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 2026-01

Senior and Head Officials Impersonation and Urgent Money Transfer Scams

Overview

Recently, cybercriminals are impersonating senior leaders, commanders, directors, and heads of offices of the AFP by creating fake social media or messaging accounts. Using stolen photos, names, and ranks, scammers contact targeted personnel through messaging platforms such as Viber, Signal, Telegram, and SMS, presenting themselves as legitimate authority figures.

The scam typically involves an urgent and confidential financial request, often framed as an emergency or restricted transaction, designed to bypass standard verification procedures.

Once the money is transferred, the scammer immediately cuts communication and disappears.

The typical attack follows this pattern:

1. A fake account is created using the name, profile photo and contact number of a senior official.
2. The scammer contacts a finance officer or authorized personnel via messaging applications.
3. An urgent request for fund transfer is made, often citing:
   - Confidential matters

- Emergency requirements
- Time-sensitive operations

4. Pressure tactics are applied, including statements such as:
    - "Kailangan ma-transfer bago 3:00 PM."
5. When funds are successfully transferred, the scammer ceases all communication.

This social engineering attack is effective as it uses real names, photos, ranks and contact number of senior leaders, it exploits organizational hierarchy and respect for authority, it creates artificial urgency to prevent verification and it use familiar language and internal context to appear legitimate. Their primary targets are the finance and administrative personnel due to their access to organizational funds.

Recommendations

In this regard, AFP personnel are advised of the following measures:

- Always verify financial requests through official channels. Contact the supposed sender using their official office number or known contact, not the number provided in the message.
- Strictly observe the two-person or multi-level approval rule. No financial transaction should be processed without proper authorization and verification.
- Do not rely on profile photos, screenshots, or names as these can easily be copied or manipulated.
- Personnel must be alert to the following warning signs:
    - "Confidential" or secret fund requests
    - Pressure to bypass standard financial procedures
    - Requests sent via unofficial communication channels
    - Messages originating from unfamiliar or newly created numbers
    - Communications sent late at night, during weekends, or outside office hours
- If you receive a suspicious message: Do not transfer any funds, preserve evidence (screenshots, message details) and verify directly with the intended sender via official channels.
- Report suspicious messages immediately. Notify the ICT Office, Cyber Incident Response Team, and chain of command without delay.

Conclusion

Senior and head officials social engineering attacks pose a serious threat to organizational integrity and financial security. Legitimate leaders follow established procedures and do not demand secret or rushed transactions. Scammers rely on urgency to prevent rational decision-making.

Think before you transfer. Verify before you act. Protect your unit. Protect your organization.