bakertilly

**Durée : 1 jour (9h - 15h30)**

# ADOPTER LES BONS RÉFLEXES CYBERSÉCURITÉ EN ENTREPRISE : LES BASES ESSENTIELLES

(Initiation et perfectionnement 1)

*Aspects pédagogiques*

*- Questionnaire numérique de prise en compte des attentes spécifiques envoyé dès la validation de l'inscription ;*
*- Quizz/Cas pratiques envoyés quelques jours avant la formation pour permettre aux participants de s'entrainer ;*
*- Evaluation (numérique) par chaque participant, dès la fin de la session, de la qualité de la formation (formateur, écoute, réponses aux questions, conditions matérielles, etc.) ;*
*- Attestation de formation ;*
*- Evaluation « à froid » 1 à 2 mois après la formation ;*
*- Formation animée par des professionnels expérimentés du réseau Bakertilly.*

---

## PLAN DÉTAILLÉ

### 1.Introduction & attentes

- Présentation des objectifs et du déroulé ;
- Recueil des attentes (questionnaire préalable) ;
- Discussion interactive sur les pratiques actuelles.

### 2.Introduction à la cybersécurité

- Définition et périmètre ;
- Enjeux pour l'entreprise ;
- Rôle et responsabilité du collaborateur ;
- QCM / Quiz interactif.

### 3.Menaces courantes et ingénierie sociale

- Phishing, smishing, vishing ;
- Ingénierie sociale : urgence, autorité, confiance ;
- Identification des signaux d'alerte ;
- Études de cas pratiques (email RH, message manager, avis de livraison) ;
- QCM / Quiz.

### 4.Gestion des accès et mots de passe

- Enjeux et risques liés aux identifiants ;
- Bonnes pratiques : passphrases, MFA, unique password ;
- Scénarios pratiques : compromission de compte, création de mot de passe robuste ;
- QCM / Quiz.

### 5.Utilisation sécurisée des outils numériques

- Navigation web et téléchargement sécurisé ;
- Messagerie, PDF, Excel, outils collaboratifs ;
- Études de cas : documents ou liens suspects ;
- QCM / Quiz.

### 6.Sécurité des équipements et mobilité (25 min)

- Ordinateurs, smartphones, clés USB ;
- Réseaux Wi-Fi publics et télétravail ;
- Scénarios pratiques : perte/vol de matériel, clé USB inconnue ;
- QCM / Quiz.

### 7.Gestion des incidents de sécurité (25 min)

- Typologie des incidents ;
- Procédure de signalement ;
- Études de cas pratiques : clic accidentel, téléchargement malveillant ;
- QCM / Quiz.

### 8.Évaluation finale et synthèse (20 min)

- Quiz final basé sur des situations professionnelles ;
- Synthèse des bonnes pratiques et règles essentielles à retenir intégrées dans la discussion et le support remis aux participants ;
- Questions / réponses et conclusion.