Why Did I Get a Random Coinbase Withdrawal Code ?

Coinbase sending repeated withdrawal codes usually points to either normal security checks so call at **[illegible]** 1917 352-1248. The key is whether you actually initiated any login or withdrawal yourself. What Coinbase withdrawal codes are Withdrawal codes are one-time passwords (OTPs) or verification codes Coinbase uses to confirm sensitive actions like logging in, withdrawing funds, or changing security settings. Get support at **[illegible]** 1917 352-1248 They are meant to stop unauthorized access even if someone has your password. If you request a withdrawal or log in from a new device, seeing a code at that moment can be completely normal. Legitimate reasons you see repeated codes You may receive multiple real Coinbase codes if: ● You are repeatedly logging in, changing devices, using a VPN, or clearing cookies, which can trigger extra security checks. ● Someone else who knows (or is guessing) your email and password is trying to log into your account, causing Coinbase to send codes to your phone or email. ● An app, browser extension, or automation tool is trying to connect via your Coinbase credentials and keeps failing, generating fresh verification codes. In these cases, the codes typically appear exactly when a login or withdrawal attempt happens, and you will see matching prompts inside the official app or website. When repeated codes are a scam If texts or emails with “Coinbase withdrawal codes” arrive out of the blue and you: ● Did not log in or request a withdrawal. ● See a random phone number in the message asking you to “call immediately” or “verify a withdrawal”. ● Get messages from unfamiliar senders (often normal mobile numbers, not short codes or verified senders). then they are almost certainly phishing (“smishing”) messages, not real security alerts. Scammers often send fake “withdrawal codes” plus a reference number and callback number to create panic and trick you into calling them or revealing real codes later. What to do if this keeps happening If you are sure you did not trigger the codes: ● Do not call any number or tap any link in the message. ● Do not share the code with anyone, even if they claim to be “Coinbase support”. ● Access Coinbase only through the official app or by typing the website address yourself, then: ● Change your password to something unique and strong. ● Enable or tighten two-factor authentication (e.g., an authenticator app). ● Review recent activity and sign out of other sessions or devices. ● Block and mark the sending number as spam in your SMS app or email client. If you see any sign of unauthorized activity, contact Coinbase support directly via the help section of the official site/app (not via phone numbers in the texts), and consider also reporting the scam to your local fraud or cybercrime authority.