Next-Gen Cybercrime Investigation & Response	
GANNDALF NextGen Collaborative Cybercrime Investigation Framework	**Course title:** **Social engineering and phishing detection**
Overall aim	Creating a new landscape with respect to advanced cybercrime investigation and prevention, based on enhanced re- and up-skilling of investigators and law enforcement officers offering training on major contemporary cybercriminal activities and learning skills to identify social engineering tactics, investigate phishing attacks, and educate the public on prevention.
Proficiency level	Advanced
Duration	1 Day (5,5 hours total, divided into 5 sessions)
Target audience	LEAs, prosecutors, and judicial actors
Number of participants	20
Learning outcomes	Learning skills to identify social engineering tactics, investigate phishing attacks, and educate the public on prevention: • Recognize different types of social engineering attacks • Understand attacker psychology and methods of manipulation • Understand how phishing campaigns are structured and delivered • Learn how to identify phishing emails and messages • Learn the investigative process after a phishing incident • Understand evidence handling and victim assistance
Main thematic areas (topics, subtopics)	**Session 1: Understanding Social Engineering (1 hour):** • What is social engineering? Human error as an attack vector • Types: phishing, vishing (voice), smishing (SMS), baiting, pretexting, impersonation • Psychological tactics used: urgency, fear, curiosity, authority, reciprocity, greed. • Real-world examples of successful social engineering attacks **Group discussion:** • Share examples or stories of social engineering attempts targeting individuals or institutions **Session 2: Phishing Tactics & Detection (1,5 hour):** • Anatomy of a phishing email (sender spoofing, malicious links, fake branding) • Types of phishing: spear phishing, business email compromise (BEC), clone phishing, whaling • Red flags and heuristics for detection • Free online tools for quick sandbox analysis (Hybrid-Analysis) • Tools and browser/email protections (SPF, DKIM, DMARC basics) **Exercise:**

This work is part of the GANNDALF project. GANNDALF has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement no. 101167951

	• Review a series of real and fake phishing emails to identify key indicators **Session 3: Investigating and Responding to Phishing Attacks (1,5 hour):** • Initial actions: isolating affected systems, collecting headers and logs • Tracing phishing links and analyzing payloads (overview) • Gathering indicators of compromise (IOCs) • Coordinating with IT, CERTs, ISPs, and email providers • Reporting and documenting phishing attacks • Tools Introduced: Email header analyzers, PhishTool, URLScan.io, VirusTotal, MXToolbox, Hybrid-Analysis **Session 4: Simulation & Public Safety Messaging (1 hour):** 1. Scenario Exercise - Simulated phishing campaign targeting a local agency: • Identify the phishing attempt • Analyze the email • Draft a short report and develop a response plan 2. Public Awareness & Prevention: • How to educate victims and the public • Creating phishing awareness messages for social media or community briefings • Collaborating with schools, businesses, and elderly communities 3. **Wrap-Up:** • Key takeaways • Best practices for prevention and awareness **Session 5: GANNDALF tools - Practical demonstration (30 min)**
Cross-cutting and/or horizontal aspects	Raising awareness, increasing in the capabilities of officers exploiting specific technologies for crime detection and investigation, enhancing re- and up-skilling of investigators and law enforcement officers, gaining a comprehensive knowledge of the numerous elements contributing to cyber-attacks
Methods and learning strategy	Trainings in person or online training, real world scenarios, case study simulations, exercises
Learning environment	Conference room with a large screen for displaying, Physical training participants should have access to a laptop to perform the exercises/ online platform
Number of trainers	1
Participants' assessment/testing	yes
Course evaluation	yes
Course certification	yes

This work is part of the GANNDALF project. GANNDALF has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement no. 101167951