Campaign kickoff:

👋 **October is European Cyber Security Awareness Month.**

This year, we're focusing on **AI Scams at Work: Spot the Red Flags**.

As AI becomes part of everyday work, attackers are also using it to create more convincing phishing emails, voice scams, fake content and other fraudulent requests. Many of the obvious warning signs we relied on in the past are becoming harder to spot.

Over the next **4 weeks**, we'll share **one short challenge each week** based on a realistic workplace scenario. Each challenge will help you identify the red flag in a common work situation and earn a **Red Flag Card**.

We'll cover:

🎣 **Week 1:** Phishing
📞 **Week 2:** Voice scams
🤖 **Week 3:** Shadow AI
🎭 **Week 4:** Deepfakes

Each challenge takes only a few minutes to complete and is designed to help you recognise how today's scams can appear in everyday work.

Keep an eye on this channel. Your first challenge will be shared next week.

#1 Weekly launch post: Phishing

🎣 **Week 1: Phishing**

Phishing is a fake message that tries to get you to click, share details, approve a sign-in or open something risky.

⚠ These messages are much easier to make convincing now. Scammers use AI too, so a phishing email can sound polished and fit the moment with very little effort.

⚠ Example: An apartment scam arrives while you are already looking for a place. The timing makes the message feel relevant, and that can be enough to lower your guard.

👉 Your action: Check whether the request fits the way this person, team or process normally works. If it changes the usual route, creates urgency or sends you to a new channel, pause and verify it through a contact or process you already trust before you act.

🎮 This week's challenge is **The Risky Ask**. You will work through a workplace scene and decide where the phishing red flag appears.

👉 Take 3 minutes to inspect this week's scenario and collect your **Red Flag Card**.

[Take the challenge]

🎧 Listen to **Ep. 1: The Risky Ask** to hear why polished messages can still be dangerous and what to check instead.

[Listen now]

Let's see if this one gets past you. Good luck.