JAGA AKUNMU

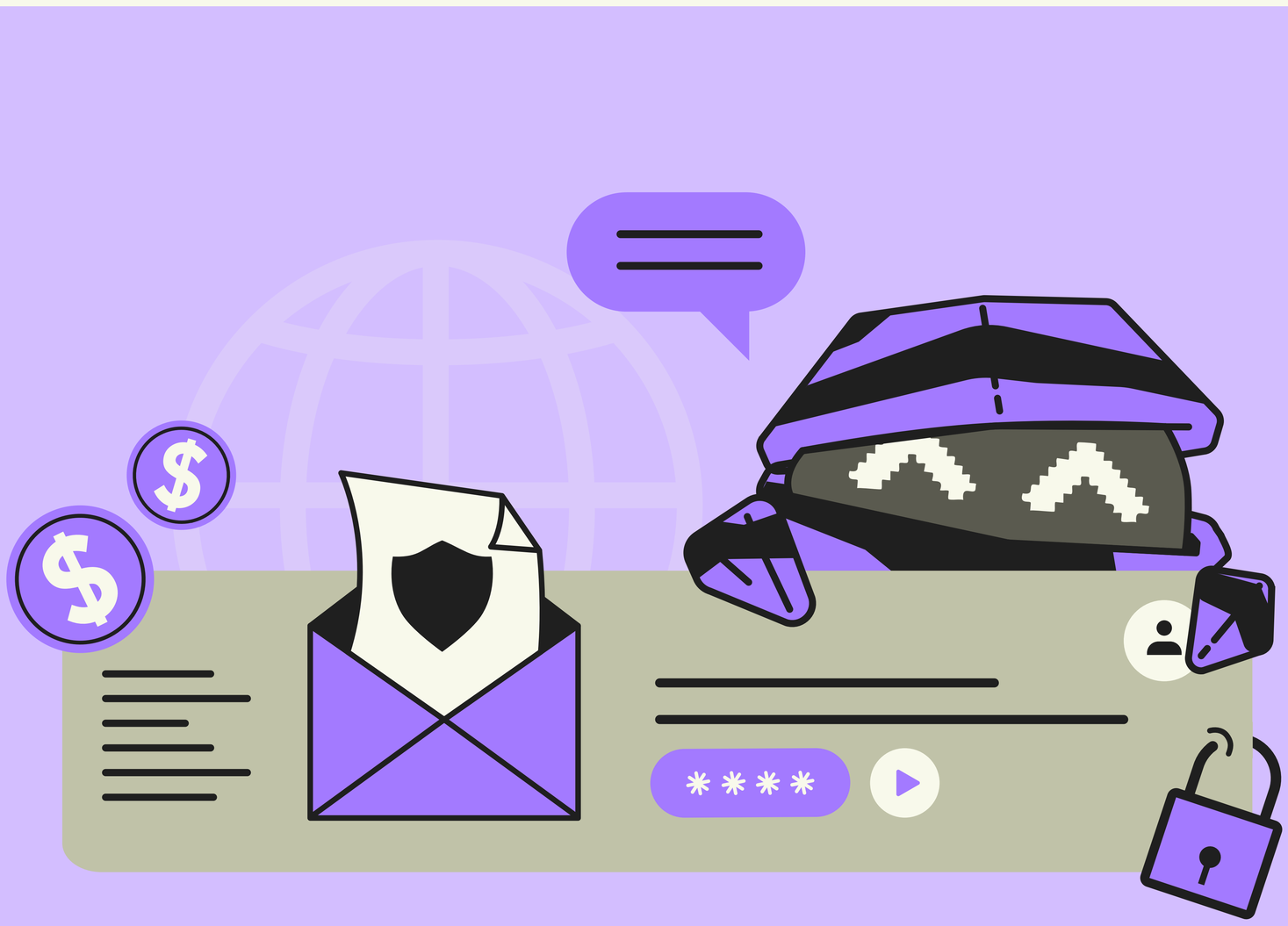
CARA MENGENALI DAN MENGHINDARI MODUS PENIPUAN DI DUNIA GIM

Didukung oleh Ekraf

EKRAF
Kementerian Ekonomi Kreatif/
Badan Ekonomi Kreatif
Republik Indonesia

CODA

APA SAJA YANG AKAN DIPELAJARI?



Gim daring (online game) saat ini bukan hanya hiburan semata, tetapi telah berkembang menjadi sebuah ekosistem ekonomi yang aktif dan bernilai tinggi. Para pemain sudah terbiasa melakukan top up, membeli skin, meningkatkan kemampuan karakter, dan mengikuti berbagai event yang diselenggarakan pada berbagai platform. Sayangnya, nilai ekonomi yang tinggi ini kerap dimanfaatkan oleh pelaku kejahatan untuk melakukan penipuan.

Penipuan yang menargetkan pemain gim semakin marak terjadi. Modus yang digunakan umumnya mengadaptasi praktik penipuan di platform e-commerce, seperti pencurian kode OTP, penggunaan formulir hadiah palsu, penyamaran sebagai pihak resmi, hingga pemalsuan bukti pembayaran. Seluruh modus ini dikemas agar tampak meyakinkan dan menyatu dengan ekosistem gim, sehingga pengguna seringkali dapat terkecoh. Meskipun hal tersebut terdengar familiar, modus penipuan tersebut kerap berhasil karena pemain sedang terburu-buru, kurang waspada, atau belum memahami ciri-ciri penipuan yang perlu diwaspadai.

Seiring meningkatnya risiko penipuan di ruang digital, pemerintah, termasuk Kementerian Ekonomi Kreatif Republik Indonesia, menempatkan perlindungan konsumen digital sebagai salah satu prioritas utama dalam pengembangan industri kreatif, khususnya pada subsektor berbasis transaksi seperti gim daring. Melalui peningkatan literasi digital pengguna, serta penguatan ekosistem transaksi gim daring yang terpercaya, pemerintah bersama-sama dengan pelaku industri, mendorong agar pemain dapat berpartisipasi secara aman dan terlindungi dari praktik penipuan daring.

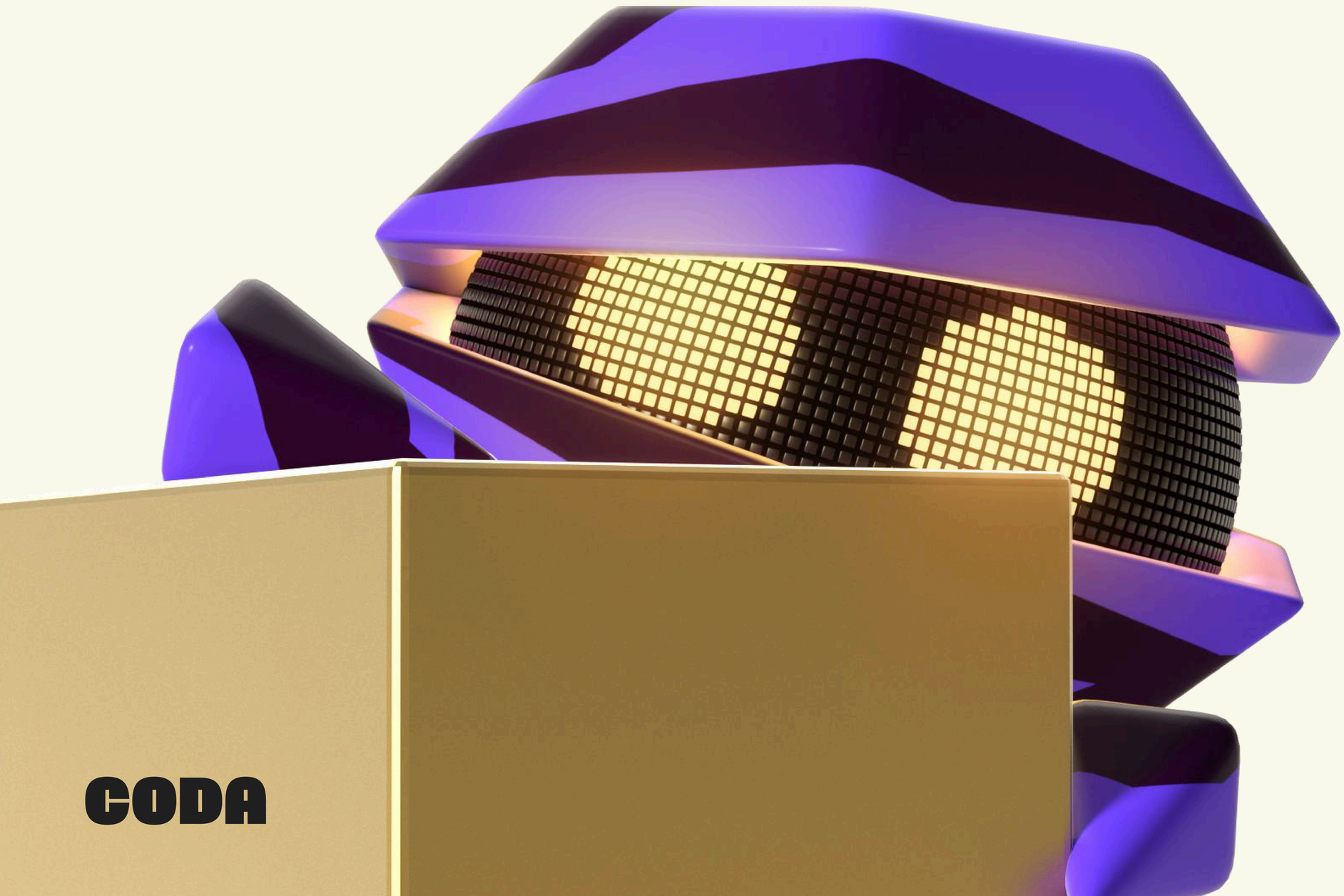
Dalam buku saku ini, kita akan melihat beberapa taktik umum yang sering digunakan oleh penipu, antara lain:

- **Situs tiruan (*phishing*)** yaitu situs yang tampilannya hampir persis dengan situs resmi penerbit gim atau platform top-up resmi.
- **Taktik rekayasa sosial (*social engineering*)**, yaitu trik yang memanfaatkan data pribadi atau hubungan pertemanan di dalam gim untuk menciptakan rasa percaya palsu.
- **Upaya pengambilalihan akun (*account takeover*)** yang dapat menyebabkan progres permainan hilang, item lenyap, atau transaksi tanpa izin.
- **Promosi palsu** yang menjanjikan “diamond murah”, “skin gratis”, atau “item eksklusif” yang pada akhirnya tidak akan diterima pemain.

Dampak dari penipuan ini tidak hanya sebatas kerugian finansial. Penipu tidak hanya merusak pengalaman bermain, tetapi mereka juga dapat membajak akun, melakukan pemerasan, merusak reputasi, hingga mencuri data pribadi. Karena modus penipuan terus berkembang, kewaspadaan pemain sangatlah penting.

Buku saku dari Coda ini hadir sebagai panduan singkat untuk membantu kamu mengenali penipuan, menghindari jebakan, serta melindungi akun, data, dan aset digital saat bermain gim daring.

DAFTAR ISI



BAGIAN I

KENALI MODUS PENIPUAN UMUM DALAM DUNIA GIM

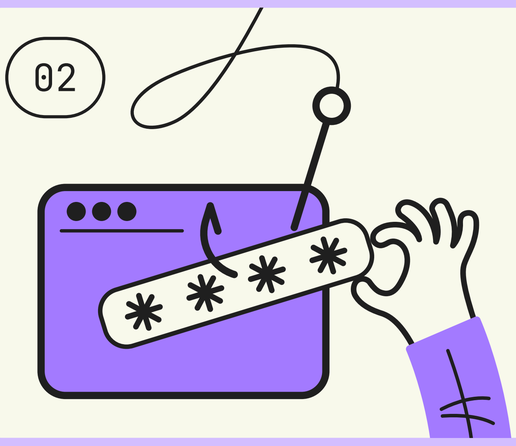
Pelaku kejahatan digital terus mencari cara baru untuk menipu pemain gim. Berikut adalah jenis penipuan yang paling umum yang paling umum ditemui, beserta gambaran cara kerjanya.

01

Penipuan *(Scam)*

Penipuan mencakup berbagai taktik yang bertujuan mencuri dana, mengambil alih akses akun, atau memperoleh data pribadi secara ilegal. Pelaku biasanya membangun kepercayaan korban terlebih dahulu, lalu mendorong mereka untuk mengirimkan uang atau membagikan informasi sensitif seperti detail login.

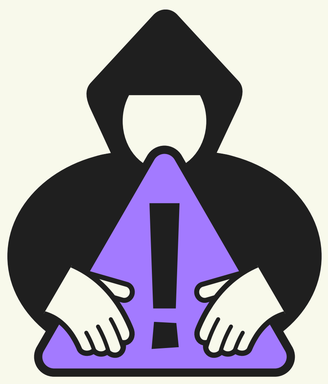
02



Situs Web Palsu *(Phishing)*

Phishing adalah metode penipuan di mana pelaku membuat situs web palsu yang tampilannya dirancang sedemikian rupa agar menyerupai platform resmi. Modus ini biasanya disebarkan melalui tautan mencurigakan pada pesan pribadi, media sosial, atau iklan palsu.

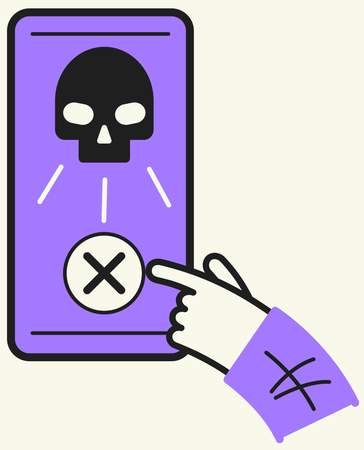
03



Rekayasa Sosial *(Social Engineering)*

Metode ini mengandalkan manipulasi psikologis untuk mengecoh korban dengan berpura-pura menjadi pihak resmi. Pelaku sering kali menciptakan rasa panik, takut, atau kasihan agar korban segera mengambil tindakan tertentu tanpa berpikir panjang. Penipu bisa menyamar sebagai teman, anggota komunitas, atau tim operasional gim untuk menekan korban agar mengikuti instruksi mereka.

04



Ancaman APK / Malware dalam Gim Daring

Penipu dapat menyebarkan file berbahaya melalui:

- Tautan yang dibagikan di Telegram atau Discord
- Deskripsi video di media sosial (e.g. Instagram, YouTube)
- Situs mengunduh aplikasi pals
- Kumpulan APK yang telah dimodifikasi

Jika file tersebut tidak berasal dari situs atau platform resmi dan terverifikasi, maka sebaiknya tidak diunduh maupun dipasang pada perangkat kamu.

05

Pengambilalihan Akun *(Account Takeover)*

Pengambilalihan akun terjadi ketika pihak tidak bertanggung jawab berhasil mengakses dan menguasai akun gim secara ilegal, sering kali tanpa disadari oleh pemilik akun. Modus ini biasanya dilakukan dengan mencuri informasi rahasia seperti username, alamat email, kata sandi, atau kode OTP.

06

Penipuan Aset Digital

Transaksi jual-beli item, tampilan karakter (*skin*), atau mata uang virtual dalam permainan merupakan area yang sangat rentan dimanipulasi oleh penipu. Setiap bentuk transaksi yang dilakukan di luar sistem resmi gim memiliki risiko keamanan yang sangat tinggi. Untuk menjamin keamanan akun dan transaksi, pastikan kamu hanya menggunakan platform top-up dan layanan pembayaran yang tepercaya serta memiliki izin resmi, seperti Codashop.

Berikut adalah beberapa taktik penipuan umum yang dapat membahayakan data pribadi serta aset gim daring kamu:

01

Formulir event atau hadiah palsu.

Penipu dapat mengirimkan tautan yang menginformasikan bahwa kamu telah memenangkan hadiah tertentu dan diminta untuk “login untuk mengklaim hadiah.” Halaman ini dibuat menyerupai situs resmi, namun bertujuan mencuri informasi akun kamu.

02

Saluran pembayaran tidak resmi atau tidak terverifikasi.

Waspadai nomor **WhatsApp, Signal, atau Telegram, pesan Instagram,** atau akun informal lainnya yang mengaku sebagai layanan gim atau penjual top up. Platform resmi tidak akan pernah meminta pembayaran melalui akun atau rekening pribadi milik individu.

03

APK palsu atau yang dimodifikasi.

Aplikasi yang menjanjikan “diamond/koin unlimited” atau fitur curang lainnya hampir selalu mengandung malware. File semacam ini berisiko mencuri data pribadi, mengambil alih akun gim maupaun keuangan, atau merusak perangkat kamu.

06

Layanan top up tidak resmi.

Membeli kredit gim dari penjual media sosial yang tidak terverifikasi mungkin tampak lebih murah, namun risikonya sangat tinggi. Mulai dari kehilangan aset dalam gim hingga pengambilalihan akun, terutama jika penjual meminta ID gim atau data akun kamu.

07

Pihak yang mengatasnamakan pemerintah atau instansi resmi.

Pelaku dapat mengklaim bahwa mereka mewakili program pemerintah, kementerian, atau asosiasi industri gim. Modus ini sering digunakan untuk meningkatkan kredibilitas dan menekan korban agar segera bertindak. Perlu diingat, instansi resmi **tidak pernah** meminta data pribadi, detail OTP, atau pembayaran langsung kepada pemain melalui pesan pribadi atau tautan tidak resmi.

CODA

04

c0dash0p.com

Menggunakan angka “0” menggantikan huruf “o”

codashop.event-top-up.co.id

Domain yang digunakan tidak resmi terafiliasi dengan Coda

Situs Asli codashop.com

Situs tiruan atau palsu.

Penipu sering meniru atau sedikit mengubah merek, logo, atau nama domain dengan mengganti huruf, simbol, atau kata tertentu agar terlihat resmi. Padahal pada kenyataannya, tidak. Perbedaan kecil saja bisa mengarahkan kamu ke situs penipuan.

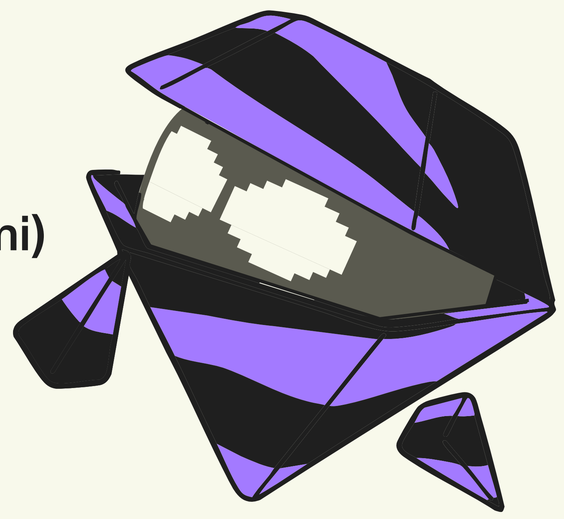
05

942048 adalah kode verifikasi Anda

Halo, Kami dari Codashop. Mohon untuk verifikasi akun Anda dengan menginfokan kode OTP dengan membalas pesan ini.

SMS SEPERTI INI BUKAN BERASAL DARI CODASHOP

Siapa pun yang meminta OTP kamu (meskipun mereka dapat terdengar resmi) sedang berupaya mencuri akunmu.



Pencurian OTP / data pribadi.

Penipu dapat menekan kamu untuk membagikan username, email, atau kode satu kali (OTP). Setelah informasi ini diperoleh, akun dapat diambil alih sepenuhnya.

BAGIAN II

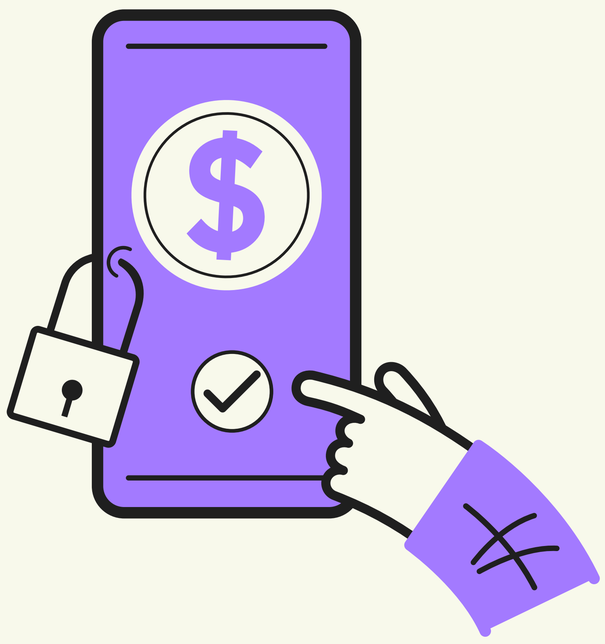
TIPS MELINDUNGI AKUN GIM & PEMBAYARAN KAMU

01

Praktik Login yang Aman

- Aktifkan verifikasi dua langkah (2FA)
- Jangan menggunakan kata sandi yang sama untuk banyak akun
- Hindari login menggunakan Wi-Fi publik
- Gunakan pengelola kata sandi (*password manager*)
- Gunakan aplikasi autentikasi (seperti Google Authenticator, Authy, dan sejenisnya) dibandingkan SMS, apabila memungkinkan

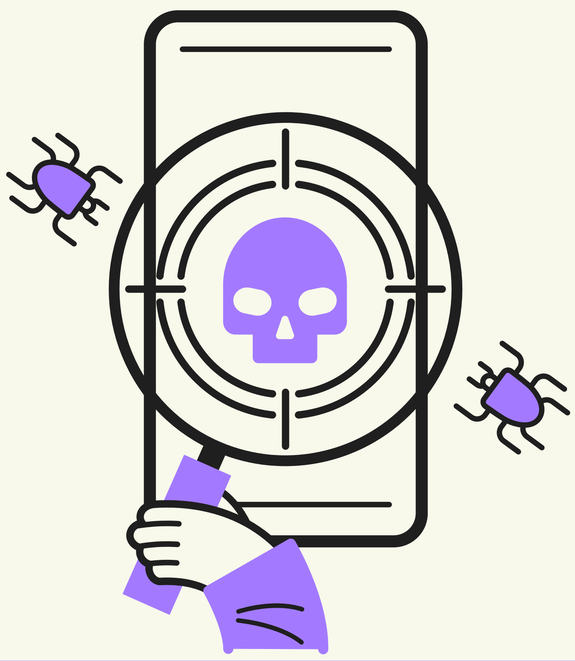
02



Pembayaran yang Aman

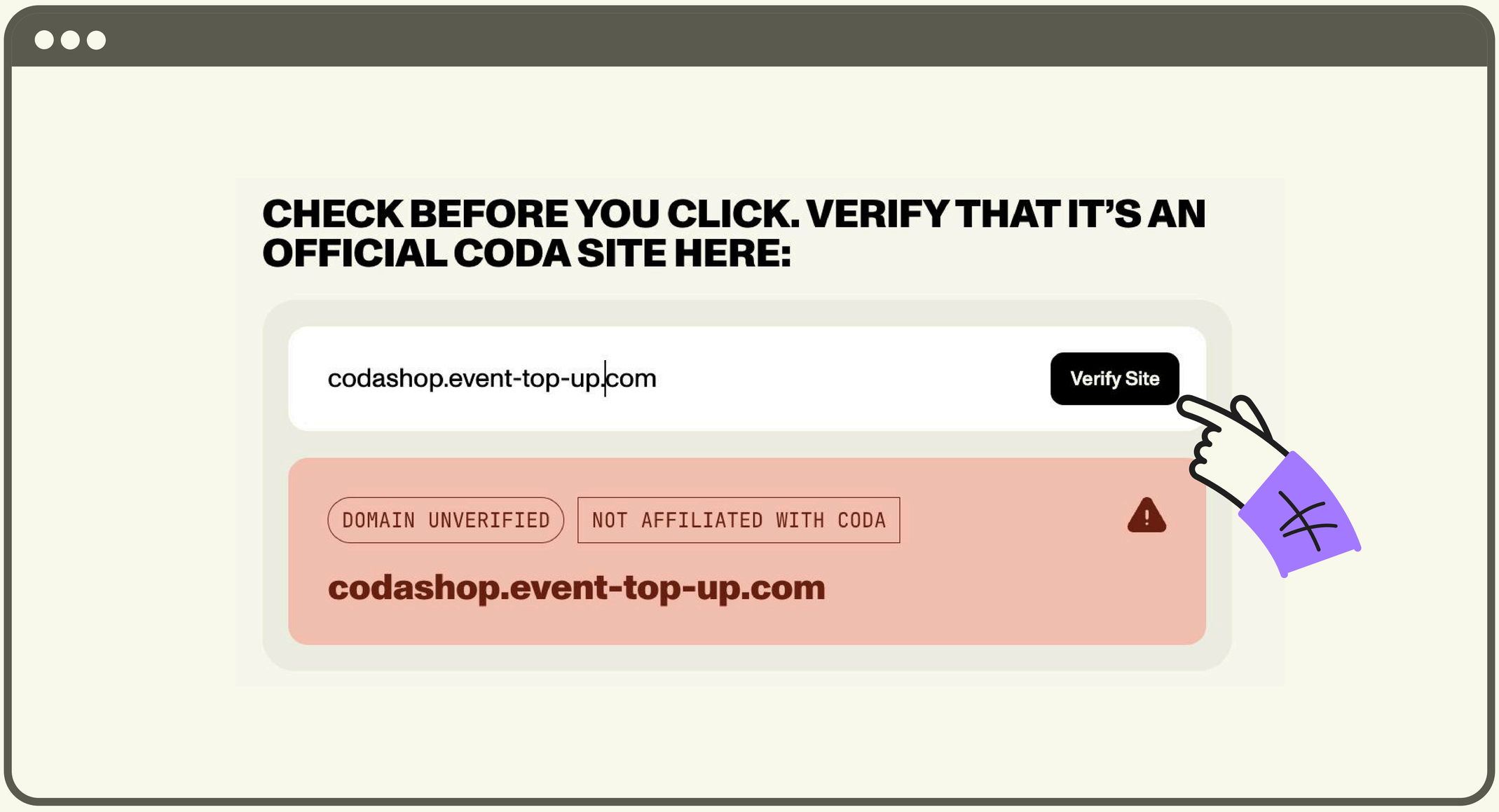
- Gunakan mitra dan platform top up resmi
- Hindari penjual dari akun pribadi yang menawarkan diskon besar-besaran
- Jangan pernah melakukan pembayaran di luar platform resmi
- Jangan membagikan data pribadi (kata sandi, OTP, atau ID gim)

03



Perlindungan Perangkat

- Hindari mengunduh APK atau mod gim
- Pasang antivirus terpercaya dan alat perlindungan browser



Verifikasi Website Resmi Codashop

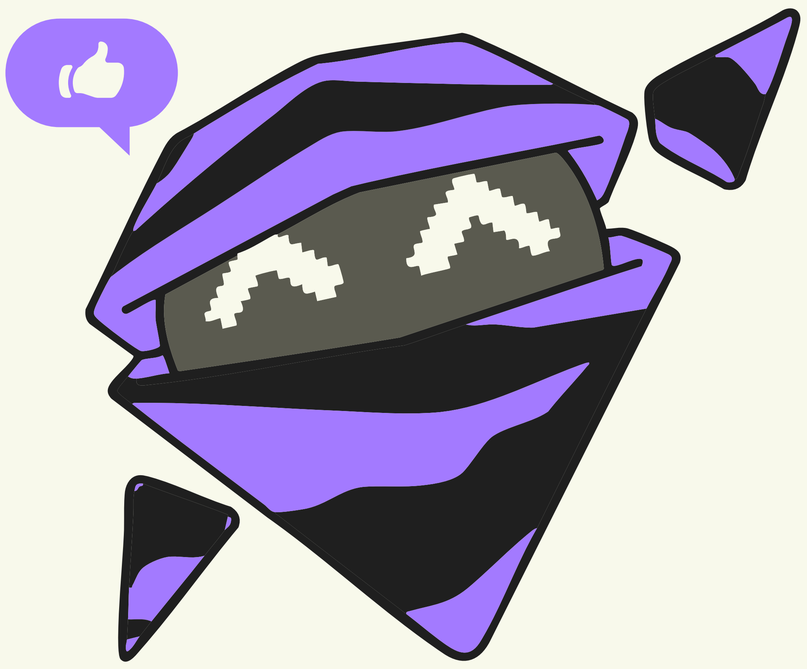
- Gunakan fitur verifikasi di website kami untuk memastikan apakah sebuah link terafiliasi resmi dengan Coda atau Codashop.

  Cek Link di Sini https://www.coda.co/online-safety/

- Cukup masukkan link yang ingin dicek, dan sistem akan langsung memberi tahu statusnya.

BAGIAN III

CHECKLIST UNTUK GAMER: DOS & DON'TS



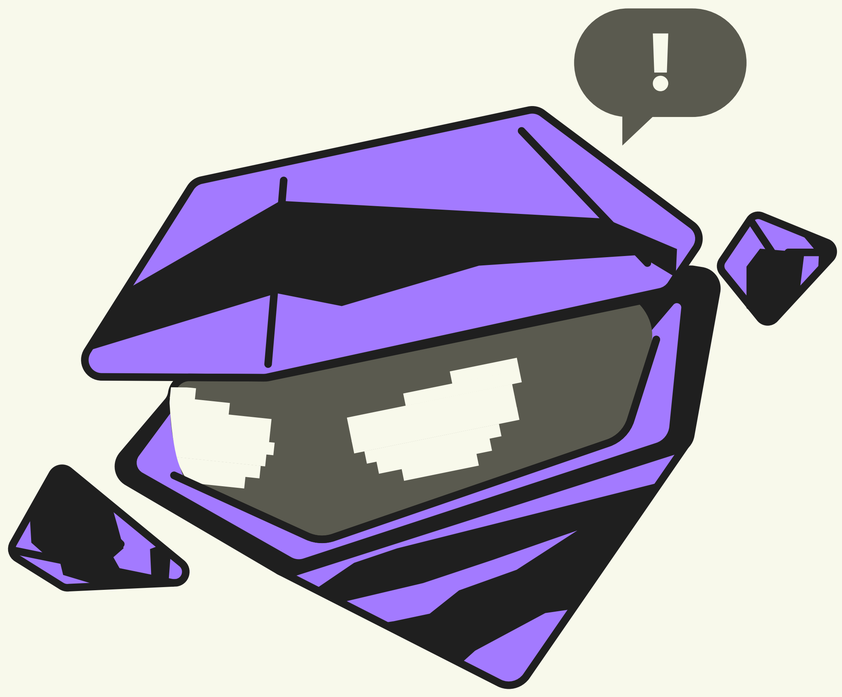
DO'S - Zona Aman

Akses kanal pembayaran resmi yang tercantum di situs atau aplikasi resmi gim atau penerbit.

- Sebagai contoh, situs Codashop (https://www.codashop.com/) menyediakan metode pembayaran terpusat dan tidak akan mengarahkan kamu ke situs pihak ketiga atau media sosial untuk menyelesaikan transaksi.

Hadiah dan *reward* akan langsung masuk ke akun gim kamu. Kamu tidak perlu "mengklaim" hadiah dengan login ke situs lain atau membayar "biaya "pengiriman".

Pastikan kebenaran informasi melalui kanal resmi sebelum menanggapi pesan tentang hadiah, pemblokiran akun, atau masalah akun.



DON'TS - Zona Bahaya

Jangan pernah membagikan OTP kepada siapa pun. Tim layanan pengguna tidak akan pernah meminta informasi tersebut.

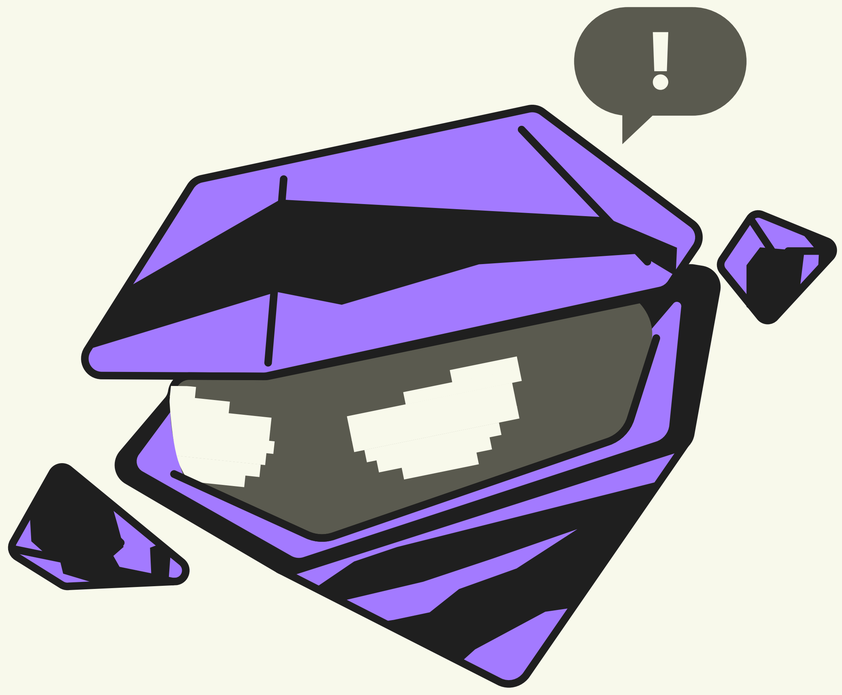
Jangan klik tautan pembayaran dari pesan pribadi. Coda tidak pernah meminta kamu melakukan pembayaran melalui tautan di WhatsApp, Telegram, Signal, SMS, maupun aplikasi pesan lainnya.

Jangan klik tautan yang menawarkan "diamond/skin gratis". Hal tersebut merupakan modus *phishing* yang kerap terjadi.

Jangan memasukkan email, kata sandi, atau kode verifikasi di halaman yang tidak kamu yakini keamanannya.

Periksa kembali domain email dan waspadai alamat email palsu (*spoofing*). Coda hanya akan menghubungi kamu melalui domain resmi seperti @coda.co, @codashop.com, atau @codapayments.com.

Jika kamu menemukan situs top up mencurigakan yang meniru merek atau terindikasi penipuan, laporkan ke saluran pembayaran terkait, platform top up resmi, atau situs pelaporan publik milik pemerintah. Melaporkan situs atau modus penipuan dapat membantu melindungi pemain lain dari penipuan serupa.



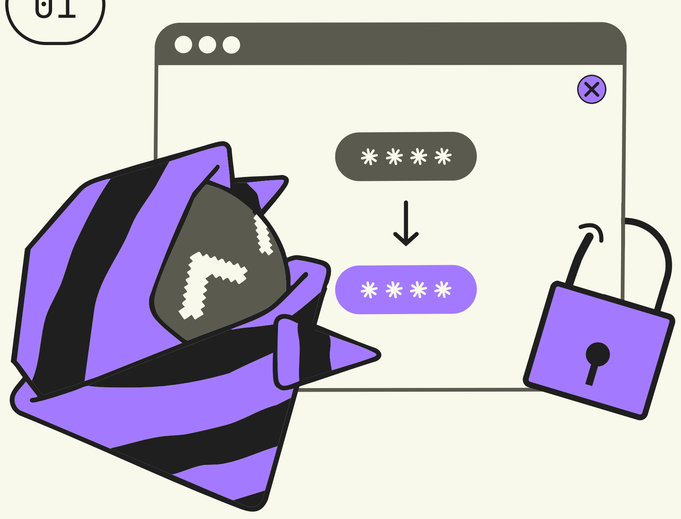
Jangan mudah percaya pesan dengan kesan mendesak yang menyebutkan bahwa akun kamu akan diblokir jika tidak segera bertindak.

Jangan menanggapi pesan pribadi dari pihak yang mengaku sebagai “admin” di WhatsApp, Discord, Telegram, atau platform lain. Admin resmi jarang, bahkan hampir tidak pernah, menghubungi pengguna secara pribadi. Selalu kunjungi situs atau aplikasi resmi untuk melakukan verifikasi.

BAGIAN IV

LANGKAH DARURAT JIKA MENJADI KORBAN @PENIPUAN

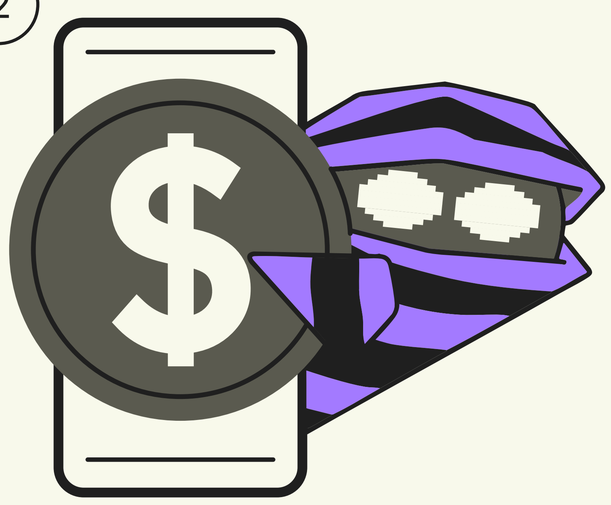
01



Amankan Akun Terlebih Dahulu

- Segera ganti kata sandi akun gim dan email yang terhubung
- Aktifkan atau atur ulang verifikasi dua langkah (2FA)
- Keluar paksa dari semua perangkat yang terhubung ke akun
- Pindai perangkat kamu dari malware atau aplikasi berbahaya
- Hubungi layanan dukungan resmi gim terkait

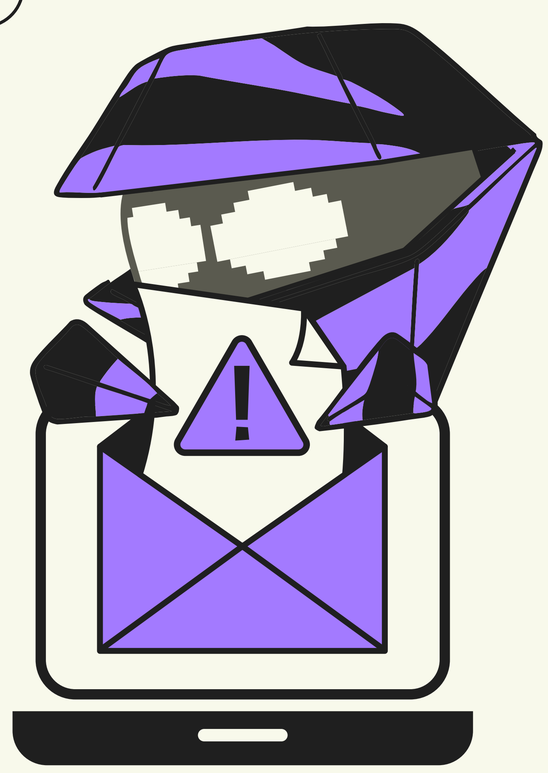
02



Amankan Uang dan Transaksi

- Segera hubungi bank atau penyedia dompet digital (e-wallet) kamu
- Blokir atau bekukan metode pembayaran jika diperlukan
- Ajukan laporan atas transaksi yang tidak sah
- Simpan semua bukti pendukung seperti tangkapan layar dan riwayat percakapan

03

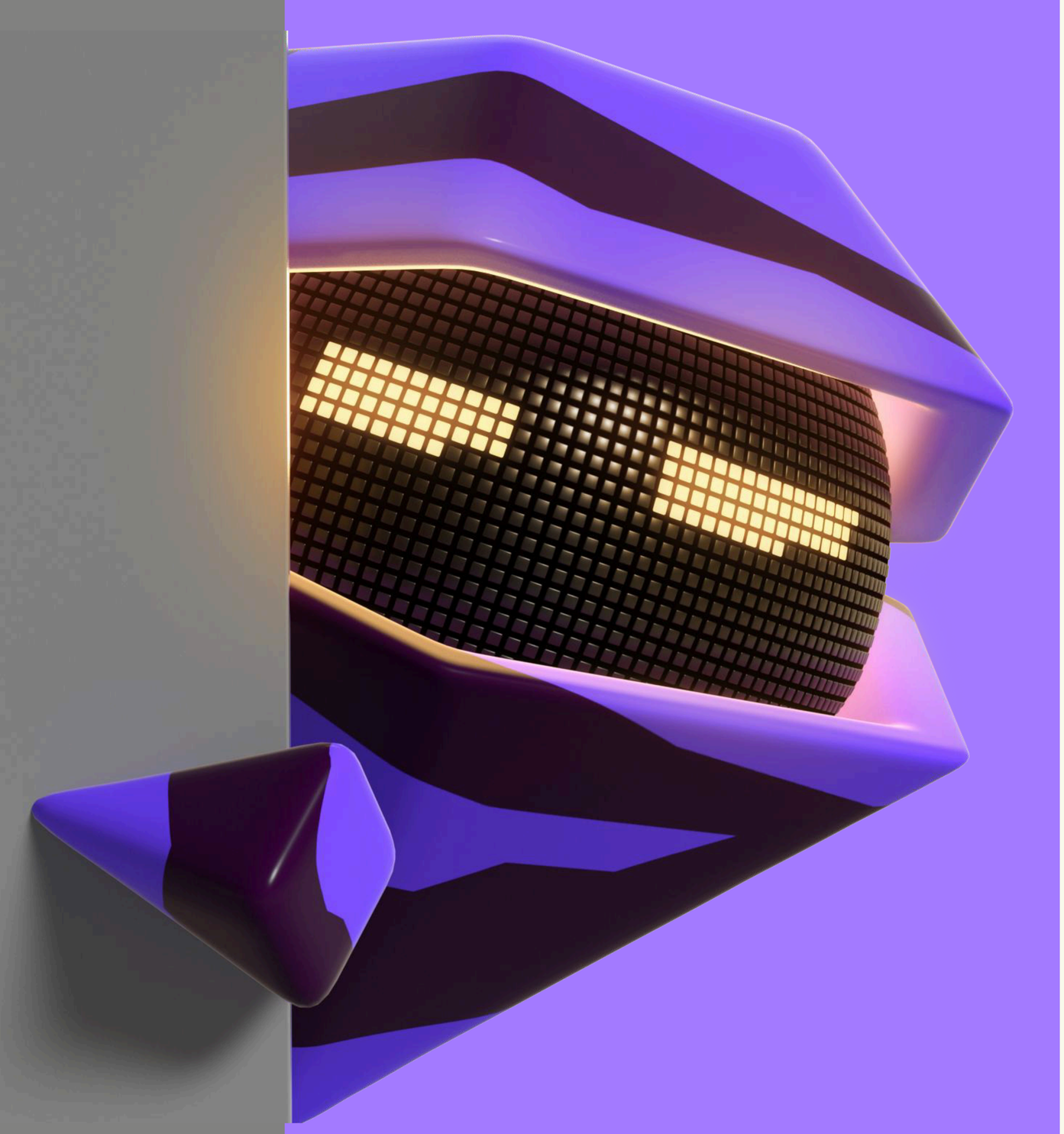


Laporkan dan Upayakan Pemulihan

- Hubungi layanan dukungan resmi saluran pembayaran (bank atau penyedia e-wallet) dan buat tiket laporan atas kasus penipuan pembayaran
- Simpan log aktivitas dan tangkapan layar sebagai bukti
- Hubungi layanan pelanggan platform top-up tempat transaksi terjadi, jika kasusnya terkait top-up
  - Contoh: Pelanggan Coda Indonesia dapat menghubungi dukungan melalui tautan https://id.support.codashop.com/hc/id
- Laporkan kejadian ke kanal pelaporan resmi pemerintah atau otoritas kejahatan siber setempat, terutama apabila melibatkan pencurian dana digital, penyalahgunaan identitas, atau akun yang diambil alih

BAGIAN V

KONTAK RESMI CODA



Untuk informasi lebih lanjut, kunjungi:

- CODA.CO
- CODA.CO/ONLINE-SAFETY
- CODASHOP.COM/INTERNATIONAL

CODA.CO

CODA