FORMATION
CYBERSÉCURITÉ

Connaître les bons gestes pour se protéger contre les cybermenaces

OBJECTIF DE LA FORMATION

Maîtriser les techniques de la cybersécurité afin d'assurer à vos collaborateurs une protection optimale contre les cybermenaces.

Les cyberattaques se développent dangereusement et menacent les entreprises et la sécurité de leurs systèmes d'informations (ou SSI). Aujourd'hui, les entreprises et organisations se doivent de se protéger contre les pirates informatiques. Ces derniers redoublent d'astuces pour s'introduire dans l'entreprise et exploiter tout ce qui est à leur portée, en particulier ces derniers temps avec le télétravail et le nomadisme.

Cette formation vous aide à développer une culture interne "cybersécurité" et permet à vos collaborateurs d'acquérir les bonnes pratiques SSI. Nous vous proposons un éclairage sur les techniques permettant d'élever le niveau de protection des données et de se prémunir contre les attaques.

À l'issu de ce parcours, vous serez capable de :

- Connaître l'environnement global de la SSI
- Protéger votre cyberespace
- Sécuriser et gérer vos mots de passe
- Connaître les différentes techniques de cyberattaques
- Éviter une cybermenace
- Naviguer en toute sécurité sur le web et vos réseaux informatique

CONTENU

- PANORAMA DE LA SSI
- SÉCURITÉ DE L'AUTHENTIFICATION
- SÉCURITÉ SUR INTERNET
- SÉCURITÉ DU POSTE DE TRAVAIL ET NOMADISME

PRÉ-REQUIS

• Aucune expérience requise

PUBLIC VISÉ

• Toute entreprise désirant sensibiliser ses collaborateurs aux cybermenaces et ainsi protéger les données de tous.

MODALITÉS D'ADMISSION

Aucune.

MODALITÉS PÉDAGOGIQUES

➜ Test d'évaluation d'entrée - Test d'évaluation après chaque module terminé - Test final

➜ Support de cours projeté via un vidéoprojecteur

➜ Exercices d'application et mises en situation

➜ Débriefing en fin de stage

\+ Accès pendant 12 mois illimité à la plateforme de cours - 24h/24 et 7j/7 pour davantage de théorie et de rappels fréquents

LOCALISATION & ACCESSIBILITÉ

• Nous formons en présentiel et en visioconférence sur toute la France

• Nos méthodes pédagogiques et nos modalités d'évaluation sont adaptables au public en situation de handicap

DURÉE DE LA FORMATION

De 3 à 6 jours maximum selon les besoins

MODALITÉS D'ÉVALUATION

Test QCM en fin de stage.

L'évaluation se fera en visioconférence ou en présentiel sous la surveillance d'un formateur ou d'un membre de l'équipe pédagogique.

Durée de l'épreuve : 30 à 45min

+ SUITE EN BAS : PROGRAMME DE FORMATION

PROGRAMME DE FORMATION

MODULE 1
Panorama de la SSI

THÈME 1 : Un monde numérique hyper-connecté

Contenu du thème :

- Une diversité d'équipement et de technologies
- Le cyberespace, nouvel espace de vie
- Un espace de non-droits ?

THÈME 2 : Un monde à hauts risques

Contenu du thème :

- Qui me menace et comment ?
- Les attaques de masse
- Les attaques ciblées
- Les différents types de menaces
- Plusieurs sources de motivation
- Les conséquences pour les victimes de cyberattaques
- Conclusion

THÈME 3 : Les acteurs de la cybersécurité

Contenu du thème :

- Le livre blanc pour la défense et la sécurité nationale
- La stratégie nationale pour la sécurité du numérique
- L'ANSSI
- Autres acteurs de la cybersécurité
- D'autres experts pour m'aider
- Conclusion

THÈME 4 : Protéger les cyberespace

Contenu du thème :

- Les règles d'or de la sécurité
- Choisir ses mots de passe
- Mettre à jour régulièrement ses logiciels
- Bien connaître ses utilisateurs et ses prestataires
- Effectuer des sauvegardes régulières
- Sécuriser l'accès Wi-fi de son entreprise ou son domicile
- Être prudent avec son smartphone ou sa tablette
- Protéger ses données lors de ses déplacements
- Être prudent lors de l'utilisation de sa messagerie
- Télécharger ses programmes sur les sites officiels des éditeurs
- Être vigilant lors d'un paiement sur Internet
- Séparer les usages personnels et professionnels
- Prendre soin de ses informations et de son identité numérique
- Conclusion

THÈME 5 : Mon rôle dans la sécurité numérique

Contenu du thème :

- Introduction
- Les données
- Risques sur les données
- Protéger les données
- Responsabilités face aux risques

MODULE 2
Sécurité de l'authentification

THÈME 1 : Principes de l'authentification

Contenu du thème :

- Introduction
- Objectif de l'authentification
- Facteurs d'authentification
- Les types d'authentification
- Limites des facteurs d'authentification
- Les risques liés aux mots de passe

THÈME 2 : Attaques sur les mots de passe

Contenu du thème :

- Introduction
- Les attaques directes
- Les attaques indirectes
- Conclusion

THÈME 3 : Sécuriser ses mots de passe

Contenu du thème :

- Introduction
- Un bon mot de passe
- Comment mémoriser un mot de passe fort ?
- Comment éviter la divulgation de mot de passe ?
- Conclusion

THÈME 4 : Gérer ses mots de passe

Contenu du thème :

- Introduction
- Gérer la multiplication des mots de passe
- Configurer les logiciels manipulant les mots de passe
- Transmettre des mots de passe sur le réseau
- Conclusion

THÈME 5 : Notion de cryptographie

Contenu du thème :

- Introduction
- Principe général
- Chiffrement symétrique
- Chiffrement asymétrique
- Signature électronique, certificats et IGC
- Conclusion

PROGRAMME DE FORMATION

MODULE 3
Sécurité sur internet

THÈME 1 : Internet : de quoi s'agit-il ?

Contenu du thème :

- Introduction
- Internet schématisé
- Cyber-malveillance
- Ingénierie sociale
- Contre-mesures possibles
- En cas d'incident
- Réseaux sociaux
- Conclusion

THÈME 2 : Les fichiers en provenance d'internet

Contenu du thème :

- Introduction
- Les formats et les extensions d'un fichier
- Y a-t-il des formats plus risqués que d'autres ?
- Y a-t-il des sources plus sûres que d'autres ?
- J'ai déjà eu recours à une pratique déconseillée sans aucun problème
- Se protéger des rançongiciels
- Conclusion

THÈME 3 : La navigation Web

Contenu du thème :

- Introduction
- Comment fonctionne concrêtement un navigateur ?
- Vous avez dit "typosquatting" ?
- Le moteur de recherche, la porte d'entrée du web
- Et les "cookies" alors ?
- Le navigateur bienveillant pour la santé de votre ordinateur
- Le contrôle parental
- Conclusion

THÈME 4 : La messagerie électronique

Contenu du thème :

- Introduction
- Présentation
- Panorama des menaces
- Bonnes pratiques de messagerie
- Les clients de messagerie
- Les messageries instantanées
- Cas particuliers

THÈME 5 : L'envers du décor d'une connexion Web

Contenu du thème :

- Introduction
- Fonctionnement basique d'une connexion web
- Utilisation d'un serveur mandataire
- HTTPS et les certificats
- Conclusion

MODULE 4
Sécurité du poste de travail et nomadisme

THÈME 1 : Application et mises à jour

Contenu du thème :

- Introduction
- Concept de vulnérabilité en sécurité informatique
- Mise à jour
- Installation d'applications

THÈME 2 : Options de configuration de base

Contenu du thème :

- Premier démarrage
- Déverrouillage et authentification
- Logiciels de sécurité
- Recommandations spécifiques aux terminaux mobiles
- Données spécifiques aux terminaux mobiles
- Chiffrement de l'appareil
- Conclusion

THÈME 3 : Configurations complémentaires

Contenu du thème :

- Introduction
- Gestion de base des comptes utilisateurs
- Gestion avancée des comptes utilisateurs
- Sauvegarde et connexion de l'appareil
- Conclusion

THÈME 4 : Sécurité des périphériques amovibles

Contenu du thème :

- Introduction
- Risques au branchement
- Chiffrement des périphériques de stockage amovible
- Durabilité
- Séparation des usages
- Effacement sécurisé
- Conclusion

THÈME 5 : Séparation des usages

Contenu du thème :

- Introduction
- Qu'est-ce que le mélange des usages ?
- Le danger du mélange des usages
- Étude de cas
- Bonnes pratiques
- Conclusion

INFORMATIONS COMPLÉMENTAIRES

DÉLAI D'ACCÈS

Le délai d'accès à la formation est d'environ 2 à 3 semaines après validation de votre dossier.

MODALITÉS DE FINANCEMENT

- ➜ OPCO
- ➜ La Région
- ➜ L'Entreprise
- ➜ Autofinancement
- ➜ Pôle Emploi

TARIFS

Demandez votre devis sur-mesure.

Mise à jour Octobre 2023

infos@afformation.fr
04 51 00 93 51