

Compte rendu : Mission 10

Noah Ripert ISI0B

Module 3 : Sécurité sur Internet

UNITÉ 1 :

Internet : de quoi s'agit-il ? : Cette unité explore en profondeur le concept d'Internet. Elle fournit probablement une compréhension approfondie des fondamentaux d'Internet.

UNITÉ 2 :

Les fichiers en provenance d'Internet : L'unité 2 met l'accent sur les fichiers provenant d'Internet, soulignant les précautions à prendre lors du téléchargement de fichiers pour assurer la sécurité.

UNITÉ 3 :

La navigation web : Cette unité aborde la navigation web, mettant en lumière les bonnes pratiques pour une expérience de navigation sécurisée.

UNITÉ 4 :

La messagerie électronique : L'unité 4 traite de la messagerie électronique et de ses enjeux de sécurité, en fournissant des conseils sur la gestion sécurisée des e-mails.

UNITÉ 5 :

L'envers du décor d'une connexion Web : La dernière unité se concentre sur l'envers du décor d'une connexion Web, offrant des informations sur les coulisses techniques de la navigation sur le Web.

En résumé, le Module 3 couvre divers aspects de la sécurité sur Internet, allant de la compréhension fondamentale d'Internet aux précautions liées au téléchargement de fichiers, à la navigation web, à la messagerie électronique et aux aspects techniques d'une connexion Web.

Module 4 : Sécurité du poste de travail et nomadisme

Le Module 4 comprend cinq unités, chacune abordant des aspects spécifiques de la sécurité du poste de travail et du nomadisme numérique.

UNITÉ 1 :

Applications et mises à jour : Cette unité souligne l'importance des applications et des mises à jour pour garantir la sécurité du poste de travail. Elle met en avant la nécessité de maintenir les logiciels à jour afin d'assurer une protection adéquate contre les menaces informatiques.

UNITÉ 2 :

Options de configuration de base : L'unité 2 se concentre sur les options de configuration de base, mettant en lumière les paramètres essentiels pour renforcer la sécurité du poste de travail. Elle aborde des ajustements fondamentaux visant à améliorer la posture de sécurité.

UNITÉ 3 :

Configurations complémentaires : Cette unité explore des configurations complémentaires pour renforcer la sécurité du poste de travail. Elle fournit des conseils sur des ajustements avancés visant à renforcer la résilience du système face aux menaces potentielles.

UNITÉ 4 :

Sécurité des périphériques amovibles : L'unité 4 examine la sécurité des périphériques amovibles, mettant en lumière les précautions à prendre lors de l'utilisation de ces dispositifs. Elle vise à sensibiliser aux risques associés à l'utilisation de périphériques externes et à promouvoir des pratiques sécurisées.

UNITÉ 5 :

Séparation des usages : L'unité 5 aborde la séparation des usages, soulignant l'importance de maintenir une distinction claire entre les activités personnelles et professionnelles sur un poste de travail. Elle met en avant des bonnes pratiques pour garantir une utilisation sécurisée et appropriée des ressources informatiques.

En résumé, le Module 4 offre une compréhension approfondie de la sécurité du poste de travail et du nomadisme numérique en couvrant des sujets allant des applications et mises à jour aux configurations avancées et à la gestion sécurisée des périphériques. Chaque unité contribue à la création d'un environnement de travail numérique sûr et efficace.

Définitions

Internet : Réseau mondial de communication permettant l'échange d'informations entre des ordinateurs connectés à travers le monde.

Téléchargement sécurisé : Processus d'obtention de fichiers depuis Internet tout en minimisant les risques de logiciels malveillants ou d'infections.

Navigation web sécurisée : Utilisation de bonnes pratiques pour garantir une expérience de navigation sans risques, en évitant les sites malveillants et en protégeant la vie privée en ligne.

Messagerie électronique sécurisée : Pratiques visant à protéger les e-mails contre les menaces telles que le phishing, les logiciels malveillants et la perte de données confidentielles.

Coulisses d'une connexion Web : Comprendre les aspects techniques sous-jacents à la navigation sur le Web, y compris les protocoles de communication et la sécurité des données.

Sécurité du poste de travail et nomadisme Mises à jour logicielles : Processus visant à maintenir les logiciels à jour pour remédier aux vulnérabilités de sécurité et bénéficier des dernières fonctionnalités.

Configuration de base : Définition des paramètres essentiels d'un poste de travail pour garantir une sécurité de base, y compris les pare-feux, les antivirus et les paramètres de connexion.

Sécurité des périphériques amovibles : Mesures de sécurité visant à protéger le système contre les menaces potentielles provenant de périphériques tels que clés USB et disques externes.

Séparation des usages : Pratique consistant à maintenir une distinction claire entre les activités personnelles et professionnelles sur un poste de travail pour renforcer la sécurité et la confidentialité.

Applications et mises à jour : Comprendre l'importance de maintenir à jour les applications pour garantir la sécurité et la stabilité du poste de travail.

Cybermalveillance : La cybermalveillance fait référence à des activités malveillantes menées à l'aide des technologies de l'information et de la communication, généralement dans le but de causer des dommages, de compromettre la sécurité des systèmes informatiques, ou d'exploiter des informations sensibles. Ces activités peuvent inclure des attaques telles que le vol de données, la propagation de logiciels malveillants, le phishing, le déni de service, et d'autres formes d'intrusions électroniques. La cybermalveillance vise à exploiter les vulnérabilités des systèmes informatiques, des réseaux, ou des utilisateurs pour des gains malveillants. La prévention et la réponse efficace à la cybermalveillance sont des enjeux clés dans le domaine de la cybersécurité.

Ingénierie sociale : L'ingénierie sociale est une pratique consistant à manipuler, tromper ou influencer les individus afin d'obtenir des informations confidentielles, un accès à des systèmes informatiques ou d'induire des actions spécifiques. Plutôt que de cibler directement les vulnérabilités technologiques, l'ingénierie sociale exploite les aspects psychologiques et sociaux pour atteindre ses objectifs. Cela peut prendre la forme de tentatives de phishing, d'appels frauduleux, de manipulation émotionnelle, ou d'autres stratagèmes visant à exploiter la confiance ou la naïveté des personnes. La sensibilisation à l'ingénierie sociale et l'éducation des utilisateurs sont des éléments clés pour prévenir les attaques basées sur cette méthode.

Rançongiciels (Ransomware) : Les rançongiciels sont des logiciels malveillants conçus pour chiffrer les fichiers sur un système informatique, rendant ainsi ces fichiers inaccessibles à l'utilisateur légitime. Les cybercriminels qui déploient des rançongiciels demandent ensuite une rançon en échange de la clé de déchiffrement permettant de restaurer l'accès aux fichiers. Ces attaques visent à extorquer de l'argent aux victimes en

exploitant la valeur de leurs données. Les rançongiciels peuvent se propager par le biais de pièces jointes malveillantes, de sites web compromis ou d'exploits de vulnérabilités logicielles. La prévention des rançongiciels implique des pratiques de sécurité telles que des sauvegardes régulières, des mises à jour logicielles, et la sensibilisation des utilisateurs aux techniques d'ingénierie sociale souvent utilisées pour diffuser ces logiciels malveillants.

Typosquatting : Le typosquatting, également connu sous le nom de "URL hijacking" ou "domain squatting", est une technique utilisée par des cybercriminels pour exploiter les erreurs de frappe courantes des utilisateurs lorsqu'ils saisissent des noms de domaines dans leur navigateur web. Les attaquants enregistrent délibérément des noms de domaines similaires à ceux de sites populaires, en exploitant souvent des fautes de frappe courantes, des omissions de lettres ou l'inversion de caractères. L'objectif du typosquatting est de diriger les utilisateurs vers des sites web malveillants qui peuvent héberger des logiciels malveillants, collecter des informations sensibles ou mettre en œuvre d'autres formes d'attaques. Les utilisateurs qui commettent des erreurs de frappe en entrant une URL peuvent être redirigés involontairement vers ces sites malveillants, mettant ainsi en danger la sécurité de leurs données et de leur système. La vigilance et la vérification minutieuse des URL sont des pratiques recommandées pour se protéger contre le typosquatting.

Chiffrement de l'appareil : Le chiffrement de l'appareil est une mesure de sécurité qui consiste à convertir les données stockées sur un appareil électronique en un format illisible sans la clé de déchiffrement appropriée. Cela offre une protection supplémentaire contre l'accès non autorisé aux informations stockées en cas de vol, de perte de l'appareil ou d'accès physique par des tiers.

secnumacademie.gouv.fr/content/course/id/3

SecNum
académie

- Accueil
- Mes ressources
- Mon attestation
- Mon profil
- Aide

UNITÉ 1

Internet : de quoi s'agit-il ?

Temps passé : 00:29:28

Score : 80%

Commencer S'évaluer

UNITÉ 2

Les fichiers en provenance d'Internet

Temps passé : 00:08:11

Score : 90%

Commencer S'évaluer

secnumacademie.gouv.fr/content/course/id/3

SecNum
académie

- Accueil
- Mes ressources
- Mon attestation
- Mon profil
- Aide

UNITÉ 3

La navigation web

Temps passé : 00:09:47

Score : 90%

Commencer S'évaluer

UNITÉ 4

La messagerie électronique

Temps passé : 00:21:33

Score : 80%

Commencer S'évaluer

secnumacademie.gouv.fr/content/course/id/3

SecNum académie

- Accueil
- Mes ressources
- Mon attestation
- Mon profil

Aide

Commencer S'évaluer

Commencer S'évaluer

Client Serveur

UNITÉ 5

L'envers du décor d'une connexion Web

⌚ Temps passé : 00:09:13 ★ Score : 100%

Commencer S'évaluer

© 2023 ANSSI

Mentions légales

Chrome Fichier Modifier Afficher Historique Favoris Profils Onglet Fenêtre Aide Ven. 1 déc. à 18:20

CYBER x CYBER x BLOC x Accue x Diagra x Group x BTS Si x missio x Comp x Modul x

secnumacademie.gouv.fr/content/course/id/4

Gmail YouTube Maps Traduire 404 Not Found Google Docs Mon Drive - Googl... Minhaji - Chaînes... Le Répertoire Isla... Prochains Évènem...

SecNum académie

- Accueil
- Mes ressources
- Mon attestation
- Mon profil

Aide

UNITÉ 1

Applications et mises à jour

Temps passé : 00:21:51 Score : 90%

Commencer S'évaluer

UNITÉ 2

Options de configuration de base

Temps passé : 00:12:43 Score : 80%

Commencer S'évaluer

Chrome Fichier Modifier Afficher Historique Favoris Profils Onglet Fenêtre Aide Ven. 1 déc. à 18:21

CYBER x CYBER x BLOC x Accue x Diagra x Group x BTS Si x missio x Comp x Modul x

secnumacademie.gouv.fr/content/course/id/4

Gmail YouTube Maps Traduire 404 Not Found Google Docs Mon Drive - Googl... Minhaji - Chaînes... Le Répertoire Isla... Prochains Évènem...

SecNum académie

- Accueil
- Mes ressources
- Mon attestation
- Mon profil

Aide

UNITÉ 3

Configurations complémentaires

Temps passé : 00:12:47 Score : 90%

Commencer S'évaluer

UNITÉ 4

Sécurité des périphériques amovibles

Temps passé : 00:08:01 Score : 80%


Commencer S'évaluer

Chrome Fichier Modifier Afficher Historique Favoris Profils Onglet Fenêtre Aide

CYBER x CYBER x BLOC x Accue x Diagra x Group x BTS S x missio x Comp x Modul x

secnumacademie.gouv.fr/content/course/id/4

Gmail YouTube Maps Traduire 404 Not Found Google Docs Mon Drive - Googl... Minhaji - Chaînes... Le Répertoire Isla... Prochains Évènem...

 SecNum
académie


Accueil

Mes ressources

Mon attestation

Mon profil

Aide



UNITÉ 5

Séparation des usages

Temps passé : 00:02:25

Score : 100%

Commencer S'évaluer

© 2023 ANSSI

Mentions légales

