CYBER SECURITE

PUBLIC
Toute personne utilisant un ordinateur

OBJECTIFS
Définir la cybersécurité et son importance.
Présenter les principaux concepts et termes.
Comprendre les concepts de base de la cybersécurité.
Connaître les menaces courantes et comment les identifier.
Apprendre des pratiques sécuritaires pour protéger les informations personnelles et professionnelles.
Acquérir des compétences pratiques pour renforcer la sécurité des systèmes et des réseaux.

PRE-REQUIS
Aucun

POSITIONNEMENT
Aucun

DUREE
Durée : 0.5 jours

LIEU
Dijon ou Chalon-sur-Saône ou sur site

EVALUATION DES ACQUIS
Evaluation en fin de formation : Démonstration

Type de validation : Attestation de formation,

MOYENS PEDAGOGIQUES
- Cours théoriques, vidéos, démonstration pratiques
- Mise en situation
- Accompagnement sur site possible

NOMBRE DE STAGIAIRES / SESSION
Mini 1 / Maxi 10

PROGRAMME

1. Introduction à la Cybersécurité (30 minutes)
Définition et importance de la cybersécurité.
Les types de menaces (malware, phishing, ransomwares, etc.).
Usurpation d'identité, les faux sites, les faux sms, …
Les dénis de service
Les principes de base de la sécurité informatique (confidentialité, intégrité, disponibilité).

2. Menaces Courantes et Comment les Identifier (30 min)
Présentation des menaces courantes.
Exemples concrets d'attaques récentes.
Signes indicateurs d'une attaque (emails de phishing, comportements inhabituels des systèmes, etc.).
Différencier le personnel et le professionnel

3. Pratiques de Sécurité Quotidiennes (30 minutes)
Gestion des mots de passe (création de mots de passe forts, gestionnaires de mots de passe keepass par exemple).
Mise à jour régulière des logiciels.
Utilisation des antivirus et des pare-feu.
Importance des sauvegardes régulières.
Exercice sur la création de mots de passe forts.
Installation et utilisation d'un gestionnaire de mots de passe.

4. Sécurité des Réseaux (30 minutes)
Introduction aux concepts de base des réseaux (routeurs, pare-feu, VPN).
Importance et configuration des pare-feu.
Configuration sécurisée d'un routeur Wi-Fi (changement du mot de passe, configuration du pare-feu).

5. Reconnaissance et Réponse aux Incidents (30 minutes)
Les étapes d'une attaque (reconnaissance, accès, exploitation, maintien).
Plan de réponse aux incidents.
Contacter les autorités et les experts en sécurité.
Simulation d'une réponse à une attaque de phishing (analyse d'un email suspect, identification des signes, actions à prendre).

V1 -2024