# E-learning
# Sensibilisation à la cybersécurité industrielle


**Domaine 01**


Domaine 02


Domaine 03


Domaine 04


Domaine 05

**NEW !**
Taux de Satisfaction

**Introduction**

**Généralités**
Les enjeux de la cybersécurité
Les entreprises face aux cyberattaques
Les problématiques et enjeux en industrie

**Les menaces**
Les menaces les plus en courantes en entreprise
Les typologies de hackers
Qu'est-ce qu'un malware ?

**Le partage d'informations sur les réseaux sociaux**
Les failles et conséquences
L'ingénierie sociale
Comportement à adopter

**L'hameçonnage**
Les failles et conséquences
L'hameçonnage et les « ishing »
Le spear-fishing et l'arnaque au président
Comportement à adopter

**Poste de travail et mots de passe**
Les bonnes procédures d'identification
Sécurité et confidentialité

**Connecter du matériel non sécurisé**
Les failles et conséquences
Les systèmes de gestion du réseau
Comportement à adopter

**Le ransomware**
Définition et évolution
Le rançongiciel en industrie
Comportement à adopter

**Charte de sécurité et bonnes pratiques**
Prévenir une cyberattaque
PCA et PRA
Les bons réflexes face à une cyberattaque

**Conclusion**

**Pour aller plus loin (OPTIONNEL)**
Le parcours de protection en industrie
Les protections intrusives et périmétrique
Les protections combinées et dynamique

## Contexte

Dans un contexte où les cybermenaces sont de plus en plus fréquentes, et ciblent de plus en plus spécifiquement le domaine industriel, former les collaborateurs de votre entreprise aux bonnes pratiques et aux approches de protection est aujourd'hui un enjeu incontournable.
En sensibilisant vos employés aux risques Cyber, à ses conséquences ainsi qu'aux moyens de protection, vous les dotez des connaissances de base nécessaires afin d'intégrer la Cyber Sécurité au sein de leurs activités quotidiennes.
Ce faisant, vous protégez à la fois vos employés eux-mêmes, les actifs de votre entreprise (protection de la donnée, continuité de service, etc.) et vos clients (prévention de rupture de la Supply Chain ou de la propagation d'une attaque).

## Objectifs

**Le stagiaire une fois formé sera en mesure de :**
Mesurer les conséquences d'une Cyberattaque en milieu industriel
Mettre en place les bonnes pratiques afin de se protéger et de protéger l'entreprise
Appréhender les fondamentaux de la Cyber Sécurité en milieu industriel

## Public

Toute personne de l'entreprises

## Prérequis

Aucun

## Matériel

Chaque participant doit suivre la formation depuis un ordinateur connecté à internet
L'accès à la plateforme de connexion, LMS, vous sera notifié par mail au démarrage de votre formation. Un support technique est proposé via le tutoriel dans la première séquence du E-learning.

**Tarifs par personne :**
**Membre Associé : 175 € HT**
**Membre Exécutif : 225 € HT**
**Non-membre : 250 € HT**

**Organisation et durée**
**2 H 30 environ**
**E-learning**

**Méthodes Pédagogiques**

La formation est interactive et ludique.
10 capsules e-learning de 10 à 20 minutes chacune, à suivre à son rythme.
Séquences de quiz pour ancrer les savoirs

**Méthodes d'évaluation**

Test d'entrée et test de sortie permettant une évaluation des compétences acquises.

**Nos Experts**

Le développement du contenu a été réalisé par des consultants ayant une expertise pratique de la Cybersécurité en milieu industriel.

**Modalités**

Inscription et délai : Bulletin d'inscription à compléter et à nous retourner.
Accès Personnes Handicapées : nous contacter pour déterminer l'aménagement à mettre en place.

SPACE
Contact : conseilformation@space-aero.org

MAJ 04/2024