Revisium

Fiche pédagogique

CYBERSÉCURITÉ DE BASE

Débuter en cybersécurité et acquérir les connaissances de base non-technique afin de comprendre et intervenir efficacement

PRÉSENTATION DE LA FORMATION

La cybersécurité est un élément incontournable pour toutes les organisations. Toutefois, il est important de signaler que cette formation n'est pas technique. Elle est destinée aux personnes décisionnaires qui ont besoin de comprendre et superviser les travaux de sécurité numérique au quotidien, mais aussi à tout utilisateur d'un ordinateur dans une organisation. La seconde partie de la formation est centrée sur l'identification des menaces, les réactions de chacun et surtout la mise en oeuvre de bonnes pratiques pour limiter les risques de cyberattaque.

OBJECTIFS PÉDAGOGIQUES

- Prendre conscience des enjeux et des risques
- Connaitre les acteurs et les ressources à disposition
- Comprendre les menaces et savoir réagir
- Mettre en oeuvre les bonnes pratiques au quotidien

MOYENS & MÉTHODES

- Documents pédagogiques
- Cahier d'exercices pratiques
- Exercices pratiques en ligne
- Nécessite un ordinateur

PUBLIC & PRE-REQUIS

- Public concerné : tout public accédant à un ordinateur dans son organisation
- Pré-requis : aucun

MODALITÉS D'ÉVALUATION

- Quiz & auto-évaluations
- Test fin de parcours
- Certificat de réalisation

TARIFS & NB DE PARTICIPANTS

- Participants : 2 à 10 maximum
- Tarif par personne : 1860 €

DÉLAIS & DURÉE

- En distanciel
- En présentiel (entreprise)
- Durée : 14 heures (2j)

Calendrier de sessions joint

CONTACT (inscriptions et handicap)

SCHOETTEL Audrey / audrey.schoettel@revisium.fr / 0 805 035 135

CYBERSÉCURITÉ DE BASE

Débuter en cybersécurité et acquérir les connaissances de base non-technique afin de comprendre et intervenir efficacement

PROGRAMME DE LA FORMATION

Module 1 : Introduction à la cybersécurité

✓ Présentation des concepts en cybersécurité
✓ Qu'est-ce que la cryptographie ?
✓ Zoom sur la cybercriminalité (exemples concrets)

Module 2 : Règlementation et acteurs de la cybersécurité

✓ Réglementation : le RGPD et le risque juridique
✓ Réglementation : le RGPD et la cybersécurité
✓ Présentation des acteurs publics en cybersécurité
✓ Les plateformes numériques à disposition du public

Module 3 : les risques identifiés

✓ Les risques de sécurité pour le site
✓ Les risques de sécurité pour les réseaux sociaux
✓ Les risques de sécurité pour les emails
✓ Risque comportemental contre risque information
✓ Les faiblesses du comportement humain

Module 4 : Les principales menaces

✓ Exploration des menaces courantes
✓ Les malwares (logiciels malveillants)
✓ Le phishing (hameçonnage)
✓ Le Smishing
✓ Les virus et les vers
✓ Le rançongiciel
✓ L'ingénierie sociale
✓ Le vol de données
✓ Le vol d'identité
✓ L'espionnage
✓ Le spam ou mail frauduleux (lien malveillant)
✓ Le bot
✓ Le sabotage informatique

CYBERSÉCURITÉ DE BASE

Débuter en cybersécurité et acquérir les connaissances de base non-technique afin de comprendre et intervenir efficacement

PROGRAMME DE LA FORMATION

Module 5 : Les protections disponibles

- ✓ Les logiciels et applications vérifiées
- ✓ La gestion des vulnérabilités
- ✓ La gestion de l'authentification et des contrôles d'accès
- ✓ La cryptographie
- ✓ Les protocoles sécurisés (https, certificat SSL…)
- ✓ La méfiance face aux messages inattendues
- ✓ Renforcer les procédures de règlement
- ✓ Ne pas relayer les informations sans les avoir vérifiées
- ✓ Eviter de se connecter aux réseaux wifi publics et non sécurisés

Module 6 : les bonnes pratiques

- ✓ Les mises à jour
- ✓ Les antivirus
- ✓ Les mots de passe robustes
- ✓ Les sauvegardes
- ✓ L'internet des objets connectés
- ✓ La formation continue
- ✓ Adopter une bonne hygiène informatique renforcée
- ✓ Sécuriser les éléments qui peuvent sortir (cryptographie)
- ✓ Ne pas relayer les informations sans les avoir vérifiées
- ✓ Séparer les usages professionnels des usages personnels (télétravail)