONTOH: Akun Facebook/Instagram diretas, lalu digunakan meminta uang kepada teman atau menyebarkan informasi palsu.

1 TUJUAN / SASARAN PELAKU



Mendapatkan keuntungan finansial



Menyalahgunakan identitas
Menggunakan akun Anda untuk menipu kontak atau melakukan aksi negatif.



Mengakses informasi pribadi
Mendapatkan data penting untuk dijual atau disalahgunakan.



Menyebarkan konten berbahaya
Menyebarkan informasi palsu, penipuan, atau tautan berbahaya kepada kontak Anda.

2 TEKNIK YANG DIGUNAKAN PELAKU



Phishing (tautan palsu)

Mengirim link palsu yang meniru situs login untuk mencuri email, password, atau kode OTP.



Social engineering

Pelaku berpura-pura menjadi orang atau lembaga terpercaya untuk memperoleh data atau kode verifikasi.



Password lemah / bocor

Menggunakan password yang mudah ditebak atau memanfaatkan password yang sudah bocor di internet.



Perangkat tidak aman

Mengakses akun melalui perangkat umum atau aplikasi berbahaya yang mencuri data login.



Akun yang dibajak bisa merugikan Anda dan orang lain.

Lindungi akun Anda, jaga data pribadi Anda!



PENCURIAN DATA PRIBADI DENGAN TARGET KAUM IBU

Pencurian data pribadi adalah tindakan mengambil informasi pribadi secara tidak sah tanpa izin.

1 TUJUAN / SASARAN PELAKU

-  **Penipuan**
Meminta uang, transaksi palsu
-  **Pembajakan akun**
Ambil alih akun media sosial, email, e-commerce, dll
-  **Penyalahgunaan identitas**
Buat pinjaman, daftar layanan, atau aktivitas ilegal
-  **Dijual di pasar gelap**
Data dijual untuk keuntungan finansial
-  **Target kejahatan lainnya**
Spam, peretasan, kejahatan siber lainnya

2 TEKNIK YANG DIGUNAKAN PELAKU

-  **Phishing (tautan palsu)**
Link palsu melalui SMS, WhatsApp, email, atau media sosial
-  **Social engineering**
Berpura-pura jadi pihak terpercaya untuk minta data
-  **Formulir palsu / hadiah**
Formulir undian palsu, promo, atau bantuan
-  **Malware / spyware**
Malware untuk mencuri data dari perangkat
-  **Kebocoran data**
Data bocor dari layanan online yang kurang aman



 **Data pribadi Anda bisa disalahgunakan untuk berbagai kejahatan!**



Lindungi data pribadi Anda!

Jangan sembarangan membagikan informasi pribadi kepada siapa pun.



ANCAMAN DISINFORMASI DENGAN TARGET KAUM IBU

Disinformasi adalah informasi palsu atau menyesatkan yang dibuat dan disebarkan dengan sengaja untuk mempengaruhi sikap, opini, atau tindakan seseorang.

CONTOH: Pesan di WhatsApp yang mengklaim produk tertentu menyembuhkan semua penyakit, padahal tidak terbukti.

1 TUJUAN / SASARAN PELAKU



Mempengaruhi opini
Membentuk cara pandang atau keyakinan yang sesuai dengan kepentingan pelaku.



Memecah belah & memicu konflik
Menimbulkan perpecahan di masyarakat atau antar kelompok.



Keuntungan finansial
Mengarahkan korban untuk membeli produk tertentu, klik tautan, atau memberi donasi.



Kepentingan politik / ideologis
Mendukung atau menjatuhkan tokoh, kebijakan, atau kelompok tertentu.

2 TEKNIK YANG DILAKUKAN PELAKU



Membuat konten palsu
Berita palsu, testimoni palsu, atau video palsu.



Manipulasi judul & isi
Menggunakan judul provokatif atau informasi yang dipelintir.



Penyebaran massif
Menyebarkan melalui WhatsApp, Facebook, TikTok, atau grup komunitas.



Akun palsu & bot
Menggunakan akun palsu atau bot untuk menyebarkan informasi palsu.





REKAYASA SOSIAL



EMAIL
PHISHING



SMISHING
(SMS/PESAN)



VISHING
(TELEPON/SUARA)





Malware & Pencurian Kredensial

Dua Teknik Utama dalam Penipuan Siber



PENYEBARAN MALWARE

Malware adalah program berbahaya yang dimasukkan ke perangkat korban untuk mencuri data atau mengendalikan perangkat.



1. Korban menerima pesan/tautan/file mencurigakan
2. Korban mengunduh atau menjalankan file/aplikasi
3. Malware terpasang di perangkat
4. Perangkat dikendalikan, data dicuri, atau aktivitas korban dipantau

TUJUAN MALWARE



PENCURIAN KREDENSIAL

Pelaku berusaha mendapatkan informasi login atau kode keamanan korban untuk mengakses akun atau layanan.



1. Korban diarahkan ke situs/login palsu atau diminta informasi
2. Korban memasukkan username, password, PIN, OTP, dll.
3. Kredensial dikirim ke pelaku
4. Pelaku menggunakan kredensial untuk masuk dan mengambil alih akun

YANG MENJADI SASARAN



5,2 MILIAR anomali trafik internet
1 Jan–15 Nov 2025

93,78%
berkaitan dengan potensi **malware**

Kerugian yang Dapat Dialami Korban

1 Kerugian finansial



Uang hilang, transaksi tidak sah, pembelian palsu, atau menjadi korban investasi/penipuan.



Uang hilang



Barang tidak diterima



Investasi/penipuan

2 Kehilangan kendali



Akun, perangkat, atau layanan digital tidak lagi berada dalam kendali korban.



Akun hilang/ tidak bisa diakses



Perangkat atau layanan diambil alih



Tidak bisa mengendalikan

3 Kehilangan privasi



Data pribadi, percakapan, foto, dokumen, atau informasi keluarga terekspos atau disalahgunakan.



Data pribadi terbuka



Percakapan & foto tersebar



Informasi keluarga disalahgunakan

4 Kerugian reputasi & sosial



Akun korban digunakan untuk menipu orang lain, menyebarkan konten palsu, atau menimbulkan konflik dengan keluarga/teman.



Akun dipakai menipu



Konten palsu disebarkan



Konflik dengan keluarga/teman

5 Dampak psikologis & pengambilan keputusan



Korban merasa takut, cemas, malu, kehilangan rasa aman, atau mengambil keputusan yang salah akibat informasi yang menyesatkan.



Takut, cemas, malu



Salah mengambil keputusan



Rasa aman berkurang



Kenali ancaman, pahami dampaknya, dan lindungi diri serta keluarga di ruang siber.



Kecerdasan Buatan

Membuat Penipuan Online Semakin Meyakinkan

AI bukan menggantikan modus penipuan lama,
AI membuat modus lama **jauh lebih meyakinkan**.



Modus Penipuan dengan AI

1 Deepfake Wajah / Video



2 Cloning Suara



3 Chatbot Penipu



4 Phishing Lebih Meyakinkan



5 Profil / Identitas Palsu



6 Iklan Palsu Berbasis Deepfake



7 Personalisasi Penipuan



8 Penipuan Massal



Contoh yang sering terjadi



Alur Penipuan dengan AI



JANGAN PERCAYA

hanya karena wajah dan suara terlihat atau terdengar seperti orang yang kita kenal.

3 PRINSIP AMAN



BERHENTI
Jangan langsung percaya



VERIFIKASI
Hubungi melalui saluran lain



JANGAN TRANSFER
Sebelum identitas dan permintaan dipastikan





CARA MENGHINDARI PENIPUAN MARKETPLACE



1 GUNAKAN MARKETPLACE RESMI



Belanja hanya di aplikasi atau website resmi.

2 PERIKSA TOKO & ULASAN



Cek rating, ulasan, jumlah transaksi, dan lama toko.

3 WASPADAI HARGA TERLALU MURAH



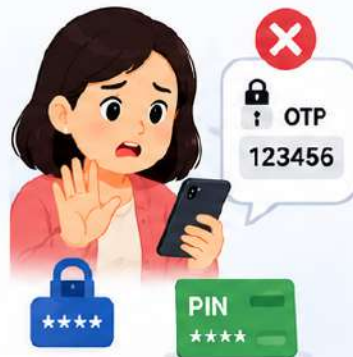
Harga jauh di bawah pasaran bisa jadi tanda penipuan.

4 JANGAN KLIK TAUTAN MENCURIGAKAN



Jangan klik tautan dari pesan, SMS, atau media sosial yang tidak dikenal.

5 JANGAN BERIKAN OTP, PIN & PASSWORD



Jangan pernah berikan kode OTP, PIN, atau password kepada siapa pun.



Jangan terburu-buru. **Periksa sebelum membeli, klik, atau membayar.**





CARA MENGHINDARI PENIPUAN PERBANKAN

🔒 Lindungi rekening dan data Anda!



1 JANGAN BERIKAN
OTP, PIN, ATAU
PASSWORD



Bank tidak akan meminta
kode OTP, PIN, atau password
Anda.

2 JANGAN PERCAYA
BEGITU SAJA PADA ORANG
YANG MENGAKU DARI BANK



Tutup komunikasi dan
hubungi bank melalui
kanal resmi.

3 JANGAN KLIK TAUTAN
PERBANKAN YANG
MENCURIGAKAN



Jangan klik tautan dari
SMS, WhatsApp, email,
atau media sosial.

4 GUNAKAN HANYA
APLIKASI & KANAL
RESMI



Akses mobile banking melalui
aplikasi resmi atau website
resmi bank.

5 PERIKSA SEBELUM
MELAKUKAN
TRANSAKSI



Periksa nama penerima,
nomor rekening, nominal,
dan detail transaksi.



Jika ragu, **hentikan!**
Hubungi bank melalui kanal resmi.



Call Center
Resmi Bank



Website
Resmi Bank



Aplikasi
Resmi Bank



Datang ke
Kantor Cabang



CARA MENGHINDARI PEMBAJAKAN AKUN

 Lindungi akun Anda, lindungi data dan privasi Anda!



1 GUNAKAN PASSWORD YANG KUAT & UNIK



Gunakan kombinasi huruf besar, huruf kecil, angka, dan simbol. Jangan gunakan password yang sama untuk beberapa akun.

2 AKTIFKAN AUTENTIKASI DUA FAKTOR (2FA)



Tambahkan lapisan keamanan dengan 2FA agar akun lebih sulit diambil alih.

3 JANGAN BERIKAN KODE OTP & KODE VERIFIKASI



Jangan pernah memberikan OTP, kode verifikasi, recovery code, atau password kepada siapa pun.

4 WASPADAI TAUTAN & PESAN MENCURIGAKAN



Jangan klik tautan login atau unduh file sembarangan dari SMS, WhatsApp, email, atau media sosial.

5 AMANKAN PERANGKAT & PERIKSA AKTIVITAS AKUN



Gunakan kunci layar, update sistem/aplikasi, dan periksa perangkat atau sesi login yang tidak dikenal.



PASSWORD adalah kunci akun.
OTP adalah kunci tambahan.

**JANGAN BERIKAN KEDUANYA
KEPADA SIAPA PUN!**





CARA MENGHINDARI PENCURIAN DATA PRIBADI



Lindungi data pribadi Anda, lindungi masa depan Anda!



1 Bagikan data
seperlunya



2 Waspada tautan
dan formulir palsu



3 Jangan berikan
kode keamanan



4 Amankan perangkat
dan akun



5 Periksa sebelum
membagikan



DATA PRIBADI ANDA BERTHARGA!

JANGAN SEMBARANG BAGIKAN, KLIK, ATAU UNGGAH.



JAGA
KERAHASIAAN



WASPADA
SETIAP SAAT



AMANKAN
AKUN



LINDUNGI DIRI
& KELUARGA



CARA MENGENALI DAN **MENGHINDARI** DISINFORMASI



1 KENALI TANDA-TANDANYA



! Judul sensasional, provokatif, membuat takut atau panik.

2 PERIKSA SUMBERNYA



! Lihat siapa yang membuat dan menyebarkan. Pastikan sumber jelas.

3 CEK KEBENARANNYA



! Bandingkan dengan sumber resmi atau media terpercaya.

4 PERIKSA TANGGAL DAN KONTEKS



! Perhatikan tanggal, lokasi, foto, dan konteks informasi.

5 JANGAN LANGSUNG PERCAYA & BAGIKAN



! Jika belum yakin benar, jangan teruskan ke grup keluarga atau teman.

INGAT!



BERHENTI



PERIKSA



VERIFIKASI



BARU BAGIKAN



Jangan langsung percaya.
Cek dulu sebelum berbagi!



Penetrasi Internet di Kalangan Anak Indonesia



Komposisi Pengguna Internet Menurut Survei APJII 2024



Gen Z
(1997–2012)

34,40%



Post Gen Z
(≥2013)

9,17%



40%

Anak usia 5–12 tahun
sudah aktif menggunakan internet

Rata-rata 4–6 jam per hari
(APJII, 2024)

Aplikasi yang diakses anak-anak di internet



Video
Streaming



Game
Online



Musik



Film dan
Serial



Media
Sosial



Chat &
Messaging



Forum
Online



Mesin
Pencarian



E-learning



Blog,
Artikel



Tidak semua yang dapat diakses anak di internet aman untuk anak.

ANCAMAN SIBER

yang Mengintai Anak



1 PERUNDUNGAN SIBER (CYBERBULLYING)



Penghinaan dan ejekan



Ancaman & intimidasi



Penyebaran foto/video tanpa izin

2 KONTEN BERBAHAYA & PREDATOR DIGITAL



Konten tidak sesuai usia



Kontak dengan orang asing



Risiko eksploitasi dan kekerasan

3 PENIPUAN ONLINE & MANIPULASI DIGITAL



Phishing & tautan palsu



Akun palsu & penipuan hadiah



Pengurian daring/ penipuan uang



LINDUNGI ANAK,
DAMPINGI & AJARI MEREKA
BERINTERNET DENGAN AMAN



Dampingi aktivitas online



Jangan bagikan data pribadi



Atur privasi & kontrol orang tua



Bangun komunikasi yang terbuka



Ancaman Peundungan Siber bagi Anak

Kenali bentuknya, pahami dampaknya, lindungi anak kita di ruang digital.



1. BENTUK PERUNDUNGAN



Menghina
dan mengejek



Menyebarkan foto/video
tanpa izin



Mengucilkan



Menyebarkan
rumor/fitnah



Mengancam atau
mengintimidasi



Menyamar sebagai korban
menggunakan akun palsu

2. CONTOH PERUNDUNGAN



Seorang anak mengunggah
foto dirinya di media sosial.



Temannya mengambil foto tersebut
lalu membuat meme yang
mempermalukan.



Meme tersebut disebar
ke grup kelas.



Teman-teman lain ikut mengejek,
anak merasa sedih, malu, dan
tidak berdaya.

3. DAMPAK PERUNDUNGAN BAGI ANAK



Emosional

Takut, malu, cemas,
sedih, kehilangan
kepercayaan diri



Sosial

Menarik diri dari
teman dan lingkungan



Akademik

Sulit berkonsentrasi
dan menurunnya
motivasi belajar



Keamanan

Merasa terancam atau
takut berada di lingkungan
sekolah maupun
ruang digital



**Bersama
Lindungi Anak**



Dampingi
dan dengarkan
anak



Atur penggunaan
internet dan aplikasi



Kenali aktivitas
digital anak



Segera bertindak
jika ada tanda-tanda
perundungan



Ciptakan lingkungan
yang aman, suportif,
dan penuh kasih



KONTEN BERBAHAYA & PREDATOR DIGITAL

yang Mengintai Anak di Ruang Siber



1. KONTEN BERBAHAYA



Konten seksual/
pornografi



Konten
kekerasan



Konten yang mendorong
perilaku berbahaya



Konten manipulatif
atau menyesatkan



Tantangan/challenge
berisiko



Bahasa kebencian
dan penghinaan

2. PREDATOR DIGITAL

Modus yang perlu diwaspadai: Grooming



Pelaku dapat berpura-pura:



3. MENGAPA ANAK RENTAN?



Belum mampu
mengenal
identitas palsu



Mudah percaya
kepada orang yang
bersikap ramah



Belum memahami
konsekuensi membagikan
foto dan data pribadi



Merasa takut menceritakan
interaksi yang mencurigakan
kepada orang tua



PENIPUAN ONLINE & MANIPULASI DIGITAL yang Mengintai Anak



Upaya menipu atau memengaruhi anak di internet agar memberikan informasi, mengklik tautan, mengirim uang, atau memberikan akses ke akun/perangkatnya.



MODUS YANG SERING MENYASAR ANAK

1 Hadiah atau giveaway palsu



Tujuannya mencuri data, mengambil alih akun, atau mengarah ke situs berbahaya.

2 Phishing dan tautan palsu



Pelaku berpura-pura sebagai platform, game, sekolah, atau teman untuk meminta data melalui tautan palsu.

3 Penipuan dalam game



Menawarkan item, skin, akun, atau mata uang game murah, lalu meminta password, OTP, atau pembayaran.

4 Akun dan identitas palsu



Pelaku menyamar sebagai teman sebaya, influencer, gamer, atau orang yang dikenal anak untuk mendapatkan kepercayaan.

5 Manipulasi dengan AI



AI digunakan untuk membuat foto, video, suara, atau percakapan palsu yang tampak meyakinkan sehingga anak lebih mudah percaya.

MENGAPA ANAK RENTAN?



Belum selalu mampu mengenali identitas palsu.



Belum memahami nilai dan risiko data pribadi.



Pesan yang terlihat menarik mudah membuat anak percaya dan penasaran.

BAGAIMANA ANAK DIMANIPULASI?

1 Menarik perhatian



2 Membangun kepercayaan



3 Membuat anak penasaran / terdesak



4 Meminta tindakan



5 Mengambil data / uang / akun



INGAT!

Jangan mudah percaya, jangan klik sembarang tautan, dan jangan pernah membagikan password atau OTP.



Jika sudah terlanjur tertipu, jangan takut atau malu. Segera ceritakan kepada orang tua atau guru agar bisa membantu!



TATA KELOLA KEAMANAN KELUARGA DI RUANG SIBER





PERAN PEMERINTAH



Aturan yang jelas

Pemerintah membuat peraturan untuk melindungi anak di dunia digital.



Perlindungan data pribadi

Pemerintah memastikan data anak aman dan tidak disalahgunakan.



Keamanan siber

Pemerintah membentuk tim dan langkah cepat untuk mengatasi ancaman di internet.

Pandangan 360° untuk Keamanan Anak di Dunia Online



PENDAMPINGAN ORANG TUA

Peran utama orang tua dalam melindungi anak saat online.



Komunikasi terbuka

Ajak anak bicara tentang pengalaman online mereka. Dengarkan dengan penuh kepercayaan.



Literasi digital

Ajarkan nilai-nilai baik dan risiko di internet agar anak bisa membuat keputusan yang tepat.



Belajar bersama

Temani anak menggunakan internet dan memanfaatkan fitur keamanan yang ada.



DUKUNGAN EKOSISTEM



Platform bertanggung jawab

Platform digital harus membuat fitur dan aturan yang aman bagi anak.



Edukasi di sekolah & masyarakat

Sekolah dan lingkungan sekitar mengajarkan cara aman berinternet.



Memberdayakan anak

Bekali anak dengan pengetahuan dan keterampilan agar percaya diri dan aman di dunia digital.



Kerja sama pemerintah, platform, orang tua, sekolah, dan masyarakat akan menciptakan ruang digital yang aman, sehat, dan menyenangkan bagi anak kita.





KEAMANAN SIBER

ADALAH TANGGUNG JAWAB BERSAMA

LINDUNGI DIRI DAN KELUARGA
DARI ANCAMAN SIBER



WASPADA
terhadap ancaman



BIJAK
dalam bertindak



SADARI
saling melindungi



AMAN
di ruang siber



KELUARGA AMAN,
HIDUP NYAMAN DI DUNIA DIGITAL ❤️