



## Scam on Social Media

## **Modus Operandi**

- Fraudsters posing as representatives social media company contact unsuspecting individuals through WhatsApp or Telegram etc.
- Offer part-time job / work from home job opportunities with just through liking and subscribing to YouTube videos.
- Upon accepting the offer, users are instructed to like YouTube videos & submit screenshots to fraudster as proof of completion.
- Fraudster uses fictitious Apps / Websites to display the earnings of users to provoke them & gain trust.
- Users are asked to invest an amount to access their earnings.
- After the receival of the amount into fraudster's account, the victim is blocked by fraudster resulting in the loss of both the invested amount & potential earnings.

## **Best Practices**

- Be wary of unknown messages offering easy make money for just clicking 'like'. Always question the legitimacy of offers that promise high earnings for minimal effort.
- If approached by someone claiming to represent a social media company employee, verify their authenticity through official channels.
- Avoid clicking on suspicious links or buttons at the behest of any stranger.
- Do not provide personal information or financial details to anyone under any circumstances.
- Keep your Social Media privacy settings at the most restricted level to deter strangers from accessing your information for targeted social engineering attacks.
- any situation, never act on emotional impulse; always consider facts & utility of the situation.

Report Cyber fraud Incident to https://www.cybercrime.gov.in or Call 1930 for assistance



CISO OFFICE