Les fondamentaux de la cybersécurité au bénéfice des opérationnels, personnel de terrain

Description

Dans un contexte où les cyberattaques touchent de plus en plus le secteur social et médico-social, la sécurisation des systèmes d'information et la protection des données sensibles deviennent des enjeux majeurs pour les établissements ou services sociaux ou médico-sociaux.

Cette formation a été conçue pour permettre au personnel oeuvrant sur le terrain, de développer une vision globale des enjeux de la cybersécurité, adaptée aux spécificités de leur activité.

Prérequis

Cette formation ne nécessite aucun prérequis, mais il est préconisé d'avoir suivi une formation au RGPD préalablement

Objectifs

- Maîtriser l'écosystème de la cybersécurité en appréhendant ses enjeux et ses acteurs
- Adopter les bons réflexes pour anticiper les cybermenaces et gérer les crises en toute sérénité
- Assurer son rôle de partie prenante dans l'organisation déployée pour la gestion d'une crise de cybersécurité
- Appliquer les mesures de continuité d'activité afin d'assurer la prise en charge des personnes à domicile
  en situation dégradée
- Gérer la reprise des activités métiers en fin de situation dégradée

Contenu

Première demi-journée :

PARTIE 1 : APPRÉHENDER LE CONTEXTE ET LES ENJEUX DE LA CYBERSÉCURITÉ DANS LE SECTEUR SOCIAL ET MÉDICO-SOCIAL

- Identifier les enjeux de la cybersécurité dans le secteur de la santé
- Reconnaître les risques spécifiques liés à l'activité du secteur social et médico-social
- Analyser les impacts des cyberattaques sur l'activité, l'organisation et sa direction
- Réaliser un focus sur les enjeux pour les activités d'aide et de soin à domicile

PARTIE 2 : DÉCRIRE L'ÉCOSYSTÈME DE LA CYBERSÉCURITÉ, SA RÈGLEMENTATION ET SON FINANCEMENT

- Gouvernance de la cybersécurité au niveau international et national : les acteurs institutionnels et leurs rôles

- Organisation des groupes d'attaquants et types d'attaques
- Notions sur l'environnement règlementaire et normatif (RGPD, Directive NIS II, Certification ISO 27001) et sur les programmes de financement de la cybersécurité

Deuxième demi-journée :

PARTIE 3 : SÉCURISER SON ACTIVITÉ ET PROTÉGER LES DONNÉES DES USAGERS

- Typologie des incidents courants dans les établissements et services sociaux et médico-sociaux

- Principes de base et bonnes pratiques de sécurité numérique :
  - » Sécurisation des équipements (smartphone, tablette, PC)
  - » Gestion des mots de passe et authentification
  - » Hameçonnage (phishing) : détecter et éviter les pièges
  - » Protéger les données des personnes accompagnées
  - » Sécuriser les échanges et accès en mobilité (connexions Wi-Fi, messageries et outils numériques professionnels)

- Cas pratiques interactifs et mises en situation :
  - » Identification d'emails et SMS frauduleux
  - » Création de mots de passe robustes
  - » Assurer la sécurité des données sensibles en situation de mobilité

PARTIE 4 : RÉAGIR AUX INCIDENTS ET ASSURER LA CONTINUITÉ D'ACTIVITÉ

- Les bonnes pratiques en cas d'incident :
  - » Exemple : Matériel perdu ou volé : actions immédiates
  - » Exemple : Suspicion d'intrusion ou d'accès non autorisé
  - » Exemple : Réagir à un email ou message frauduleux
  - » Exemple : Fuite ou divulgation accidentelle de données

- Organisation en cas de crise : qui contacter et comment réagir ?
  - » Les bons réflexes pour alerter en interne
  - » Rôles et responsabilités dans la gestion de crise
  - » Bonnes pratiques de communication internes et externes
  - » Capitalisation sur les retours d'expérience de gestion de crise

- Les principes de continuité et de reprise d'activité en cas de cyberattaque ou panne informatique :
  - » Identification des services essentiels
  - » Définition du mode de fonctionnement des services sans outils numériques (mode dégradé)
  - » Reprise des données dans les outils au retour à la normale Maintien à jour et amélioration continue des principes de continuité et de reprise d'activité.

- Cas pratiques interactifs et mises en situation :
  - » Cas pratique : Adopter les premiers réflexes en cas d'incident
  - » Simulation : Une cyberattaque bloque l'accès aux outils numériques, comment continuer à

assurer les soins et la prise en charge ?
» Cas pratique : Adopter les bonnes pratiques d'alerte et de communication.

Méthodes pédagogiques

Les activités sont conçues pour alterner entre différentes méthodes pédagogiques en partant des besoins des participants :

- Méthode expositive : *support, textes de références, vidéos etc.*
- *Méthode interrogative : quizz, questionnements à l'oral etc.*
- *Méthode active : brainstorming, activité ludiques, jeux de rôles, études de cas, exercices pratiques etc.*
- *Méthode expérientielle : analyse de pratiques, débriefing, mise en commun, débat etc.*
- *Méthode démonstrative : simulation, démonstration par le(la) formateur(rice) si besoin*

Évaluation de la formation

Tout au long de la formation, le formateur réalise une évaluation formative via des questionnements, des exercices d'application et des études de cas. A la fin de la formation, une évaluation sommative est réalisée pour valider les acquis et l'atteinte des objectifs par le stagiaire.

Durée : 7 heures de formation en distanciel réparties sur 2 semaines (2 séances de 3,5 heures)
Intervenants : Consultant et formateur en SI de Santé
Publics : intervenants métiers de terrain (Infirmiers, aides-soignants, personnels de l'aide à domicile), accompagnant les usagers à domicile

Date des formations

- Nous contacter pour les dates