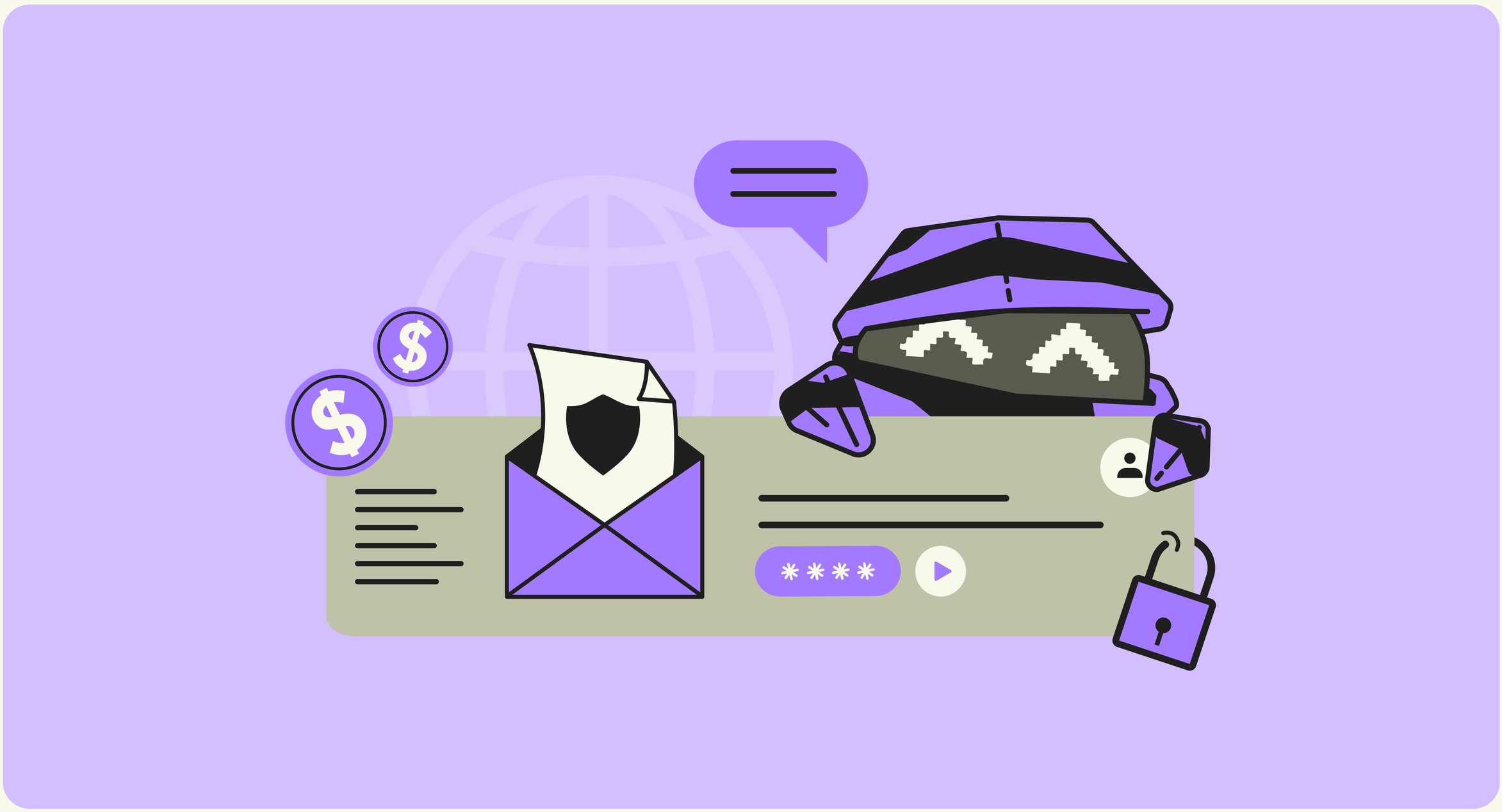
GUARD YOUR GAME

HOW TO SPOT AND AVOID THE TOP GAMING SCAMS

CODA

WHAT YOU'LL LEARN FROM THIS BOOKLET



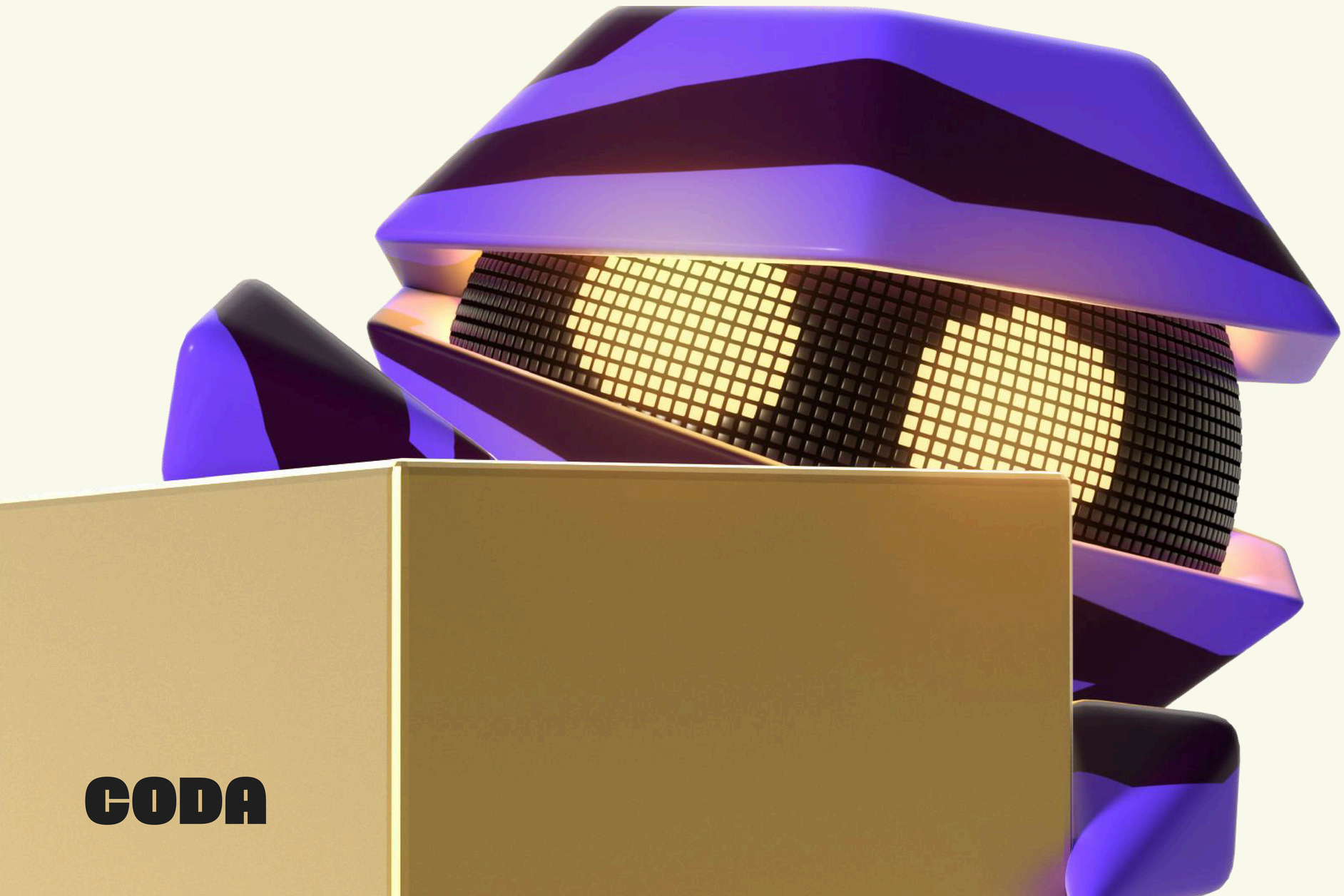
Online gaming today is more than just entertainment; it's a vibrant digital economy. Players top up credits, purchase skins, upgrade characters, and join events across multiple platforms. With so much value flowing through the ecosystem, scammers see a prime opportunity. Scams targeting gamers are everywhere. Many borrow familiar e-commerce tactics, such as OTP theft, fake reward forms, impersonation, and falsified payment proofs. These are deceptively repackaged to blend seamlessly into gaming environments. These scams feel familiar, yet they often succeed when players are rushing, distracted, or unaware of what to look out for.

As we go through this booklet, we will see how scammers often use tactics such as:

- **Phishing sites (a.k.a. copycat websites)** that look almost identical to official game publishers and top-up platforms.
- **Social engineering tricks** that use your personal details or in-game friendships to create fake trust.
- **Account takeover attempts** that lead to stolen progress, missing items, or unauthorized spending.
- **Fake promotions** promising "cheap diamonds," "free skins," or "exclusive items" that never actually arrive.

The impact goes beyond financial loss. Scammers are known to hijack accounts, blackmail, damage reputations, compromise personal data, and ultimately ruin the gaming experience. And because scam tactics constantly evolve, being vigilant is crucial. This is Coda's quick guide on spotting scams, avoiding common traps, and protecting your accounts, data, and assets when gaming.

TABLE OF CONTENTS



SECTION I

UNDERSTANDING COMMON THREATS IN GAMING FRAUD

Bad actors are always looking for new ways to trick gamers. Here are the most common scams you might encounter and how they usually work.

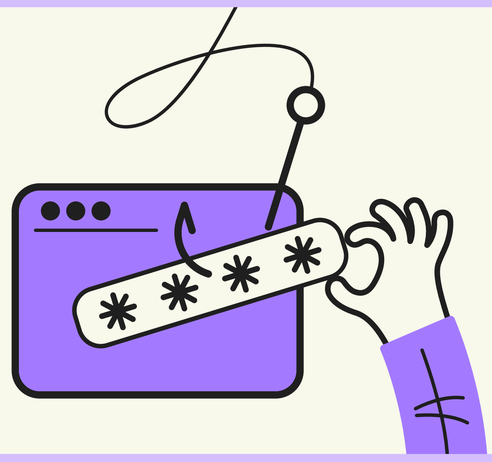
01

Scam

Scams are deceptive tactics used to steal your money, account access, or personal data.

Their goal: To make you trust them enough to transfer money or reveal your login details.

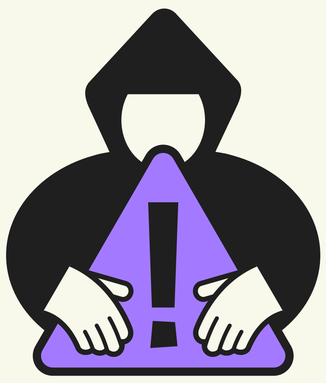
02



Phishing

Phishing is when scammers imitate legitimate websites or platforms and trick users into entering login details. Phishing often happens through links in messages, comments, social posts, or fake ads.

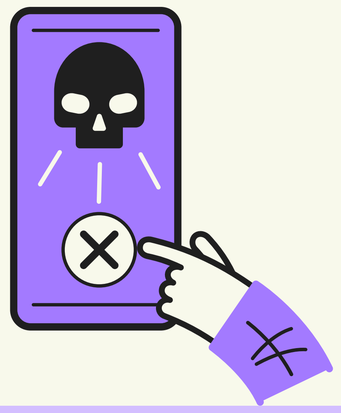
03



Social Engineering

Emotional manipulation designed to **create urgency, fear, or sympathy.** Scammers may impersonate friends, community members, or support teams to pressure you into taking action.

04



APK / Malware Threats in Gaming

Scammers may distribute harmful files via:

- Telegram / Discord / Roblox shared links
- Video descriptions in social media channels (e.g. Instagram, Youtube)
- Fake download websites
- Modified APK repositories

If it didn’t come from an **official or verified website or platform,** don’t install it.

05

Account Takeover (ATO)

When scammers gain access to your gaming account, often without you noticing. This is usually done by stealing sensitive information such as usernames, email addresses, passwords, or OTP codes.

06

Asset Fraud

Gamers often trade items, skins, or currency, and scammers know this. If it’s not through an **official in-game system** or a verified seller, it’s a high-risk transaction. Use only trusted, authorized top-up and payment platforms, such as Codashop, to stay safe.

These are some common scam tactics that can compromise your personal data and put your gaming assets at risk.

01

Fake event or reward forms.

Scammers may send links claiming you’ve won a prize and must “log in to claim your gift.” These pages are designed to steal your account details.

02

Look-alike websites.

Scammers may **copy or slightly alter a brand’s trademark, logo, or name in the URL** by changing the letters, symbols, or even full phrases to make the link look official when it isn’t. One small difference can lead you to a scam site. For example:

- Real website: **codashop.com**
- Fake phishing site: **c0dash0p.com** (using “zero” instead of “o”)

03

Informal or unverified payment channels.

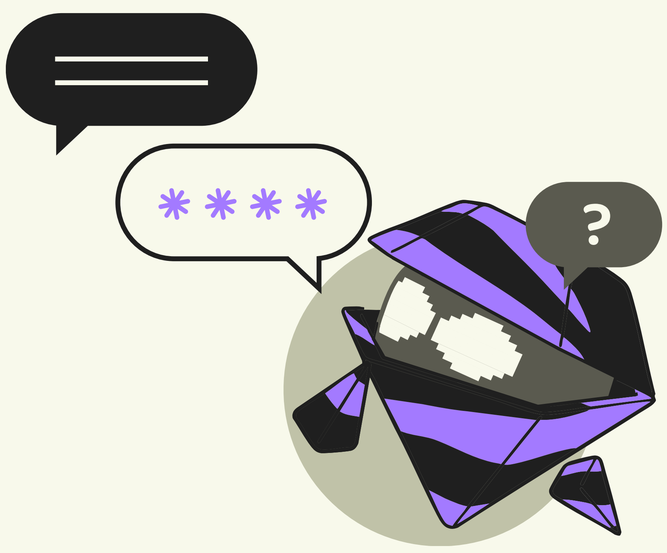
Be cautious of **WhatsApp, Signal, and Telegram numbers, Instagram DMs, or other informal accounts** pretending to be game support or top-up sellers. Legitimate platforms will never ask you to pay through random personal accounts.

04

Fake or modified APKs.

Apps promising “unlimited diamonds/coins” or other cheats may contain malware that steals your data or damages your device.

05



OTP / credential theft.

Scammers may pressure you to share your username, email, or one-time password (OTP). Once they have this information, they can take over your account.

Note: Anyone asking for your OTP (even if they sound official) is attempting to steal your account.

06

Unofficial top-up services.

Buying game credits from unverified social media sellers may look cheaper, but it carries a high risk of losing your account or in-game assets, especially if they ask for your gamer ID.

SECTION II

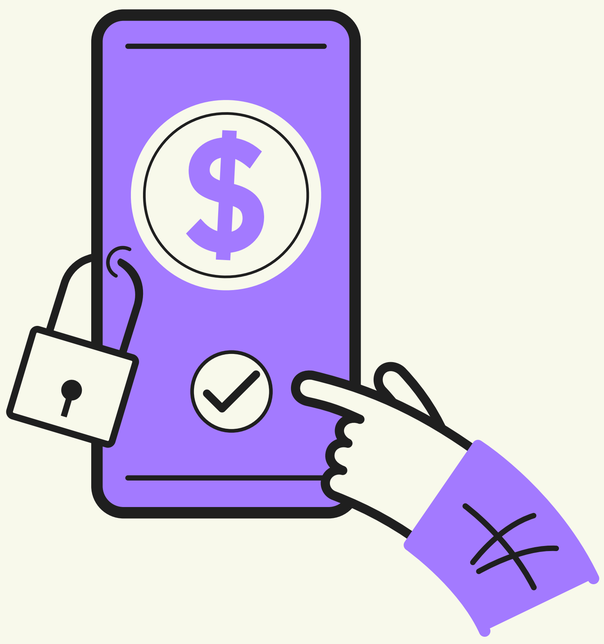
TIPS ON PROTECTING YOUR GAME & PAYMENT ACCOUNTS

01

Safe Login Practices

- Enable 2FA
- Don’t reuse passwords
- Avoid logging in using public Wi-Fi
- Use password managers
- Use an authentication app (Google Authenticator, Authy, etc.) instead of SMS where possible.

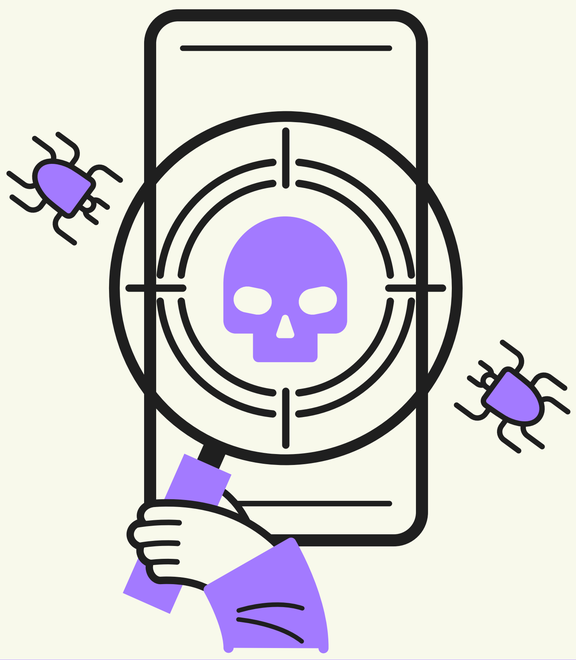
02



Safe Payments

- Use official top-up partners and platforms
- Avoid individual sellers offering large discounts
- Never transfer “outside the platform”
- Never share your personal credentials (password, OTP, gamer ID)

03

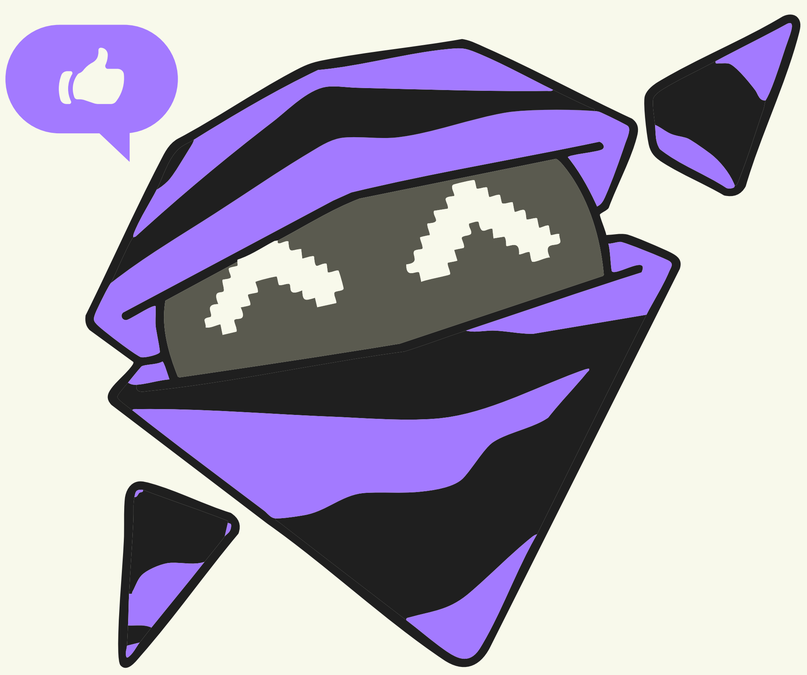


Device Protection

- Avoid downloading APKs or game mods
- Install reputable antivirus and browser protection tools

SECTION III

QUICK GAMER CHECKLIST: DOS & DON’TS



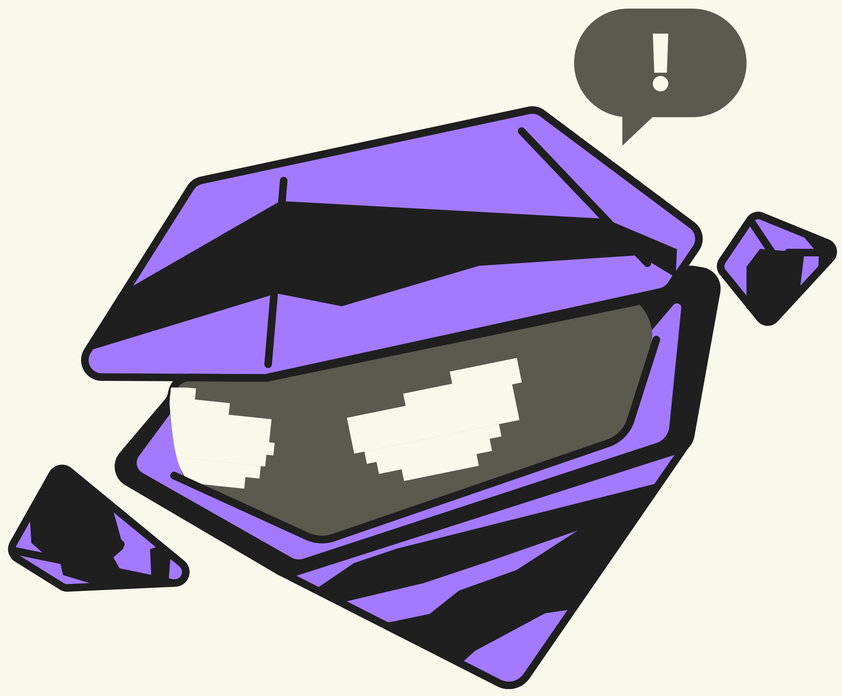
DO’S - The Safe Zone

Use only official payment channels listed on the game or publisher’s website/app.

- For instance, Codashop website (https://www.codashop.com/) centralizes payment methods and will not redirect you to a third-party site or social channel to complete transactions.

Rewards and prizes are credited directly to your game account. You will never need to "claim" them by logging into an external site or paying a "delivery fee."

Verify announcements on official pages before responding to messages about rewards, bans, or account issues.



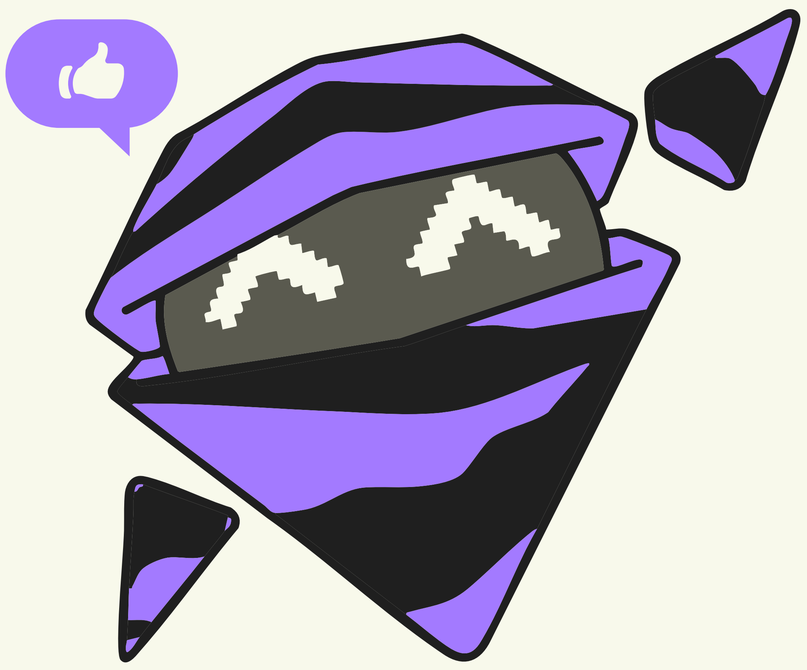
DON’TS - The Danger Zone

Don’t share your OTP with anyone, no customer support team will ever ask for it.

Don’t click on a payment link from a direct message. Coda will never ask you to click a link to make a payment via WhatsApp, Telegram, Signal, SMS, or other messaging channels.

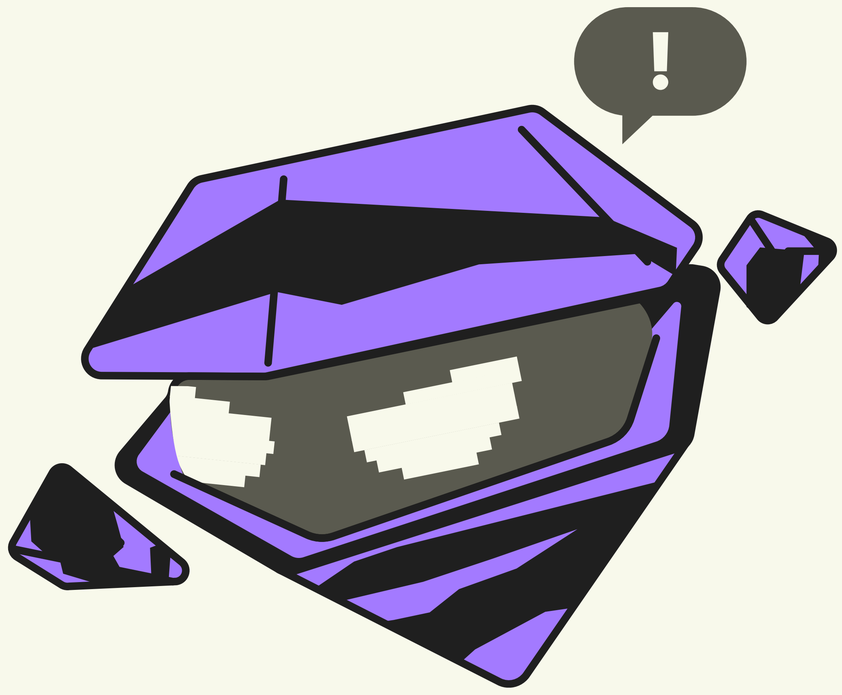
Don’t click on “free diamonds/skins” links — these are common phishing scams.

Don’t give your email, password, or verification code on pages you’re unsure about.



Double-check the domain of an email and be aware of “spoofed” email addresses. Coda will only contact you from official domains (e.g., @coda.co, @codashop.com, @codapayments.com).

If you encounter a suspicious top-up website that imitates a brand or appears to be a scam, report it to the relevant payment channel, official top-up platform, or a public reporting site run by local authorities. Reporting helps protect other players from falling victim to the same scam.



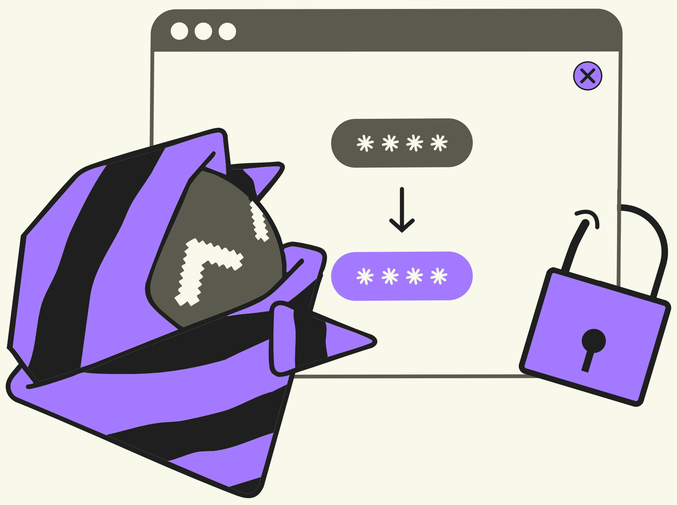
Don’t trust “urgent” messages claiming your account will be banned unless you act immediately.

Don’t engage with private messages from “admins” on WhatsApp, Discord, Telegram, or other platforms. Real admins rarely, if ever, reach out individually. Instead, go directly to the official website or app to verify.

SECTION IV

WHAT TO DO @IF YOU'RE A VICTIM

01



Secure Your Account First

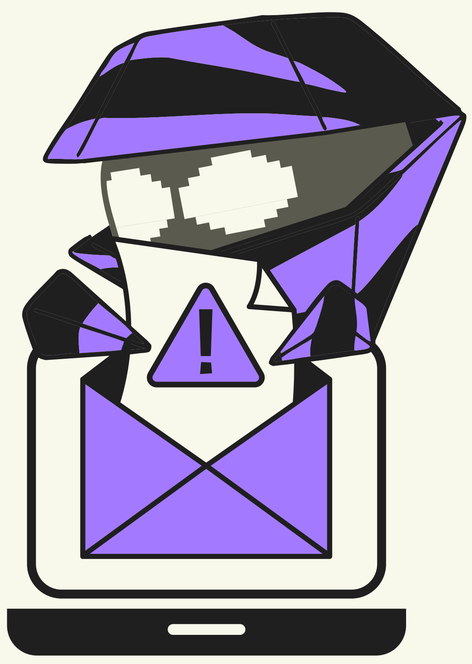
- Change password immediately
- Enable/reset 2FA
- Force log out from all devices
- Scan your device for malware
- Contact official game support

02

Secure Your Money

- Contact your bank or e-wallet provider immediately
- Freeze payment methods if needed
- Dispute unauthorized charges
- Keep all evidence (screenshots, chat history)

03



Report and Recover

- Contact the payment channel's (bank or e-wallet provider) official support ticket for payment scams
- Keep logs and screenshots
- Customer support channel where the top-up occurred, if it's related to a top-up issue.
  - For instance, Coda Indonesia customers may seek support via https://id.support.codashop.com/hc/id
- If funds were stolen or your identity was compromised, report the case to your local cybercrime authority.

SECTION V

OFFICIAL CODA CONTACT CHANNELS

More information, visit:

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

CODA.CO

CODA