Subject: Fraudsters sending Fake Job Offer SMSs to perpetrate Cyber Crime.

Threat Summary

A new trend in financial cyber fraud has been observed where fraudsters send Fake Job Offer SMSs to perpetrate Cyber Crime. Fraudsters place online advertisements claiming that they can give jobs where one can make large amount of money working from home with little time and effort.

A job scam occurs when a fraudster poses as an employer or recruiter, and offers attractive employment opportunities, which require job seekers to pay some money in advance. The SMSs sent by fraudsters offer high-paying part-time jobs to siphon off victims' money and their personal information.

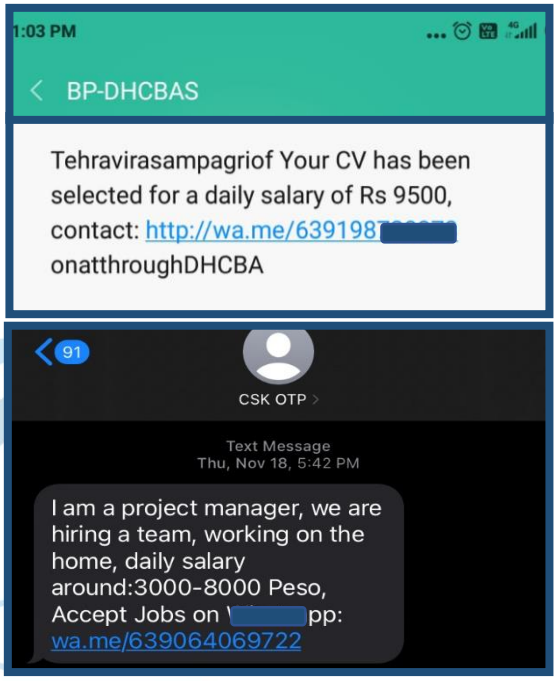

Fig. 01 – Sample SMSs perpetrating job frauds

Modus Operandi

- Fraudsters send text messages saying that "Your CV has been selected for a job", "Accept this job and earn daily salary", etc. to their targets.
- The message is generally sent via an SMS-Header to make it look credible. The messages include a **wa.me** link (used for the WhatsApp's "click to chat" feature). It allows users to begin a chat with anybody without having their phone number being saved.
- Once the link is clicked WhatsApp conversation with the fraudster starts, the fraudster asks the victim to start the registration process on a malicious website link.
- When the victim enters his/her personal details on the provided registration link, the sensitive personal data is compromised.
- After that the fraudster asks the victim to add money to their account for verification & registration process.

- The money sent by the innocent victims is siphoned off by the fraudsters, and the cybercriminals leverage the stolen sensitive personal/financial information to perpetrate further financial cyber crimes.

Suggestions

- Avoid tempting job offers sent via text messages or emails by unknown senders.
- Scrutinize the job offering company online (use words like “scam,” “fraud,” or “complaint” with company name to online search & verify if similar scams are happening).
- Avoid making any payment without authenticating the employer for registration or other purposes.
- Securitize the SMS-Headers to confirm the authenticity of a job offer.
- Fraudsters typically show urgency in their requests. Scrutinize properly, if a request seems too urgent.
- Report any such incidents on the *cybercrime.gov.in* portal and follow *@CyberDost* on Twitter, YouTube, Facebook, Instagram, Public, Koo and LinkedIn to know more about safety tips.

Regards,

Indian Cyber Crime Coordination Centre
CIS Division, MHA
011-23438207