FORMATION

BONNES PRATIQUES ET DÉTECTION DES RISQUES CYBER EN ÉTABLISSEMENT DE SANTÉ

Format d'intervention

En présentiel ou à distance

Mode d'intervention

Intra Inter

Votre secteur d'activité

S Sanitaire M Médico-Social

Vous êtes

Médecin, cadre de santé, secrétaire médicale, agent administratif ou tout autre utilisateur du système d'information et vous êtes amené à échanger avec des organisations et des personnes tierces à l'E.S.

Date et lieu

Pour l'inter : information disponible sur le site
Pour l'intra : sur demande

- 1/2 jour : 09h00-12h30

Tarifs

Devis sur demande

Référence LY133

PRÉSENTATION

Avec des attaques cyber de plus en plus fréquentes, il est essentiel que votre personnel soit sensibilisé et informé sur les risques numériques et leurs impacts.

L'objectif est d'instaurer une culture de cybersécurité, afin de réduire les risques associés au facteur humain et de contribuer à la sécurisation des systèmes d'information et à la protection des données patients.

OBJECTIFS PÉDAGOGIQUES

- **Identifier** les risques de malveillance cyber et leur impact sur les établissements de santé
- **Repérer** les situations à risque pour anticiper les menaces.
- **Adopter** les comportements et mesures d'évitement adéquats.
- **Corriger** les conséquences d'une erreur d'interprétation pour limiter les impacts.

PRÉREQUIS

Cette formation ne nécessite pas de prérequis.

INTERVENANT

Cette formation est animée par un(e) consultant(e) spécialisé(e) en management des risques technologiques.

MÉTHODE PÉDAGOGIQUE

Alternance d'apports théoriques, retours d'expérience et mises en situation.

PROGRAMME

1. Introduction et présentation

2. Contexte & Notions clés

- Vocabulaire
- Chiffres clés de la cyber malveillance pour le secteur de la santé
- Exemples de cyber attaques et de leurs impacts sur les activités

3. Comprendre la menace

- Les typologies de la menace, leurs motivation et modes opératoires

4. Une défense à plusieurs niveaux

- A l'échelle nationale : le cadre réglementaire
- A l'échelle de l'établissement : les équipes et les outils

5. L'utilisateur, le rempart ultime

- Le rôle de l'utilisateur et l'hygiène informatique quotidienne
- Les bons réflexes en cas d'erreur
- Mise en situation & jeu de rôle pour valider les connaissances acquises
- Rappel des notions clés et présentation de la fiche des « 10 règles d'Or du Cyber champion »

6. Conclusion

- Session de questions/réponses
- Bilan de la formation & retour à chaud
- Ressources additionnelles pour aller plus loin

EVALUATION

Tout au long de la formation des exercices ou des quiz permettent d'évaluer l'acquisition des connaissances et des compétences et l'atteinte des objectifs
Une évaluation de la satisfaction des participants est recueillie en fin de formation

Je demande un devis

formation.santesocial@relyens.eu

+33 (0)4 72 75 50 15

Relyens Mutual Insurance
18 rue Edouard Rochet - 69372 LYON Cedex 08 - FRANCE
Tél : +33 (0)4 72 75 50 25 - www.relyens.eu

Société d'Assurance Mutuelle à cotisations fixes
Entreprise régie par le code des assurances - 779 860 881 RCS Lyon
Organisme de formation professionnelle déclaré sous le n° 82690051369 auprès du Préfet de région
N°TVA Intracommunautaire : FR 79779860881

Mise à jour juillet 2025 – tous droits réservés