Programme
2026

FORMATION “RECONNAÎTRE ET DÉJOUER LES ATTAQUES”

Cyber trankil

www.cyber-trankil.fr

Votre formateur

Je m'appelle Rémi, je travaille dans l'informatique depuis plus de 10 ans. Développeur web de formation, j'ai évolué vers le support technique et l'accompagnement utilisateurs. Un terrain qui m'a amené à intervenir au quotidien dans des entreprises de toutes tailles.

Au contact des équipes, j'ai réalisé une chose : la cybersécurité est partout dans les discours, mais presque nulle part dans les pratiques. Pas par négligence, mais parce que personne ne l'explique de manière concrète à ceux qui en ont vraiment **besoin**.

Ma conviction : la cybersécurité ne doit pas être réservée aux experts en informatique. Elle concerne tout le monde, et peut s'expliquer sans jargon pour être comprise de tous.

Concrètement, faire appel à mes formations, c'est permettre à vos collaborateurs et vous-même de reconnaître les menaces du quotidien, d'adopter les bons réflexes, et de devenir le premier rempart de votre entreprise

Objectifs de la formation

À l'issue de cette formation, les participants seront capables d'identifier les mécanismes psychologiques exploités par les attaquants, de reconnaître un email, un SMS ou un site frauduleux grâce à des indices concrets, et de réagir efficacement face à une tentative de manipulation. Ils connaîtront les scénarios d'attaque les plus courants en entreprise et sauront appliquer les trois réflexes universels : ralentir, vérifier par un autre canal, signaler.

Modalités

Public concerné : tous publics

- TPE / PME
- Indépendants
- Associations
- Collectivités

Contenu adapté à tout secteur d'activité

Pré-requis :
Aucun prérequis n’est nécessaire pour suivre cette formation.

En présentiel dans vos locaux ou en distanciel par visioconférence avec partage d'écran

Durée : 2h30

Contenu de la formation

1. Ingénierie sociale : mécanismes, leviers et techniques

- *Comprendre pourquoi les attaques sociales sont si efficaces*
- *Identifier les mécanismes psychologiques exploités par les attaquants*
- *Reconnaître les techniques d'ingénierie sociale les plus courantes*

2. Les scénarios d'attaque les plus courants en entreprise

- *Reconnaître les scénarios réels auxquels les TPE/PME sont confrontées*
- *Comment réagir dans chaque situation*

3. Reconnaître un email frauduleux

- *Identifier les indices d'un email malveillant*
- *Savoir analyser un email suspect sans risquer de se faire piéger*

4. Reconnaître un SMS et un site internet frauduleux

- *Identifier les indices d'un SMS malveillant (smishing)*
- *Savoir analyser une URL et un site web avant d'y entrer ses données*