ADVISORY

TAU/ADV/004 Dated 8th April 2025

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

सत्यमेव जयते

Indian
Cyber
Crime
Coordination
Centre

सहवीर्यं करवावहै • Working Together With Vigour

RISE IN *"FAKE CAPTCHA FILLING JOBS"* BASED CYBERCRIME

There has been significant rise in complaints pertaining to online scams involving fraudulent CAPTCHA-filling jobs, wherein victims are lured with promises of high earnings for minimal effort. These schemes, primarily propagated through social media platforms, job portals, messages, or emails, are designed to defraud individuals by collecting personal data, demanding upfront payments, and withholding remuneration for completed tasks, thereby resulting in significant financial loss.

MODUS OPERANDI

- **Initial Contact: -** Fraudsters promote high-paying CAPTCHA-filling jobs on social media, job portals, or messaging platforms and claims of earning significant income with minimal effort are emphasized making it appealing to job seekers.
- **Registration Process:** Victims, in order to start earning by Captcha Filling, are asked to register by paying registration fee, training fee, or software/application charges. Scammers sometimes present fabricated agreements to create an illusion of legitimacy.
- **Work Assignment:** Upon registration, victims are given access to a fake CAPTCHA-solving platform for performing tasks that involve solving thousands of CAPTCHAs for an amount under strict deadlines.
- **Non-Payment:** After a few weeks or months, victims are denied payouts and withdrawal of purported earnings on grounds of alleged inaccuracies in work, rendering their earnings invalid. This is often followed by delays or non-processing of withdrawals and further demands for additional payments under the pretext of taxes, processing charges, commissions, or membership upgrades. Thereafter, the scammers discontinue communication and abscond with the victims' deposits.

PRECAUTIONS

- Fake captcha jobs or illegal part-time jobs often **promise high earnings** but demand upfront fees and capture personal/financial information**.**
- **The Red Flags** in such scams are upfront payment, unrealistic earning promises, delayed or denied withdrawals, and overemphasis on referral programs for increased income.
- **Research for the platform's legitimacy** through reviews and forums, avoid sharing sensitive personal/financial information.
- **Report cyber frauds** immediately by calling 1930 or at www.cybercrime.gov.in.
- Regularly update yourself on the latest cybercrime, and for prevention tips, follow **@cyberdost** on social media.