Sensibilisation des utilisateurs à la cybersécurité

Date et durée

Code formation : CYB01-OPC
Durée : 1 jour
Nombre d'heures : 6 heures

Description

Dans le domaine de l'informatique, toute entreprise confondue peut-être victime d'une attaque. Peu importe que vous soyez **salarié ou chef d'entreprise** d'une PME ou bien d'une PMI proposant des services ou que vous ayez un parc informatique, vous devenez une cible potentielle. Être la **cible d'une cyberattaque** est susceptible de nuire aux activités en ligne et au système d'information à différents niveaux. Allant de la simple lenteur jusqu'à la désactivation totale des services, une telle situation peut engendrer des difficultés considérables pour une entreprise et ses collaborateurs.
En suivant cette **formation sur la sécurité informatique**, vous vous familiariserez avec les risques et les menaces qui existent au quotidien. Elle permettra à chacun de bénéficier de toutes les informations nécessaires pour acquérir **les bons réflexes et les bonnes pratiques** lors de l'utilisation des équipements informatiques. Comprendre **les incidences que peut avoir une action utilisateur** au niveau de la sécurité du système d'information, mettre en place une politique de sécurité, connaître les différentes solutions de prévention sont autant de sujets qui seront abordé lors de ce **cours de sensibilisation à la cybersécurité**.

Objectifs

En suivant la **formation sensibilisation des utilisateurs à la cybersécurité**, vous validerez les objectifs suivants :

- connaître les types de menaces informatiques qui peuvent affecter les utilisateurs dans les environnements professionnels et privés ;
- comprendre les risques potentiels et les impacts sur la sécurité des systèmes informatiques de l'entreprise ;
- prendre conscience de l'importance d'une prévention dans ce domaine ;
- mettre en œuvre des mesures de protection contre les menaces ;
- adopter les bonnes pratiques et les bons réflexes informatique.

Points forts

Un formateur expert dans le domaine de la cybersécurité, une auto-évaluation de vos connaissance informatique via un QCM, une validation de vos acquis en fin de formation et des travaux pratiques.

Modalités d'évaluation

Quiz / QCM
Travaux Pratiques

Pré-requis

Suivre la **formation sensibilisation des utilisateurs à la cybersécurité**, ne nécessite aucun prérequis.

Public

Cette formation s'adresse aux publics suivants :

- toute personnes qui utilise des équipements informatique dans le cadre de leur activité professionnelle ;
- les chefs d'entreprise ou les responsables IT qui souhaitent sensibiliser leur personnel à la sécurité informatique et qui veulent mettre en place une politique de sécurité informatique.

Cette formation s'adresse aux profils suivants

Chef d’entreprise / Dirigeant
Responsable sécurité informatique
Directeur des Systèmes d'Information (DSI)
Administrateur système
Architecte informatique / SI
Ingénieur système

Programme

Module 1 : sécurisation du patrimoine numérique de l'entreprise

- Le contexte et les enjeux de la cybercriminalité.
- Les briques concernées par la sécurité (système d'information, logiciels, réseau, web et données).
- Les actifs numériques à protéger en priorité.

Module 2 : panorama des menaces informatiques

- Les différentes typologies de menace.
- La gestion de la messagerie face aux menaces.
- La navigation et le téléchargement de fichiers face aux menaces.

Module 3 : gestion des risques liés aux périphériques

- La poste de travail sous Windows.
- Les disques internes ou externes, les clés USB, les supports réseau, comment se différencient-ils en termes de risques ?
- Les bonnes pratique à adopter.

Module 4 : sécurisation hors ligne

- La sécurité des connexions en dehors de l'entreprise.
- L'utilisation de VPN pour accéder aux ressources de l'entreprise à distance.

Module 5 : réaction face aux attaques

- Les mesures préventives à adopter en cas d'attaque.
- L'évaluation des impacts provoqués par une ou plusieurs menaces.

Module 6 : mise en place d'une protection durable

- L'acquisition des bons réflexes face aux menaces.
- La gestion de son antivirus, de son pare-feu, de ses sauvegardes, etc.
- Les règles de bonne conduite informatique.