Date de la dernière MAJ : 04/07/2024
Formacode(s) : 70654

LA CYBERSECURITE EN ENTREPRISE

Compétences visées :

- Maîtriser les bases de la cybersécurité en entreprise ;
- Découvrir et intégrer les bonnes pratiques d'une utilisation sécurisée des outils informatique ;
- Planifier et organiser ses actions en cas de cyberattaque ;
- Mettre en place des mesures de protection durable.

Public visé :

- Tout public

Durée du programme :

- 7 heures

Prérequis :

- Maîtrise de l'outil informatique et bureautique ;
- Maîtrise de la langue française.

Tarif : 2400€
(Prise en charge possible, nous contacter pour plus d'informations.)

Modalités de financement : Plan de développement des compétences, auto-financement.

Modalités d'admission :
Auto-positionnement. Notre équipe de conseillers en formation reste disponible pour vous accompagner, n'hésitez à nous contacter.

Localisation et accessibilité :
Distanciel et/ou présentiel.
Nos locaux sont adaptés pour accueillir les personnes à mobilité réduite. Si vous êtes en situation de handicap, contactez-nous pour échanger sur les modalités de suivi de la formation.

Méthodes pédagogiques :
Lors de la formation plusieurs méthodes et techniques sont utilisées afin de mettre le stagiaire au cœur de son apprentissage dont il est acteur en permanence.
Une alternance des différentes méthodes active, démonstrative, interrogative et expositive est réalisée lors des animations de séquences de formation.

Les techniques utilisées sont : le travail de sous-groupe, mise en situation, jeux de rôle, étude de cas et brainstorming.

Modalités d'évaluation des acquis :

- Évaluation des acquis en cours de formation : questionnaire, étude de cas, quiz ;
- Test en fin de formation : QCM.

Programme :

Maîtriser les bases de la cybersécurité en entreprise :

- Identifier les cas classiques d'attaques au quotidien ;
- Définir ce qu'est une cyberattaque et la cybercriminalité ;
- Examiner les failles de sécurité ;
- Clarifier le vocabulaire technique associé aux cyberattaques (sniffing, spoofing, smurfing, hijacking, etc.) ;
- Différencier les profils des attaquants internes et externes ;
- Évaluer le niveau de menace pour son activité.

Découvrir et intégrer les bonnes pratiques d'une utilisation sécurisée des outils informatique :

- Prioriser la sécurisation des mots de passe et des données stockées dans le cloud ;
- Protéger la boîte mail contre ses dangers potentiels ;
- Gérer les risques associés aux clés USB en pratique ;
- Adopter des pratiques sécurisées pour se connecter hors de l'entreprise, incluant l'utilisation de VPN ;
- Réagir efficacement aux différentes formes de chantage informatique (demande de rançon, etc.).

Planifier et organiser ses actions en cas de cyberattaque :

- Identifier les modes de propagation d'une attaque informatique ;
- Réagir à une attaque en suivant les comportements et gestes appropriés ;
- Évaluer les dégâts causés par une attaque informatique ;
- Apprendre à mettre en quarantaine les systèmes pour limiter la propagation d'une attaque ;
- Décontaminer son ordinateur après une attaque ;
- Déterminer qui contacter en fonction du type d'attaque (service informatique, police, justice, etc.) ;
- Reconnaître et gérer les situations de cyberharcèlement.

Mettre en place des mesures de protection durable :

- Acquérir les bons réflexes au quotidien pour maintenir une cybersécurité efficace ;
- Identifier les contraintes réglementaires et juridiques en matière de cybersécurité ;
- Appliquer une mise à jour régulière de son ordinateur et de ses logiciels comme mesure cruciale pour la sécurité ;
- Gérer l' antivirus et le parefeu pour assurer une protection quotidienne ;
- Sauvegarder ses données : un geste salvateur ;
- Administrer la gestion des données sensible au sein de l'entreprise ;
- Appliquer les méthodes d'authentification et de contrôle d'accès pour renforcer la sécurité ;
- Elaborer un plan de reprise de l'activité (PRA) pour préparer la continuité après un incident ;
- Promouvoir et encourager la mise en œuvre de la politique de sécurité de l'entreprise.

Délais d'accès :
Entrées et sorties permanentes. Habituellement, les accès sont ouverts 24 heures ouvrées après la réception du dossier complet et la validation du financement.

Contactez-nous !
www.crc-formation.fr
04.94.88.58.59
contact@crc-formation.fr
245, avenue de l'université
Le nouveau parc St Clair
83160 LA-VALETTE-DU-VAR