**Cybersécurité en Entreprise**

**Protégez Votre Activité, Sensibilisez Vos Équipes**

**Durée : 2J**

**Population cible : Collaborateurs, managers et professionnels débutants en cybersécurité souhaitant acquérir les connaissances essentielles pour sécuriser leur environnement de travail et leurs données personnelles.**

**Objectifs :**

* **Se familiariser avec les concepts fondamentaux de la cybersécurité et les principales menaces actuelles**
* **Approfondir ses connaissances théoriques et pratiques en protection des données et gestion des risques numériques**
* **Connaître les bonnes pratiques de sécurité applicables au quotidien (mots de passe, emails, navigation web)**
* **Développer des réflexes de vigilance et savoir réagir face à un incident de sécurité**

**Méthodologie**

**Démarche interactive et participante, avec enchaînement de séquences pédagogiques ayant successivement pour but d'amener le participant à explorer, comprendre, acquérir puis maîtriser les compétences visées :**

* **Brefs exposés et présentations**
* **Réflexions, échanges sur les apprentissages, partage d'expérience**
* **Exercices et cas pratiques (individuels et en groupe)**
* **Questions-réponses**
* **Débriefings**

**Formateur :**

**M. Harchaoui Oussama, expert en cybersécurité et formateur, fort de 19 ans d’expérience dans l’IT et la Data au sein d’Orange France. Il a amorcé en 2021 une spécialisation en cybersécurité et met depuis son expertise au service de la DTSI Orange France et de ses filiales à l’international, en les accompagnant dans la sécurisation de leurs systèmes d’information, la montée en compétence de leurs équipes et la sensibilisation à la sécurité numérique.**

**Domaines d’expertise :**

* **Sécurité des systèmes d’information et gestion des risques**
* **Audit de sécurité applicative (SAST/DAST) & approche DevSecOps**
* **Pilotage de projets et management technique**
* **Certifications : *SANS SEC488 (Cloud Security)*, *RSSI-HS2 (Gouvernance)***

**Approche pédagogique :  
Grâce à son double profil IT/Data et cybersécurité, Le formateur relie la théorie à la pratique à travers des cas concrets et des scénarios issus du terrain. Il s’attache à rendre la sécurité accessible, pragmatique et immédiatement opérationnelle.**

**Objectif :  
Contribuer à former une nouvelle génération de professionnels capables de relever avec efficacité les défis actuels de la cybersécurité.**

**Programme :**

***MODULE 1 :* Fondamentaux de la Cybersécurité**

**Objectif :** Acquérir les bases nécessaires pour comprendre les enjeux de la sécurité numérique.  
**Contenu :**

* Définitions clés : cybersécurité, cybermenace, cyberattaque
* Enjeux stratégiques pour les entreprises (toutes tailles et secteurs)
* Acteurs de la cybersécurité et typologie des menaces

#### **MODULE 2 : Le Phishing et les attaques de manipulation**

**Objectif :** Identifier les tentatives de phishing et adopter les bons réflexes.  
**Contenu :**

* Reconnaître les différents types de phishing : e-mails, SMS, appels
* Exemples concrets et analyse de cas réels
* Bonnes pratiques pour se protéger et signaler une tentative

***MODULE 3 :* Les Malwares et leurs impacts**

**Objectif :** Comprendre comment les logiciels malveillants compromettent les systèmes.  
**Contenu :**

* Typologie : virus, ransomwares, spywares, chevaux de Troie
* Modes de propagation et signaux d’alerte
* Conséquences pour l’entreprise et exemples d’incidents

***MODULE 4 :* Risques et Facteur Humain**

**Objectif :** Comprendre les conséquences des attaques et l’importance du comportement humain.  
**Contenu :**

* Impacts financiers, opérationnels et réputationnels des cyberattaques
* Le facteur humain : ingénierie sociale, manipulation et tromperie
* Études de cas : attaques via erreurs humaines

***Module 5 :* Bonnes Pratiques Quotidiennes**

**Objectif :** Adopter des habitudes numériques sûres dans un cadre professionnel.  
**Contenu :**

* Navigation sécurisée et gestion des téléchargements
* Sécurité sur les réseaux sociaux et communication interne
* Sensibilisation à la confidentialité des informations

#### **Module 6** : **Les Bases de la Protection**

**Objectif :** Mettre en place les premiers niveaux de défense personnelle et professionnelle.  
**Contenu :**

* **Gestion des mots de passe :** bonnes pratiques, MFA, gestionnaires
* **Sécurité des e-mails :** reconnaissance des pièces jointes et liens malveillants
* **Sécurité des appareils :** mises à jour, antivirus, verrouillage, sauvegardes

#### **Module 7 :** Protection des Données Sensibles et Travail à Distance

**Objectif :** Préserver la confidentialité et l’intégrité des données, y compris hors site.  
**Contenu :**

* Classification et chiffrement des données
* Contrôles d’accès et gestion des partages
* Bonnes pratiques pour le télétravail et l’utilisation de VPN sécurisés