Organisme de formation : ENDKOO, 4 Rue de la charité 69002 LYON, France sous le numéro SIRET 83475061400028. Enregistré sous le n° de déclaration d'activité :84691626269

ENDKOO›

Nom de la formation:	Formation DECOUVERTE Social Engineering 1/2 journée
Résumé de la formation:	Cette formation de demi-journée vise à sensibiliser les participants aux différentes techniques de manipulation utilisées dans le Social Engineering. Les participants apprendront à reconnaître et à se protéger contre les attaques de phishing, à comprendre les principes de manipulation mentale et à créer et gérer des mots de passe en toute sécurité.
Matériel :	Un ordinateur pour chaque participant, une présentation PowerPoint, des exemples d'e-mails de phishing, des exemples de manipulation mentale
Pour qui :	Cette formation s'adresse aux employés de tous les niveaux, en particulier ceux qui ont des responsabilités en matière de sécurité informatique ou qui sont exposés à des risques de Social Engineering.
Enjeu :	Le Social Engineering est une menace croissante pour les entreprises, et il est important que les employés soient conscients des risques et sachent comment se protéger contre ces attaques.
Prérequis :	Aucun prérequis n'est nécessaire, cette formation est destinée à tous les niveaux. Etre disposé à apprendre de nouveaux concepts et de nouvelles technologies.
Objectifs :	Comprendre les différentes techniques de manipulation utilisées dans le Social Engineering Reconnaître et se protéger contre les attaques de phishing Comprendre les principes de manipulation mentale Créer et gérer des mots de passe en toute sécurité Mettre en place des mesures de sécurité pour se protéger contre les attaques de Social Engineering
Durée :	1/2 journée (3.5 heures)
Points forts et méthodes :	La formation est conçue pour être pratique et interactive, avec des exercices pratiques pour tester les compétences acquises. Les participants auront également l'occasion de mettre en pratique les compétences acquises dans un environnement de groupe. Le formateur est spécialisé dans le numérique depuis 2003. Méthodologie avec théorie à 50% et pratique à 50% (exercices en lignes)
Modalités :	Formation à distance uniquement via Microsoft Teams
Délais d'accès :	Formation intra entreprise – Délais à négocier avec l'entreprise dont inférieur à 2 mois
Support pédagogique :	Un support pédagogique et une palette d'exercice sera remis à chaque participant

Organisme de formation : ENDKOO, 4 Rue de la charité 69002 LYON, France sous le numéro SIRET 83475061400028. Enregistré sous le n° de déclaration d'activité :84691626269

ENDKOO›

Les modalités d'évaluations des acquis :	En début et en fin de formation, les stagiaires h/f réalisent un test de positionnement (auto évaluation) via GoogleForms de leurs connaissances et compétences en liens avec les objectifs de la formation. L'écart entre les 2 évaluations permet de mesurer leurs acquis.
Accessibilité aux personnes handicapées :	Le support de formation est disponible en format numérique, il est accessible aux personnes handicapées en utilisant des outils d'accessibilité.
Les modalités d'évaluations de la satisfaction et suivi de la prestation	Dans le cadre de notre démarche qualité, toutes nos formations font l'objet d'une évaluation « à chaud » (en fin de formation) et « à froid » (4 mois après la fin de la formation) par stagiaire h/f. Une feuille d'émargement sera signée par demie journée pour chaque stagiaire ainsi que pour le formateur qui justifiera la présence des participants.
Tarifs :	445€HT
Programme de formation:	Introduction au Social Engineering (30 minutes)
	But : Comprendre les différentes techniques de manipulation utilisées dans le Social Engineering
	Exercice : Discuter des exemples récents de Social Engineering et identifier les techniques utilisées
	Phishing (1 heure)
	But : Apprendre à reconnaître et à se protéger contre les attaques par phishing
	Exercice : Effectuer une formation sur la reconnaissance des e-mails de phishing et effectuer un test de sensibilisation pour vérifier la compréhension des concepts
	Manipulation mentale (45 minutes)
	But : Comprendre comment les manipulateurs utilisent les principes de la psychologie pour influencer les gens
	Exercice : Discuter des exemples de manipulation mentale dans la vie quotidienne et identifier les principes de psychologie utilisés
	Sécurité des mots de passe (45 minutes)
	But : Apprendre à créer des mots de passe forts et à les gérer en toute sécurité
	Exercice : Discuter des meilleures pratiques de création et de gestion des mots de passe et effectuer un test pour vérifier la compréhension des concepts
	Sensibilisation à la sécurité (30 minutes)
	But : Comprendre les mesures de sécurité à prendre pour protéger contre les attaques de Social Engineering
	Exercice : Discuter des mesures de sécurité à prendre pour protéger contre les attaques de Social Engineering et vérifier la compréhension des concepts
	Evaluation finale (30 minutes)
	But : Vérifier la compréhension globale des concepts de Social Engineering
	Exercice : Passer un test d'évaluation pour vérifier la compréhension des concepts de Social Engineering