

26749 - Phishing Campaign Specialist

Location: Mons, Belgium.

Period: 166 (start on 16 Dec. 2026)

Deadline: 10 Nov. 2026

Duties/Roles:

- Support and coordinate entities: Act as the primary service contact, provide advice or comprehensive campaign support according to entity needs, coordinate stakeholders, and promote consistent practices and knowledge sharing;
- Plan and execute campaigns: Define objectives, audiences, scenarios, and schedules; configure, test, validate, execute, and review campaigns aligned with organizational awareness objectives;
- Manage phishing templates: Create and maintain an approved, reusable template library, support entity-developed templates, and adapt scenarios for different audiences, languages, and business contexts;
- Maintain threat relevance: Monitor phishing and social engineering trends, recommend realistic simulation scenarios, and share relevant threat insights and lessons learned;
- Administer the platform and coordinate the provider: Manage user access and roles, support platform whitelisting across NATO entities, track vendor issues and service requests, and communicate relevant platform changes;
- Support license and contract management: Track license usage, contractual dates, and renewal requirements; identify optimization opportunities; and coordinate timely renewal preparation, with commercial, procurement, contractual, and approval decisions retained by designated organizational owners;
- Deliver reporting and analysis: Produce entity-level, consolidated, and management reports using consistent metrics and definitions, highlighting campaign results, trends, risk indicators, and recommended follow-up actions;
- Maintain documentation, compliance, and improvement: Maintain procedures, standards, and deliverables in agreed repositories and formats at agreed frequencies; follow applicable policies, privacy requirements, and governance processes; and recommend improvements to campaign effectiveness and service delivery.

Skills, Knowledge, Experience Required:

Mandatory:

- The candidate must have a currently active NATO SECRET security clearance
- A minimum requirement of a Bachelor's degree at a nationally recognised/certified University in a related discipline and 3 years post-related experience;
- Or exceptionally, the lack of a university degree may be compensated by the demonstration of a candidate's particular abilities or experience that is/are of interest to NCIA, that is, at least 10 years extensive and progressive expertise in duties related to those in this Statement of Work;
- Experience managing or supporting enterprise phishing simulation campaigns and using phishing simulation and security awareness platforms;
- Strong understanding of phishing and social engineering techniques, email technologies, and relevant security controls;
- Ability to design realistic scenarios and templates, with attention to detail in campaign configuration and validation;
- Strong analytical skills to consolidate and normalize results across entities and produce clear operational and management reports;
- Effective stakeholder management and vendor coordination, working with technical and non-technical teams;
- Strong organizational skills to manage multiple entities, campaigns, priorities, and deadlines;
- Strong written and verbal English communication skills, with the ability to work independently and proactively identify issues.

Desirable:

- Experience delivering phishing simulation, security awareness, and human-risk management programs across large, federated, multinational, or multi-entity organizations;
- Knowledge of threat intelligence, current phishing trends, mail security gateways, and related email security environments;
- Experience developing dashboards, KPIs, and awareness metrics using Excel, Power BI, or similar tools, alongside automation, scripting, APIs, or platform integrations;
- Understanding of privacy, data protection, and employee considerations, plus experience with procurement, contract management, or software licensing;
- Relevant cybersecurity certifications or professional qualifications.

Required Level of Security Clearance:

NATO SECRET.