

CYBERSECURITE - INITIATION A L'HYGIENE INFORMATIQUE

Objectifs : Appréhender les enjeux et la nature des attaques potentielles à destination du système informatique de l'entreprise. Connaître et s'approprier les pratiques et règles à observer et les dispositifs à mettre en œuvre afin de limiter une grande partie des risques liés à l'usage des systèmes d'information.

Public : Artisan, commerçant(e), dirigeant(e) ou collaborateur(trice) d'une PME ou d'une TPE désirant préserver la sécurité de l'ensemble des équipements informatiques professionnels.

Pré-requis

- Maîtriser les bases de l'outil informatique et du système d'exploitation Windows.
- Pratiquer Internet (Consultation de sites, utilisation de moteurs de recherche...).

Durée 07 (sept) heures de formation, soit **2 demi-journées de 3 heures 30**.

Cette formation, si elle est individuelle, peut, à la demande formelle de l'apprenant(e), et après un entretien préalable à sa mise en œuvre, faire l'objet d'un ajustement personnalisé de son programme. Cette adaptation "**sur mesure**" est destinée à répondre au plus juste aux attentes et objectifs de l'élève, en tenant compte tout à la fois de ses acquis antérieurs en informatique et internet et des spécificités de ses activités et de sa structure professionnelles.

Remédier à un incident informatique dans l'urgence peut s'avérer bien plus couteux que le prévenir...

- Le Hardware : Pannes mécaniques, électriques et électroniques / Anticiper pour mieux y remédier.
- Cybercriminalité - TPE, ne pas sous-estimer le danger.
- Des menaces multiples et complexes / Se préserver des conséquences.
- Les logiciels espions "grand public".
- Les Hackers / Espionner - Dérober - Asservir - Rançonner - Neutraliser.
- Les types de cyberattaques.
- Les Malwares / Inventaire / Nuisances / Conséquences / Défense.
- Focus sur les ransomwares et le Darknet.
- Antivirus et Anti-Malwares.
- Les garanties reconstitution de données de vos assureurs.
- Les sauvegardes des données / Supports externalisés / Cloud : confidentialité et sécurité.
- Les mises à jour du système d'exploitation, des logiciels et des applications. Unité centrale et périphériques.
- Mots de passe : 10 règles à respecter pour les élaborer - Générateurs de mots de passe aléatoires.
- Sécurisation des accès Wi-Fi - Mise à jour de la box - Clé de sécurité.
- La protection des données / CNIL - Déclaration de fichiers : Finalité - Pertinence - Conservation - Droits - Sécurité.
- Les risques internes - Délégations d'utilisation - Comptes Administrateur et Utilisateurs.
- Informatique nomade - Sécuriser les PC mais également les tablettes et smartphones.
- Messagerie - Le Phishing - Liens et pièces jointes.
- Téléchargements / Consultations : Les risques multiples du n'importe quoi, n'importe où...
- Effectuer des paiements en ligne / Bénéficiaires référencés / Sites sécurisés.
- Réseaux sociaux : Vos Posts : Diffusion d'informations sensibles - Paramètres de confidentialité.
- Obtenir de l'information spécifique et de l'assistance en ligne.
- Demain... Nouveaux modes opératoires des hackers. Objets connectés. Reconnaissance vocale.

EVALUATION DES ACQUIS DE LA FORMATION / Exercices pratiques

Analyse et synthèse des apports personnels des participant(e)s - Echanges.

Communication & Informatique & Internet & Marketing

Gérard MAITROT - Consultant & Formateur - 3, rue Maurice Romagon 10000 TROYES
06 72 51 58 59 - 03 25 42 80 37 - contact@gerard-maitrot.fr - www.gerard-maitrot.fr
Déclaration d'activité enregistrée sous le numéro **21 10 00778 10** auprès du Préfet de la région de Champagne Ardenne
SIRET 401 504 378 00035 - APE 7022Z - RCP Groupama 16376085 0001