Almada
Software & Security

Technical offer for government bodies and institutions

Security Awareness & Staff Training Programme

Preparing your people to withstand phishing and social engineering and to protect official data, with results measured before and after training.

Prepared for _____

Reference _____

Date _____

Almada · Tripoli, Libya

almada.biz · info@almada.biz

01

Introduction

Government bodies and institutions now rely on email and digital systems for their correspondence and services, and their staff have become attackers' first target. Most security incidents do not begin with a technical flaw but with a convincing message or a call impersonating an official body or a senior manager.

In this offer, Almada proposes a complete security awareness and staff training programme that combines interactive workshops, safe phishing simulation and objective measurement of results, adapted to the organisation and to every level of its staff.

The programme at a glance

4
training tracks by job role

5
delivery phases, from assessment to follow-up

Before / after
objective measurement with a management report

4+
training languages: Arabic, English, Turkish, French and more

About Almada

Almada is a Libyan company based in Tripoli working in software development and cybersecurity. Our work includes CACUS, a system for detecting phishing emails, and we provide security assessments, website scanning and security awareness to public and private organisations.

02

Programme objectives

01 Improve staff ability to detect phishing in email, SMS and messaging apps.

02 Enable staff to resist social engineering, even under pressure or in the name of authority.

03 Establish everyday security discipline in line with recognised information-security standards.

04 Build a culture of data classification: what may be shared, with whom, and through which channel.

05 Enable senior management to assess risk and make sound decisions during incidents.

06 Build a culture of early, blame-free reporting of incidents and suspicious messages.

Target groups

- Senior management and leadership
- Administrative and finance staff
- Front-desk and public-service staff
- IT teams
- New employees
- Faculty and students (educational institutions)

03

Training tracks

Track	Audience	Suggested duration	Main topics
General awareness	All staff	3-hour workshop	Phishing detection, passwords and two-step verification, data classification and sharing, incident reporting.
Leadership	Senior management	2-hour briefing	Risk assessment, fraud targeting and impersonating executives, decisions during an incident, legal and reputational responsibility.
Technical teams	IT	2 days	Security policies, secure administration of systems and accounts, incident detection and response, email protection.
Newcomers	New staff and students	2 hours	Personal digital safety, social media, protecting accounts and devices.
Phishing simulation	Agreed groups	4–6 week campaign	Safe simulated phishing with written approval, measuring click and report rates before and after training.

Durations are suggestions and are adjusted to the organisation's needs and number of trainees.

Detailed topics

- Phishing by email, SMS and WhatsApp
- The “Stop · Verify · Report” protocol under pressure
- Passwords and two-step verification
- Everyday risk assessment
- Social engineering: authority, urgency and fear
- Data classification and sharing rules
- Personal devices, USB drives and remote work
- Responding to and reporting incidents

04

Delivery methodology

01 Baseline assessment

A short questionnaire and an optional initial phishing simulation establish current awareness per department.

02 Planning & tailoring

Content and examples tailored to the organisation, its systems and its staff's language; schedule approved.

03 Training workshops

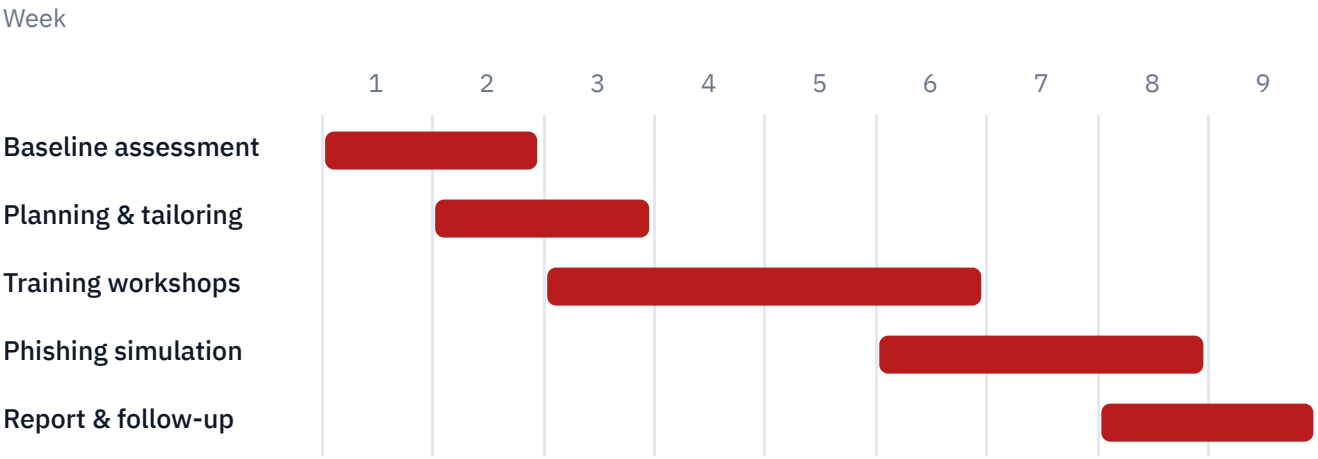
Interactive workshops with real regional examples, role-play and practical exercises.

04 Phishing simulation

A safe simulated campaign measures what was learned in real conditions.

05 Report & follow-up

A before/after report for management, recommendations and a periodic refresher plan.



Typical schedule for a mid-sized organisation; shortened or extended with the number of trainees.

05

Deliverables

- Baseline assessment report per department
- Training materials tailored to the organisation, in Arabic (other languages on request)
- Workshops for each approved track
- Safe phishing simulation campaign and results report
- Final before/after report for senior management with recommendations
- Certificates of attendance
- Short awareness guide and posters for internal distribution

Measures of success

Phishing link click rate	falls between the first and second simulation
Suspicious-message report rate	rises between the first and second simulation
Knowledge assessment score	compared before and after, per department
Attendance and completion	per training track

Confidentiality and data protection

- A non-disclosure agreement (NDA) is signed before work begins.
- Phishing simulations run only with the organisation's written approval.
- No passwords or real data are collected during simulations.
- Results are delivered as anonymous summaries unless the organisation requests otherwise.
- Simulation data is deleted after the final report is delivered.

06

Training team

Academic qualifications

Most of the team are academics holding postgraduate degrees in cybersecurity.

Research and practice

Experience in phishing-detection research and systems, and in assessing the security of systems and websites.

Many languages

Training in Arabic, English, Turkish, French and other languages.

Every level

Experienced in explaining security to non-technical audiences, from leadership to new staff and students.

Delivery formats

- On-site at your premises
- Remote, live online
- Blended (on-site and remote)
- Annual programme with periodic sessions

07

Financial basis

The financial offer is submitted separately once the scope is agreed, on the following basis:

Item	Basis
Training workshops	Number of trainees and number of tracks
Phishing simulation	Number of recipients and number of campaigns
Assessment and reports	Included in the full programme
Annual programme	Annual fee covering periodic sessions, simulations and reports

Special rates are available for government bodies and educational institutions.

What we need from you

- A named coordinator for communication and follow-up
- A training room with a projector (for on-site training)
- The groups and number of trainees
- Written approval of the phishing simulation and its scope

Next steps

1. A short introductory meeting to understand your needs
2. Agree the scope, tracks and number of trainees
3. We send the financial offer and schedule
4. Sign the agreement and begin the baseline assessment

08

Contact

Address
11 June Rd, Furnaj, Tripoli, Libya

Phone / WhatsApp
+218 91 020 0020

Email
info@almada.biz

Website
almada.biz/security/awareness

Approval

	For the organisation	For Almada
Name		
Title		
Signature		
Date		

This is a general technical offer, completed by a financial offer and schedule tailored to the organisation.