

CYBERSÉCURITÉ

DURÉE TOTALE : 26H

PRÉREQUIS :

Avoir des connaissances de l'environnement Windows ou Macintosh.

PROGRAMMES DÉTAILLÉS

PANORAMA DE LA SSI

Unité 1 - Un monde numérique hyper-connecté

- Une diversité d'équipements et de technologies.
- Le cyberspace, nouvel espace de vie
- Un espace de non-droits ?

Unité 2 - Un monde à hauts risques

- 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

Unité 3 - Les acteurs de la cybersécurité

- 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

Unité 4 - Protéger le cyberspace

- 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

OBJECTIFS DE LA FORMATION :

Cette formation Cybersécurité vous permettra, en 125 modules, de vous sensibiliser et vous initier à la cybersécurité ; quel que soit votre niveau, apprenez et assimilez des notions de base de la SSI utiles au travail comme à la maison.

• 125 modules répartis en 4 domaines de 5 unités chacun

- Prendre soin de ses informations et de son identité numérique
- Conclusion

Unité 5 - Mon rôle dans la sécurité numérique

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

SÉCURITÉ DE L'AUTHENTIFICATION

Unité 1 - Principes de l'authentification

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

Unité 2 - Attaques sur les mots de passe

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

Unité 3 - Sécuriser ses mots de passe

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

Unité 4 - Gérer ses mots de passe

- 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

Unité 5 - Notions de cryptographie

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

SÉCURITÉ SUR INTERNET

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

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

Unité 2 - Les fichiers en provenance d'Internet

- 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

Unité 3 - La navigation Web

- Introduction
- Comment fonctionne concrètement 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

Unité 4 - La messagerie électronique

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

Unité 5 - L'envers du décor d'une connexion Web

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



SÉCURITÉ DU POSTE DE TRAVAIL ET NOMADISME

Unité 1 - Applications et mises à jour

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

Unité 2 - Options de configuration de base

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

Unité 3 - Configurations complémentaires

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

Unité 4 - Sécurité des périphériques amovibles

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

Unité 5 - Séparation des usages

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



SCANNER POUR EN SAVOIR PLUS SUR LES FORMATIONS