

# Comprendre le phishing-ingénierie sociale (Les attaques par ingénierie sociale)

Référence : **SECINGB**

Durée : **1 jour (7 heures)**

Certification : **Aucune**



## CONNAISSANCES PRÉALABLE

- Savoir utiliser les outils informatiques et communicants (téléphone, ordinateur, messagerie, Internet, ...)
- Aucune connaissance spécifique demandée

## PROFIL DES STAGIAIRES

- Toute personne voulant identifier les attaques par ingénierie sociale

## OBJECTIFS

- Définir les pratiques de l'ingénierie sociale
- Identifier les menaces potentielles
- Réagir et alerter son organisation

## CERTIFICATION PRÉPARÉE

- Aucune

## MÉTHODES PÉDAGOGIQUES

- 6 à 12 personnes maximum par cours, 1 poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions

## FORMATEUR

- Consultant-Formateur expert Sécurité User

## MÉTHODES D'ÉVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

## ACCESSIBILITÉ DE LA FORMATION

- EduGroupe met en place un ensemble de dispositifs pour accueillir, accompagner et adapter ses formations aux personnes en situation de handicap (PSH).
- Notre référent(e) handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à [referent.handicap@edugroupe.com](mailto:referent.handicap@edugroupe.com) pour tout besoin d'aménagement, afin de vous offrir la meilleure expérience possible.

## CONTENU DU COURS

### 1. Introduction

- Définir l'ingénierie sociale
- Lister les risques liés à l'ingénierie sociale

### 2. Les vulnérabilités humaines

- Identifier les sentiments, comportements et instincts de l'humain
- Lister les vulnérabilités courantes
- Énumérer les modes de perception
- Définir la PNL, programmation neuro-linguistique

### **3. Les attaques par ingénierie sociale**

- Inciter à faire une action
- Manipuler une personne
- Créer un faux document
- Usurper une identité

### **4. Le phishing (hameçonnage)**

- Identifier le phishing par e-mail
- Identifier le phishing via le web
- Identifier le phishing par téléphone
- Signaler un phishing

### **5. Sensibilisation du personnel**

- Respecter la politique d'accès aux locaux
- Identifier les bonnes pratiques
- Réaliser des audits de sécurité

### **6. Études de cas**

- Mise en pratique sur des cas d'ingénierie sociale