Programme de formation

La cybersécurité pour tous

Objectifs :

Avec ce qui se passe dans le monde, la Russie, l'Ukraine, le Moyen-Orient, la Chine, la Corée du Nord… il se développe une forme de guerre hybride. Cette cyberguerre ne concerne pas que les Etats, et les cyberattaques frappent de plus en plus tout le monde, puisque tout est connecté et numérisé. On pense que nos structures culturelles n'intéresseront pas les cybercriminels alors que les cyberattaques se font souvent "au hasard". On pense que la cybersécurité est le rôle du responsable informatique alors que c'est l'affaire de tous et au quotidien. Il existe des moyens simples pour limiter ces risques.

A l'issue de cette formation, les participants seront en mesure de :
- identifier la philosophie et les enjeux de la cybersécurité
- identifier les questions liées à la sécurité informatique
- définir les actions à mener
- connaître les risques juridiques
- mettre en œuvre des mesures correctives

A l'issue de cette formation, l'entreprise sera en capacité de progresser dans son travail d'identification des risques cyber, et de mettre en place les premières mesures pour les limiter et les maîtriser.

Publics et prérequis :

Cette formation s'adresse à toute personne employée dans une entreprise quel que soit sa taille.

Méthodes pédagogiques et moyens techniques :

Cette formation est ancrée dans la réalité quotidienne des participants. Elle alterne des temps d'apports théoriques avec de nombreuses mises en situation personnelles et questionnements sur les pratiques quotidiennes des participants.

Durée :

7 heures.

Programme :

Au cours de cette formation seront notamment abordées les thématiques suivantes :

Comprendre les enjeux de la cybersécurité
Un monde de données, ultraconnecté
Le cyberespace, un monde très réglementé
La cybersécurité et la cybercriminalité
Les menaces : la cyberattaque

Apprécier les principales cyberattaques

Le fishing
Les malware
Le cheval de Troie
Les vers et les virus
L'attaque en déni de service
Les ransomware
Les SPAMS

Cerner la cybercriminalité
L'identité numérique et l'anonymat
L'e-réputation
L'usurpation d'identité
Les photos montages et les deepfakes
Le harcèlement en ligne
La vie privée et l'utilisation de données à caractère personnel
La divulgation d'informations confidentielles
Le « revenge porn »
La diffamation et l'injure

Faire de la cybersécurité l'affaire de tous…
Les principales mesures à mettre en œuvre
Les mots de passe
Les politiques internes et chartes d'utilisation
Guides et séances de sensibilisation

Questions et études de cas

Validation des acquis et évaluation :
La méthode pédagogique est centrée sur des allers et retours entre contenus théoriques et questionnements en rapport avec la situation professionnelle des stagiaires. En conséquence, la validation par le formateur des acquis de la formation, de la compréhension des questions abordées et de l'évolution des compétences se fait tout au long de l'action par un système de questions/réponses, d'exercices, de questionnaires et d'échanges entre les participants et lui même. Une attestation de suivi de formation est remise à chaque participant à l'issue du module. Elle précise les dates de réalisation et le volume horaire suivi.

Documentation :
La documentation pédagogique remise aux participants est composée d'un support synthèse, des apports théoriques et d'une bibliographie.