

APPRENDRE EN S'AMUSANT AVEC YESMINE CONSULTING

Objectifs

- Accroître la sensibilisation des utilisateurs aux risques liés à la sécurité informatique.
- Transmettre les connaissances nécessaires pour se protéger contre les menaces.
- Promouvoir l'adoption de bonnes pratiques en matière de sécurité informatique.
- Réduire le nombre d'incidents de sécurité.

Public concerné et prérequis

Ce programme s'adresse à tout utilisateur de poste informatique ou téléphone.

Aucun prérequis.

Format de la formation

La formation, d'une durée de 7h30, est divisible en 3 séances de 2h30 chacune (1 thème par séance).

Chaque séance se déroule en 4 étapes :

- **Escape Game ou jeu de société (45 minutes)** : Mise en situation.
- **Formation (60 minutes)** : Formation sous forme de présentation projetée. Session interactive pour apprendre les bases de la sécurité informatique et échanger sur les bonnes pratiques.
- **Quiz (15 minutes)** : Test de connaissances sous forme de quiz.
- **Bilan (15 à 30 minutes)**

Les séances sont indépendantes les unes des autres. Il est donc possible de choisir 1, 2 ou 3 thèmes.

Thèmes

- **La sécurité au quotidien**
 - Les types de menaces.
 - Les comportements à éviter.
 - Les bons réflexes à adopter.
- **Repérer et éviter le phishing**
 - Vocabulaire : Phishing, smishing, vishing, quishing, ...
 - Apprendre à reconnaître les courriels, messages, appels et courriers frauduleux.
 - Des idées d'outils pour vous aider au quotidien.
- **La gestion des mots de passe**
 - L'importance des mots de passe et les dangers qu'ils représentent.
 - Qu'est-ce qu'un mot de passe complexe ? Comment le créer et le retenir ?
 - Bien gérer ses mots de passe.

Programme

<p>Les motivations et conséquences du piratage</p> <ul style="list-style-type: none"> • Sabotage • Appropriation de données • Usurpation d'identité • Vol de données bancaires • Atteinte à la réputation • Revente des données 	<p>Comment procèdent les pirates</p> <ul style="list-style-type: none"> • Accès aux locaux • Connexion aux réseaux • Les entrées physiques • Le phishing • Les malwares • L'usurpation • Les réseaux sociaux • Le faux support technique • L'ingénierie sociale • Les plateformes de transfert • Les courriers • Les QR code
<p>Les mots de passe</p> <ul style="list-style-type: none"> • Les mots de passe trop simples • Les mots de passe accessibles • La confidentialité du mot de passe • Les mots de passe complexes • La gestion des mots de passe 	<p>Usage professionnel et usage privé</p> <ul style="list-style-type: none"> • Pourquoi séparer les deux ? <p>Réseaux sociaux et cyberharcèlement</p> <ul style="list-style-type: none"> • Définition • Causes et conséquences • Qui contacter ?
<p>Les 10 règles d'or de la sécurité informatique</p> <ul style="list-style-type: none"> • A connaître et à appliquer 	

Modalité d'évaluation

Quiz.

Lieu

Dans vos locaux ou votre lieu d'évènements.

Modalité d'évaluation

A partir de 50 euros HT par thème et par personne.