Campaign Intro:

👋 **Der Oktober ist der Europäische Monat der Cybersicherheit.**

Dieses Jahr konzentrieren wir uns auf das Thema **KI-Betrug am Arbeitsplatz: Warnsignale erkennen**.

KI ist nicht nur Teil unseres Arbeitsalltags geworden, sondern wird genauso alltäglich auch von Angreifern genutzt, um überzeugendere Phishing-Mails, Voice-Scams, gefälschte Inhalte und andere betrügerische Anfragen zu erstellen. Viele der offensichtlichen Warnzeichen, auf die wir uns in der Vergangenheit verlassen haben, werden immer schwerer zu erkennen.

In den nächsten **4 Wochen** werden wir **jede Woche eine kurze Challenge** teilen, die auf einem realistischen Szenario am Arbeitsplatz basiert. Bei jeder Challenge können Sie das Warnsignal in einer gängigen Arbeitssituation identifizieren und eine **Red-Flag-Karte** verdienen.

Wir decken folgende Themen ab:

🎣 **Woche 1:** Phishing
📞 **Woche 2:** Voice-Scam
🤖 **Woche 3:** Schatten-KI
🎭 **Woche 4:** Deepfakes

Jede Challenge dauert nur wenige Minuten und soll Ihnen helfen zu erkennen, wie die heutigen Betrugsmaschen im Arbeitsalltag auftreten können.

Behalten Sie diesen Kanal im Auge. Ihre erste Challenge wird nächste Woche geteilt.

#1 Week Challenge: Phishing

🎣 **Woche 1: Phishing**

Phishing ist eine gefälschte Nachricht, die versucht, Sie dazu zu bringen, zu klicken, Details zu teilen, eine Anmeldung zu genehmigen oder etwas Riskantes zu öffnen.

⚠ Diese Nachrichten sind heute viel leichter überzeugend zu gestalten. Auch Betrüger setzen KI ein und können mit sehr geringem Aufwand dafür sorgen, dass eine Phishing-Mail ausgefeilt formuliert ist und genau zum richtigen Zeitpunkt eintrifft.

⚠ Beispiel: Eine Betrugsmail mit einem Wohnungsangebot kommt genau dann, wenn Sie gerade auf Wohnungssuche sind. Das Timing lässt die Nachricht relevant erscheinen, und das kann ausreichen, um Ihre Wachsamkeit zu verringern.

👉 Ihre Aktion: Prüfen Sie, ob die Anfrage zur normalen Arbeitsweise dieser Person, dieses Teams oder dieses Prozesses passt. Wenn sie nicht auf dem üblichen Weg ankommt, Dringlichkeit erzeugt oder Sie zu einem neuen Kanal leitet, halten Sie inne und überprüfen Sie sie über einen Kontakt oder Prozess, dem Sie bereits vertrauen, bevor Sie darauf reagieren.

🎮 Die Challenge dieser Woche ist **die riskante Bitte**. Sie werden eine Szene am Arbeitsplatz durcharbeiten und entscheiden, wo das Phishing-Warnsignal auftaucht.

👉 Nehmen Sie sich 3 Minuten Zeit, um das Szenario dieser Woche zu prüfen und Ihre **Red-Flag-Karte** zu sammeln.

[An der Challenge teilnehmen]

🎧 Hören Sie sich **Episode 1: „Die riskante Bitte“** an, um zu erfahren, warum auch perfekt formulierte Nachrichten gefährlich sein können und worauf Sie stattdessen achten sollten.

[Jetzt anhören]

Mal sehen, ob Sie diese Challenge durchschauen. Viel Glück.