PROGRAMME DE FORMATION

COMMENT METTRE EN PLACE UNE SECURITE INFORMATIQUE FIABLE DANS SON ENTREPRISE

Vos contacts

IFRB PAYS DE LA LOIRE

Stéphanie Truchon	02 40 20 36 66
Nathalie Milsent	06 70 73 40 15
Laurence Le Dréau	02 40 20 37 54

contact@paysdelaloire.ifrb.fr

Lieu(x) et date(s) 2017

Saint Herblain le 19 octobre 2017

Durée

1,00 jour(s)7:00 heures

Coût de la formation

270,00€ HT Forfait /personne

Public

Dirigeant d'entreprise, personnel de direction, toute personne qui souhaite être sensibilisée à la sécurité informatique.

Pré-requis

Utilisateurs réguliers des outils informatiques et communicants (téléphone, ordinateur, messagerie, Internet, ...).

Effectif

De 6 à 10 participants

Formateur

Un consultant de DIGITEMIS

Moyens pédagogiques et supports

Support de formation, diaporama, alternance d'apports théoriques et de mises en situation avec différents supports.
Guide des bonnes pratiques de l'informatique

Objectifs pédagogiques :

Etre capable de :

- Prendre conscience des comportements à risque au sein de son entreprise
- D'identifier les principales règles d'usage en matière de sécurité informatique.

Programme

1. La sécurité informatique : comprendre les menaces et les risques
   - Introduction : cadre général, qu'entend-on par sécurité informatique (menaces, risques, protection) ?
   - Comment une négligence peut-elle créer une catastrophe ? Quelques exemples.
   - Les composantes d'un SI et leurs vulnérabilités. Systèmes d'exploitation client et serveur.
   - Réseaux d'entreprise (locaux, site à site, accès par Internet).
   - Réseaux sans fil et mobilité. Les applications à risques : Web, messagerie...
   - Base de données et système de fichiers. Menaces et risques de violation des données.
   - Typologie des risques. La cybercriminalité en France. Le vocabulaire usuel (sniffing, spoofing, smurfing, hijacking, phishing, viching...).
2. La protection de l'information et la sécurité du poste de travail
   - Vocabulaire. Confidentialité, signature et intégrité. Comprendre les contraintes liées au chiffrement.
   - Schéma général des éléments cryptographiques. Windows, Linux ou MAC OS : quel est le plus sûr ?
   - Gestion des données sensibles. La problématique des ordinateurs portables.
   - Quelle menace sur le poste client ? Comprendre ce qu'est un code malveillant.
   - Comment gérer les failles de sécurité ? Le port USB. Le rôle du firewall client.
3. L'authentification de l'utilisateur et les accès depuis l'extérieur
   - Contrôles d'accès : authentification et autorisation.
   - Pourquoi l'authentification est-elle primordiale ?
   - Le mot de passe traditionnel.
   - Authentification par certificats et token.
   - Accès distant via Internet. Comprendre les VPN.
   - De l'intérêt de l'authentification renforcée.
   - Agir pour une meilleure sécurité : les aspects sociaux et juridiques. La CNIL.
   - La cybersurveillance et la protection de la vie privée.
   - La charte d'utilisation des ressources informatiques.
   - La sécurité au quotidien. Les bons réflexes.

Siret n° 402 112 866 000 23 - Code APE 85.59A - Déclaration d'activité enregistrée sous le numéro 52 44 04286 44 auprès du préfet de la région Pays de la Loire. Cet enregistrement ne vaut pas agrément de l'Etat.

PROGRAMME DE FORMATION

COMMENT METTRE EN PLACE UNE SECURITE INFORMATIQUE FIABLE DANS SON ENTREPRISE

Lieu(x) et date(s) 2017

Saint Herblain le 19 octobre 2017

Durée

1,00 jour(s)7:00 heures

Coût de la formation

270,00€ HT Forfait /personne

Public

Dirigeant d'entreprise, personnel de direction, toute personne qui souhaite être sensibilisée à la sécurité informatique.

Pré-requis

Utilisateurs réguliers des outils informatiques et communicants (téléphone, ordinateur, messagerie, Internet, ...).

Effectif

De 6 à 10 participants

Formateur

Un consultant de DIGITEMIS

Moyens pédagogiques et supports

Support de formation, diaporama, alternance d'apports théoriques et de mises en situation avec différents supports.
Guide des bonnes pratiques de l'informatique

Suite programme :

4. Comment s'impliquer dans la sécurité du SI ?
   - Analyse des risques, des vulnérabilités et des menaces.
   - Les contraintes réglementaires et juridiques.
   - Pourquoi mon organisme doit respecter ces exigences de sécurité ?
   - Les hommes clés de la sécurité : comprendre le rôle du RSSI et du Risk Manager.
   - Agir pour une meilleure sécurité : les aspects sociaux et juridiques. La CNIL.
   - La cybersurveillance et la protection de la vie privée.
   - La charte d'utilisation des ressources informatiques.
   - La sécurité au quotidien. Les bons réflexes.
5. Le RGPD
   - Présentation de la nouvelle règlementation
   - Comment s'y conformer
6. Exercices et tests :
   - Questions – réponses
   - QCM
7. Conclusion