Almada
Software & Security



A free guide from Almada

Security Awareness Guide for Staff

How to spot phishing, resist social engineering and protect your organisation's data — in minutes.

First edition · 2026

almada.biz

01

The ten golden rules

Most breaches don't start with a technical flaw but with a person who believed a message or a call. These ten rules stop most of them. Pin them up by your desk.

01 Never share a password or verification code with anyone, even if they say they are IT support or the bank.

02 Urgency is a warning sign. The harder you are pushed to act now, the more you need to stop.

03 Verify any request for money or data through a second channel you already know, never the number or link in the message.

04 Open important sites by typing the address yourself or from bookmarks, not from a link you received.

05 Don't open an attachment you weren't expecting, especially archives or files ending in .exe, .scr or .js.

06 Turn on two-step verification for email and important accounts.

07 Use a different password for every account, ideally with a password manager.

08 Lock your screen whenever you leave your desk, even for a minute.

09 Never plug an unknown USB drive into a work computer.

10 If in doubt, report it. Reporting early never embarrasses you; it protects everyone.

02

How to spot a phishing message

Phishing is a message designed to make you click a link, open an attachment, or send data or money. It can arrive by email, SMS, WhatsApp or social media.

Eight warning signs

Urgency and threats
“Within 24 hours or your account will be closed.”

Unexpected sender
Someone you've never dealt with, or a new number claiming to be someone you know.

Look-alike domain
yourbank-verify.com instead of yourbank.ly, or one swapped letter.

Asks for sensitive data
Password, code, card number, a photo of your ID.

Short or hidden link
bit.ly and similar hide the real destination.

Strange attachment
invoice.pdf.exe, or a password-protected archive.

Too good to be true
A prize, a refund, a job you never applied for.

Asks for secrecy
“Don't tell anyone, this is sensitive.”

Read the link from the end
The real domain is the part just before the first “/”. Everything in front of it can be written however the scammer likes.

`https://login.yourbank.ly/account` — Genuine

`https://yourbank.ly.secure-login.co/account` — Fake

`https://yourbank-ly.com/verify` — Fake

03

Social engineering: how attackers persuade you

A social engineer doesn't hack computers; they hack trust, using natural feelings to make you act before you think. Know the technique and it loses half its power.

Technique	How it works	Example	Your response
Authority	Poses as a manager or official body.	*“I'm the head of department. Make the transfer now, no questions.”*	Call the manager on their known number before acting.
Urgency	Takes away your time to think.	*“The audit is in an hour, send the file immediately.”*	Real deadlines survive five minutes of checking.
Fear	Threatens a penalty or a loss.	*“Your account is hacked, install this to protect it.”*	Hang up and contact official support yourself.
Curiosity & greed	Offers a reward or a secret.	*“Staff salary list leaked — see attachment.”*	Don't open what you didn't ask for; report it.
Helpfulness	Exploits your wish to help.	*“I'm new and forgot my badge, hold the door?”*	Politely direct them to reception or security.
Familiarity	Gathers details to seem close.	*Names your colleague and project to earn trust.*	Knowing details is not proof of identity.

04

Under pressure: Stop · Verify · Report

The most dangerous moments are the ones where you're told to act immediately. Three fixed steps protect you however convincing the story is:

01

Stop

Don't act in the moment. Take a breath. A genuine request can wait a few minutes.

02

Verify

Contact the requester through a channel you already know: their saved number, official email or office. Never the number or link in the message.

03

Report

Tell IT or information security, even if you did nothing. Your report may save a colleague who received the same message.

Ready-made lines to say with confidence

“I'll call you back on the official number we have on file.”

“Our policy doesn't allow me to share that over the phone.”

“Please send the request in writing to the official email and I'll pass it to my manager.”

“I can't install any software without IT approval.”

A genuine requester won't be angry that you checked. Only a scammer gets angry.

05

What to share, and with whom

Not all data is equal. Before you send a file or answer a question, ask: how is this information classified, and who is allowed to see it?

Classification	Examples	Sharing allowed
Public	Published announcements, public contact numbers, advertised services.	With anyone, through any channel.
Internal	Internal circulars, organisation chart, work manuals.	With colleagues only, through official channels.
Confidential	Staff, citizen and customer data, contracts, financial data.	Only with those who need it for their work, securely and with approval.
Strictly confidential	Passwords, security plans, sovereign documents, payment data.	Only with explicit authorisation and a defined procedure.

Before you send

- Check the recipient's name and address letter by letter; autocomplete makes mistakes.
- Don't send work data to your personal email or through unapproved apps.
- Remove unnecessary data from a file before sharing it.
- Don't post photos from your office that show screens, documents or access badges.

06

Everyday habits that protect you

Passwords

- A long sentence is easier to remember and harder to crack than a short complex word.
- A different one for every account, and a password manager to remember them.
- Change it immediately if you think it was exposed.

Two-step verification

- Turn it on for email, banking and social media.
- An authenticator app is better than SMS.
- Never read a code out to anyone.

Devices

- Install updates; don't postpone them.
- Lock your screen when you leave (Win + L).
- Don't install software from unofficial sources.

Away from the office

- Avoid public Wi-Fi for work, or use your organisation's VPN.
- Watch who can see your screen in public places.
- Never leave your laptop in a car or unattended.

07

Clicked a suspicious link? It's OK — act now

Mistakes happen to anyone. What makes the difference is acting fast. The first minutes matter more than anything.

1. Disconnect the device from the network (cable or Wi-Fi) if you opened an attachment or installed something.
2. Change your password immediately from another, clean device if you typed it into the page.
3. Tell IT or information security right away and describe exactly what happened.
4. Don't delete the message; the security team may need it to protect others.
5. If money is involved, contact the bank immediately to stop the transaction.

Quick check before any click

- [ ] Was I expecting this message?
- [ ] Do I know the sender, and is the domain or number really right?
- [ ] Is it pushing urgency, secrecy or threats?
- [ ] Is it asking for data, money or a software install?
- [ ] Can I verify through another channel before I act?

A

Almada
Software & Security

A free guide from Almada

Want to train your whole team?

This guide is a start. Almada delivers security awareness programmes and practical training for ministries, government bodies, companies and educational institutions: interactive workshops, safe phishing simulations, and a report that measures improvement before and after.

Our trainers are academics, most holding postgraduate degrees in cybersecurity, and train in Arabic, English, Turkish, French and other languages, at every level of education.

Book an introductory session · almada.biz/security/awareness

Website
almada.biz

Email
info@almada.biz

Phone / WhatsApp
+218 91 020 0020

You may print and share this guide freely within your organisation, unmodified.