SENSIBILISATION CYBERSÉCURITÉ

Durée
3.50 heures (0.5 jour)

Profils des apprenants
- Salariés utilisant des outils numériques dans le cadre de leur activité professionnelle.
- Collaborateurs administratifs, commerciaux, RH, managers ou équipes terrain connectées.
- Toute personne souhaitant renforcer ses réflexes en cybersécurité.

Prérequis
- Aucun niveau technique en cybersécurité n'est requis.
- Utilisation régulière d'un ordinateur, d'une messagerie ou d'un smartphone professionnel recommandée.

Processus :
Recueil de besoin, validation prérequis, devis/convention, convocation. Pour toute inscription contacter notre service commercial sur contact@axio-protech.com. Délai d'accès: 3 semaines. Personnalisation via DUERP/consignes site.

Modalités d'accès aux personnes en situation de handicap :
Pour les personnes en situation de handicap, nous étudions les actions que nous pouvons mettre en place pour favoriser leur apprentissage à travers un questionnaire avant formation. Nous nous appuyons également sur un réseau de partenaires locaux.
Contact référent handicap: maud.hoffmann@axio-formation.com.

Qualité et indicateurs de résultats :
Taux de présence VS taux d'abandon, taux de satisfaction à chaud et à froid, taux de réussite à l'évaluation finale.

OBJECTIFS PÉDAGOGIQUES.

- Identifier les principales cybermenaces rencontrées en entreprise.
- Repérer les signes d'une tentative de phishing ou d'ingénierie sociale.
- Appliquer les bonnes pratiques de sécurisation des accès et des données.
- Adopter les bons réflexes face à un incident ou une suspicion d'attaque.
- Contribuer à la prévention des risques numériques dans leur environnement professionnel.

CONTENU DE LA FORMATION.

1. Comprendre les enjeux de la cybersécurité

- Définition et enjeux pour les entreprises.
- Conséquences d'une cyberattaque : financières, opérationnelles, juridiques et réputationnelles.
- Panorama des cybermenaces actuelles.
- Les principales menaces numériques :
  - Phishing et spear phishing.
  - Ransomwares.
  - Usurpation d'identité.
  - Ingénierie sociale.
  - Fuites de données.
  - Arnaques au président et fraudes au virement.
- Comportements à risque les plus fréquents.
- Impact des mauvaises pratiques en entreprise.
- Importance de la vigilance collective.

2. Identifier les tentatives de phishing et les comportements frauduleux

- Reconnaître un e-mail frauduleux
  - Analyse d'un expéditeur suspect.
  - Détection des liens dangereux.
  - Pièces jointes malveillantes.
  - Signes de manipulation psychologique : urgence, pression, menace, récompense.
- Identifier les techniques d'ingénierie sociale
  - Manipulation téléphonique.
  - Faux support informatique.
  - Faux fournisseurs ou partenaires.
  - Techniques utilisées sur les réseaux sociaux.
- Réagir correctement face à une tentative d'attaque
  - Vérifications à effectuer avant d'agir.
  - Procédures internes de signalement.
  - Réflexes à adopter en cas de doute.

3. Sécuriser ses accès et ses usages numériques

- Créer un mot de passe robuste.
- Éviter les erreurs fréquentes.
- Utiliser un gestionnaire de mots de passe.
- Comprendre l'intérêt de la double authentification (MFA).
- Utilisation sécurisée des clés USB et périphériques externes.
- Protection des données sensibles.
- Bonnes pratiques en télétravail et mobilité.
- Navigation sécurisée.
- Utilisation des réseaux Wi-Fi publics.
- Sécurité des smartphones professionnels.
- Gestion des accès et des droits utilisateurs.

4. Adopter les bons réflexes en cas d’incident

- Identifier les premiers signes d’un incident.
- Isoler et sécuriser le poste concerné.
- Alerter les interlocuteurs internes compétents.
- Éviter les actions aggravantes.
- Culture cybersécurité en entreprise.
- Mise en place de bonnes pratiques collectives.
- Élaboration d’un plan d’action individuel
- Identifier ses axes d’amélioration.
- Définir des engagements concrets applicables immédiatement.

ÉQUIPE PÉDAGOGIQUE.

Notre équipe pédagogique maîtrise l'ensemble des sujets proposés à la formation. Nous construisons nos programmes en identifiant les besoins en compétences des futurs apprenants et en collaboration avec nos experts métiers.

Pour tout besoin lié à la pédagogie, notre référente est Maud : maud.hoffmann@axio-formation.com (également référente handicap)
Pour tout besoin d'ordre administratif ou logistique, notre référente est Emilie : emilie.vannieuwenborg@axio-formation.com

Moyens pédagogiques et techniques

- **En présentiel :** -- Accueil des participants dans une salle dédiée à la formation ou en entreprise - Documents supports de formation projetés - Analyse d'exemples d'attaques et d'e-mails frauduleux - Etudes de cas concrets - Quizz et activités collectives en salle - Mise à disposition en ligne de documents supports à la suite de la formation
- **En distanciel :** - Classes virtuelles via l'interface Digiforma - Support de formation partagé - Activités d'entrainement en synchrone - Etudes de cas concrets - Messagerie instantanée permettant de dialoguer avec le formateur et les autres apprenants (si collectif)
- **En intra-entreprise**, les exemples et exercices peuvent être adaptés à l'environnement réel de l'entreprise : quais, zones d'attente, entrepôts, flux piétons/engins, organisation interne, protocole de sécurité et consignes spécifiques.

Dispositif de suivi de l'exécution de l'évaluation des résultats de la formation

- Feuilles d'émargement.
- Autoévaluation de positionnement en début et fin de formation.
- Exercices d'entraînement tout au long de la formation
- Questionnaire de satisfaction à chaud et à froid
- Remise d'une attestation de fin de formation
- Évaluation finale des acquis réalisée le jour de la formation, en fin de session, permettant de vérifier la capacité des participants à identifier les cybermenaces, détecter une tentative de phishing et appliquer les bonnes pratiques de sécurité numérique.
- L'évaluation finale comprend : - Une étude de cas ou mise en situation professionnelle ou l'analyse d'un e-mail frauduleux ou d'un scénario d'attaque.
- Cette formation ne constitue pas une autorisation de conduite ni une habilitation réglementaire. L'organisme Axio PROTECH forme et évalue les participants dans le cadre de mises en situation pédagogiques. L'employeur reste responsable de l'application des procédures internes, des autorisations nécessaires et des conditions de sécurité sur le site.