ANABIOZ
CONSEIL & FORMATION

FICHE DESCRIPTIVE DE FORMATION

Référence : 240732
Durée : 1 jour (7 heures)
de 9h à 12h30 et 13h30 à 17h
Lieu : en présentiel

LA CYBERSECURITE AU QUOTIDIEN

Initiation

Public concerné :
Tout utilisateur des outils informatiques

Nombre de participants :
Minimum : 5 / Maximum : 10

Méthodes Pédagogiques :
- Test de positionnement avant la formation
- Alternance d'apports théoriques et de mises en situations sous le contrôle du formateur
- Manipulations par le stagiaire sur ordinateur
- Echanges et validations régulières tout au long de la formation
- Validation des acquis par un quiz.

Prérequis :
- Être à l'aise avec l'usage d'un ordinateur (Windows, clavier et souris)

Besoins matériels / documentaires :
Salle avec moyen de projection et des ordinateurs (1 ou 2/personne) ayant un accès internet

Intervenant :
Formateur expérimenté
Minimum 5 ans d'expérience

Modalités et délais d'accès :
En amont de la contractualisation, un entretien permet d'analyser les Besoins et un devis de formation est adressé au client.
Les dates sont déterminées entre le Client et le Prestataire.
L'action de formation peut débuter dans un délai de 2 mois après signature du devis.
Le suivi de l'exécution de l'action de formation est réalisé au moyen de feuilles d'émargements, co-signées par le stagiaire et l'intervenant.

Sanction : certificat de réalisation

Objectif professionnel :
Identifier les bonnes pratiques en matières de cybersécurité

Objectifs opérationnels et évaluables :
A l'issue de l'action de formation, les stagiaires seront capables de :
1. Reconnaître les menaces informatiques courantes
2. Appliquer les bonnes pratiques
3. Préparer un plan minimum de continuité et de reprise d'activité

Contenu :

1. INTRODUCTION A LA CYBERSECURITE

Principes de base de la cybersécurité
- Confidentialité, intégrité et disponibilité des informations.
- Concepts de menace, vulnérabilité et risque.

2. LES MENACES COURANTES

- Malware (logiciels malveillants)
- Types de malware : virus, chevaux de Troie, ransomwares, spyware, etc.
- Méthodes de propagation et signes d'infection.

- Phishing et Ingénierie Sociale
- Reconnaître les tentatives de phishing par email, téléphone ou réseaux sociaux.
- Techniques d'ingénierie sociale courantes et comment s'en protéger.

- Attaques par Déni de Service (DoS) et Déni de Service Distribué (DDoS)
- Fonctionnement et impact des attaques DoS et DDoS.

- Intrusions et Violations de Données
- Techniques d'intrusion courantes : exploitation des vulnérabilités, attaques par force brute, etc.
- Conséquences des violations de données et importance de la protection des informations sensibles.

3. LES BONNES PRATIQUES EN MATIERE DE CYBERSECURITE

- Principe de base des bonnes pratiques

- Hygiène numérique.
- Configuration sécurisée des systèmes
- Gestion des mots de passe et utilisation d'un gestionnaire

Contacts pédagogique, administratif et handicap : 05 56 310 310 – info@anabioz.fr
11 Rue Blanqui 33300 BORDEAUX
APE : 4741Z – SIRET : 504 593 310 00056 – RCS Bordeaux – SARL au capital de 5 000€ - Organisme assujetti à la TVA
anabioz.fr

- Authentification Multi-facteurs (MFA)

- Importance et mise en place de la MFA.

- Sécurité des Emails et des communications

- Reconnaître les emails frauduleux et tentative de phishing
- Bonnes pratiques pour sécuriser les communications électroniques

- Navigation Sécurisée sur Internet

- Utiliser des navigateurs sécurisés et à jour.
- Reconnaître les sites web de confiance et éviter les sites douteux.

- Utilisation Sécurisée des Dispositifs Mobiles

- Mettre en place des mesures de sécurité sur les smartphones et tablettes.
- Installer des applications provenant de sources fiables uniquement.
- Sécurité des usages pro-perso

4. LA GESTION DES INCIDENTS DE SECURITE

- Détection et Réponse aux Incidents

- Reconnaître les signes d'un incident de sécurité.
- Procédures de signalement des incidents.

- Plans de Continuité et de Reprise d'Activité

- Importance de la planification de la continuité des opérations.
- Stratégies de sauvegarde et de récupération des données.

VERIFICATION DES ACQUIS – Quiz

Indicateurs de résultats sur la thématique La cybersécurité au quotidien :
Ils seront communiqués dès que disponible

Conditions de réussite :
- Ne pas utiliser son téléphone portable pendant la formation
- Ne pas s'absenter pendant la formation
- Les stagiaires doivent être acteur pendant la journée
- Mettre en application au plus vite les acquis dans l'entreprise après la formation
- Prendre des notes tout au long de la formation

Déclaration d'activité enregistrée sous le numéro 75 33 10 83 033 auprès du préfet de région de Nouvelle-Aquitaine.
Cet enregistrement ne vaut pas agrément de l'Etat

Date :

Signature client avec cachet

Accessibilité aux personnes en situation de handicap
Conformément à la règlementation (Loi du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées / Articles D. 5211-1 et suivants du code du travail), Anabioz peut proposer des aménagements (technique, organisationnel et/ou pédagogique) pour répondre aux besoins particuliers de personnes en situation de handicap. Le cas échéant, l'organisme de formation mobilise des compétences externes (Centre de Ressources Formation Handicap Nouvelle-Aquitaine…) pour la recherche de solutions permettant l'accès aux formations.

Contacts pédagogique, administratif et handicap : 05 56 310 310 – info@anabioz.fr
11 Rue Blanqui 33300 BORDEAUX
APE : 4741Z – SIRET : 504 593 310 00056 – RCS Bordeaux – SARL au capital de 5 000€ - Organisme assujetti à la TVA
anabioz.fr