NCRIC | Northern California Regional Intelligence Center

Fusing Information, Talent And Training For A Safer Society.

Advisory Bulletin

(U) SCOPE: NCRIC bulletins provide real-time updates on incidents and situations of urgent interest to NCRIC partners including officer safety alerts, BOL requests, threat warnings and ongoing incidents. NCRIC bulletins may include raw reporting that has not been fully evaluated in order to provide timely situational awareness.

21 July 2026

(U) Aggressive Phishing Campaign Targeting Public and Private Sector Organizations

THIS IS AN EXERCISE

(**(U) Summary:** Threat actors are conducting a widespread phishing campaign targeting government agencies, critical infrastructure, healthcare organizations, educational institutions, financial services, transportation entities, and private businesses. The campaign uses credential harvesting, business email compromise, malicious attachments, and spoofed cloud service login portals.

(U) Threat Activity: Observed tactics include fraudulent Microsoft 365 and Google Workspace login pages, account security notifications, payroll and HR-themed emails, vendor impersonation, invoice fraud, and MFA fatigue attacks. Adversaries are leveraging publicly available information to increase legitimacy and improve targeting.

(U) Potential Impacts: Successful compromise may result in credential theft, unauthorized network access, ransomware deployment, data exfiltration, operational disruption, financial fraud, and compromise of sensitive information.

(U) Indicators: Unexpected login requests, urgent requests for action, suspicious attachments, domains closely resembling legitimate organizations, unsolicited MFA prompts, and requests to change payment or account information.

(U) Considerations: Organizations should reinforce phishing awareness training, validate email authentication controls (SPF, DKIM, DMARC), implement phishing-resistant MFA, monitor authentication logs, and promptly investigate reported phishing attempts.

(U) Reporting: Report suspicious cyber activity through organizational reporting channels. Significant cyber incidents should be reported to appropriate law enforcement and cybersecurity partners. Preserve email headers, attachments, and relevant logs for investigative purposes.