



# Se Protéger contre l'Escroquerie

Lien : <https://innov-systems.com/formation/se-protoger-contre-lescroquerie>

 DURÉE  
**3 jours (21h)**

 RÉFÉRENCE  
**SEC11**

 CATÉGORIE  
**Fondamentaux  
Sécurité Informatique**

## OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- ✓ Avoir les compétences nécessaires pour se défendre contre les attaques de l'ingénierie sociale
- ✓ Apprendre les méthodes techniques et psychologiques de manipulation, de persuasion utilisée par les hackers

## POUR QUI ?

- ✓ Personnel de sécurité
- ✓ Chefs de projet
- ✓ Toute personne désirant apprendre à se défendre contre les attaques de l'ingénierie sociale



## Programme détaillé

### 1 / Ingénierie sociale ou piratage psychologique

- Qu'est-ce que l'ingénierie sociale ?
- Règles et fonctionnement
- Comprendre ce type d'attaque dans une logique d'entreprise
- Comprendre la typologie de l'ingénierie sociale et de ses menaces en ligne

### 2 / Penser comme un hacker

- Envisager des angles d'attaques
- Passer en revue les méthodes de manipulation
- Examiner les questions légales et sociales

### 3 / Ingénierie sociale et réseaux sociaux

- Concept et limites
- Phishing et réseaux sociaux
- Recrutement 2.0, comportement des employés et contenus affichés en ligne
- Application de mesures de protection et leur suivi

### 4 / Elaborer des défenses pour contrer les menaces d'ingénierie sociale

- Sensibiliser et former les collaborateurs
- Vulnérabilité humaine et sécurité de l'entreprise
- Gérer les incidents. Rôle du support technique
- Documentation et gestion des vecteurs d'attaque

### 5 / Collecter les informations et l'intelligence

- Identification des sources d'information

- Collecte des informations cible
- Réduction de la fuite d'informations

## 6 / Identifier les modèles de communication

- Profiler une architecture de l'information
- Gestion des problèmes de communication

## 7 / Les méthodes pour soutirer les informations

- Solliciter les informations
- Techniques d'interrogation
- Les techniques d'écoute passive vs. active
- Établir l'authenticité
- Mettre en application le besoin de connaître les règles

## 8 / Obtenir l'accès physique

- Contourner les contrôles technologiques
- Identifier les simples faiblesses
- Évaluer les contrôles physiques
- Protéger les données des voleurs

## 9 / Se servir de la psychologie et de la persuasion

- Exploitation de la Programmation neuro-linguistique
- Identification de l'étourderie
- Vaincre la raison par le fuzzing
- Teste de la Preuve sociale
- Profiter de l'autorité implicite
- Exiger de l'action avec les « quid pro quo »
- Évaluer les faiblesses
- Reconnaître les supercheries

- Normaliser les réponses avec des scripts

## 10 / Mettre en œuvre des contre-mesures de management

- Traitement des problèmes avec l'audit
- Création d'un périmètre de travail
- Minimiser la gêne
- Identification des attaques et des tentatives
- Gagner en perspective grâce aux audits

## Approche pédagogique

- ✓ Support Ecrit et Projection
- ✓ Exposés Interactifs, Podcasts et Vidéos
- ✓ Brainstorming et Jeux de Rôle
- ✓ Cas Pratiques et Labs inclus pour leur impact opérationnel
- ✓ Test de Validation des Acquis des Connaissances

## Prochaines dates programmées

 22 au 24 Juil. 2026

 Présentiel - Casablanca

 16 au 18 Sep. 2026

 Distanciel

 11 au 13 Nov. 2026

 Distanciel

 Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

## Réservation & Renseignements

 Téléphone : +212 522 247 210

 Email : [contact@innov-systems.com](mailto:contact@innov-systems.com)

 Web : <https://www.innov-systems.com>