Le cerveau : porte d'entrée du Hacker

Réf. PSY-BIA-01

1. Description de la formation

Dans un monde où la cybersécurité repose encore majoritairement sur des solutions techniques, cette formation propose une approche originale et indispensable : comprendre l'humain comme maillon central de la chaîne de sécurité. En explorant les biais cognitifs et les mécanismes psychologiques exploités par les attaquants, les participants découvrent comment l'ingénierie sociale contourne les protections techniques les plus avancées.

Au fil d'une journée rythmée par des cas concrets, des outils visuels, des jeux de rôle et des échanges collectifs, cette formation permet d'identifier les failles humaines, de renforcer les défenses mentales et d'adopter des réflexes durables face aux manipulations. Une plongée essentielle dans les stratégies des hackers… pour mieux s'en protéger.

2. Détails de la Formation

Objectifs pédagogiques

- Identifier les principales techniques d'ingénierie sociale
- Reconnaître les biais cognitifs courants
- Analyser des cas réels d'attaques
- Mettre en œuvre des stratégies mentales de défense

Prérequis

Aucun prérequis technique n'est exigé. Une sensibilité aux enjeux de cybersécurité est un plus.

Matériel requis

Le stagiaire doit avoir accès à un ordinateur qui possède un clavier, souris, écran, connexion Internet, un micro et une caméra.

Durée

1 jour (7 heures)

Public visé

Toute personne curieuse des mécanismes psychologiques exploités par les attaquants.

Documents fournis à la fin de la formation

Il est remis aux stagiaires :

- Le plan de déroulement de la formation
- Le support de formation et les énoncés des exercices au format PDF

Moyens pédagogiques

La formation s'appuie sur une pédagogie active et variée pour favoriser l'engagement des participants et l'ancrage des apprentissages. Des slides illustrées et des schémas facilitent la compréhension des concepts, tandis que des études de cas immersives permettent de se confronter à des situations réelles. Les jeux de rôle et les tests cognitifs stimulent la réflexion individuelle et collective en mettant en pratique les notions abordées. Un glossaire est fourni pour un repérage rapide des biais cognitifs et des ressources PDF complémentaires sont distribuées à l'issue de la session. Tout au long de la journée, les participants bénéficient d'un accompagnement personnalisé à travers des échanges oraux et des retours ciblés, favorisant une progression adaptée à chacun.

Modalités d'évaluation

Les participants seront évalués par des : quiz, exercices pratiques et QCM de validation.

Accessibilité

Formation en ligne accessible avec des outils d'assistance sur demande.

Conditions inscription

Inscription préalable nécessaire, au moins 2 semaines avant le début de la formation.

Tarif

390 € TTC (TVA non applicable, art. 293 B du CGI)

3. Programme de la Formation

JOUR 1 :

Matin :

- Accueil et tour de table : Identifier les attentes et représentations.
- Pourquoi cette formation ? Comprendre les limites de la cybersécurité technique, et le rôle du facteur humain.
- Le facteur humain : chiffres, jurisprudence, cas réels. Identifier les erreurs humaines et biais en action.
- Études de cas. Déconstruire les attaques emblématiques.
- Glossaire des biais cognitifs : Référentiel commun.

Après-midi :

- Techniques d'ingénierie sociale : phishing, vishing, baiting, etc. et leurs mécaniques.
- Défenses cognitives & stratégies mentales : Détection de biais et réflexes mentaux.
- Arsenal de contre-mesures : Fiches par biais, défenses orales/écrites, jeu de rôle.
- Synthèse finale et clôture : Règles mentales, QCM final, ressources bonus.

Sessions en INTRA (dans votre entreprise) également possibles, veuillez nous contacter.

Session en langue française par défaut, anglais possible sur demande.

4. Contact

Courriel : contact@coditrust.com

Formateur : Matthias DE FORNI

Référant handicap : Anthony DESSIATNIKOFF