Impersonation Scam Targeting Cybersecurity Job Seekers via LinkedIn

Date of Incident: June 12, 2025
Type of Threat: Social Engineering / Federal Impersonation / Employment Scam

---

Summary

I identified a LinkedIn post made by an individual falsely claiming to be a Special Agent with NCIS. The post directly referenced me and encouraged contact with a third-party "recruiter" using a Gmail address. After engaging, I discovered that this was a monetized career coaching pitch misrepresented as federal job placement assistance.

Timeline of Events

| Time | Event | |---|---| | ~2:00 PM | LinkedIn post by "SA Lawrence C Richard" appears | | ~3:00 PM | Commented and received engagement from fake profile | | ~4:00 PM | Contacted “Dustin Elder” via Gmail | | ~5:00 PM | Received initial friendly response (included NCIS referral) | | ~6:30 PM | Received feedback + resume review and pitch for paid service | | ~7:30 PM | Fake profile disappears from LinkedIn | | ~9:00 PM | Report prepared and submitted to NCIS_Tips@ncis.navy.mil |

Key Indicators of Deception

- Use of Gmail address for “recruiter” contact
- Profile claiming to be NCIS Special Agent with no verifiable background
- Vanishing post/account
- Escalation to paid service after initial trust was gained
- Targeting of cert-earning cyber students

Actions Taken

- Preserved evidence via screenshots
- Reported impersonation to NCIS
- Compiled forensic timeline of communication

- Initiated personal awareness campaign (optional)

Lessons Learned

- Federal impersonation is increasingly used to exploit cyber job seekers
- Scams are becoming more targeted, using LinkedIn activity and cert posts
- Professional skepticism, evidence preservation, and proper escalation are critical in early-career cyber roles

---

Prepared by Hunter Nicholes on June 13, 2025