ACTION DE FORMATION

FORMATIONS COURTES

Devenir acteur de sa sécurité numérique et de celle de son entreprise

Votre contact

Carole COURANT
05 49 61 20 66
courantc@poitou.ifrb.fr

Durée

1,00 jour(s)
7:00 heures

Public

Le chef d'entreprise et tous les collaborateurs ayant accès à une source numérique de l'entreprise (tablette, smartphone, ordinateur..)

Pré-requis

NC

Moyens pédagogiques et supports

Un apport théorique couplé à de nombreux exercices pratiques et mise en situation.
Support pédagogique remis à chaque participant.

Profil de l'intervenant

Consultant formateur en sécurité informatique, responsable en gestion et management d'entreprise, DPO (Délégué à la Protection des Données) externe enregistré à la CNIL.

Objectifs de la formation

Savoir identifier, comprendre et éviter les risques numériques

Objectifs pédagogiques

- Prendre connaissance des comportements à risque au sein de son entreprise
- Identifier les principales règles d'usage en matière de sécurité informatique
- Savoir mettre en pratique les règles de protection liées aux antivirus, mots de passe et navigation sur le web

Contenu

- Introduction : cadre général, évaluation des connaissances par QCM

PARTIE 1 : Se faire peur...pour comprendre.

- Identifier et comprendre les différences entre web et internet
- Pourquoi les « petits » intéressent les cybercriminels
- Etes vous une cible de choix : questionnement et présentation
- Les techniques de cyberattaques les plus fréquentes :
  - Le Phishing
  - Le SpearPhishing
  - La « Faute au Président » :
- Comment s'en prémunir
- RGPD et sécurité informatique
  - Connaitre et comprendre les obligations
  - Identifier les risques juridiques
- Les impacts sur la vie de l'entreprise

PARTIE 2 : Se protéger

- Hygiène générale
  - Quel compte utiliser
  - Mises à jour et Antivirus, Pourquoi ?
  - Focus sur les Smartphones
- Authentification par mot de passe
  - Les techniques « humaines »
  - Présentation d'un coffre-fort »
- Rendre ses données illisibles :
  - Principes et usages
  - Présentation d'une solution
- Surfer en toute sécurité
  - Paramétrer son navigateur
  - Apprendre à détecter des sites trompeurs
  - Mails frauduleux et pièces jointes, comment agir.

PARTIE 3 : Comment réagir en cas d'attaque

- Connaitre les « gestes d'urgence »
- Mise en pratique par exercice

QCM de fin de formation permettant d'évaluer l'acquisition des connaissances. En cas de résultats > à 60 bonnes réponses, une attestation de réussite est délivrée. Pour tout résultat < à 60, une attestation de suivi est délivrée.