H E A D Q U A R T E R S
ARMED FORCES OF THE PHILIPPINES CYBER COMMAND
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN 2025-04

The Rising Threat of Text Scams

Overview

Recent findings from the U.S. Federal Trade Commission (FTC) highlight a significant increase in financial losses attributed to text message-based scams, totaling a reported $470 million in 2024. This figure is believed to be conservative, as many incidents remain unreported. The evolving sophistication of social engineering tactics underscores a persistent threat vector that requires continued vigilance and enhanced countermeasures across both public and private sectors. The primary attack surface of scammers are mobile endpoints by using social engineering and phishing attacks. Potential implications from their victims are credential compromise, identity theft, financial fraud and exposure to larger fraud networks.

The FTC report identified the following as the most prevalent forms of SMS-based scams:

1. Package Delivery Phishing

Threat actors impersonate delivery services to prompt users into paying fictitious redelivery fees, thereby harvesting sensitive payment credentials.

2. Employment Offer Scams

Scammers masquerade as recruiters offering illegitimate job opportunities. Victims are either defrauded of funds for supposed job requirements or lured into divulging personally identifiable information (PII).

3. Impersonation via Fake Fraud Alerts

These SMS messages emulate legitimate financial institutions, warning of unauthorized transactions. Victims are socially engineered into transferring funds under the guise of account protection.

4. Toll Violation Scams

Fraudulent notifications claim unpaid toll fees. The goal is to create urgency and redirect victims to spoofed websites for credential and payment data harvesting.

2. Wrong Number / Conversational Social Engineering

These campaigns initiate via an innocent “wrong number” text and evolve into long-term confidence schemes such as romance scams or “pig butchering,” aimed at extorting large sums or stealing identities.

Recommendations:

To mitigate the growing risk of SMS-based threat campaigns, the following security controls and procedural enhancements are advised:

1. User Awareness and Security Training

- Conduct targeted phishing simulation exercises, especially focused on mobile vector scenarios.
- Provide briefings and security advisories on emerging scam tactics and impersonation techniques.

2. Zero Trust Mobile Policy

- Enforce strong mobile device management (MDM) policies.
- Implement app whitelisting and denylist enforcement for unknown or high-risk URLs received via SMS.

3. Multi-Factor Authentication (MFA)

- Mandate MFA for all access to sensitive systems and accounts, reducing risk from credential compromise.

4. Threat Detection and Endpoint Monitoring

- Deploy advanced threat detection on mobile devices capable of identifying malicious URLs or unauthorized downloads.
- Integrate SMS phishing telemetry into SIEM platforms for early warning indicators.

5. Incident Reporting and Response

- Standardize reporting mechanisms for suspicious SMS messages across the organization.
- Ensure Cyber Incident Response Teams are trained to triage and investigate text-based phishing attempts.

6. Continuous Intelligence Gathering

- Collaborate with other government agencies, threat intelligence platforms, and law enforcement agencies to maintain situational awareness of ongoing scam campaigns and TTPs (Tactics, Techniques, and Procedures).

Conclusion

The surge in text message-based scams is a stark reminder of the evolving nature of social engineering and mobile-based threat vectors. With attack methods becoming increasingly deceptive and harder to detect, a layered approach encompassing user education, technical defenses, and real-time threat intelligence is essential. Proactive vigilance and institutional readiness remain our strongest assets in combating these threats.

Reference: *https://www.malwarebytes.com/blog/news/2025/04/text-scams-grow-to-steal-hundreds-of-millions-of-dollars*