Programme de Formation

Renforcer la cybersécurité au travail et à domicile

Organisation

Début : **Fin :** **Durée :** 7 heures

Mode d'organisation : Mixte

Contenu pédagogique

Public visé

- Administrateurs
- Employés de mutuelle
- Responsables de la sécurité informatique
- Responsables des ressources humaines (RH)
- Directeurs des opérations
- Responsables de la conformité
- Responsables de la communication interne
- Responsables de la gestion des crises

Objectifs pédagogiques

Les risques cybers se développent et évoluent à un rythme alarmant dans notre monde de plus en plus connecté. Réalité incontournable du quotidien personnel et professionnel, cette formation opérationnelle fait le point sur les nouvelles pratiques de la cyber criminalité, allant des attaques de phishing sophistiquées aux ransomwares dévastateurs.

L'objectif est de donner des clefs de compréhension concrètes et en lien avec l'actualité pour savoir comment réagir aux différentes situations, toujours du point de vue de l'utilisateur final non spécialiste.

Que vous soyez un employé d'entreprise, un entrepreneur indépendant ou un particulier soucieux de sa sécurité en ligne, cette formation vous équipera des connaissances essentielles pour naviguer en toute sécurité dans le cyberespace.

- Comprendre les principaux types d'attaques cyber et leurs évolutions, incluant les dernières techniques de social engineering, les attaques par déni de service distribué (DDoS), et les menaces persistantes avancées (APT).
- Analyser les conséquences d'une attaque cyber sur les entreprises et les individus, en examinant des études de cas réels et leurs impacts financiers, réputationnels et opérationnels.
- Identifier les bonnes pratiques pour se prémunir des attaques, telles que l'utilisation de mots de passe forts, l'authentification à deux facteurs, la mise à jour régulière des logiciels, et la sauvegarde sécurisée des données.
- Développer une culture cyber efficace au sein de votre organisation ou de votre foyer, en promouvant la vigilance, la formation continue et la communication ouverte sur les menaces potentielles.
- Apprendre à reconnaître les signes d'une attaque en cours et les étapes immédiates à suivre pour minimiser les dommages.

- Explorer les ressources et outils disponibles pour renforcer votre sécurité en ligne, y compris les logiciels antivirus, les gestionnaires de mots de passe et les VPN.

Description

1. **Introduction à la Cybersécurité**
- Présentation des objectifs de la journée
- Importance de la cybersécurité dans le contexte actuel

2. **Panorama de la Sécurité des Systèmes d'Information (SSI)**
- Aperçu des différents types de menaces et risques numériques
- Exemples d'attaques récentes et de leurs conséquences

3. **Sécurisation des accès et authentification**
- Sécurité de l'authentification
- Discussions sur les meilleures pratiques et outils d'authentification
- Importance de la culture de sécurité dans l'entreprise

4. **Sécuriser son poste de travail**
- Sécurité du poste de travail et nomadisme
- Bonnes pratiques pour les employés en télétravail
- Exercice pratique sur l'identification des menaces

5. **Sécurité sur internet et nouveaux risques**
- Contenus de sécurité sur internet
- Types d'attaques et évolutions des pratiques
- Que faire face à un phishing ?

6. **Analyse des conséquences des attaques**
- Coûts et conséquences non financières d'une attaque
- Études de cas d'attaques célèbres et leurs impacts

7. **Principes de défense et bonnes pratiques**
- Défenses techniques et astuces pour se prémunir des cybermenaces
- Rappel des principales notions de cybersécurité et bonnes pratiques

8. **Conclusion et résumé des principales idées**
- Résumé des 4 principales idées à retenir
- Importance de la culture cyber au sein des entreprises
- Questions et discussions ouvertes entre participants

Prérequis

Aucun prérequis nécessaire.

Modalités pédagogiques

- **Apports théoriques :** présentation des concepts clés, modèles et méthodologies par des experts du domaine. Utilisation de supports visuels et d'exemples concrets pour faciliter la compréhension.
- **Échanges et discussions :** sessions interactives permettant aux participants de partager leurs expériences, poser des questions et débattre des enjeux actuels. Animation de tables rondes et de groupes de réflexion pour favoriser l'apprentissage collaboratif.
- **Études de cas :** analyse approfondie de situations réelles ou fictives pertinentes au domaine d'étude. Travail en petits groupes pour développer des solutions et stratégies, suivi de présentations et de feedback constructif.
- **Exercices pratiques :** mise en application des connaissances acquises à travers des simulations,

jeux de rôles, et projets concrets. Utilisation d'outils et de technologies spécifiques au domaine pour renforcer les compétences pratiques des participants.

Moyens et supports pédagogiques

- **Support de formation numérique :** Plateforme d'accès aux modules de cours, quiz d'auto-évaluation, ressources téléchargeables (PDF, infographies)
- **Études de cas :** Analyses approfondies de situations réelles, scénarios complexes à résoudre en groupe, retours d'expérience d'entreprises, exercices de mise en pratique basés sur des cas concrets
- **Supports numériques :** Présentations multimédias, tableaux blancs virtuels, outils de collaboration en ligne.
- **Discussions et échanges :** Sessions de questions-réponses en direct.

Modalités d'évaluation et de suivi

L'évaluation sera continue avec des questions, discussions, exercices pratiques et études de cas pour vérifier l'application des connaissances. Une synthèse et un feedback en fin de formation mesureront les acquis et la réalisation des objectifs pédagogiques. Un Certificat de Réalisation signé par le Responsable de l'organisme de formation et mentionnant les compétences visées est remis au participant à la fin de la formation. Le contenu de ce document atteste la mise en œuvre du processus d'évaluation.

La présente formation, dans sa configuration actuelle, n'a pas encore fait l'objet d'une évaluation formelle en termes de taux de satisfaction et de pourcentage de réussite des participants.

Informations sur l'admission

Inscriptions : Les pré-inscriptions se font en ligne sur notre site web, via l'extranet Entreprise ou par mail à formation@ugm-opera.fr jusqu'à trois semaines avant le début de la formation. en inter.

Pour les demandes en Intra, un délai de prévenance de minimum 6 semaines avant la date de formation souhaitée est requis.

Les places sont attribuées par ordre d'inscription et sous réserve d'un nombre de participants minimum et de dossier administratif complet.

Conditions d'Annulation : Les annulations sont possibles jusqu'à 15 jours avant le début de la formation avec remboursement intégral. Passé ce délai, un pourcentage des frais de formation sera retenu.

Informations sur l'accessibilité

Nos locaux ne sont malheureusement pas accessibles aux personnes à mobilité réduite.

Cependant, un soutien personnalisé peut être mis en place pour les participants ayant des besoins spécifiques.

Si vous avez des contraintes particulières liées à une situation de handicap, nous vous invitons à nous contacter en amont afin que nous puissions, dans la mesure du possible, adapter la formation.

Vous pouvez exprimer vos besoins spécifiques en nous écrivant à l'adresse handicap@ugm-opera.fr