JOINT NEWS RELEASE

PROTECTING AGAINST CRYPTOCURRENCY SCAM INVOLVING FAKE JOB OFFERS AND COMPROMISE OF SOFTWARE SYSTEM

The Singapore Police Force (SPF) and the Cyber Security Agency of Singapore (CSA) would like to alert members of the public and businesses to a cryptocurrency-related scam involving fake job offers and compromised software systems, which has resulted in losses amounting to USD11.8 million (approximately S$15 million). This advisory outlines the methods employed by these scammers, as well as recommended measures for businesses and individuals to protect themselves against similar scams and cyber-intrusions.

Cryptocurrency Theft via Social Engineering and Malicious Software

2 In this variant, the victim was first approached on LinkedIn by a scammer impersonating a recruiter from a cryptocurrency-related company. The scammer communicated with the victim via email, using a spoofed domain that closely resembled the legitimate company's domain. The victim attended several video interviews conducted over Google Meet, during which the interviewer's video remained disabled throughout.

3 The victim was then directed to a spoofed website to complete a technical coding assessment on his company-issued device. During this assessment, the victim was induced to unknowingly download malicious software. The malware enabled the scammer to bypass authentication controls to harvest internal company credentials, and used them to carry out cryptocurrency transfers.

Recommended Prevention and Mitigation Measures

4 SPF and CSA would like to advise businesses and individuals, particularly those in the technology and cryptocurrency sectors, to adopt the following precautionary measures:

a) **Be Wary of Social Engineering Tactics**. Stay vigilant and look out for scams, phishing, and social engineering. Developers and technical professionals are more likely to be targeted through malicious coding assignments. Malicious actors may impersonate recruiters, employers, or business partners to gain trust and induce victims to disclose information, download files, or execute code. Businesses should put in place measures to educate their employees.

b) **Verify Recruiter and Company Identities**. Take steps to verify recruiters and companies through official channels before responding to job offers or potential interviews. Exercise caution if interviewers refuse to enable their video during calls, or if you are asked to communicate through unofficial platforms or unfamiliar websites.

c) **Exercise Caution with Technical Assessments.** Do not execute code or download files from unknown or unverified sources. Scan software and dependency packages with reputable security tools before use, preferably in an environment isolated from company systems. Untrusted content should not be run on devices or systems.

5 SPF and CSA also advise businesses to consider the following advanced measures to further uplift cyber hygiene:

a) **Protect API Keys and Internal Credentials.** API keys and internal credentials should be stored securely, with access restricted on a need-to-know basis, tightly controlled, and logged. Use short-lived credentials where possible, and promptly revoke suspected compromised sessions. Businesses should implement transaction limits, approval workflows, and other safeguards at the API level that cannot be bypassed by direct API calls.

b) **Strengthen Multi-Factor Authentication.** While multi-factor authentication (MFA) is an important safeguard, individuals and businesses should be aware that session token harvesting can bypass MFA. Consider implementing additional controls such as device binding, anomalous login detection, and short session token expiry windows.

c) **Monitor for Unusual Access and Lateral Movement.** Individuals and businesses should watch for suspicious logins, unfamiliar devices, unexpected access to accounts or systems, privilege escalation, and lateral movement across networks. Deploy network monitoring tools to detect suspicious network activity, including unexpected outbound traffic from internal servers to external IP addresses. Where possible, segment development and production systems to limit lateral movement.

d) **Secure Code Repositories and Deployment Pipelines.** Businesses should implement strict access controls and continuous monitoring for code repositories and automated deployment systems. Changes to deployment instructions should be subject to multi-party review and approval. Businesses should also regularly audit access logs to detect any unusual activity.

6 If compromise is suspected, affected devices or systems should be isolated immediately, active sessions revoked, credentials reset, and access logs reviewed. Individuals and businesses should notify their internal cybersecurity teams or service providers without delay, and assess whether accounts, repositories, internal servers, or approval workflows have been altered.

7 Anyone with information relating to such crimes may call the Police Hotline at 1800-255-0000, or submit the information online at www.police.gov.sg/i-witness. All information will be kept strictly confidential. If you require urgent Police assistance, please dial '999'.

8 If in doubt, members of the public may visit www.scamshield.gov.sg, call the 24/7

ScamShield Helpline at 1799 or download the ScamShield app to check, detect and block scams. Together, we can ACT against Scams to safeguard our community.

SINGAPORE POLICE FORCE
CYBER SECURITY AGENCY SINGAPORE
14 AUG 2026 @ 9.00PM