Campaign kickoff:

👋 **Le mois d'octobre est le Mois européen de la sensibilisation à la cybersécurité.**

Cette année, nous avons choisi le thème **« Les escroqueries augmentées à l'IA dans le cadre professionnel : cherchez l'erreur. »**.

Nous utilisons de plus en plus l'IA dans notre travail au quotidien. Les cyberattaquants aussi s'en servent pour créer des e-mails de phishing, des arnaques téléphoniques, des contenus mensongers et d'autres demandes frauduleuses de plus en plus crédibles. Les signaux d'alerte évidents que nous avions autrefois l'habitude de repérer sont aujourd'hui de plus en plus difficiles à voir.

Au cours des **4 prochaines semaines**, nous vous proposerons **chaque semaine un bref défi** basé sur un scénario réaliste en milieu professionnel. Chacun de ces défis vous permettra d'apprendre à identifier les signaux d'alerte dans une situation courante de la vie professionnelle et de remporter une **carte « Alerte rouge »**.

Voici les thématiques abordées :

🎣 **Semaine 1 :** Phishing
📞 **Semaine 2 :** Arnaques téléphoniques
🤖 **Semaine 3 :** Shadow IA
🎭 **Semaine 4 :** Deepfakes

Chaque défi ne prend que quelques minutes. Il vous aidera à mieux discerner les situations où des tentatives d'attaques peuvent surgir dans votre environnement de travail quotidien.

Continuez à nous suivre sur cette chaîne. Premier défi : la semaine prochaine.

#1 Week: Phishing

🎣 Semaine 1 : Phishing

Le plus étonnant dans le phishing aujourd'hui, c'est qu'il peut commencer par une demande insignifiante.

Dans la plupart des cas, les attaquants n'exigent pas directement des mots de passe ou des coordonnées bancaires. Ils commencent par une demande à laquelle il est facile de dire « oui », comme ouvrir un document ou approuver une connexion.

Ce simple « oui » qu'on accorde entre deux réunions ou en faisant le ménage dans sa boîte mail juste avant d'aller manger peut être suffisant pour donner accès à un hacker.

Souvent, des e-mails qui semblent rapides à traiter peuvent, en réalité, nécessiter un examen plus approfondi. Ils sont bien écrits. Ils sonnent juste. Rien de suspect, à première vue. Juste un détail à régler avant de poursuivre la journée.

Le défi de cette semaine s'intitule : **La demande risquée**. Jouez la scène dans votre environnement professionnel, prenez la décision et tentez de repérer le signal d'alarme dans cette tentative de phishing.

👉 Prenez 3 minutes pour étudier le scénario de cette semaine et tenter de remporter votre carte « Alerte rouge ».
[Relever le défi]

🎧 Écoutez l'épisode 1 — La demande risquée pour découvrir pourquoi les anciens indices de phishing comme les fautes de frappe ou de grammaire ont perdu de leur pertinence et quels sont les éléments à surveiller aujourd'hui.
[Écouter]

Trouverez-vous l'erreur ? Bonne chance.