AI Security Awareness for Staff

A short, high-impact session that protects your company from the new wave of AI-driven threats — and from accidental data leaks.

WHO IT'S FOR	FORMAT	LENGTH
All staff — a whole-company awareness session.	In-house workshop or all-hands session	60–90 minutes

What your team walks away with

Spot AI-powered scams, deepfakes and data leaks — and use AI tools without putting the company at risk.

What you'll learn

- ✓ Recognise how attackers now use AI for phishing, voice cloning and deepfakes
- ✓ Spot a fake before it costs you or the company
- ✓ Tell safe ways of using AI tools at work from unsafe ones
- ✓ Know exactly what should never be shared with an AI tool
- ✓ Act quickly and correctly the moment something looks wrong
- ✓ Leave with a one-page AI safe-use guide every employee can follow

Curriculum

01 How attackers now use AI: phishing, voice and deepfakes

- Why cheap AI has made scams more convincing and easier to run at scale
- AI-written phishing by email, text, voice call and QR code
- Cloned voices and deepfake video used to impersonate people you know
- Fake messages built from public information about you and your company
- Why old warning signs like bad grammar no longer keep you safe

02 Spotting a fake before it costs you

- The tell-tale signs of an AI-powered scam
- Urgency, authority and secrecy as classic manipulation tactics
- Cues that an audio or video call may be a deepfake
- Impersonation of executives, suppliers and the IT help desk
- Pausing on any request to move money or change details

03 Verify before you act

- Checking a request through a known, trusted channel — not the one it came from
- Calling back on a number you already have, never one you were given
- Confirming unusual payment or data requests with a second person
- A simple habit of slowing down before high-stakes actions
- Real-world scenarios to practise the verify-first reflex

04 Safe and unsafe ways to use AI tools at work

- Which everyday ways of using AI tools are safe and which aren't
- Approved company tools versus random tools off the internet
- Why some tools are risky: they may keep or train on what you enter
- Shadow AI — the danger of unapproved tools no one signed off
- A simple decision step: is this task and data OK for AI?

05 What never to share with an AI tool

- The information that must never be pasted into an outside AI tool
- Customer data, personal data, passwords and confidential files
- How a quick copy-paste can leak more than you realise
- Recognising sensitive data even when it isn't labelled
- Safe alternatives when you still want the tool's help

06 What to do when something looks wrong

- Exactly who to tell and how, the moment you're suspicious
- Why reporting fast matters even more than being certain
- A no-blame culture so people own up to mistakes and near-misses
- What to do if you think you've already clicked or shared something
- Turning the whole team into an early-warning system

07 A one-page safe-use guide for everyone

- The safe-use rules distilled onto a single page
- A quick checklist for spotting and verifying a likely fake
- The 'never share this' list every employee keeps
- Who to contact and how to report, at a glance
- A guide that works for every role, no technical background needed

You keep

> A one-page AI safe-use guide for every employee.

Arthiq — live, in-person AI training for high-stakes teams.

Book a session: founders@arthiq.co · https://arthiq.co