PROGRAMME DE FORMATION

CYBERSÉCURITÉ

2 formats au choix

Durée en individuel : 25h à distance ou en présentiel

Zoom sur les spécificités de l'individuel : flexibilité, personnalisation, aménagement du programme, le tout en fonction de vos besoins et convenance. Avec démarrage immédiat en fonction de vos disponibilités et de celles du formateur.

2 lieux au choix

De chez vous, à distance ou dans nos locaux
au 8 bis rue de l'Eperon 75006 Paris.
Métro Saint Michel ou Odéon
Parking Vinci à la Place St André des Arts

Equipement

En présentiel, nous mettons à votre disposition des ordinateurs PC équipés des licences adéquates mises à jour. À distance, c'est à vous de jouer et d'avoir un ordinateur équipé des licences adéquates. Dans ce cas, notre équipe peut vous conseiller.

Public visé et pré-requis- Salariés, demandeurs d'emploi, auto entrepreneurs, particuliers ou bénévoles souhaitant progresser dans l'acquisition de connaissances et savoirs. Pour chacun, une maîtrise basique de l'ordinateur est demandée.

Accessibilité - Nos formations sont accessibles aux personnes en situation de handicap, notamment grâce à notre partenariat avec une structure spécialisée pour nous permettre d'adapter nos formations aux besoins de chacun. Si vous êtes concerné(e), n'hésitez pas à contacter notre référent en toute confidentialité. Chlomo Zenou - 01 43 29 28 45 - chlomo.peaj@gmail.com

Méthodes et moyens pédagogiques

Tout au long de la formation, des temps théoriques alternent avec des temps pratiques (créations de contenus, exercices, recherches, simulations, jeux, études de cas...). Des supports écrits sont transmis au stagiaire en versions numérique et papier. En amont de la formation, un test de positionnement ou un entretien téléphonique sont réalisés pour définir les besoins et demandes des stagiaires afin que la formation corresponde au mieux.

En présentiel - En appui des temps théoriques, un diaporama et un écran mural sont utilisés, tout en laissant place à une forte interactivité entre les stagiaires et les formateurs.

En distanciel - Une solution à distance permettant la vidéo, le son, le partage d'écran, l'enregistrement des sessions, est utilisée : la formation est ainsi organisée sous la forme de classe virtuelle ou de visioconférence ou de elearning. Un assistant technique est également sollicité afin d'apporter une aide aux stagiaires qui auraient du mal à se connecter.

Formateurs expérimentés - Experts dans le milieu de la cybersécurité, tous nos formateurs cumulent de nombreuses journées de formation auprès de différents organismes dont notre structure.

Evaluation - À l'issue de la session,

Un test de fin de formation (QCM, créations, exercices, projet, présentation orale) est réalisé afin de valider les acquis.

Dans le cas des formations certifiantes, un examen complémentaire est proposé pour lequel le stagiaire reçoit ultérieurement une attestation de passage ainsi qu'un certificat si réussite.

Chaque stagiaire est invité à participer à un bilan oral "a chaud" complété par un questionnaire "à froid" envoyé quelques semaines plus tard, pour connaître l'impact de la formation suivie et d'en mesurer les apports au niveau professionnel.

Chaque stagiaire reçoit une attestation de fin de formation reprenant les compétences acquises ou en cours d'acquisition ainsi qu'une attestation de présence. Dans le cas des formations à distance, un certificat de réalisation est délivré par nos soins.

Tarifs & financement

Nos tarifs sont nets de TVA, par heure et par personne, déjeuner non compris

Cette formation est éligible à l'ensemble des financements liés à la formation continue : OPCO, AIF, Financements personnels. N'hésitez pas à nous contacter pour des conseils.

SESSION EN INDIVIDUEL 25H - 1750 €

Certification incluse : NON

Je réserve ma place

Je souhaite un devis pour un groupe déjà constitué

Les détails finaux concernant la formation (lieu, durée, présentiel, distanciel...) sont indiqués dans le devis et la convention, remis avec le règlement intérieur de PEAJ.

Une question ? Besoin d'aide ? S'inscrire ?

Contactez-nous au 01 43 29 28 45
contact.peaj@gmail.com
marielucie.peaj@gmail.com
www.peaj.org

PROGRAMME DE FORMATION

CYBERSÉCURITÉ

OBJECTIFS

- Comprendre les principaux éléments qui assurent une sécurité dans l'utilisation des TIC (Technologies de l'Information et de la Communication) au quotidien
- Savoir identifier et signaler des activités malveillantes d'un type particulier

PROGRAMME

LES MENACES

- Faire la différence entre les données et les informations
- Comprendre le terme : cybercriminalité
- Comprendre la différence entre hacker (hacking), cracker (cracking) et pirater dans un but éthique (ethical hacking)
- Connaître les menaces majeures pour la sécurité des données comme : les incendies, les inondations, les guerres, les tremblements de terre
- Connaître les menaces pour la sécurité des données causées par : les employés, le fournisseur d'accès, les personnes externes

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 comme : le cryptage des données, l'utilisation de mots de passe
- Comprendre les caractéristiques de base de la sécurisation de l'information
- Identifier les principales règles de protection, de conservation et de contrôle des données / données privées en vigueur dans votre pays
- Comment mettre en place des directives (lignes de conduite / guidelines) et des réglementations (policies) en matière d'utilisation des TIC

SÉCURITÉ PERSONNELLE DES FICHIERS

- Comprendre le terme : ingénierie sociale (social engineering) et ses implications comme : la collecte d'informations, la fraude, l'accès au système informatique
- Comprendre les effets de l'activation / la désactivation des macros dans les options de sécurité des applications
- Utiliser un mot de passe pour les fichiers comme : les documents, les fichiers compressés, les classeurs / feuilles de calculs
- Comprendre les avantages et les limites du cryptage des données

SÉCURISER ET SAUVEGARDER LES DONNÉES

- Connaître les méthodes pour s'assurer de la sécurité physique des dispositifs numériques mobiles
- Connaître l'importance de maîtriser la procédure de sauvegarde (backup) en cas de perte de

fichiers, de données comptables, d'historique de navigation et de signets
- Identifier les paramètres d'une procédure de sauvegarde
- Sauvegarder des données

DESTRUCTION DES DONNEES SECURISEE

- Savoir détruire de manière définitive des données qui se trouvent dans un lecteur ou dans un dispositif numérique mobile
- Connaître la différence entre un effacement et une totale destruction (définitive) de données
- Les méthodes habituelles de suppression définitive de données