Sécurité des TIC
PCIE
(Éligible au CPF)

Durée : 1 jour

Référence : F06-PCIE-SECURITE-1

Objectifs pédagogiques

Les participants seront préparés au passage de la certification PCIE et seront capables de :
- Comprendre les concepts clés relatifs à l'importance d'assurer la sécurité des données
- Protéger un ordinateur, un dispositif numérique mobile, un réseau
- Connaître les différents types de réseaux, de connexions et leurs composants spécifiques
- Naviguer sur le World Wide Web et communiquer en toute sécurité sur Internet
- Comprendre les problèmes de sécurité liés à la communication
- Sauvegarder et restaurer des données de manière appropriée et sécurisée

Population concernée

Utilisateurs au quotidien des TIC (Technologies de l'Information et de la Communication) dans le milieu professionnel ou à titre personnel.

Connaissances requises

Maitrise d'un outil connecté, et avoir des notions de partage de données et d'informations.

Profil de l'intervenant

Formateur senior en bureautique (30 ans d'expérience), titulaire d'une Licence professionnelle « Gestion des Ressources Humaines - Conception et réalisation de formations pour adultes » et certifié PCIE.

Moyens pédagogiques

Rappel des objectifs et des prérequis en tour de table.
Alternance théorie - pratique continue tout au long du stage.
Un support de cours par stagiaire.
Un poste informatique par stagiaire.
Un poste informatique formateur avec vidéo projecteur.
Feuille de présence à la demi-journée obligatoire.

Méthodes d'évaluation

Contrôle continu par des exercices tout au long du stage.
Évaluation finale des acquis par le formateur à la demande du client.
Évaluation du stage par chaque stagiaire (questionnaire de satisfaction).
Attestation individuelle de formation avec durée (en heures) du stage.

Déroulé pédagogique détaillé page suivante

Évaluation du niveau initial avec le test PCIE en début de formation

Préparation à la certification

1 Concepts de sécurité

Menaces sur les données

Faire la différence entre les données et les informations

Comprendre le terme « cybercriminalité »

Comprendre la différence entre hacker, cracker et pirater

Connaître les menaces majeures pour la sécurité des données

Connaître les autres menaces pour la sécurité des données

Valeur de l'information

Comprendre pourquoi il est important de protéger les informations personnelles

Comprendre pourquoi il est important de protéger des données commerciales sensibles

Identifier les mesures à prendre pour empêcher les accès non-autorisés aux données

Comprendre les caractéristiques de base de la sécurisation de l'information

Identifier les principales règles de protection, de conservation et de contrôle des données

Comprendre l'importance de créer et d'adopter des directives et des réglementations

Sécurité personnelle

Comprendre le terme « ingénierie sociale » et ses implications

Identifier les méthodes employées pour l'ingénierie sociale

Comprendre le terme « vol d'identité » et ses implications dans les domaines personnels, financiers, des affaires, et légaux

Identifier les méthodes de vol d'identité

Sécurité des fichiers

Comprendre les effets de l'activation / la désactivation des macros

Utiliser un mot de passe pour les fichiers

Comprendre les avantages et les limites du cryptage des données

2 Logiciels malveillants

Définition et fonctionnement

Comprendre le terme « logiciel malveillant »

Reconnaître les différentes techniques adoptées par les logiciels malveillants pour rester masqués

Types

Reconnaître les différents types d'infections produits par les logiciels malveillants et comprendre comment ils agissent

Reconnaître les types de vols de données, les bénéfices produits par l'emploi de logiciels malveillants de vol de données et comprendre comment ils fonctionnent

Protection

Comprendre comment fonctionne un logiciel anti-virus et identifier ses limites

Analyser/scanner des lecteurs, dossiers, fichiers spécifiques avec un logiciel anti-virus

Comprendre le terme « quarantaine » et l'effet d'une quarantaine sur des fichiers infectés ou suspects

Comprendre l'importance de télécharger et d'installer régulièrement les mises-à-jour des anti-virus

3 Sécurité réseau

Réseaux

Comprendre le terme « réseau » et reconnaître les principaux types de réseaux

Comprendre le rôle de l'administrateur réseau

Comprendre l'utilité et les limites d'un pare-feu

Connexions réseaux

Connaître les différentes façons de se connecter à un réseau

Comprendre que le fait de se connecter à un réseau peut entraîner des problèmes de sécurité

Sécurité en environnement sans fil

Connaître l'importance d'imposer la saisie d'un mot de passe pour protéger l'accès à un réseau

Connaître les différents types de sécurisation d'un réseau

Être conscient que l'utilisation d'un réseau non-protégé peut permettre l'espionnage

Se connecter à un réseau sans fil protégé / non-protégé

Contrôle d'accès

Comprendre l'utilité d'un compte utilisateur pour se connecter à un réseau et l'importance de toujours passer par la saisie d'un nom d'utilisateur et d'un mot de passe pour accéder au réseau

Connaître les bonnes pratiques en matière de mot de passe

Connaître les principales possibilités de contrôle d'accès biométrique

4 Utilisation sécurisée du Web

Navigation Web

Savoir que certaines activités en ligne ne devraient être effectuées que sur des pages sécurisées

Reconnaître un site Web sécurisé

Etre conscient des risques de redirection vers des sites malveillants

Comprendre le terme « certificat numérique »

Comprendre le terme « mot de passe à usage unique »

Choisir les réglages appropriés pour activer, désactiver la fonction de remplissage automatique

Comprendre le terme « mouchard électronique »

Choisir les réglages appropriés pour autoriser, bloquer les mouchards électroniques

Supprimer les données personnelles dans un navigateur

Comprendre le but, la fonction et les types de logiciels de contrôle de contenu

Réseaux sociaux

Comprendre l'importance de ne pas diffuser d'informations confidentielles sur des réseaux sociaux

Etre attentif à l'importance d'appliquer les bons réglages de confidentialité

Comprendre les risques potentiels lors de l'utilisation des réseaux sociaux

5 Communications

E-Mail

Comprendre le rôle du cryptage / décryptage d'un e-mail

Comprendre le terme « signature numérique »

Créer et ajouter / importer un certificat numérique

Être conscient de la possibilité de recevoir des e-mails frauduleux et non-sollicités

Comprendre le terme « hameçonnage ». Identifier les principales caractéristiques d'hameçonnage

Etre conscient du risque d'infecter l'ordinateur par des logiciels malveillants

Messagerie instantanée

Comprendre le terme « messagerie instantanée » et ses utilisations possibles

Comprendre les failles de sécurité liées aux messageries instantanées

Connaître les méthodes pour assurer la confidentialité lors de l'utilisation des messageries instantanées

6 Gestion de la sécurité des données

Sécuriser et sauvegarder les données

Connaître les méthodes pour s'assurer de la sécurité physique des dispositifs numériques mobiles

Identifier les paramètres d'une procédure de sauvegarde

Sauvegarder des données

Restaurer et valider la restauration de données en provenance d'une sauvegarde

Destruction sécurisée

Comprendre l'importance de pouvoir détruire de manière définitive des données

Faire la distinction entre un effacement et une totale destruction de données

Identifier les méthodes habituelles de suppression définitive de données

Passage de la certification PCIE en fin de formation