ARMY CRIMINAL INVESTIGATION DIVISION

CRIME PREVENTION

ALERT | EXECUTIVE IMPERSONATION

Authorized for widest release without restrictions.

Adversaries are creating fake online accounts to impersonate senior leaders. In the fourth quarter of 2025 alone, the Army CID's Digital Persona Protection Program identified over 73,000 such accounts targeting Army leadership.

These criminals study public data from professional networking sites to craft convincing "spear-phishing" attacks. This form of social engineering exploits our sense of duty to trick personnel into bypassing security protocols, which can lead to serious breaches.

WARNING SIGNS

SIGN	DESCRIPTION
The Request	An urgent, unexpected, or last-minute demand for sensitive data, credentials, or system access that violates standard procedures.
The Pressure	An unusual emphasis on speed and secrecy. The message may use phrases like, "This is a sensitive project, your discretion is required," to prevent you from verifying the request.
The Sender	The message comes from an unofficial channel, such as a personal email address (e.g., gmail.com) or text message. The display name may look correct, but the underlying email or phone number is wrong, or the tone feels inconsistent with the person they are impersonating.

PREVENTION BEST PRACTICES

- Sanitize Your Digital Footprint: Limit the professional details you share on public websites that an adversary could leverage.
- Check Your Online Presence: Periodically search for yourself online to see what an attacker sees. Maximize privacy settings on your social and professional accounts.
- Question Urgency: Scrutinize any request that deviates from standard procedure, regardless of how important it seems.
- Verify, Then Trust: Confirm all unusual directives with a quick phone call.

Spear-phishing: A cyberattack that uses extensive research on a target's personal and professional life to craft highly convincing, personalized messages.

IF YOU SUSPECT AN ATTACK

STOP.

- Do not reply, click on links, or open attachments.

VERIFY.

- Contact the sender using a trusted channel, like a phone number or email from an official directory. Never use the contact information provided in the suspicious message.

REPORT.

- Immediately notify your IT or cybersecurity department. Do not forward the message.

SUBMIT A TIP

Reporting is Anonymous

https://www.cid.army.mil/Submit-a-Tip/

SUBMIT A TIP