L'AKADÉMIE DU DIGITAL · PROGRAMME DE FORMATION Certification Qualiopi en cours de préparation

Ingénierie Sociale & Phishing

FOR-CYBER-M4-A · Cybersécurité & Conformité

Comprendre et déjouer les manipulations humaines de la cyberfraude

DURÉE
7 h

TARIF
450 € HT

PUBLIC
Entreprises & particuliers

DÉLAI D'ACCÈS
Accès sous 2 jours ouvrés après validation du besoin et des prérequis.

Tarifs indiqués « à partir de », hors devis spécifique et promotions. Prix HT, à partir de 2 participants. TVA 20 %.

Objectifs pédagogiques

- Comprendre les mécanismes psychologiques de l'ingénierie sociale (leviers d'influence et de manipulation)
- Identifier les principales techniques d'attaque : phishing, spear phishing, vishing, smishing, usurpation, prétexting
- Repérer les signaux d'alerte d'un message ou d'une sollicitation frauduleuse
- Réagir correctement face à une tentative et savoir signaler un incident
- Sensibiliser et entraîner son entourage ou son équipe (campagnes de simulation)
- Adopter des réflexes durables de vigilance numérique

Public concerné

- Tout collaborateur, quel que soit son niveau technique
- Fonctions exposées : accueil, administratif, comptabilité/finance, RH, commercial, direction
- Référents sécurité et managers souhaitant sensibiliser leurs équipes

Prérequis

- Savoir utiliser un ordinateur ou un smartphone et une messagerie électronique.
- Utiliser régulièrement des outils numériques du quotidien.
- Avoir une sensibilisation de base à la cybersécurité (module Initiation conseillé).
- Disposer d'une motivation à renforcer sa vigilance et celle de son équipe.

Programme

THÉORIE Module Théorique — Comprendre l'ingénierie sociale

Ce module explique ce qu'est l'ingénierie sociale et pourquoi l'humain est le maillon ciblé, en décryptant les leviers psychologiques exploités (autorité, urgence, peur, curiosité, appât du gain, réciprocité, preuve sociale). Il dresse un panorama des techniques (phishing, spear phishing, vishing, smishing, usurpation d'identité, prétexting, arnaque au président, fraude au faux fournisseur), détaille l'anatomie d'une attaque de phishing, les signaux d'alerte et les réflexes à adopter en cas de doute ou d'incident (signalement interne, Cybermalveillance.gouv.fr).

Objectif : comprendre les mécanismes de l'ingénierie sociale et savoir repérer les tentatives de manipulation pour mieux s'en protéger.

- Décryptage des leviers psychologiques de la manipulation.
- Panorama complet et concret des techniques d'attaque.
- Signaux d'alerte et réflexes de signalement, dans une finalité défensive.

Évaluation : QCM sur les techniques et les leviers psychologiques, exercice d'identification de signaux d'alerte.

Accueil & présentation	15 min	Présenter le programme, les objectifs et le cadre éthique/défensif. Présentation orale, support visuel (slides), tour de table.	
Qu'est-ce que l'ingénierie sociale ?	35 min	L'humain comme maillon ciblé ; pourquoi les attaques fonctionnent. Exposé interactif, exemples, échanges.	Questions orales de compréhension.
Leviers psychologiques	45 min	Autorité, urgence, peur, curiosité, appât du gain, réciprocité, preuve sociale. Exposé, décryptage de cas, discussion.	QCM sur les leviers.
Panorama des techniques	1h00	Phishing, spear phishing, vishing, smishing, usurpation, prétexting, arnaque au président. Exposé illustré, exemples réels, anatomie d'une attaque.	Exercice d'identification de signaux d'alerte.
Réagir & signaler	40 min	Signaux d'alerte (expéditeur, liens, pièces jointes) ; réflexes et signalement. Exposé, check-list, ressources (Cybermalveillance).	QCM intermédiaire.
Synthèse	10 min	Résumer les points clés et préparer l'atelier. Récapitulatif, feedback des participants.	QCM rapide de fin de module.

ATELIER **Atelier Pratique — Détecter, réagir et sensibiliser**

Les participants analysent une collection de faux messages (emails, SMS, scénarios d'appel) et repèrent collectivement les indices, se mettent en situation face à un scénario d'attaque (jeu de rôle, prise de décision), construisent une fiche réflexe « repérer et réagir » et conçoivent les grandes lignes d'une mini-campagne de sensibilisation (messages clés, simulation de phishing éthique et encadrée).

Objectif : savoir détecter une tentative, réagir correctement et sensibiliser son entourage ou son équipe.

- Analyse de cas réels variés (email, SMS, appel).
- Mise en situation par jeu de rôle et prise de décision.
- Production d'une fiche réflexe directement utilisable.
- Conception d'une mini-campagne de sensibilisation éthique.

Évaluation : production des livrables (analyse de cas, fiche réflexe, plan de sensibilisation), restitution orale courte et revue collective.

Lancement de l'atelier	15 min	Présenter l'objectif et le cadre éthique des simulations. Présentation, rappel du cadre (sans donnée réelle), groupes.	
Analyse de faux messages	55 min	Analyser emails, SMS et scénarios d'appel ; repérer les indices. Étude de cas guidée, repérage collectif, grille d'analyse.	Livrable : analyse de cas.
Mise en situation	50 min	Réagir face à un scénario d'attaque (jeu de rôle, décision). Jeu de rôle, débriefing collectif, bonnes réactions.	Observation ; participation au jeu de rôle.
Fiche réflexe	40 min	Construire une fiche réflexe « repérer et réagir ». TP, gabarit de fiche réflexe, accompagnement.	Livrable : fiche réflexe.
Campagne de sensibilisation	30 min	Concevoir une mini-campagne (messages clés, simulation éthique) ; présenter. Modèle de campagne, présentations courtes, feedback.	Évaluation sommative : plan de sensibilisation + QCM final.
Enquête de satisfaction	10 min	Recueillir la satisfaction à chaud. Questionnaire de satisfaction.	Enquête de satisfaction.

Modalités et moyens pédagogiques

Formation en présentiel dans nos locaux ou dans vos locaux, en groupe restreint. Alternance d’apports théoriques, d’ateliers pratiques et de mises en situation.

Matériel requis :

8 Go de Ram

Modalités d’évaluation

Évaluation des acquis en cours et en fin de formation, attestation de fin de formation remise à chaque stagiaire.

Accessibilité

Formation accessible aux personnes en situation de handicap. Contactez-nous avant l’inscription pour étudier les aménagements nécessaires.

Financement

Devis ou convention de formation sur demande. La certification Qualiopi est en cours de préparation : l’éligibilité aux financements OPCO sera ouverte après son obtention.

Audit de certification prévu au T1 2027. Aucune éligibilité OPCO avant l’obtention.