

Intitulé du module :

Cybersécurité, sensibilisation

Contenu du programme

Module 1 - Introduction aux cybermenaces (1h) :

Panorama des menaces actuelles : phishing, ransomware, attaques par mot de passe, ingénierie sociale et hameçonnage ciblé. Quiz interactif "mythe ou réalité" pour déconstruire les idées reçues et sensibiliser le groupe. Construction collaborative d'une carte mentale des menaces par type et niveau de risque. Livrable : fiche mémo des 6 menaces principales et leurs signaux d'alerte.

Module 2 - Adopter les bonnes pratiques (1h30) :

Atelier mots de passe : unicité, robustesse, utilisation d'un gestionnaire (KeePass, Bitwarden). Exercice "Démasquer un faux mail" : analyser des e-mails suspects et identifier les indices de phishing. Navigation sécurisée : sites HTTPS, mises à jour automatiques, vigilance sur les réseaux Wi-Fi publics. Réflexes essentiels au quotidien pour réduire les risques d'intrusion.

Module 3 - Identifier et réagir aux intrusions (1h) :

Reconnaissance des signes d'une compromission : comportements anormaux, ralentissements, messages inhabituels. Procédure de réaction en 4 étapes : repérer, isoler, alerter, signaler auprès du référent sécurité. Jeu de rôle : simulation d'un incident cyber en équipe. Livrable : fiche réflexe "Que faire en cas d'incident cyber ?"

Module 4 - Enjeux des données sensibles (1h) :

Identification des données à protéger : personnelles, financières, stratégiques et confidentielles. Risques métiers : vol de données clients, atteinte à la réputation, sanctions RGPD jusqu'à 4 % du CA mondial. Exercice de cartographie des données sensibles de l'entreprise et construction d'une matrice de criticité par secteur d'activité.

Module 5 - Sécuriser son environnement numérique (1h30) :

Outils essentiels : antivirus, pare-feu, chiffrement, mises à jour régulières. Règle des sauvegardes 3-2-1 (3 copies, 2 supports différents, 1 copie hors site). Gestion des droits d'accès et principe du moindre privilège. Sécurité mobile et politique BYOD. Audit pratique du poste de travail et vérification des paramètres de sécurité.

Objectifs pédagogiques

Ce module vise à fournir aux salariés une compréhension claire et opérationnelle des enjeux de cybersécurité dans leur quotidien professionnel. Il s'agit d'identifier les principales cybermenaces, d'adopter les bons réflexes de prévention et de réaction, de protéger les données sensibles et de contribuer à la sécurité numérique collective de l'entreprise.

Public visé

Salariés utilisant mails, Internet ou logiciels au quotidien, tous secteurs confondus. Toute personne souhaitant renforcer sa vigilance face aux risques cyber essentiels dans l'environnement professionnel.

Prérequis

Aucun prérequis technique. Avoir une utilisation régulière d'un poste informatique et d'un réseau dans le cadre de son activité professionnelle.

Modalités pédagogiques

Les formations s'appuient sur des méthodes pédagogiques actives, centrées sur l'apprenant et ancrées dans la réalité des TPE/PME. Alternance d'apports théoriques, d'ateliers pratiques, de mises en situation et de cas concrets. Échanges de pratiques, travail en sous-groupes et accompagnement personnalisé tout au long du parcours.

Durée de formation en heures et en jours

7 heures soit 1 jour

www.formasup.com

pedagogie@formasup.com

05.63.20.10.00