Chapitre: 02
Internet, Web, Cloud et sécurité

CHAPITRE 2 : Internet, Web, Cloud et sécurité

2.1. Introduction à Internet et au Web

Internet est un **réseau mondial** interconnectant des millions d'ordinateurs et d'appareils à travers le monde. Le **Web** (World Wide Web) est un service qui utilise Internet pour accéder à des documents hypertextes. Cette distinction est essentielle : Internet est l'infrastructure, le Web est l'une de ses applications.

Définition officielle (UIT) :

Internet est un « réseau informatique mondial constitué d'un ensemble de réseaux interconnectés utilisant le protocole IP (Internet Protocol) pour communiquer ».

Tableau 2.1 : Internet vs Web

Critère	Internet	Web
Définition	Infrastructure réseau mondiale	Service de consultation de documents
Nature	Réseau physique et logique	Application logicielle
Protocole principal	IP, TCP	HTTP, HTTPS
Inventeur	Vinton Cerf, Bob Kahn (1970s)	Tim Berners-Lee (1989)
Services	Web, mail, FTP, VoIP, streaming…	Pages HTML, sites, applications

2.1.1. Historique et évolution

Cette frise chronologique retrace les grandes étapes de l'évolution d'Internet, depuis ARPANET jusqu'au Web 3.0 et à l'Internet des objets. Elle permet de situer les ruptures technologiques majeures et de comprendre la transformation des usages numériques (figure 2.1).



Figure 2.1 : Évolution historique d'Internet

Le tableau 2.2 présente l'évolution historique d'Internet.

Tableau 2.2 : Évolution historique d'Internet

Période	Technologie	Caractéristiques
1969	ARPANET	4 universités américaines connectées
1983	TCP/IP	Protocole unique de communication
1989-1991	World Wide Web	Invention du Web par Tim Berners-Lee
2000-2010	Web 2.0	Réseaux sociaux, blogs, wikis
2010-2020	Cloud & Mobile	Smartphones, IoT, Big Data
2020+	IA & Web 3.0	Intelligence artificielle, métavers

2.1.2. Terminologies du Web

Le tableau 2.3 définit les principaux termes techniques du Web (URL, HTTP, DNS, HTML, etc.). Il constitue un glossaire indispensable pour comprendre le fonctionnement d'Internet.

Tableau 2.3 : Terminologies du Web

Terme	Signification	Rôle
URL	Uniform Resource Locator	Adresse d'une ressource sur le Web
HTTP	HyperText Transfer Protocol	Protocole de transfert des pages Web
HTTPS	HTTP Secure	Version sécurisée (chiffrée) de HTTP
HTML	HyperText Markup Language	Langage de description des pages Web
CSS	Cascading Style Sheets	Langage de mise en forme
DNS	Domain Name System	Traduit les noms de domaine en adresses IP
IP	Internet Protocol	Protocole d'adressage et de routage des données
FTP	File Transfer Protocol	Transfert de fichiers
SMTP	Simple Mail Transfer Protocol	Envoi d'e-mails

Cette figure 2.2 décompose une URL en ses différents éléments. Elle permet de comprendre la structure d'une adresse Web et le rôle de chaque partie (protocole, domaine, chemin, paramètres).

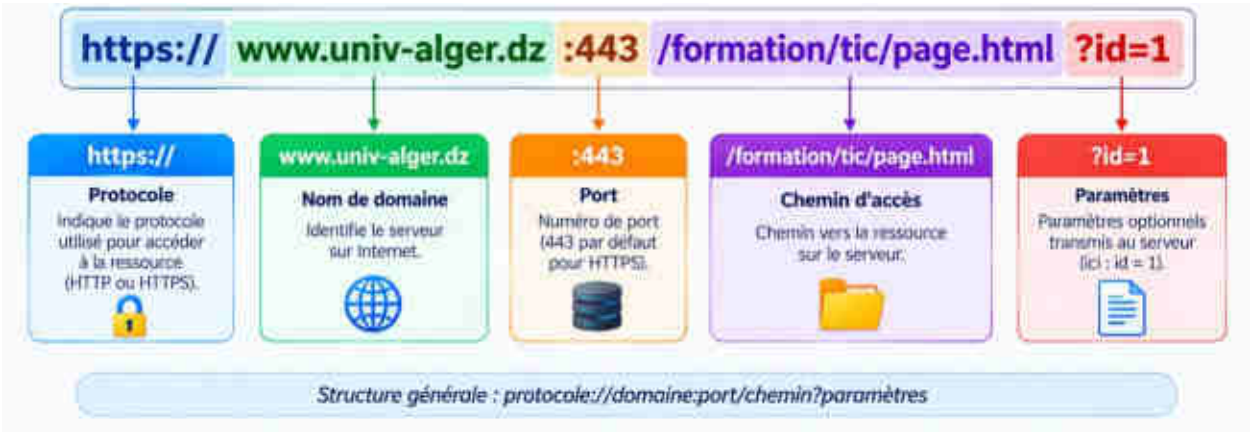


Figure 2.2 : Structure d'une URL

2.1.3. Navigateurs Web

Le tableau 2.4 compare les principaux navigateurs Web (Chrome, Firefox, Edge, Safari, Opera) selon leur éditeur, leur moteur de rendu, leur type de licence et leurs avantages. Il aide à choisir un navigateur adapté à ses besoins.

Tableau 2.4 : Comparaison des navigateurs Web

Navigateur	Éditeur	Moteur	Licence	Avantages
Google Chrome	Google	Blink	Gratuit	Rapide, extensions nombreuses
Mozilla Firefox	Mozilla	Gecko	Libre	Vie privée, open source
Microsoft Edge	Microsoft	Blink	Gratuit	Intégré à Windows, rapide
Safari	Apple	WebKit	Gratuit	Optimisé macOS/iOS
Opera	Opera Software	Blink	Gratuit	VPN intégré, économie de données

2.2. Recherche sur le Web

2.2.1. Outils de recherche

Le tableau 2.5 distingue les différents outils de recherche sur le Web (moteurs de recherche, répertoires, métamoteurs, indexations automatiques) avec leur principe de fonctionnement et des exemples. Il aide à comprendre comment retrouver efficacement l'information.

Tableau 2.5 : Outils de recherche

Outil	Principe	Exemples
Moteur de recherche	Indexation automatique + algorithme de classement	Google, Bing, DuckDuckGo
Répertoire	Classement manuel par catégories	Yahoo Directory (ancien)
Métamoteur	Interroge plusieurs moteurs simultanément	Dogpile, MetaCrawler
Indexation automatique	Robots (crawlers) qui parcourent le Web	Googlebot, Bingbot
Recherche spécialisée	Base de données thématique	Google Scholar, PubMed

Cette figure 2.3 illustre le fonctionnement d'un moteur de recherche : les robots parcourent le Web, indexent les pages, puis répondent aux requêtes des utilisateurs. Elle permet de comprendre les coulisses de la recherche en ligne.



Figure 2.3 : Fonctionnement d'un moteur de recherche

2.2.2. Affinage de la recherche

Le tableau 2.6 présente les opérateurs booléens et les techniques d'affinage de recherche (guillemets, tiret, site:, filetype:, etc.). Il permet d'obtenir des résultats plus précis et pertinents.

Tableau 2.6 : Opérateurs et techniques de recherche

Opérateur / Technique	Signification	Exemple
ET / AND	Les deux termes	TIC AND éducation
OU / OR	L'un ou l'autre	smartphone OR tablette
SAUF / NOT	Exclut un terme	java NOT script
" "	Expression exacte	"intelligence artificielle"
-	Exclut un mot	apple -fruit
site:	Limite à un site	site:univ-alger.dz
filetype:	Type de fichier	filetype:pdf TIC
*	Joker (remplace un mot)	réseau * informatique
intitle:	Dans le titre	intitle:"cours TIC"

La figure 2.4 (diagramme de Venn) illustre les opérateurs booléens ET, OU et SAUF. Il montre comment combiner les mots-clés pour affiner une recherche.

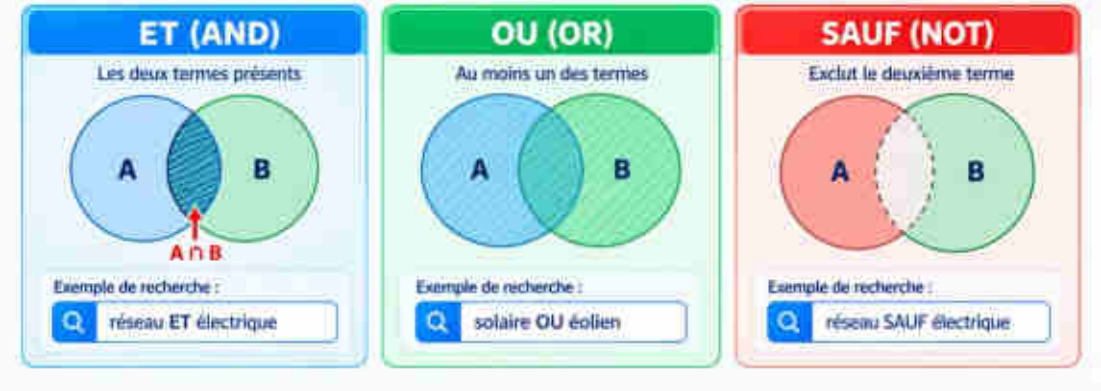


Figure 2.4 : Opérateurs booléens (diagramme de Venn)

2.2.3. Évaluation de la fiabilité des sources

Le tableau 2.7 propose une grille de critères pour évaluer la fiabilité d'une source d'information sur le Web (auteur, date, source, objectivité, etc.). Il aide à distinguer les informations fiables des informations douteuses.

Tableau 2.7 : Grille d'évaluation de la fiabilité

Critère	Question à se poser	Indicateur de fiabilité
Auteur	Qui est l'auteur ?	Expert reconnu, institution
Date	Quand a été publié ?	Date récente, actualisée
Source	Quel est le site ?	Site officiel, université, revue
Objectivité	Quel est l'objectif ?	Informer, pas vendre
Références	Y a-t-il des sources ?	Citations, bibliographie
Exactitude	Les faits sont-ils vérifiables ?	Recoupement avec d'autres sources
Public	À qui s'adresse le contenu ?	Public académique, professionnel

2.3. Réseaux informatiques

2.3.1. Types de réseaux

Le tableau 2.8 classe les réseaux selon leur étendue géographique (PAN, LAN, MAN, WAN, CAN, SAN) avec leurs caractéristiques, leur débit et des exemples. Il permet de comprendre les différentes échelles de communication réseau.

Tableau 2.8 : Types de réseaux

Type	Signification	Étendue	Exemple
PAN	Personal Area Network	Quelques mètres	Bluetooth, NFC
LAN	Local Area Network	Bâtiment, campus	Réseau d'école, d'entreprise
MAN	Metropolitan Area Network	Ville	Réseau municipal
WAN	Wide Area Network	Pays, monde	Internet, 4G/5G
CAN	Campus Area Network	Campus universitaire	Réseau d'université
SAN	Storage Area Network	Centre de données	Réseau de stockage

Cette figure 2.5 illustre les différents types de réseaux (PAN, LAN, MAN, WAN) et leur étendue géographique. Elle permet de visualiser la hiérarchie des réseaux, du plus local au plus global.



Figure 2.5 : Types de réseaux (PAN, LAN, MAN, WAN)

2.3.2. Équipements réseau

Le tableau 2.9 présente les principaux équipements réseau (routeur, switch, modem, point d'accès, pare-feu) avec leur fonction et leur rôle dans une

infrastructure. Il permet de comprendre le matériel nécessaire à la connexion des réseaux.

Tableau 2.9 : Équipements réseau

Équipement	Fonction	Rôle
Routeur	Interconnecte des réseaux	Dirige les données entre réseaux
Switch (commutateur)	Connecte les appareils d'un LAN	Aiguille les données localement
Modem	Convertit les signaux	Relie le réseau à Internet
Point d'accès (AP)	Diffuse le Wi-Fi	Connexion sans fil
Pare-feu (Firewall)	Filtre le trafic	Protège contre les intrusions
Répéteur	Amplifie le signal	Étend la couverture réseau

La figure 2.6 illustre l'architecture client-serveur : les clients (ordinateurs, mobiles) envoient des requêtes à un serveur qui les traite et renvoie les réponses. Il montre le modèle fondamental du fonctionnement d'Internet.

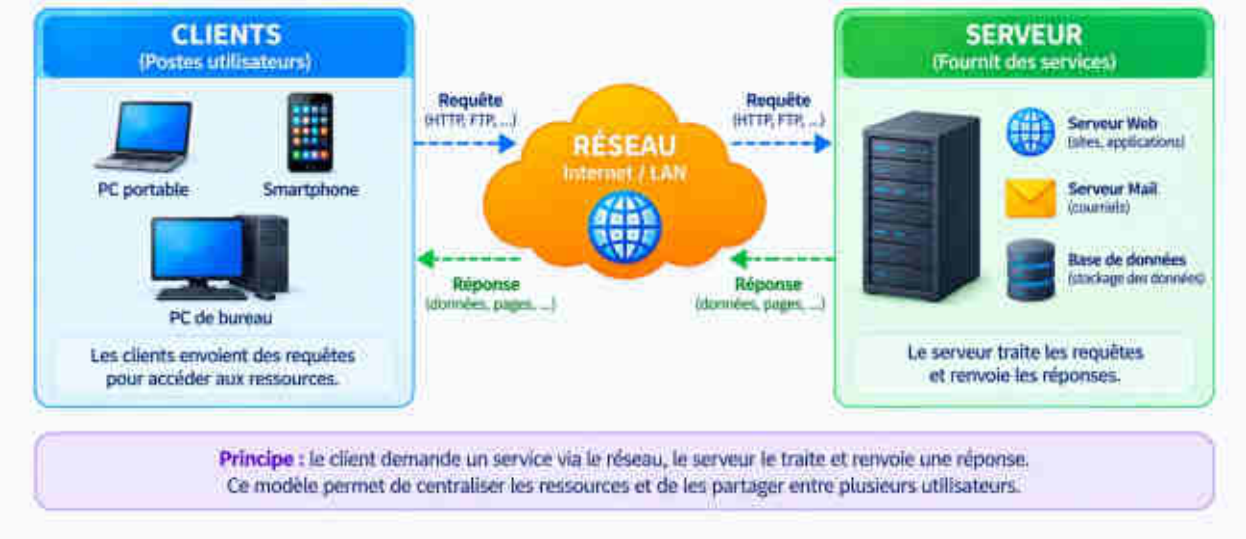


Figure 2.6 : Architecture client-serveur

2.4. Cloud computing et collaboration

2.4.1. Définition et modèles

Le **cloud computing** (informatique en nuage) est l'utilisation de serveurs distants via Internet pour stocker, traiter et gérer des données, plutôt que de recourir à un ordinateur local ou à un serveur physique.

Le tableau 2.10 définit les principaux modèles de services cloud : les trois fondamentaux (IaaS, PaaS, SaaS) et deux modèles complémentaires (DaaS, STaaS)

avec leur signification, leur fonction et des exemples. Il permet de distinguer les niveaux de service offerts par le cloud.

Tableau 2.10 : Modèles de services cloud

Modèle	Signification	Fonction	Exemples
IaaS	Infrastructure as a Service	Infrastructure virtuelle	AWS EC2, Azure VM
PaaS	Platform as a Service	Plateforme de développement	Google App Engine, Heroku
SaaS	Software as a Service	Logiciel en ligne	Gmail, Google Docs, Office 365
DaaS	Desktop as a Service	Bureau virtuel	Windows 365, Citrix
STaaS	Storage as a Service	Stockage en ligne	Google Drive, Dropbox

Cette pyramide (figure 2.7) illustre les trois modèles de cloud computing (IaaS, PaaS, SaaS) et leur niveau d'abstraction. Elle montre comment le cloud s'adapte aux besoins des utilisateurs, du développeur à l'utilisateur final.

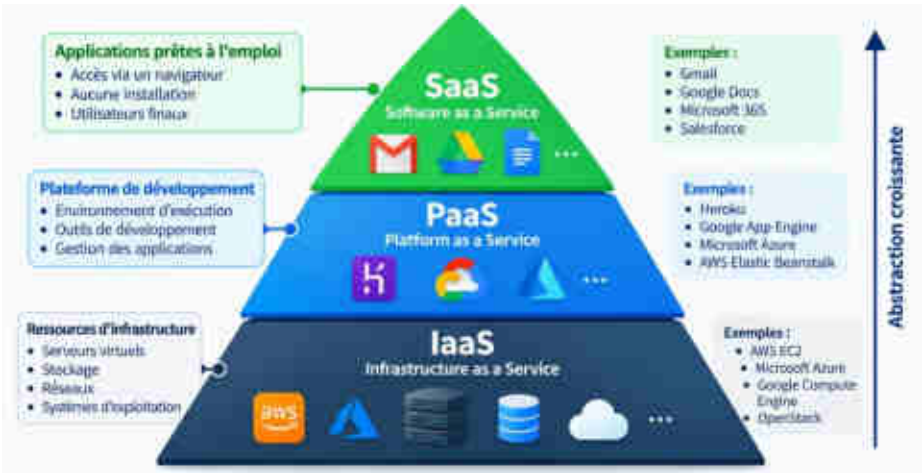


Figure 2.7 : Pyramide des modèles cloud (IaaS, PaaS, SaaS)

Le tableau 2.11 illustre les avantages et inconvénients du cloud.

Tableau 2.11 : Avantages et inconvénients du cloud

Avantages	Inconvénients
Accessibilité 24h/24	Dépendance à Internet
Coût réduit (pas d'infrastructure)	Confidentialité des données
Scalabilité (adaptation aux besoins)	Localisation des serveurs
Collaboration en temps réel	Perte de contrôle
Sauvegarde automatique	Coûts à long terme
Mises à jour automatiques	Interopérabilité limitée

2.4.2. Stockage en ligne

Le tableau 2.12 compare les principaux services de stockage en ligne (Google Drive, Dropbox, OneDrive, iCloud) selon leur espace gratuit, leur intégration et leurs particularités. Il aide à choisir un service adapté à ses besoins.

Tableau 2.12 : Services de stockage en ligne

Service	Éditeur	Espace gratuit	Intégration	Particularité
Google Drive	Google	15 Go	Google Workspace	Collaboration native
Dropbox	Dropbox	2 Go	Multi-plateforme	Synchronisation rapide
OneDrive	Microsoft	5 Go	Microsoft 365	Intégré à Windows
iCloud	Apple	5 Go	Écosystème Apple	Optimisé macOS/iOS
Mega	Mega	20 Go	Multi-plateforme	Chiffrement de bout en bout

2.4.3. Bureautique en ligne et collaboration

Le tableau 2.13 met en correspondance les fonctions bureautiques (traitement de texte, tableur, présentation) avec les suites en ligne (Google Workspace, Microsoft 365, OnlyOffice). Il facilite le choix d'un outil collaboratif.

Tableau 2.13 : Suites bureautiques en ligne

Fonction	Google Workspace	Microsoft 365	OnlyOffice
Traitement de texte	Docs	Word Online	Document
Tableur	Sheets	Excel Online	Spreadsheet
Présentation	Slides	PowerPoint Online	Presentation
Stockage	Google Drive	OneDrive	OnlyOffice Cloud
Visioconférence	Google Meet	Microsoft Teams	Talk
Prix	Gratuit / payant	Payant	Gratuit / payant

Le tableau 2.14 présente les principaux outils de visioconférence (Zoom, Google Meet, Microsoft Teams, Webex) avec leurs fonctionnalités et leurs limites. Il permet de choisir l'outil adapté à un usage pédagogique ou professionnel.

Tableau 2.14 : Outils de visioconférence

Outil	Éditeur	Participants (gratuit)	Durée (gratuit)	Particularité
Zoom	Zoom	100	40 min	Très répandu
Google Meet	Google	100	60 min	Intégré à Gmail
Microsoft Teams	Microsoft	100	60 min	Intégré à Office
Webex	Cisco	100	50 min	Sécurité renforcée
Jitsi	Open source	Illimité	Illimité	Libre et gratuit

2.5. Cybersécurité et protection des données

2.5.1. Définition et principes

La **cybersécurité** (ou sécurité de l'information) est l'ensemble des moyens techniques, organisationnels et juridiques visant à protéger les données, les systèmes et les réseaux contre les accès non autorisés, les modifications, les vols ou les destructions.

Le tableau 2.15 définit les trois principes fondamentaux de la sécurité de l'information (confidentialité, intégrité, disponibilité) avec leur signification et des exemples. Il constitue la base de toute politique de sécurité.

Tableau 2.15 : Les trois principes de la sécurité (CIA)

Principe	Signification	Objectif	Exemple
Confidentialité	Confidentiality	Empêcher l'accès non autorisé	Chiffrement, mots de passe
Intégrité	Integrity	Garantir l'exactitude des données	Signatures numériques, hachage
Disponibilité	Availability	Assurer l'accès aux données	Sauvegardes, redondance

Le triangle (figure 2.8) illustre les trois principes fondamentaux de la sécurité de l'information (CIA) : confidentialité, intégrité et disponibilité. Il montre leur complémentarité et leur importance égale dans toute politique de sécurité.



Figure 2.8 : Triangle CIA (Confidentialité, Intégrité, Disponibilité)

2.5.2. Menaces et attaques

Le tableau 2.16 décrit les principales menaces informatiques (phishing, virus, ransomware, spyware, etc.) avec leur mode d'action et leurs conséquences. Il permet d'identifier les risques et d'adopter les bonnes pratiques.

Tableau 2.16 : Types de menaces informatiques

Menace	Mode d'action	Conséquence
Phishing (hameçonnage)	Faux e-mails/sites imitant des organismes	Vol d'identifiants, données bancaires
Virus	Programme malveillant auto-répliquant	Corruption de fichiers
Ransomware (rançongiciel)	Chiffre les données et demande une rançon	Perte d'accès aux données
Spyware (logiciel espion)	Collecte des informations à l'insu	Surveillance, vol de données
Cheval de Troie	Se cache dans un logiciel légitime	Accès à distance, backdoor
Ver (Worm)	Se propage via le réseau	Saturation des réseaux
Adware	Affiche des publicités intempestives	Ralentissement, pollution
DDoS	Saturation d'un serveur par des requêtes	Indisponibilité du service
Ingénierie sociale	Manipulation psychologique	Obtention d'informations confidentielles

La figure 2.9 illustre les principales menaces informatiques et leur mode de propagation. Il montre comment les attaquants exploitent les failles humaines et techniques pour compromettre les systèmes.

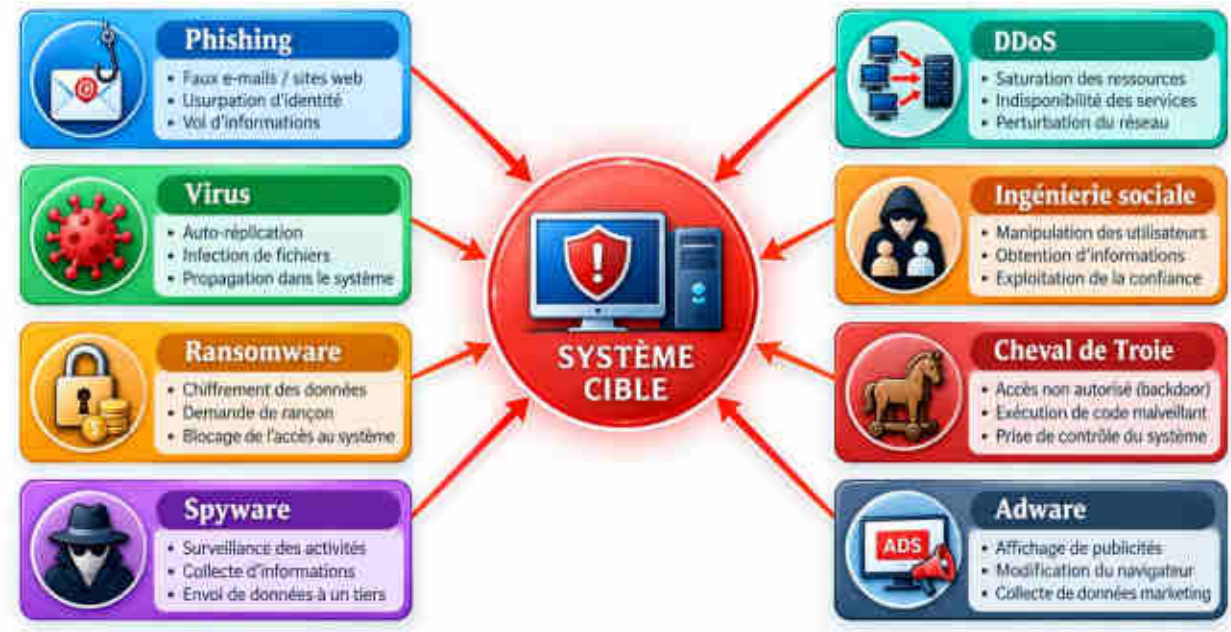


Figure 2.9 : Principales menaces informatiques

2.5.3. Bonnes pratiques de sécurité

Le tableau 2.17 liste les bonnes pratiques de sécurité à adopter au quotidien (mots de passe forts, 2FA, mises à jour, sauvegardes, etc.) avec leur objectif et leur mise en œuvre. Il constitue un guide pratique pour se protéger en ligne.

Tableau 2.17 : Bonnes pratiques de cybersécurité

Pratique	**Objectif**	**Mise en œuvre**
Mots de passe forts	Empêcher le devinage	12+ caractères, majuscules, chiffres, symboles
Authentification 2FA	Double vérification	Code SMS, application d'authentification
Mises à jour régulières	Corriger les failles	Activer les mises à jour automatiques
Sauvegardes régulières	Récupérer les données	Règle 3-2-1
Antivirus à jour	Détecter les menaces	Scanner régulièrement
Pare-feu activé	Filtrer le trafic	Activer le firewall système
Vigilance phishing	Éviter les pièges	Vérifier l'expéditeur, les liens
Chiffrement	Protéger les données	HTTPS, VPN, chiffrement disque
Verrouillage d'écran	Empêcher l'accès physique	Mot de passe, biométrie

La figure 2.10 illustre les principales bonnes pratiques de cybersécurité à adopter pour protéger ses données et ses systèmes. Elle montre les mesures essentielles à mettre en place au quotidien.



Figure 2.10 : Bonnes pratiques de cybersécurité

2.5.4. Conduite en cas d'incident de sécurité

La figure 2.11 présente les étapes de la conduite à tenir en cas d'incident de sécurité : détection, confinement, éradication, récupération, retour d'expérience et notification. Il montre comment réagi efficacement face à une cyberattaque.



Figure 2.11 : Conduite en cas d'incident de sécurité

Le tableau 2.18 décrit les étapes à suivre en cas d'incident de sécurité (détection, confinement, éradication, récupération, retour d'expérience). Il fournit une procédure claire pour réagir efficacement.

Tableau 2.18 : Procédure en cas d'incident de sécurité

Étape	Action	Objectif
1. Détection	Identifier l'incident	Reconnaître l'attaque
2. Confinement	Isoler le système affecté	Empêcher la propagation
3. Éradication	Supprimer la menace	Nettoyer le système
4. Récupération	Restaurer les données	Reprendre l'activité
5. Retour d'expérience	Analyser l'incident	Éviter la récidive
6. Notification	Alerter les autorités	Conformité légale

2.6. Conclusion

Ce deuxième chapitre a permis d'explorer le **fonctionnement d'Internet et du Web**, depuis leur genèse jusqu'à leurs applications modernes. Nous avons distingué Internet (l'infrastructure) du Web (le service), et présenté les terminologies essentielles (URL, HTTP, DNS, IP) ainsi que les navigateurs qui permettent d'y accéder.

Nous avons ensuite étudié les **outils de recherche** : moteurs, répertoires, métamoteurs, avec leurs techniques d'affinage (opérateurs booléens, guillemets, recherche avancée) et les critères d'évaluation de la fiabilité des sources. Ces compétences sont indispensables pour naviguer efficacement dans la masse d'informations disponibles.

Les **réseaux informatiques** ont été présentés selon leur étendue (PAN, LAN, MAN, WAN), leurs équipements (routeur, switch, modem, pare-feu) et leur architecture (client-serveur). Cette base permet de comprendre comment les données circulent d'un point à un autre.

Le **cloud computing** a été défini avec ses trois modèles principaux (IaaS, PaaS, SaaS), ses avantages (accessibilité, scalabilité, collaboration) et ses limites (dépendance à Internet, confidentialité). Les services de stockage en ligne et les suites bureautiques collaboratives ont été comparés.

Enfin, la **cybersécurité** a occupé une place centrale : définition, principes fondamentaux (confidentialité, intégrité, disponibilité), principales menaces (phishing, virus, ransomware, etc.), bonnes pratiques (mots de passe forts, 2FA, mises à jour, sauvegardes) et procédure de réaction en cas d'incident. Ces connaissances sont essentielles pour évoluer sereinement dans un environnement numérique de plus en plus menacé.

En résumé, ce chapitre a doté l'étudiant des **compétences nécessaires pour utiliser Internet de manière efficace, collaborative et sécurisée**. Il prépare le

terrain pour le chapitre suivant, consacré à l'éthique numérique et à l'intelligence artificielle.

Références chapitre 2 :

Internet, Web, Cloud et sécurité

1. Ouvrages de référence

1. **KUROSE, James F. ; ROSS, Keith W.** *Computer Networking: A Top-Down Approach*. 8e éd. Pearson, 2021. ISBN 978-0-13-668155-7.
   → Ouvrage de référence sur les réseaux informatiques, couvrant Internet, le Web, les protocoles et la sécurité.
2. **TANENBAUM, Andrew S. ; WETHERALL, David J.** *Computer Networks*. 6e éd. Pearson, 2021. ISBN 978-0-13-676405-2.
   → Manuel classique sur les réseaux, avec une approche progressive des couches et des protocoles.
3. **STALLINGS, William.** *Cryptography and Network Security: Principles and Practice*. 8e éd. Pearson, 2022. ISBN 978-0-13-670722-6.
   → Référence en sécurité informatique : cryptographie, authentification, protocoles sécurisés.

2. Polycopiés et cours universitaires

4. **Université de Biskra.** *Information and Communication Technologies — Chapitre 2 : Initiation à la technologie Web*. Support de cours en ligne.
   → Cours détaillé sur Internet, le Web, les moteurs de recherche et les opérateurs booléens.
5. **Université d'Oran 2.** *Polycopié : Réseaux informatiques et Internet*. Faculté des Sciences Économiques, 2023.
   → Introduction aux réseaux, aux protocoles et aux services Internet.
6. **OpenClassrooms.** *Comprendre le cloud computing*. Cours en ligne, 2024.
   → Introduction pédagogique aux modèles cloud (IaaS, PaaS, SaaS) et à leurs usages.

3. Normes et bonnes pratiques

7. **ISO/IEC 27001:2022.** *Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences*. Genève : ISO, 2022.
   → Norme internationale de référence pour la gestion de la sécurité de l'information.
8. **ANSSI.** *Guide des bonnes pratiques de l'informatique*. Paris : Agence Nationale de la Sécurité des Systèmes d'Information, 2023.

→ Guide pratique sur la sécurité des postes de travail, mots de passe, mises à jour et sauvegardes.

4. Rapports institutionnels

9. **UIT.** *Measuring Digital Development: Facts and Figures 2024*. Genève : Union Internationale des Télécommunications, 2024.
   → Rapport statistique sur l'accès à Internet, la couverture réseau et la fracture numérique dans le monde.
10. **ENISA.** *Threat Landscape Report 2024*. Athènes : Agence de l'Union européenne pour la cybersécurité, 2024.
    → Rapport annuel sur les principales menaces informatiques (phishing, ransomware, DDoS) et leur évolution.

5. Ressources numériques et encyclopédiques

11. **MDN Web Docs.** *Comment fonctionne le Web*. Mozilla Foundation.
    → Documentation de référence sur les technologies du Web (HTTP, DNS, HTML, CSS).
12. **Cloud Security Alliance.** *Top Threats to Cloud Computing 2024*. CSA, 2024.
    → Rapport sur les principales menaces liées au cloud computing.