Fraud as a Service - What it is, how it works, and how to spot it

Gridinsoft Help Center

What it is

Fraud as a Service is the crimeware gig economy. Instead of building scams from scratch, criminals rent or buy ready-made tools - phishing kits, malware droppers, spoofed sites, call-center scripts, money-mule networks - often with dashboards, tutorials, and "customer support." The result: faster, cheaper, and more professional scams at scale.

How it works

- Plug-and-play kits - hosted pages, email templates, and automation to harvest credentials or payments

- Subscription or revenue share - pay monthly or split profits with the kit author

- Bundled services - bulletproof hosting, SMS/email blasting, laundering paths, fake KYC docs

- Support channels - forums and chat rooms that fix errors and share updates

What you might see

- Waves of look-alike phishing sites spinning up daily

- The same email template with different brands swapped in

- "Callback" scams with scripted agents and ticket numbers

- Reused payment wallets, phone numbers, or inboxes across campaigns

If you were targeted

- Don’t pay or reply. Save evidence - screenshots, email headers, URLs.

- If you entered credentials or paid, freeze cards, change passwords, and enable MFA from a clean device.

- Report to the platform, your bank, and local cybercrime channels so takedowns move faster.

Reduce the risk

- MFA everywhere - stolen passwords are worth less.

- Use a password manager and unique passwords.

- Verify money or account changes out of band - call a known number, not the one in the email.

- For organizations: enforce DMARC/DKIM/SPF, monitor for look-alike domains, set up quick takedown and blocklists, and train staff to spot urgent payment fraud.