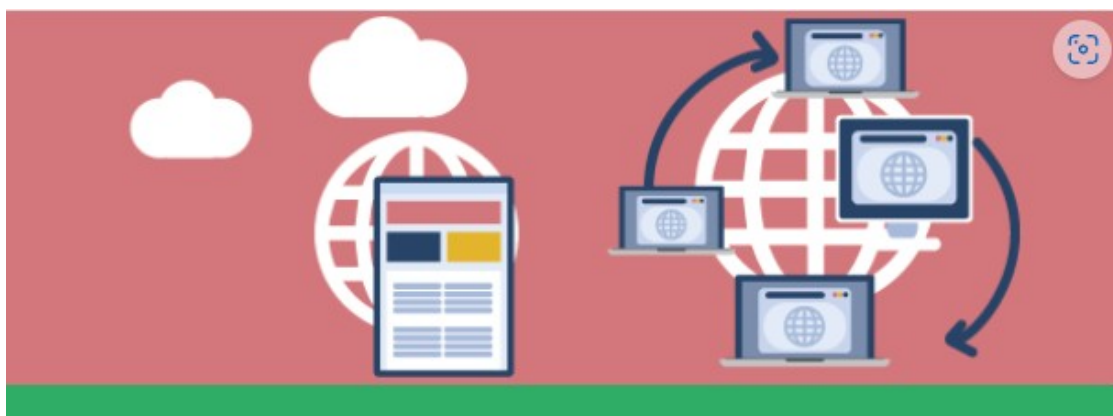
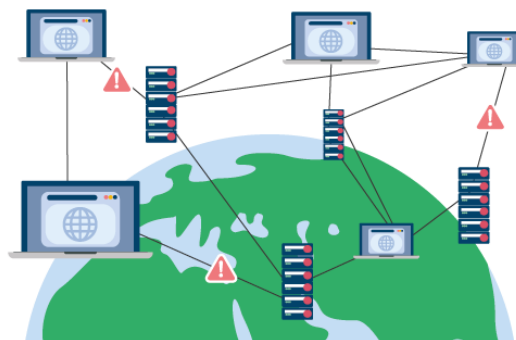


## MODULE 3 : Sécurité sur Internet

### UNITÉ 1 : Internet : de quoi s'agit-il ?

Cette unité introduit les concepts fondamentaux d'Internet, y compris son fonctionnement et son infrastructure. Elle aide les apprenants à comprendre les bases du réseau, la manière dont les informations circulent, et pourquoi la sécurité est un aspect crucial sur Internet. Avoir une compréhension claire d'Internet est essentiel pour saisir les enjeux de sécurité en ligne. Par exemple, connaître le rôle des adresses IP aide à comprendre comment les données sont envoyées et reçues, et pourquoi masquer son IP (par un VPN, par exemple) peut protéger sa vie privée. Le concept des DNS (Domain Name System) permet aussi de saisir comment des cyberattaques, comme le "DNS spoofing", peuvent rediriger les utilisateurs vers des sites frauduleux.



#### UNITÉ 1

### Internet : de quoi s'agit-il ?

🕒 Temps passé : 00:06:54

★ Score : 100%

Commencer

S'évaluer

## UNITÉ 2 : LES FICHIERS EN PROVENANCE D'INTERNET

Cette unité met en garde contre les risques liés au téléchargement de fichiers, en enseignant comment vérifier leur provenance et leur sécurité.

Par exemple, télécharger des fichiers d'un site douteux ou via des liens dans des emails non sollicités peut introduire des virus ou des logiciels espions. Les formats de fichiers comme les fichiers ZIP ou .exe sont souvent utilisés pour dissimuler des malwares, alors qu'un antivirus ou un scan avant ouverture peuvent détecter les menaces.

### FORMATS LES PLUS EXPLOITÉS



### UNITÉ 2

## Les fichiers en provenance d'Internet

🕒 Temps passé : 00:08:45

★ Score : 80%

Commencer

S'évaluer

## UNITÉ 3 : LA NAVIGATION WEB

Cette unité aborde la sécurité de la navigation en ligne, en expliquant des concepts comme les certificats SSL pour vérifier si un site est sécurisé (https:// avec le cadenas). Par exemple, lors de transactions bancaires, vérifier ce cadenas garantit que les données sont chiffrées. Elle met également en garde contre le phishing : un utilisateur pourrait recevoir un email semblant provenir de sa banque avec un lien vers une fausse page de connexion, conçue pour voler ses identifiants.



# https



# http



### UNITÉ 3

## La navigation web

🕒 Temps passé : 00:13:04

★ Score : 80%

Commencer

S'évaluer

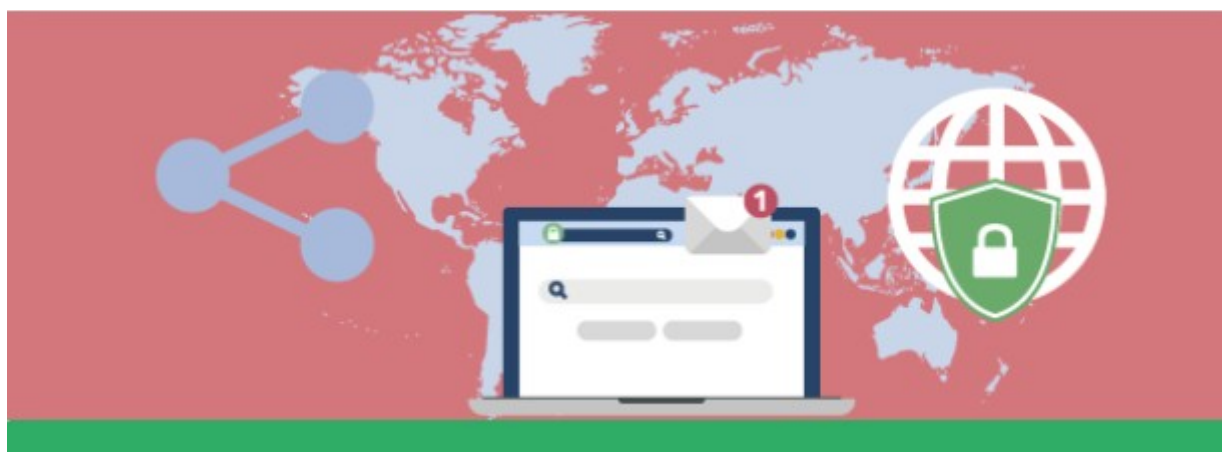
## UNITÉ 4 : LA MESSAGERIE ÉLECTRONIQUE

La messagerie est un vecteur d'attaque privilégié pour les cybercriminels. Par exemple, les emails de phishing se font passer pour des entreprises connues et contiennent des liens menant à des pages factices destinées à voler des informations de connexion. Certains emails peuvent aussi contenir des pièces jointes infectées, comme des fichiers PDF ou Word, qui lancent des malwares à l'ouverture. Cette unité enseigne comment reconnaître ces attaques (en vérifiant par exemple l'adresse email de l'expéditeur et les fautes d'orthographe).

### CLIENTS LOURDS



### CLIENTS LÉGERS



### UNITÉ 4

## La messagerie électronique

🕒 Temps passé : 00:08:06

★ Score : 80%

Commencer

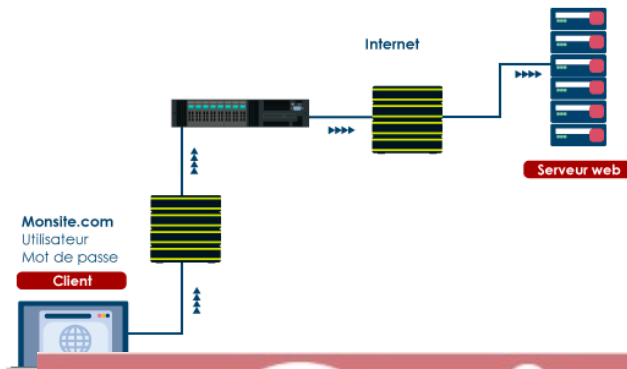
S'évaluer

## **UNITÉ 5 : L'ENVERS DU DÉCOR D'UNE CONNEXION WEB**

Cette unité permet de comprendre ce qui se passe lorsqu'on se connecte à un site, en mettant en lumière des concepts comme les "cookies" et le suivi en ligne.

Par exemple, des publicités en ligne utilisent des cookies pour suivre la navigation de l'utilisateur, collectant des données qui peuvent être revendues ou exploitées. Elle explique aussi les risques des connexions non sécurisées (HTTP) sur des réseaux publics, comme dans un café, où un pirate pourrait intercepter les données échangées (attaque de type "Man-in-the-Middle").

## RAPPEL SUR LES CONNEXIONS HTTP



Lorsque l'on considère des connexions HTTP classiques, celles-ci consistent en des messages « en clair » sur internet.

Cela signifie que tous les équipements réseau entre le client et le serveur peuvent voir le contenu de la requête et de la réponse.



### UNITÉ 5

## L'envers du décor d'une connexion Web

🕒 Temps passé : 00:15:42

★ Score : 80%

Commencer

S'évaluer

## MODULE 4 : SECURITE DU POSTE DE TRAVAIL ET NOMADISME

### UNITÉ 1 : APPLICATION ET MISE A JOUR

Cette unité met en évidence l'importance des mises à jour logicielles pour corriger les failles de sécurité et éviter les vulnérabilités.

Par exemple, ne pas mettre à jour son système d'exploitation ou ses applications peut laisser des "portes ouvertes" pour des logiciels malveillants qui exploitent des failles connues. Les mises à jour automatiques permettent de maintenir un poste de travail sécurisé sans attendre l'intervention de l'utilisateur.

## **UNITÉ 2: OPTION DE CONFIGURATION DE BASE**

Cette unité explique comment configurer les paramètres de base pour renforcer la sécurité du poste de travail.

Par exemple, activer un mot de passe de connexion sécurisé ou utiliser une double authentification limite l'accès aux utilisateurs non autorisés. Configurer l'écran pour se verrouiller automatiquement après quelques minutes d'inactivité est aussi une mesure de base pour éviter qu'un intrus accède aux données d'un appareil laissé sans surveillance.

## **UNITÉ 3 : CONFIGURATION COMPLÉMENTAIRE**

Cette unité va au-delà des options de base pour renforcer la sécurité. Par exemple, l'activation d'un pare-feu personnel permet de contrôler le trafic réseau entrant et sortant, ce qui empêche les connexions non autorisées. Activer des outils comme l'antivirus, configurer des restrictions sur les installations d'applications, et gérer les accès des applications aux données sensibles constituent également des protections avancées pour empêcher les intrusions.

## **UNITÉ 4 : SECURITE DES PERIPHERIQUES AMOVIBLES**

Cette unité aborde les risques liés aux périphériques amovibles, comme les clés USB, qui peuvent introduire des virus ou être utilisés pour voler des données.

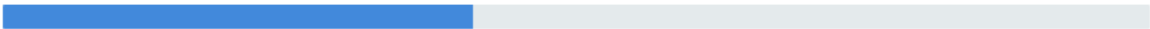
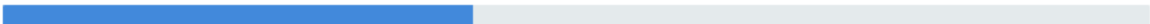
Par exemple, brancher une clé USB inconnue trouvée sur un bureau ou dans un espace public peut exposer l'ordinateur à des infections par malware. Il est donc essentiel de scanner tous les périphériques amovibles avec un antivirus avant de les utiliser ou de restreindre les permissions d'accès à ces périphériques.

## **UNITÉ 5 :SÉPARATION DES USAGES**

Cette unité explique comment séparer les usages personnels et professionnels pour éviter les risques de contamination.

Par exemple, utiliser le même appareil pour le travail et pour naviguer librement sur Internet ou pour des loisirs (téléchargements de films, jeux, etc.) augmente le risque d'infection. En séparant les usages, on limite l'exposition des données professionnelles et on évite que des informations sensibles soient compromises par des activités personnelles.

Pour obtenir une attestation de réussite, vous devez suivre l'intégralité des modules et obtenir un score supérieur à 80% aux évaluations de chacune des unités.

MODULES	PROGRESSION	SCORE
PANORAMA DE LA SSI	0.0%	0.0%
SÉCURITÉ DE L'AUTHENTIFICATION	0.0%	0.0%
SÉCURITÉ SUR INTERNET	82.0%	84.0%
SÉCURITÉ DU POSTE DE TRAVAIL ET NOMADISME	82.0%	80.0%
Progression:		41%
		
Score moyen au quiz:		41%
		

**Vous ne remplissez pas les critères requis pour éditer votre attestation.**  
**Vous n'avez pas suivi 100% des cours.**  
**Vous n'avez pas validé 80% de bonnes réponses à toutes les évaluations.**



