Sécurité Informatique

Public concerné : Toute personne concernée par une démarche sécurité au sein de l'entreprise.

Niveau requis :
L'environnement Windows.

Objectif : Comprendre les problématiques liées à la sécurité informatique. Adopter les bonnes attitudes et les bons réflexes.

Moyens pédagogiques :

- Grilles d'évaluation de niveau.
- Formateurs recrutés pour leurs expériences professionnelles et leurs compétences pédagogiques
- 8 personnes maximum / stage
- 1 ordinateur par personne
- Chaque notion est expliquée au tableau et suivie immédiatement d'un exercice pratique.
- Les exercices évoluent en difficulté au fur et à mesure du stage.
- Un support de cours sera remis à chaque participant en fin de formation.
- Assistance téléphonique gratuite.

Niveau /certification obtenue :
Possibilité de validation PCIE.

Durée : 1 jours : 7 heures

Délai d'acceptation :
Mise en place de vos cours dès acceptation de votre financement

Accessibilité handicapé :
Condition d'accueil et d'accès au public en situation d'handicap

La sécurité pour l'entreprise et le télétravailleur

Contexte et enjeux de la cybercriminalité
Les briques concernées par la sécurité (système, logiciel, réseau, web, données)
Quels sont les biens à protéger ?
Les moyens pour garantir une meilleure sécurité
Le facteur humain

Contexte législatif

Le cadre législatif de la sécurité
Les responsabilités civile et pénale
Les principales lois.
Le rôle de la CNIL et son impact pour la sécurité en entreprise

Panorama des menaces

Les différentes typologies de menace (attaques intrusives – injection SQL, passive – phishing, destructrices – virus, etc.).
Détails sur les Advanced Persistent Threat (Attaque persistante avancée)
Rôle des entreprises dans ces attaques.
Focus sur l'ingénierie sociale
Les comportements à l'intérieur et à l'extérieur de l'entreprise.

Les périphériques et le poste de travail

Vocabulaire réseau de base (passerelle, DNS, DHCP)
Que fait un firewall d'entreprise ?
Les risques encourus avec les périphériques
Le poste de travail pour Windows
Disque interne/externe, clé USB, réseau : quelles différences pour les risques ?
Exemple de propagation de virus par clef USB
Les réflexes à adopter avec les « corps étrangers »

Public concerné : Toute personne concernée par une démarche sécurité au sein de l'entreprise.

Niveau requis :
L'environnement Windows.

Objectif : Comprendre les problématiques liées à la sécurité informatique. Adopter les bonnes attitudes et les bons réflexes.

Moyens pédagogiques :
- Grilles d'évaluation de niveau.
- Formateurs recrutés pour leurs expériences professionnelles et leurs compétences pédagogiques
- 8 personnes maximum / stage
- 1 ordinateur par personne
- Chaque notion est expliquée au tableau et suivie immédiatement d'un exercice pratique.
- Les exercices évoluent en difficulté au fur et à mesure du stage.
- Un support de cours sera remis à chaque participant en fin de formation.
- Assistance téléphonique gratuite.

Niveau /certification obtenue :
Possibilité de validation PCIE.

Durée : 1 jours : 7 heures

Délai d'acceptation :
Mise en place de vos cours dès acceptation de votre financement

Accessibilité handicapé :
Condition d'accueil et d'accès au public en situation d'handicap

Sécurité Informatique

(Suite)

Nomadisme et travail à domicile – Problématiques liées au BYOD
Risques liés à l'accueil du portable d'un visiteur dans l'entreprise
Se connecter sans risque hors de l'entreprise (réseaux publics, télétravail, chez un client...)
La communication unifiée UcaaS
L'accès distant (VPN) aux ressources de l'entreprise

Exploitation de l'ingénierie sociale
La réception des messages (SPAM, faux messages...)
Le mauvais usage de la retransmission des messages
Les courriers électroniques de taille importante
L'usurpation d'identité

Risques liés à Internet
Navigation et surprises
Les problèmes liés au téléchargement de fichiers
Limites de l'ultra protection des navigateurs
Peut-on « rattraper » une information divulguée ?
Votre boîte mail : comment se protéger de tous ses dangers ?
Le risque des clés USB : Que faire en pratique ?

Réagir en cas d'attaque
Le comportement à adopter et les gestes de premier secours en cas d'attaque informatique
Évaluer les dégâts d'une attaque informatique

Mettre en place une protection durable
Acquérir les bons réflexes quotidiens
Comment bien réagir aux différentes formes de chantage informatique (demande de rançon...)
Mettre à jour son ordinateur et ses logiciels : une mesure simple mais primordiale
Gérer son antivirus et son pare-feu pour sécuriser son quotidien
Sauvegarder ses données : un geste salvateur
Mettre en place un plan de reprise de l'activité

Synthèse et conclusion
Synthèse des points abordés
Savoir évaluer les risques
Règles de bonnes conduites