

# Sécurité sur internet

## 1) Internet de quoi s'agit-il ?

Internet est un réseau, c'est un moyen qui permet aux machines de communiquer entre eux. Il a été développé dans un objectif militaire.

Au début des années 1980, internet adopte la suite de protocoles TCP/IP, qui sont encore utilisés aujourd'hui et permet d'établir plus facilement l'interconnexion des différentes machines. Cela a notamment permis de développer la téléphonie, la télévision et les réseaux sociaux.

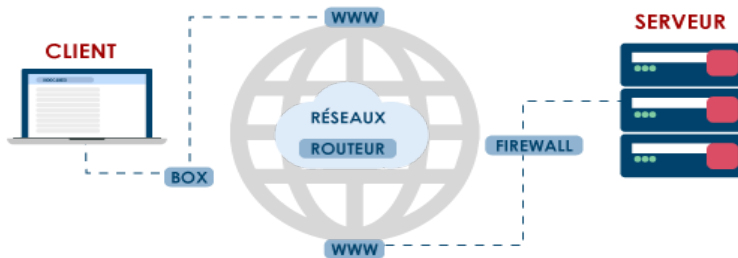
Le fonctionnement d'internet : un utilisateur envoie une requête, cette requête va être transmise vers un serveur. La requête est une information mais son contenu est celui d'une multitude de bits qui composent la requête.

Le serveur web va lire cette requête, puis va y répondre en conséquence.

C'est le **routeur** qui est chargé d'acheminer les données.

La circulation des données se base sur des règles très strictes régularisées par le protocole.

Le protocole est l'équivalent du code de la route. Pour communiquer et échanger les courriels, le serveur de messagerie utilise le protocole SMTP (Simple Mail Transfer Protocol).



## a) L'utilité d'Internet est multiple :

- recherche d'informations sur les moteurs de recherche.

- moyens de communications : adresse électronique

- apparition de la fibre a permis de multiplier la vitesse d'échanges d'informations et de navigations sur internet.

Avec l'émergence d'Internet de nouveaux utilisateurs détournent l'objectif premier de la création d'internet : échanger des informations entre des partis de confiance .

De nos jours, les utilisateurs d'internet, à leur insu, sont en constantes proies face aux cybermalveillances.

## b) Internet un réseau pratique mais dangereux :

Une des principales idées reçues par les utilisateurs, tant dans la sphère privée qu'en entreprise, consiste à penser que les cybermalveillances ne les concernent pas.

Si dans les débuts de l'informatique, le seul risque encouru était de voir son ordinateur dysfonctionner à cause d'un virus, les attaques peuvent désormais avoir de bien plus fâcheuses conséquences.

Sans pour autant se décourager d'utiliser les nombreuses possibilités offertes par le développement d'Internet, il est au contraire important de démystifier les attaques informatiques qui touchent notre quotidien et de présenter des moyens simples et efficaces d'éviter d'en être victime. La sécurité passe avant tout par la connaissance et la compréhension des risques.

## C) Les systèmes mises en place pour sécuriser internet :

Il n'existe pas de navigateur idéal, chaque navigateur a ses qualités et ses défauts.

Choisissez celui qui vous convient en fonction de vos besoins. L'adresse de messagerie de l'expéditeur n'est pas un **critère fiable** puisque celle-ci peut facilement être usurpée.

Pour éviter que les données soient facilement interceptées, les cryptographes ont créé le protocole **SSL** puis **TLS** (HTTPS). Pour résumer ce que nous avons vu dans cette unité, avant d'afficher une page web, le navigateur doit connaître l'adresse du serveur web correspondant à l'aide d'un ou plusieurs **serveurs DNS**. Lorsque l'**adresse IP** est obtenue, le navigateur demande une page du site au serveur web. L'utilisation d'un **serveur mandataire** (ou proxy) peut vous permettre d'optimiser l'ouverture de pages web déjà consultées, d'améliorer la sécurité de vos navigations et d'empêcher une éventuelle infection. L'information et la sensibilisation des utilisateurs restent la pierre angulaire de la défense contre l'ingénierie sociale. Afin de répondre à l'augmentation du nombre d'attaques informatiques, l'État a décidé de mettre en place un dispositif national d'assistance aux victimes d'actes de cybermalveillance.

## 2) Sécurité du poste de travail et nomadisme:

### A) Les bons gestes à avoir :

Les applications à installer sur vos matériels (postes informatiques, tablettes ou smartphones) doivent être choisies soigneusement selon les besoins réels pour mener à bien une activité et ne pas parasiter des postes. Il faut privilégier les sites des éditeurs officiels et veillez à ne pas installer de programmes supplémentaires inutiles. Pour se protéger au mieux de ces vulnérabilités, il est nécessaire de faire les **mise à jour** proposées par les éditeurs au plus vite, si possible dès leur parution, afin de **limiter les impacts**.

Le paramétrage par défaut est une première mesure de sécurisation. Le choix d'un paramétrage avancé doit rester réservé à des personnes plus aguerries aux règles de filtrage réseau. Cependant le facteur le plus important est de rester vigilant et de faire preuve de bon sens.

### B) Les configurations à mettre en place :

Afin d'assurer la sécurité de vos matériels il est important d'effectuer **des configurations complémentaires** à celles définies par défaut.

Il est important de créer différents comptes avec des droits différents, mais aussi de sauvegarder régulièrement les données, de contrôler les différentes interfaces (Wi-Fi, NFC, micro, etc.) et d'activer le verrouillage automatique sur les matériels.

Et de ne pas prêter votre téléphone pour éviter des modifications incontrôlées sur vos données.

### C) Les sécurités des périphériques amovibles:

Tous les supports de stockage ont une durée de vie plus ou moins limitée, il est donc nécessaire de faire au minimum **deux copies de sauvegarde** (sur des supports de stockage différents) des données que vous ne voudriez pas perdre, et de choisir des supports de stockage adaptés à la durée de conservation souhaitée.

Supprimer les fichiers sensibles ne suffit pas, il est également recommandé de **procéder à un effacement par réécriture du fichier** via un outil dédié pour s'assurer de la réelle destruction des données.

### D) Séparation des usages:

Les usages et les mesures de sécurité associés aux environnements professionnels et personnels sont différents, c'est pourquoi il est fortement **conseillé de séparer le matériel utilisé. De plus, selon l'ANSSI, les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, smartphone, etc.) personnels et professionnels.**

**Il est donc vivement recommandé de séparer les usages personnels des usages professionnels :**

- Ne jamais utiliser vos équipements personnels pour travailler sur des projets sensibles.
- Ne pas héberger de données professionnelles sur vos équipements personnels (clé USB, téléphone, etc.) ou sur des moyens personnels de stockage en ligne.
- Éviter de connecter des supports amovibles personnels (clés USB, disques durs externes, etc.) aux ordinateurs de l'entreprise.
- Respecter le cloisonnement (c'est-à-dire les infrastructures physiques et informatiques) mis en place par votre service informatique.

## Définitions

-**Botnet** : réseau de terminaux infectés par un/des malwares , souvent à utilisation malveillante.

-**Rançonnement** : attaque malveillante à but de nuire au bon fonctionnement de leur terminaux afin de couper leur activité. **Les pirates demandent alors une rançon** en contrepartie d'un arrêt de l'attaque. Pour effectuer cette attaque, les pirates utilisent un rançongiciel.

-**La défiguration de site** (aussi parfois vu sous le terme « défacement » par anglicisme) consiste à modifier une partie d'un site web, affichant alors des éléments choisis par le pirate.

-**MALVERTISING** : le pirate intégrera du contenu malveillant sur des **fausses publicités** en ligne pour essayer de piéger les visiteurs de sites web sans passer par le propriétaire du site en question.

-**l'ingénierie sociale** (plus connue sous son nom anglais « social engineering ») désigne l'ensemble des attaques informatiques mettant l'accent sur les vulnérabilités humaines. Elle est souvent utilisée par les pirates pour arriver à leurs fins en parallèle d'attaques plus techniques. Ils ont recours à de nombreuses ruses qu'il convient de savoir déjouer autant que possible.

-**L'hameçonnage ou le phishing** consiste à obtenir du destinataire d'un courriel, d'apparence légitime, qu'il transmette ses **coordonnées bancaires** ou ses **identifiants de connexion à des services financiers**, afin de lui **dérober de l'argent**.

-**Un fichier** n'est fondamentalement qu'une suite de 0 et de 1 compréhensibles par l'ordinateur.

-**L'extension**, c'est **le suffixe du nom du fichier**, La convention veut que l'extension du fichier corresponde à son format, cela permet non seulement d'identifier rapidement le format du fichier mais aussi de lui associer un logiciel par défaut (c'est-à-dire le logiciel automatiquement choisi pour l'ouvrir).

-**Internet** désigne le réseau informatique qui relie par le biais du **protocole de communication IP** (Internet Protocol) des millions d'ordinateurs à l'échelle mondiale.

-**Le World Wide Web** ou **Web** désigne une des utilisations possibles d'Internet. Il a été inventé plusieurs années après Internet et désigne un **système hypertexte public qui fonctionne sur Internet et permet de consulter des pages web et de naviguer entre elles via des hyperliens**.

-**Un nom de site** est associée à une adresse IP sur laquelle du contenu est hébergé.

-**L'objectif du « typosquatting »** est de réserver un nom dont la typographie est proche d'un site officiel pour tromper l'utilisateur ou nuire à l'entité.

-**Un cookie** est un objet associé à un site web stocké sur l'ordinateur, qui permet à ce site de stocker des informations relatives au client et de récupérer ces informations lors d'une visite ultérieure du client.

-**Navigation privée** permet de limiter les traces de navigation laissées sur l'équipement lors de notre passage, mais attention elle ne préserve pas des menaces et on est encore loin de l'accès totalement anonyme sur le grand réseau Internet ! C'est d'ailleurs généralement rappelé lors de l'activation de ce mode : votre fournisseur d'accès ou votre entreprise dispose toujours de traces des sites auxquels vous accédez.

-Un **pourriel** est une communication électronique non sollicitée.

-Le **DNS** (Domain Name System) est le nom d'un service hiérarchique distribué jouant le rôle d'annuaire pour Internet.

-**vulnérabilité**: une faille dans la conception, l'exécution ou la gestion d'un système informatique

-Les « **black hats** » qui cherchent des failles pour les exploiter à des fins de malveillances ou de profits.

-Les « **white hats** » qui cherchent des failles pour les remonter aux éditeurs et fabricants afin qu'ils améliorent leurs outils.


-pare-feu : blocage des connexions entrantes et sortantes du réseau.

## Annexes :

-Les clients de la messagerie :



-Connexion web :

 Serveur DNS = adresse du serveur web

Serveur mandataire (proxy) = affichage rapide et sécurisé

HTTPS (+ image de cadenas + couleur verte) = **version sécurisée de HTTP**

Enfin, lorsque vous naviguez sur internet et avant toute transaction, saisie de coordonnées bancaires ou saisie des mots de passe, vous devez vous assurer que le « S » sur « HTTPS » est présent. Pour cela, vérifier la présence du cadenas, voire d'une coloration verte de la barre d'adresses du navigateur. Vous pouvez aussi utiliser des signets (favoris/bookmarks) pour enregistrer les sites et éviter les fautes de frappe par la suite (typosquatting). En l'absence de ces éléments vous devez considérer que le site consulté n'est probablement pas de confiance !



## UNITÉ 5

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

🕒 Temps passé : 00:11:31

★ Score : 80%

Commencer

S'évaluer



## UNITÉ 5

### Séparation des usages

🕒 Temps passé : 00:16:51

★ Score : 80%

Commencer

S'évaluer



#### UNITÉ 1

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

🕒 Temps passé : 01:26:47

★ Score : 90%

Commencer

S'évaluer



#### UNITÉ 2

### Les fichiers en provenance d'Internet

🕒 Temps passé : 00:29:32

★ Score : 80%

Commencer

S'évaluer



#### UNITÉ 3

### La navigation web

🕒 Temps passé : 00:22:14

★ Score : 80%

Commencer

S'évaluer



#### UNITÉ 4

### La messagerie électronique

🕒 Temps passé : 00:44:28

★ Score : 80%

Commencer

S'évaluer



#### UNITÉ 1

### Applications et mises à jour

🕒 Temps passé : 00:37:27

★ Score : 80%

Commencer

S'évaluer



#### UNITÉ 2

### Options de configuration de base

🕒 Temps passé : 00:17:43

★ Score : 100%

Commencer

S'évaluer



#### UNITÉ 3

### Configurations complémentaires

🕒 Temps passé : 00:34:59

★ Score : 90%

Commencer

S'évaluer



#### UNITÉ 4

### Sécurité des périphériques amovibles

🕒 Temps passé : 00:31:52

★ Score : 90%

Commencer

S'évaluer

