



# INGENIERIE SOCIALE : SE PROTEGER CONTRE L'ESCROQUERIE

— <b>Public</b>	Les gestionnaires de ressources humaines, le personnel de sécurité de site, le personnel de sécurité des réseaux, les gestionnaires de projet ou les autres personnes désireuses d'apprendre des techniques de défense contre les escroqueries
— <b>Durée</b>	3 jours - 21 heures
— <b>Pré-requis</b>	Aucun
— <b>Objectifs</b>	Dans ce cours, vous obtenez les compétences pour vous défendre contre les attaques de l'ingénierie sociale qui menacent la sécurité des entreprises. Vous apprenez les méthodes techniques et psychologiques de manipulation, de persuasion utilisées par les hackers. De plus, cette formation intègre les activités conçues pour comprendre les motivations et les méthodes utilisées par les hackers pour mieux protéger votre entreprise et prévenir la violation de données à caractère personnel.
— <b>Méthodes pédagogiques</b>	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
— <b>Moyens techniques</b>	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
— <b>Modalité d'évaluation des acquis</b>	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
— <b>Délai d'accès</b>	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
— <b>Accessibilité handicapés</b>	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

## 1. ÉVALUER LES RISQUES POUR L'ENTREPRISE

- Évaluer les menaces de l'ingénierie sociale
- Analyser des cas d'étude classiques

## 2. PENSER COMME UN HACKER

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

## 3. IDENTIFIER LES SOURCES D'INFORMATION

- Collecter des informations de façon active et passive
- Exploiter le Google hacking
- Exploiter les médias sociaux

#### 4. COLLECTER DES INFORMATIONS CIBLE

- Copier des informations de sites avec Maltego
- Dumpster diving pour les secret et l'intelligence
- Profiler les utilisateurs pour obtenir leur mot de passe

#### 5. MINIMISER LA FUITE D'INFORMATIONS

- Sécuriser la fuite d'informations
- Mettre en œuvre des stratégies d'élimination sécurisées

#### 6. PROFILER UNE ARCHITECTURE DE L'INFORMATION

- Mettre en oeuvre le modèle de communication Berlo
- Source
- Message
- Chaîne
- Destinateur
- Déterminer les faiblesses de communication

#### 7. GÉRER LES PROBLÈMES DE COMMUNICATION

- Vérifier la source
- Sécuriser la chaîne d'informations

#### 8. SOUTIRER LES INFORMATIONS

- Solliciter les informations
- Techniques d'interrogation
- Comparer les techniques d'écoute passive vs. active

#### 9. ATTÉNUER LES TECHNIQUES POUR SOUTIRER LES INFORMATIONS

- Établir l'authenticité
- Mettre en application le besoin de connaître les règles

#### 10. CONTOURNER LA SÉCURITÉ

- Contourner les contrôles technologiques
- Identifier les simples faiblesses

#### 11. SÉCURISER L'ENVIRONNEMENT

- Évaluer les contrôles physiques
- Protéger les données des voleurs

#### 12. IMITER N'IMPORTE QUI

- Mettre en œuvre des techniques d'usurpation d'adresse
- Tromper avec la célérité au changement

#### 13. SE PROTÉGER CONTRE L'IMPOSTURE ET LA CONTREFAÇON

- Scripter les réponses pour vaincre la manipulation
- Rester vigilant et reconnaître la communication illicite

## 14. EXAMINER LES FAIBLESSES HUMAINES

- Exploiter la Programmation neuro-linguistique
- Identifier l'étourderie
- Vaincre la raison par le fuzzing

## 15. IMPOSER UN COMPORTEMENT

- Tester la Preuve sociale
- Profiter de l'autorité implicite
- Exiger de l'action avec les « quid pro quo »

## 16. RENFORCER LA RÉSISTANCE POUR ALLER VERS LA PERSUASION

- Évaluer les faiblesses
- Reconnaître les supercheres
- Normaliser les réponses avec des scripts

## 17. ÉVALUER LES VULNÉRABILITÉS DE L'INGÉNIERIE SOCIALE

- Traiter les problèmes avec l'audit
- Créer un périmètre de travail
- Minimiser la gêne

## 18. CRÉER UNE STRATÉGIE EXHAUSTIVE

- Identifier les attaques et les tentatives
- Gagner en perspective grâce aux audits
- Mener des formations efficaces sur la prise de conscience des questions de sécurité

## NOUS CONTACTER

### Siège social

16, ALLÉE FRANÇOIS VILLON  
38130 ÉCHIROLLES

### Téléphone

04 76 23 20 50 - 06 81 73 19 35

### Centre de formation

87, RUE GÉNÉRAL MANGIN  
38000 GRENOBLE

### E-mail

contact@audit-conseil-formation.com

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !



ACF Audit Conseil Formation



@ACF\_Formation



ACFauditconseilformation