Programme
2026

FORMATION “PROTÉGER SES ACCÈS”

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 de créer et gérer des mots de passe robustes à l'aide d'un gestionnaire, d'activer la double authentification sur leurs comptes sensibles, d'appliquer les bonnes pratiques de mise à jour sur leurs postes et appareils mobiles, et de sécuriser leur environnement de travail au quotidien. Ils sauront également identifier les risques liés aux comptes partagés et appliquer le principe du moindre privilège dans la gestion des accès.

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. Comprendre les risques liés aux mots de passe

- *Comprendre comment les mots de passe sont volés en pratique*
- *Mesurer concrètement les conséquences d'un mot de passe compromis*

2. Créer des mots de passe robustes

- *Savoir distinguer un mot de passe faible d'un mot de passe fort*
- *Maîtriser au moins 2 méthodes pour créer un mot de passe mémorisable et robuste*

3. Gérer ses mots de passe au quotidien

- *Comprendre pourquoi la mémoire humaine ne suffit plus*
- *Savoir choisir et utiliser un gestionnaire de mots de passe*

4. La double authentification (2FA) - Pourquoi & comment ?

- *Comprendre le principe de la 2FA et pourquoi elle est indispensable*
- *Connaître les différents types de 2FA et leurs niveaux de sécurité*
- *Activer la 2FA sur au moins un compte critique*

5. Pourquoi les mises à jour sont importantes ?

- *Comprendre le lien entre une mise à jour non faite et une vulnérabilité exploitable*
- *Savoir quoi mettre à jour, quand, et comment*

6. Sécuriser son environnement de travail au quotidien

- *Identifier les comportements à risque du quotidien*
- *Adopter des réflexes simples qui réduisent drastiquement la surface d'attaque*

7. Comptes utilisateurs, droits et accès partagés

- *Comprendre pourquoi la gestion des accès est un enjeu de sécurité critique*
- *Identifier les mauvaises pratiques courantes autour des comptes partagés*
- *Adopter le principe du moindre privilège au quotidien*