المركز الجامعي نور البشير – البيض
Centre Universitaire Nour Bachir
El Bayadh

Module : Fondements des TIC et environnement numérique
1re année – Tronc commun

Année universitaire
2026 – 2027

Fondements des TIC et environnement numérique

Séance 4

Internet, Web, Cloud et sécurité

Concepts, terminologies et navigateurs





Internet
(réseau mondial)

Web
(service en ligne)

Cloud
(informatique en nuage)

Sécurité
(cybersécurité)



Groupe : FR-G1

Durée : 3 h
(1 h 30 Cours + 1 h 30 TD/TP)

Plan de la séance

01	Introduction et objectifs de la séance	5 min
02	Internet : concepts, fonctionnement et terminologies	20 min
03	Le Web : services, technologies et usages	15 min
04	Navigateurs Web : rôles, exemples et fonctionnalités	15 min
05	Le Cloud (informatique en nuage) : principes et services	20 min
06	Sécurité numérique : menaces, protection et bonnes pratiques	20 min
07	Synthèse et questions	5 min



Objectif global

Comprendre Internet et le Web, utiliser un navigateur, découvrir le Cloud et adopter les bonnes pratiques de sécurité.

Objectifs pédagogiques

À la fin de cette séance, l'étudiant sera capable de :



01 Définir Internet et le Web et distinguer leurs rôles et leurs principales différences.

02 Maîtriser les terminologies essentielles (URL, HTTP/HTTPS, DNS, IP, nom de domaine, etc.).

03 Utiliser et exploiter efficacement un navigateur Web (Chrome, Firefox, Edge, etc.).

04 Comprendre le principe et les services du Cloud Computing (IaaS, PaaS, SaaS, stockage et collaboration).

05 Identifier les principales menaces en ligne (phishing, virus, ransomware, etc.) et les moyens de protection.

06 Adopter les bonnes pratiques de sécurité et de protection des données personnelles (mots de passe, 2FA, sauvegarde, etc.).

Pourquoi étudier Internet, le Web, le Cloud et la sécurité ?



Une nécessité dans la vie quotidienne

Études et formation
(e-learning, ressources, MOOCs)



Travail et entreprise
(télétravail, collaboration, Cloud)



Communication
(e-mail, messagerie, visioconférence)



Services et achats en ligne
(e-commerce, banques, administration)



Information et médias
(actualité, vidéo, réseaux sociaux)



Un enjeu majeur

- **Comprendre** le fonctionnement du monde numérique.
- **Utiliser** efficacement et en toute **sécurité** les services en ligne.
- **Exploiter** les avantages du **Cloud** (stockage, accès, collaboration).
- **Se protéger** contre les menaces (phishing, virus, piratage, etc.).
- **Adopter un usage responsable et éthique** d'Internet et du Web.

En résumé

Étudier Internet, le Web, le Cloud et la sécurité permet d'être un utilisateur **compétent, autonome, productif et responsable** dans la société numérique.

Internet : définition et fonctionnement

Définition

Internet est un **réseau mondial** de réseaux interconnectés qui permet l'échange de données et l'accès à de nombreux services à l'échelle mondiale.

Caractéristiques principales

- Réseau mondial (sans frontières).
- Interconnexion de réseaux hétérogènes.
- Échange de données (en temps réel).
- Utilisation de protocoles standards (TCP/IP).
- Accès à de multiples services (Web, e-mail, Cloud, etc.).

Comment fonctionne Internet ?



Le rôle des protocoles

Un **protocole** est un ensemble de règles qui permet la communication entre les appareils sur Internet.

Exemples :

TCP/IP | HTTP/HTTPS | FTP | SMTP

Principaux services d'Internet

Le Web	E-mail	Cloud	Messagerie instantanée	Multimédia en ligne
(consultation de sites)	(messagerie électronique)	(stockage et partage)	(WhatsApp, etc.)	(vidéo, audio, etc.)

Idée à retenir

Internet est l'**infrastructure mondiale** qui relie des millions d'appareils et permet d'accéder à une grande variété de services numériques.

Les caractéristiques principales d'Internet

Réseau mondial

Un réseau de réseaux interconnectés à l'échelle de la planète.

Accès permanent (24/7)

Disponible en continu, à tout moment et en tout lieu.

Échange de données

Transmission rapide de différents types de données (texte, image, vidéo, son, fichiers, etc.).

Interopérabilité

Relie des équipements et des systèmes différents (ordinateurs, smartphones, objets connectés, etc.).



Accessibilité et ouverture

Ouvert à un grand nombre d'utilisateurs (étudiants, entreprises, administrations, etc.).

Évolutivité

Un réseau en constante expansion (nouveaux services et utilisateurs).

Diversité de services

Accès à de nombreux services : Web, e-mail, Cloud, visioconférence, réseaux sociaux, commerce en ligne, etc.

Besoin de sécurité

Nécessite des mesures de protection (antivirus, pare-feu, mots de passe, etc.) face aux menaces en ligne.

En résumé

Internet est un réseau mondial, ouvert, évolutif et riche en services, qui facilite la communication, l'accès à l'information et la collaboration, tout en nécessitant une sécurité adaptée.

Le Web (World Wide Web) : définition

Définition

Le Web (World Wide Web) est un service d'Internet qui permet de consulter, de publier et de partager des informations sous forme de pages Web interconnectées (sites Web).

Comment fonctionne le Web ?



Technologies clés du Web

- **HTML : structure et** contenu de la page (titres, textes, images...).
- **CSS : mise en forme** et présentation (couleurs, styles, mise en page...).
- **JavaScript : interactivité** (formulaires, animations, fonctions dynamiques...).

Exemples de sites Web

Google	Wikipédia	YouTube	Moodle	Sites marchands
(recherche)	(encyclopédie)	(vidéo)	(formation)	(achats en ligne)

Internet vs Web : quelle différence ?

Critère	Internet	Web (WWW)
Nature	Réseau mondial de réseaux	Service d'Internet
Rôle	Transporter les données et connecter les réseaux	Consulter et publier des pages (sites Web)
Exemple	La connexion (réseau)	Les sites Web (Google, Wikipédia...)

À retenir

Le Web est une application d'Internet qui repose sur des pages Web reliées entre elles et accessibles via un navigateur Web.

Internet vs Web : quelle différence ?

Comparaison synthétique

Critère	Internet	Web (WWW)
Définition	Réseau mondial de réseaux interconnectés.	Service d'Internet permettant de consulter des pages Web.
Nature	Infrastructure de communication.	Application / service.
Rôle	Transporter les données et connecter les appareils.	Publier, consulter et partager des informations.
Technologies	TCP/IP, routeurs, réseaux, FAI, DNS...	HTML, CSS, JavaScript, HTTP/HTTPS.
Exemples	La connexion réseau (ADSL, fibre, 4G/5G, Wi-Fi).	Google, Wikipédia, YouTube, Moodle, etc.

Relation entre Internet et le Web

Internet : l'infrastructure (le réseau)



Web (WWW) : un service qui fonctionne sur Internet



Idée clé

Internet est le **réseau** (l'autoroute), tandis que le Web est un **service** qui utilise ce réseau (les sites et leurs contenus).

La relation entre Internet et le Web

Idée principale

Le Web est un service qui fonctionne sur Internet.

Autrement dit, Internet est le réseau (l'infrastructure), et le Web est l'un des services qu'il transporte.

Analogie simple



Internet = le réseau (la route)



Web = un service sur cette route (une station de services)

Représentation de la relation



Les services d'Internet (exemples)



Web (WWW)



E-mail (messagerie)



Transfert de fichiers (FTP)



Cloud (stockage, partage)



Streaming (vidéo, audio)

Position du Web dans l'ensemble d'Internet



À retenir

Internet est la **plateforme de communication mondiale**, et le Web (WWW) est un **service** parmi d'autres services offerts par Internet.

Les terminologies essentielles d'Internet

Internet — Réseau mondial de réseaux interconnectés.

Web (WWW) — Service d'Internet permettant de consulter des pages Web.

URL — Adresse unique d'une ressource sur le Web (ex. : https://www.univ-elbayadh.dz).

Adresse IP — Identifiant numérique d'un appareil sur le réseau (ex. : 192.168.1.10).

DNS — Service qui traduit un nom de domaine en adresse IP (ex. : www.google.com → 142.250.185.206).

Nom de domaine — Nom lisible d'un site Web (ex. : google.com, univ-elbayadh.dz).



Routeur — Équipement qui oriente et achemine les données entre plusieurs réseaux.

Serveur — Ordinateur qui fournit des services Web, e-mail, fichiers, etc.

Client — Appareil ou logiciel qui demande et utilise un service (navigateur, application, etc.).

HTTP / HTTPS — Protocoles de communication Web (HTTPS = version sécurisée et chiffrée de HTTP).

Navigateur Web — Logiciel permettant de consulter des sites Web (Chrome, Firefox, Edge, etc.).

Wi-Fi — Technologie d'accès sans fil à Internet.

À retenir

Ces terminologies sont les notions de base pour comprendre le fonctionnement d'Internet et l'utilisation du Web et de ses services.

L'URL : Uniform Resource Locator

Définition

L'URL (Uniform Resource Locator) est l'adresse unique qui permet de localiser et d'accéder à une ressource sur le Web (page, image, vidéo, fichier, etc.).

Structure d'une URL

`https://` `www.` `univ-elbayadh.dz` `/course/tic` `?sem=2` `#intro`

Protocole	Sous-domaine	Nom de domaine	Chemin	Paramètres	Ancre
(méthode d'accès)	(optionnel)	(identifie le site)	(ressource sur le site)	(informations supplémentaires)	(section dans la page)



Rôle

- Identifier la ressource.
- Indiquer son emplacement sur Internet.
- Permettre son accès via un navigateur Web.

Principaux protocoles

- **https://** — Connexion sécurisée (chiffrement des données) – Recommandé.
- **http://** — Connexion non sécurisée (données en clair).

Exemples d'URL

- https://www.google.com (site Web)
- https://www.univ-elbayadh.dz (site institutionnel)
- https://www.youtube.com/watch?v=abc123 (vidéo)

À retenir

Une URL est composée d'un **protocole**, d'un **nom de domaine**, d'un **chemin** et éventuellement de **paramètres** et d'une **ancre**.

HTTP et HTTPS : les protocoles de communication

Définition

HTTP (HyperText Transfer Protocol) et HTTPS (HTTP Secure) sont des **protocoles de communication** qui permettent l'échange de données entre un navigateur Web (client) et un serveur Web.

Rôle

- Transférer les pages Web et leurs contenus.
- Définir le format des échanges entre client et serveur.
- Assurer la sécurité des données avec HTTPS.

Principe de fonctionnement



Comparaison HTTP vs HTTPS

Critère	HTTP	HTTPS
Sécurité	Non (données en clair)	Oui (données chiffrées)
Protocole	http://	https://
Port par défaut	80	443
Certificat SSL/TLS	Non	Oui (certificat numérique)
Usage conseillé	Sites simples (peu sensibles)	Sites sensibles (banques, e-commerce, comptes, etc.)

Exemples d'URL

http://www.exemple.dz	Connexion non sécurisée
https://www.exemple.dz	Connexion sécurisée (Recommandée)

Certificat SSL/TLS



Le protocole HTTPS utilise un certificat SSL/TLS qui chiffre les données et authentifie l'identité du site Web.

À retenir

HTTP permet l'échange de données sans sécurité, tandis que **HTTPS** ajoute un chiffrement (SSL/TLS) pour protéger la confidentialité et l'intégrité des données.

Le DNS : Système de Noms de Domaine

Définition

Le DNS (Domain Name System) est un service qui traduit un nom de domaine (ex. : www.google.com) en adresse IP (ex.:142.250.185.206) pour permettre l'accès aux sites Web.

Rôle

- Associer un nom facile à retenir à une adresse IP.
- Localiser le serveur d'un site Web sur Internet.
- Rendre la navigation plus simple et rapide.

Principe de fonctionnement du DNS



Exemples de résolution DNS

Nom de domaine	Adresse IP (exemple)
www.google.com	142.250.185.206
www.youtube.com	142.250.184.206
www.wikipedia.org	208.80.154.224
www.univ-elbayadh.dz	41.111.154.10

Structure d'un nom de domaine

www. univ-elbayadh dz

- www. : Sous-domaine (optionnel)
- univ-elbayadh : Nom de domaine (identifiant du site)
- dz : Extension (TLD) (pays : Algérie)

Quelques serveurs DNS publics

Service	Adresse(s) DNS
Google	8.8.8.8 / 8.8.4.4
Cloudflare	1.1.1.1 / 1.0.0.1
OpenDNS	208.67.222.222 208.67.220.220

Hiérarchie du DNS



À retenir

Le DNS fait le lien entre un nom de domaine et une adresse IP. Il agit comme un annuaire d'Internet, indispensable pour accéder aux sites Web.

L'adresse IP : identifier un appareil sur Internet

Définition

L'adresse IP (Internet Protocol) est un identifiant numérique unique attribué à chaque appareil connecté à un réseau (ordinateur, smartphone, serveur, etc.).

Rôle

- Identifier un appareil sur un réseau.
- Permettre la communication entre les appareils.
- Acheminer les données vers la bonne destination.

Les deux versions d'adresse IP

IPv4

- Version la plus utilisée.
- Adresse sur 32 bits.
- Format décimal : 4 nombres (0–255) séparés par ".".

Ex. : 192.168.1.10

IPv6

- Version moderne (Internet des objets, croissance du Web).
- Adresse sur 128 bits.
- Format hexadécimal : 8 blocs séparés par ":".

Ex. : 2001:db8:85a3::8a2e:370:7334

Types d'adresses IP

Adresse publique : Unique sur Internet, visible depuis l'extérieur (ex. : 41.111.154.10).

Adresse privée : Utilisée à l'intérieur d'un réseau local (LAN), non accessible directement depuis Internet (ex. : 192.168.1.10).

Format d'une adresse IPv4

192 . 168 . 1 . 10

← 4 octets (32 bits) →

Chaque octet ∈ [0 – 255]

Exemples d'adresses IP

Type	Exemple
Publique (IPv4)	41.111.154.10
Privée (IPv4)	192.168.1.10
IPv6	2001:db8:85a3::1

Exemple de réseau (LAN)



À retenir

L'adresse IP est un identifiant numérique qui identifie un appareil et permet la communication sur un réseau (Internet ou réseau local).

Les noms de domaine et les extensions

Définition

Le nom de domaine est un **nom lisible et facile à mémoriser** qui identifie un site Web sur Internet et remplace son adresse IP (ex. : www.google.com).

Rôle

- Identifier un site Web sur Internet.
- Faciliter l'accès et la mémorisation.
- Donner une identité (organisation, marque, institution, etc.).

Structure d'un nom de domaine

www. | **univ-elbayadh** | **.dz**

- **www.** — Sous-domaine (optionnel)
- **univ-elbayadh** — Nom de domaine (identifie le site)
- **.dz** — Extension (TLD) (pays : Algérie)

Principales catégories d'extensions

Catégorie	Exemples	Signification / Usage
Génériques	.com, .org, .net	Usages généraux (entreprise, organisation, réseau, etc.).
Éducatives	.edu, .ac	Universités et établissements d'enseignement.
Gouvernementales	.gov	Organismes et services publics.
Territoriales (pays)	.dz, .fr, .tn, .us	Sites liés à un pays ou une région (.dz : Algérie).
Professionnelles	.info, .biz, .co	Information, activités commerciales, entreprises, etc.

Les extensions (TLD)

.TLD

L'extension (TLD : Top-Level Domain) est la partie finale du nom de domaine (ex. : .com, .org, .dz) qui indique la nature ou le pays du site.

Exemples de noms de domaine

www.google.com	Site commercial mondial (moteur de recherche).
www.univ-elbayadh.dz	Site universitaire algérien.
www.wikipedia.org	Encyclopédie libre (organisation à but non lucratif).

Règles de choix d'un bon nom de domaine

- Court et facile à mémoriser.
- Clair et pertinent (lié au contenu).
- Sans caractères spéciaux (é, à, ç, %, ...).
- Utiliser une extension appropriée (ex. : .dz pour l'Algérie).

www.

À retenir

Le **nom de domaine** est **l'identité lisible** d'un site Web, et son **extension (TLD)** précise sa **nature** (ex. : .com, .org) ou son **pays** (ex. : .dz).

Les serveurs Web et l'hébergement des sites

Définition

Un **serveur Web** est un ordinateur (physique ou virtuel) qui stocke les fichiers d'un site Web (pages, images, vidéos, ...) et les met à disposition des utilisateurs via Internet (HTTP/HTTPS).

Rôle

- Stocker et publier les sites Web.
- Traiter les requêtes des navigateurs.
- Fournir les pages et les ressources aux utilisateurs.

Principe de fonctionnement (modèle client–serveur)



Types d'hébergement

Mutualisé	VPS (Virtuel)	Dédié	Cloud
Plusieurs sites sur le même serveur. Économique.	Serveur virtuel dédié. Plus de contrôle et de performances.	Un serveur exclusif pour un seul site. Hautes performances.	Ressources flexibles et évolutives (à la demande). Très disponible.

Hébergement d'un site Web

L'hébergement (ou hosting) est un service qui fournit un serveur et les ressources nécessaires (espace de stockage, bande passante, sécurité, ...) pour rendre un site Web accessible sur Internet 24h/24.

Exemples de serveurs Web

Serveur Web	Logo	Caractéristiques principales
Apache		Libre, stable, très utilisé.
Nginx	NGINX	Rapide, léger, haute performance.
Microsoft IIS	IIS	Serveur Web de Microsoft.
LiteSpeed	LiteSpeed	Performant et économe en ressources.

À retenir

Un **serveur Web** héberge et publie un site sur Internet. L'**hébergement** fournit les ressources nécessaires pour le rendre accessible en permanence.

Les principaux services d'Internet

Définition

Les services d'Internet sont un ensemble d'applications et de ressources accessibles via le réseau Internet pour communiquer, chercher, partager, stocker et collaborer.

Rôle

- Faciliter la communication.
- Accéder à l'information.
- Partager et échanger des fichiers et des données.
- Travailler et collaborer à distance.



Web (WWW)



Consulter et publier des pages Web (sites, actualités, cours, ...).

FTP (File Transfer Protocol)

Transférer des fichiers entre un ordinateur et un serveur (ex. : FileZilla).

Streaming

Lire des contenus multimédias en continu (vidéos, musique, TV en ligne) (ex. : YouTube, Netflix).

Messagerie instantanée



Échanger des messages, des fichiers et des appels (ex. : WhatsApp, Telegram).

E-mail (courrier électronique)



Envoyer et recevoir des messages électroniques (ex. : Gmail, Outlook).

Cloud (informatique en nuage)



Stocker, synchroniser et partager des fichiers en ligne (ex. : Google Drive, OneDrive, Dropbox).

Visioconférence



Communiquer en temps réel en audio et vidéo (ex. : Zoom, Google Meet, Microsoft Teams).

Réseaux sociaux



Partager des informations, interagir et collaborer (ex. : Facebook, Instagram, YouTube, LinkedIn).

À retenir

Internet offre une variété de services complémentaires (Web, e-mail, transfert de fichiers, Cloud, streaming, visioconférence, réseaux sociaux) pour s'informer, communiquer et collaborer.

Le courrier électronique (E-mail)

Définition

Le courrier électronique (E-mail) est un service Internet qui permet d'envoyer, recevoir et gérer des messages électroniques (texte, fichiers, images, ...) entre utilisateurs.

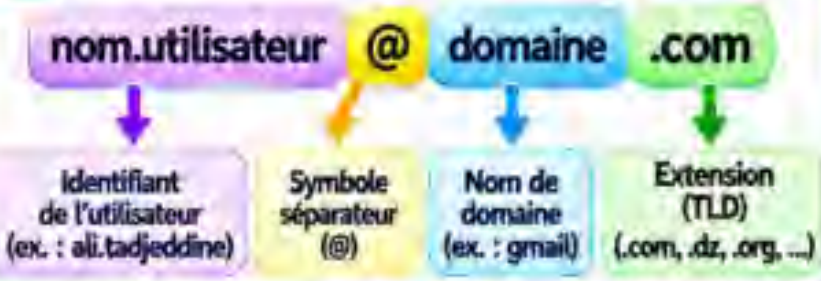
Rôle

- Communication rapide et à faible coût.
- Échange de documents et de fichiers.
- Usage personnel, professionnel et universitaire.

Principe de fonctionnement



Structure d'une adresse e-mail



Principaux services de messagerie

Gmail (gmail.com)	Outlook (outlook.com)	Yahoo Mail (yahoo.com)

Avantages

- Rapidité et accessibilité (24h/24, partout).
- Envoi de fichiers (documents, images, ...).
- Coût réduit (gratuits ou peu coûteux).
- Organisation (dossiers, recherche, filtres).

Exemple d'interface (Gmail)



Bonnes pratiques

- Utiliser un mot de passe fort et unique.
- Ne pas ouvrir les pièces jointes suspects.
- Vérifier l'expéditeur du message.
- Activer la vérification en deux étapes (2FA).

À retenir

L'e-mail est un service Internet essentiel qui permet de communiquer, d'échanger des fichiers et de collaborer, de manière simple, rapide et sécurisée.

Le transfert de fichiers : FTP (File Transfer Protocol)

Définition

Le FTP (File Transfer Protocol) est un protocole Internet qui permet de **transférer des fichiers** entre un ordinateur (client) et un serveur (serveur FTP) via un réseau (Internet).

Principe de fonctionnement



Principaux clients FTP

- **FileZilla** (gratuit, multi-plateforme)
- **Cyberduck** (Windows, macOS)
- **WinSCP** (Windows)

Paramètres courants

Hôte (serveur)	ex. : ftp.univ-elbayadh.dz
Port (FTP)	21
Nom d'utilisateur	ex. : etudiant
Mot de passe	********
Mode de transfert	Actif ou Passif

Rôle

- Déposer des fichiers sur un serveur.
- Télécharger des fichiers depuis un serveur.
- Gérer et organiser des fichiers à distance (ajout, suppression, renommage, etc.).

Exemple d'utilisation : FileZilla



Avantages

- Transfert de fichiers simple et efficace.
- Compatible avec de nombreux systèmes.
- Permet la gestion des fichiers à distance.

Cas d'utilisation

- Publication d'un site Web (transfert des fichiers sur un serveur).
- Partage de documents de grande taille.
- Sauvegarde et synchronisation de fichiers.

Alternative sécurisée : SFTP

SFTP (SSH File Transfer Protocol) est une version sécurisée du FTP :

- Chiffrement des données.
- Authentification sécurisée.
- Port par défaut : 22.



À retenir

Le FTP est un protocole de transfert de fichiers qui permet d'envoyer, de télécharger et de gérer des fichiers entre un client et un serveur sur Internet.

Les navigateurs Web : définition et rôle

Définition

Un navigateur Web (ou navigateur Internet) est un logiciel qui permet d'accéder aux sites Web, de les consulter et d'interagir avec leurs contenus (textes, images, vidéos, formulaires, ...).

Principales fonctions



Exemples de navigateurs Web

Google Chrome · Mozilla Firefox · Microsoft Edge · Safari (Apple) · Opera

Rôle

- Accéder aux sites Web via une URL.
- Afficher les pages Web et leurs contenus.
- Interagir avec les services en ligne (recherche, e-mail, formulaires, ...).

Interface d'un navigateur (ex. : Google Chrome)



Bonnes pratiques

- Utiliser un navigateur à jour.
- Privilégier les sites sécurisés (https://).
- Activer le bloqueur de fenêtres pop-up.
- Installer des extensions fiables.
- Vider régulièrement le cache et les cookies.

À retenir

Un navigateur Web est un logiciel indispensable pour accéder, consulter et utiliser les services du Web de manière simple, rapide et sécurisée.

Présentation de l'interface d'un navigateur Web

Objectif

Identifier et comprendre les principaux éléments de l'interface d'un navigateur Web (exemple : Google Chrome) et leur rôle.

Rôle

- Accéder aux sites Web (URL).
- Naviguer entre les pages (Précédent / Suivant).
- Gérer plusieurs onglets.
- Personnaliser et sécuriser la navigation.

Interface de Google Chrome : principaux éléments



Description des éléments

1	Précédent / Suivant	Revenir à la page précédente ou aller à la page suivante.
2	Actualiser	Recharger la page en cours.
3	Barre d'adresse (URL)	Saisir l'adresse d'un site Web (ex. : https://www.google.com).
4	Favoris (Signet)	Enregistrer le site dans les favoris pour un accès rapide.
5	Menu	Accéder aux paramètres, à l'historique, aux téléchargements, ...
6	Onglet	Afficher plusieurs sites dans une même fenêtre.
7	Nouvel onglet	Ouvrir une nouvelle page (nouvel onglet).
8	Commandes de la fenêtre	Réduire, agrandir/restaurer et fermer le navigateur.
9	Barre des favoris	Accès rapide aux sites les plus utilisés (ex. : Cours, YouTube, Drive, ...).

Exemples d'actions courantes

- Saisir une URL et visiter un site
- Ajouter un favori
- Organiser les favoris (en dossiers)
- Télécharger un fichier
- Installer une extension (ex. : bloqueur de pub)

Bonnes pratiques

- Utiliser la navigation sécurisée (HTTPS).
- Maintenir le navigateur à jour.
- Installer des extensions fiables.
- Ne pas enregistrer de données sensibles sur des sites non sécurisés.

À retenir

L'interface d'un navigateur Web est composée d'éléments simples (onglets, barre d'adresse, favoris, menu, ...) qui facilitent la navigation, l'accès aux sites et la gestion des services du Web.

Les principaux navigateurs Web : comparaison

Objectif

Comparer les principaux navigateurs Web afin d'identifier leurs caractéristiques, avantages, limites et cas d'utilisation.

Critères de comparaison

- Performance (vitesse).
- Sécurité et confidentialité.
- Consommation de ressources (RAM).
- Extensions et fonctionnalités.
- Compatibilité et disponibilité (OS).

Comparaison des principaux navigateurs Web

Critère	Chrome	Firefox	Edge	Safari	Opera
Éditeur	Google	Mozilla	Microsoft	Apple	Opera Software
Systèmes (OS)	Windows, macOS, Linux, Android, iOS	Windows, macOS, Linux, Android, iOS	Windows, macOS, Android, iOS	macOS, iOS	Windows, macOS, Linux, Android, iOS
Performance (vitesse)	★★★★☆	★★★★☆	★★★★★	★★★★★	★★★★☆
Sécurité / Confidentialité	Élevée	Élevée (orientée vie privée)	Élevée	Très élevée (écosystème Apple)	Élevée (VPN intégré)
Consommation RAM	Élevée	Modérée	Modérée	Faible	Modérée
Extensions	Très nombreuses	Nombreuses	Nombreuses (compatibles Chrome)	Limitées	Nombreuses
Fonctionnalités spéciales	Synchronisation, applications Google	Protection renforcée de la vie privée	Intégration Microsoft 365, IA (Copilot)	Optimisé Apple, faible énergie	VPN, bloqueur de publicités, mode turbo



Cas d'utilisation (exemples)

- Études / Recherche → Chrome ou Firefox.
- Travail (Microsoft) → Edge.
- Écosystème Apple → Safari.
- Navigation sécurisée / VPN → Opera.

Recommandation

- Choisir le navigateur selon vos besoins (performance, sécurité, confidentialité, écosystème).
- Il est possible d'utiliser plusieurs navigateurs selon les usages (ex. : Chrome pour le quotidien et Firefox pour la vie privée).

Avantages et limites

- **Chrome** : + Rapide, riche en extensions. − Consomme beaucoup de RAM.
- **Firefox** : + Respecte la vie privée (open source). − Moins rapide que Chrome.
- **Edge** : + Performant, intégré à Windows (Microsoft 365). − Collecte de données Microsoft.
- **Safari** : + Très rapide et économe (macOS/iOS). − Extensions limitées.
- **Opera** : + VPN et bloqueur de publicités intégrés. − Moins utilisé que les autres.

À retenir

Chaque navigateur Web a ses atouts et ses limites. Le choix du meilleur navigateur dépend de vos besoins, de votre système et de vos priorités (vitesse, sécurité, confidentialité, ...).

Les moteurs de recherche et leur fonctionnement

Définition

Un moteur de recherche est un service Web qui permet de trouver rapidement des informations (pages Web, images, vidéos, documents, ...) sur Internet à partir de mots-clés.

Principe de fonctionnement d'un moteur de recherche

1. **Exploration (Crawling)** — Des robots (crawlers) parcourent le Web et collectent les pages.
2. **Indexation (Indexing)** — Les pages collectées sont analysées, organisées et stockées dans un index (une grande base de données).
3. **Traitement de la requête** — Le moteur analyse les mots-clés saisis par l'utilisateur.
4. **Classement (Ranking)** — Les résultats les plus pertinents sont affichés selon plusieurs critères (pertinence, qualité, popularité, ...).

Exemples de moteurs de recherche

Google	Le plus utilisé, très complet.
Bing (Microsoft)	Intégré à Windows, avec l'IA (Copilot).
Yahoo	Recherche générale et actualités.
DuckDuckGo	Respecte la vie privée (ne trace pas l'utilisateur).
Ecosia	Moteur écologique (finance la plantation d'arbres).

Rôle

- Rechercher des informations sur le Web.
- Accéder rapidement à des ressources fiables.
- Explorer des contenus variés (sites, images, vidéos, articles, ...).

Exemple de recherche (Google)

Google — photosynthèse plantes — Requête (mots-clés)

Tous | Images | Vidéos | Actualités | Livres | Web | Plus › — Types de résultats

Wikipédia
https://fr.wikipedia.org › Photosynthèse
Photosynthèse — Wikipédia
La photosynthèse est le processus par lequel les plantes transforment l'énergie lumineuse en énergie chimique ... — Résultat (lien, titre et extrait)

Avantages

- Accès rapide à une grande quantité d'informations.
- Simple et gratuit.
- Résultats variés (texte, image, vidéo, ...).
- Outils de filtrage (date, langue, type de contenu).

Conseils et recherches avancées

Opérateur / Astuce		Exemple
"..."	Rechercher une expression exacte	"énergie solaire"
site:	Limiter la recherche à un site	site:edu.dz
filetype:	Rechercher un type de fichier	photosynthèse filetype:pdf
- (moins)	Exclure un mot des résultats	éolien -voiture

À retenir

Un moteur de recherche explore, indexe et classe les pages du Web pour fournir des résultats rapides et pertinents à partir de mots-clés.

Comment effectuer une recherche efficace sur Internet

Objectif

Apprendre à formuler des requêtes efficaces afin d'obtenir des résultats pertinents, fiables et rapides sur le Web.

Étapes d'une recherche efficace

1. **Définir le besoin** — Préciser le sujet et l'objectif de la recherche.
2. **Choisir les bons mots-clés** — Utiliser des mots simples, précis et pertinents.
3. **Utiliser des opérateurs** — Affiner la requête (« », AND, OR, -, site:, filetype:).
4. **Évaluer les résultats** — Vérifier la fiabilité, la date et la source de l'information.

Opérateurs de recherche utiles

Opérateur	Rôle	Exemple
« ... »	Rechercher une expression exacte	"énergie solaire"
AND	Exiger la présence de plusieurs mots	photosynthèse AND lumière
OR	Rechercher l'un ou l'autre terme	plante OR végétal
- (moins)	Exclure un mot des résultats	Jaguar -voiture
site:	Limiter la recherche à un site précis	site:edu.dz TIC
filetype:	Rechercher un type de fichier	filetype:pdf photosynthèse

Pourquoi ?

- Gagner du temps.
- Obtenir des informations de qualité.
- Éviter les résultats non pertinents.
- Filtrer et affiner sa recherche.

Exemple pratique : recherche sur Google

Google "photosynthèse" site:edu.dz filetype:pdf

PDF https://www.univ-elbayadh.dz › cours

La photosynthèse chez les plantes.pdf

Cours de biologie : mécanisme de la photosynthèse, rôle de la lumière et des pigments chlorophylliens ...

Bonnes pratiques

- Utiliser des mots-clés précis et pertinents.
- Combiner plusieurs opérateurs.
- Privilégier les sites fiables (edu, org, gov, revues scientifiques).
- Vérifier la date de publication.
- Comparer plusieurs sources.

À éviter

- Utiliser des mots trop généraux (ex. : plante).
- Copier des informations sans vérifier la source.
- Se limiter au premier résultat.
- Utiliser des sites non fiables ou sans auteur.

À retenir

Une recherche efficace repose sur des **mots-clés précis**, l'utilisation d'**opérateurs** et la vérification de la **fiabilité des sources.**

Évaluer la fiabilité des informations sur le Web

Objectif

Savoir vérifier la **crédibilité**, la **qualité** et la **pertinence** des informations trouvées sur Internet.

Pourquoi ?

- Éviter la désinformation et les fausses nouvelles (fake news).
- Utiliser des sources sérieuses et fiables.
- Produire un travail académique de qualité (rapport, exposé, mémoire, ...).

Critères d'évaluation d'une source (méthode CRAAP)

C	Actualité (Currency)	• L'information est-elle récente ? • La date de publication est-elle indiquée ?
R	Pertinence (Relevance)	• L'information répond-elle à mon besoin ? • Est-elle adaptée au contexte (cours, recherche, ...) ?
A	Autorité (Authority)	• Qui est l'auteur ? (expert, chercheur, institution) • Quelles sont ses qualifications et sa réputation ?
A	Exactitude (Accuracy)	• Les informations sont-elles justes et vérifiables ? • Sont-elles appuyées par des sources ou des références ?
P	Objectivité (Purpose)	• Quel est le but du site ? (informer, vendre, influencer ?) • L'information est-elle neutre et équilibrée ?

Exemples de sources : fiables ou non ?

Sources fiables (à privilégier)

- Sites institutionnels : .edu.dz, .gov.dz (ex. : univ-elbayadh.dz, mesrs.dz)
- Revues scientifiques : ScienceDirect, Springer, IEEE Xplore, Wiley.
- Organismes reconnus : OMS (who.int), FAO (fao.org), AIE (iea.org).



Sources non fiables (à éviter)

- Blogs ou sites personnels sans auteur identifié.
- Sites à visée commerciale ou publicitaire.
- Pages sans références ni date de publication.



Signes d'une information peu fiable



- Titre sensationnel ou exagéré.
- Absence d'auteur ou auteur inconnu.
- Aucune référence ni source citée.
- Informations contradictoires.
- Nombreuses fautes d'orthographe.

Bonnes pratiques



- Vérifier l'auteur et l'organisme éditeur.
- Contrôler la date et la mise à jour.
- Croiser l'information avec plusieurs sources.
- Privilégier les sources académiques et institutionnelles.
- Citer correctement les sources dans vos travaux.

À retenir

Une information fiable est **récente**, **pertinente**, issue d'un auteur ou d'un organisme **crédible**, **vérifiable** et présentée de manière **objective**.

Les cookies et la navigation sur le Web

Définition

Un cookie est un **petit fichier texte** enregistré sur votre appareil par un site Web pour mémoriser des informations liées à votre navigation.

Comment fonctionnent les cookies ?



1. Visite d'un site Web
2. Le site enregistre un cookie sur votre appareil
3. Lors des visites suivantes, le site lit le cookie pour vous reconnaitre

Types de cookies

Essentiels (techniques)	Nécessaires au bon fonctionnement du site (ex. : session, sécurité).
De préférence	Mémorisent vos choix (langue, thème, ...).
De statistiques (analytiques)	Mesurent l'audience et améliorent le site (ex. : Google Analytics).
Publicitaires (marketing)	Affichent des publicités personnalisées selon votre navigation.

Rôle (utilité)

- Se souvenir de vos préférences.
- Maintenir votre session ouverte.
- Personnaliser votre expérience.
- Analyser la fréquentation du site.
- Proposer des contenus et publicités adaptés.

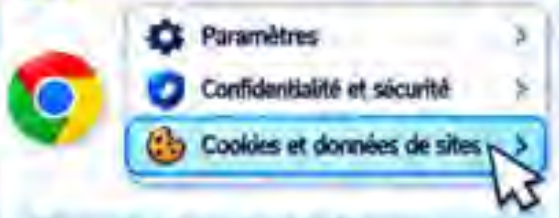
Avantages

- Navigation plus fluide et plus rapide.
- Expérience personnalisée (langue, contenu, ...).
- Mémorisation des préférences et des connexions.

Risques / Inconvénients

- Suivi de la navigation (profilage).
- Atteinte possible à la vie privée.
- Collecte de données personnelles (sans consentement clair).
- Publicités ciblées parfois intrusives.

Gérer les cookies dans le navigateur



Exemple : Dans Google Chrome
Paramètres → Confidentialité et sécurité → Cookies et données de sites.

Bonnes pratiques

- Accepter uniquement les cookies nécessaires.
- Personnaliser vos préférences.
- Supprimer régulièrement les cookies.
- Utiliser la navigation privée (mode incognito).
- Lire la politique de confidentialité du site.

À retenir

Les cookies **facilitent la navigation** et **personnalisent l'expérience**, mais ils peuvent aussi suivre votre activité. Il est important de les **gérer** pour **protéger votre vie privée.**

La navigation privée et la protection de la vie personnelle

Définition

La navigation privée (ou incognito) est un mode du navigateur qui permet de naviguer **sans enregistrer certaines informations locales** sur l'appareil (historique, cookies, formulaires, ...).

Comment ça fonctionne ?



1. Ouverture d'une fenêtre privée (incognito).
2. Les données de navigation ne sont pas enregistrées localement.
3. À la fermeture, les données temporaires (historique, cookies, ...) sont supprimées.

Navigation privée dans les principaux navigateurs

Google Chrome	Ctrl + Shift + N	Fenêtre de navigation privée
Mozilla Firefox	Ctrl + Shift + P	Fenêtre privée
Microsoft Edge	Ctrl + Shift + N	InPrivate
Opera	Ctrl + Shift + N	Fenêtre privée
Safari (macOS)	⌘ + Shift + N	Navigation privée

Objectif

- Limiter les traces de navigation sur l'appareil.
- Renforcer la confidentialité ponctuellement.
- Éviter l'enregistrement de l'historique, des cookies et des données de formulaires.

Navigation normale vs navigation privée

Élément	Navigation normale	Navigation privée
Historique de navigation	Enregistré	Non enregistré
Cookies	Conservés	Supprimés à la fermeture
Données de formulaires	Enregistrées	Non enregistrées
Fichiers téléchargés	Conservés	Conservés
Favoris (bookmarks)	Disponibles	Disponibles

Avantages

- Plus de confidentialité sur l'appareil.
- N'enregistre pas l'historique ni les cookies.
- Utile sur un ordinateur partagé (labo, bibliothèque, ...).
- Limite le suivi local par les sites.

Limites

- Ne rend pas anonyme sur Internet.
- Ne cache pas votre adresse IP (visible par votre fournisseur d'acces).
- N'empêche pas le suivi en ligne par d'autres moyens (ex. : compte, empreinte du navigateur).
- Ne protège pas des logiciels malveillants.

Bonnes pratiques pour protéger sa vie privée

- Utiliser la navigation privée selon le besoin.
- Gérer et supprimer régulièrement les cookies.
- Éviter de se connecter à des comptes sensibles sur un appareil public.
- Utiliser un VPN pour masquer l'adresse IP.
- Maintenir le navigateur à jour et utiliser un antivirus.

À retenir

La navigation privée **limite l'enregistrement des traces locales**, mais elle ne garantit pas **l'anonymat complet** sur Internet. Pour une meilleure protection, il faut adopter **plusieurs mesures.**

Le Cloud Computing : définition et principes

Définition

Le Cloud Computing (ou informatique en nuage) est un modèle qui permet d'accéder, via Internet, à des ressources et des services informatiques (serveurs, stockage, logiciels, etc.) à la demande, sans les posséder localement.

Principe de fonctionnement



Modèles de services (selon l'usage)

IaaS (Infrastructure as a Service)
→ Ressources matérielles virtuelles (serveurs, stockage, réseau).
Ex. : Amazon EC2, Microsoft Azure.

PaaS (Platform as a Service)
→ Environnement de développement et d'exécution d'applications.
Ex. : Google App Engine, Heroku.

SaaS (Software as a Service)
→ Logiciels accessibles en ligne, prêts à l'emploi.
Ex. : Google Drive, Microsoft 365.

Pourquoi ?

- Accéder à ses données et applications partout.
- Disposer de ressources puissantes et flexibles.
- Réduire les coûts matériels et de maintenance.
- Faciliter le travail collaboratif.

Types de déploiement

Cloud public	Ressources partagées par plusieurs utilisateurs. (Ex. : Google Cloud, AWS)
Cloud privé	Ressources dédiées à une seule organisation. (Ex. : cloud d'une université)
Cloud hybride	Combinaison des deux (modèle public + privé).

Exemples de services Cloud

- Google Drive (Stockage, partage)
- OneDrive (Stockage, synchro)
- Dropbox (Stockage, partage)
- Microsoft 365 (Bureautique en ligne)
- Gmail (Messagerie en ligne)
- Google Photos (Sauvegarde de photos)

Avantages

- Accessibilité (partout, à tout moment).
- Flexibilité et évolutivité (ressources à la demande).
- Réduction des coûts (moins d'équipements).
- Sauvegarde et sécurité des données (haute disponibilité).

Limites

- Dépendance à une connexion Internet.
- Risques liés à la confidentialité des données.
- Coût variable selon l'usage et le volume.
- Dépendance au fournisseur (verrouillage possible).

À retenir

Le Cloud Computing permet d'utiliser, via Internet, des ressources et des services informatiques à la demande, de manière flexible, économique et sécurisée.

Les types de Cloud : public, privé et hybride

Objectif

Comprendre les différents types de Cloud (public, privé et hybride) afin de choisir le modèle adapté à ses besoins.

Pourquoi ?

- Répondre à des besoins variés.
- Maîtriser les options de déploiement.
- Optimiser les coûts et la sécurité.
- Assurer la flexibilité et la continuité des services.

Définition et caractéristiques

Cloud public



- Ressources partagées entre plusieurs utilisateurs.
- Géré par un fournisseur externe (ex. : AWS, Google Cloud, Azure).
- Coût réduit et mise en service rapide.

Cloud privé



- Ressources dédiées à une seule organisation.
- Contrôle et sécurité élevés.
- Peut être hébergé en interne ou chez un fournisseur.

Cloud hybride



- Combinaison du Cloud public et du Cloud privé.
- Flexibilité et meilleure optimisation des ressources.
- Permet de garder les données sensibles en privé et les autres en public.

Exemples d'utilisation

Cloud public :
Stockage et partage de fichiers (ex. : Google Drive, Dropbox).

Cloud privé :
Hébergement des données sensibles d'une université (ex. : gestion des étudiants).

Cloud hybride :
Plateforme de recherche (université) : données sensibles en privé et calcul intensif en public.

Comparaison des trois types de Cloud

Critère	Cloud public	Cloud privé	Cloud hybride
Sécurité	Moyenne à élevée	Élevée	Élevée (selon la configuration)
Coût	Faible	Élevé	Intermédiaire
Gestion	Par le fournisseur	Par l'organisation	Mixte
Flexibilité	Élevée	Moyenne	Élevée
Mise en service	Très rapide	Plus longue	Rapide et évolutive

Avantages et inconvénients

Avantages (globaux)

- Accès aux ressources à la demande.
- Évolutivité et haute disponibilité.
- Réduction des coûts (selon le modèle).
- Continuité et sauvegarde des données.

Inconvénients (possibles)

- Dépendance à la connexion Internet.
- Risques de sécurité et de confidentialité.
- Coûts variables (usage et stockage).
- Complexité de gestion (surtout en hybride).

À retenir

On distingue trois types de Cloud : **public** (partagé et économique), **privé** (dédié et sécurisé) et **hybride** (une combinaison des deux), à choisir selon **les besoins**, la **sécurité** et **le budget**.

Les services Cloud : stockage, partage et collaboration

Définition

Les services Cloud sont des applications en ligne qui permettent de **stocker des données**, de **les partager** et de **travailler à plusieurs** à distance, via Internet.

Objectifs

- Sauvegarder et accéder aux données partout.
- Partager facilement des fichiers.
- Travailler en équipe en temps réel.
- Synchroniser les données entre plusieurs appareils.

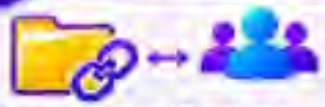
Principaux services Cloud

Stockage en ligne



- Conserver des fichiers dans le Cloud (documents, photos, vidéos, ...).
- Accès sécurisé depuis tout appareil (PC, tablette, smartphone).

Partage de fichiers



- Envoyer un lien de partage.
- Définir des droits d'accès (lecture, modification, ...).
- Collaborer sur les mêmes fichiers.

Collaboration en ligne



- Créer, modifier et commenter des documents en temps réel.
- Travailler à plusieurs sur un même projet (coédition).

Exemples de services populaires

Google Drive	Stockage, partage et bureautique en ligne (Docs, Sheets, Slides).
OneDrive	Stockage et collaboration (Microsoft 365).
Dropbox	Stockage et partage simples, synchronisation rapide.
iCloud	Stockage et synchronisation (écosystème Apple).
Microsoft 365	Suite collaborative (Word, Excel, PowerPoint en ligne).

Avantages

- Accessibilité 24 h/24, 7 j/7.
- Sauvegarde et sécurité des données.
- Travail collaboratif et productivité.
- Synchronisation automatique.
- Réduction des coûts (pas de serveur local).



Limites / précautions

- Dépendance à une connexion Internet.
- Risques de confidentialité (accès non autorisé).
- Espace de stockage parfois limité dans les offres gratuites.
- Nécessité de bien gérer les droits de partage.

Exemples d'utilisation (étudiants et enseignants)

- Sauvegarde des cours et des TP.
- Partage de documents et de ressources.
- Rédaction collaborative de rapports (Docs, Word Online).
- Gestion de projet et planification de groupe.
- Sauvegarde des travaux et accès depuis la maison.

Bonnes pratiques

- Utiliser un mot de passe fort et l'authentification à deux facteurs.
- Classer et organiser ses fichiers (dossiers, noms clairs).
- Contrôler régulièrement les droits de partage.
- Sauvegarder les données importantes dans plusieurs endroits.

À retenir

Les services Cloud facilitent le **stockage**, le **partage** et la **collaboration** des données, à distance, de manière **flexible**, **sécurisée** et **accessible** sur plusieurs appareils.

La sécurité sur Internet : enjeux et objectifs

Définition

La sécurité sur Internet est l'ensemble des mesures techniques, organisationnelles et comportementales visant à **protéger les données, les systèmes et les utilisateurs** lors de l'utilisation d'Internet.

Enjeux (pour l'utilisateur et l'organisation)

- Protection des données personnelles et sensibles.
- Maintien de la confiance dans les services en ligne.
- Continuité des activités (études, travail, services).
- Respect des lois et de la réglementation (ex. : RGPD).



Objectifs de la sécurité

- Assurer la confidentialité des informations.
- Garantir l'intégrité des données (non altération).
- Assurer la disponibilité des services (accès fiable).
- Prévenir, détecter et réduire les risques et les attaques.

Principales menaces

- Virus et malwares (logiciels malveillants).
- Hameçonnage (phishing) (vol de données).
- Piratage (accès non autorisé).
- Rançongiciel (ransomware) (chiffrement puis rançon).
- Réseaux non sécurisés (ex. : Wi-Fi public).

Les 3 principes fondamentaux (Triade CIA)

Confidentialité	Seules les personnes autorisées accèdent aux données.
Intégrité	Les données restent exactes et non modifiées.
Disponibilité	Les services et les données sont accessibles au bon moment.

Bonnes pratiques pour une navigation sécurisée

- Utiliser des mots de passe forts et uniques.
- Activer l'authentification à deux facteurs (2FA).
- Mettre régulièrement à jour le système et les logiciels.
- Utiliser un antivirus et un pare-feu (firewall).
- Privilégier les sites sécurisés (HTTPS).
- Éviter les réseaux Wi-Fi publics non sécurisés.
- Sauvegarder régulièrement ses données (Cloud ou disque externe).

À retenir

La sécurité sur Internet vise à **protéger** les données, garantir leur **intégrité** et leur **disponibilité**, et à **réduire les risques** liés aux menaces en ligne, grâce à des bonnes pratiques simples et efficaces.

Les virus informatiques et les logiciels malveillants

Définition

Un virus informatique est un logiciel malveillant (malware) qui s'infiltre dans un système, se réplique et peut perturber son fonctionnement, voler des données ou endommager des fichiers.

Principaux types de logiciels malveillants (malwares)

Virus
S'attache à des fichiers et se propage.

Ver (Worm)
Se propage automatiquement sur le réseau.

Cheval de Troie (Trojan)
Se fait passer pour un logiciel légitime.

Logiciel espion (Spyware)
Collecte des informations à l'insu de l'utilisateur.

Rançongiciel (Ransomware)
Chiffre les données et demande une rançon.

Logiciel publicitaire (Adware)
Affiche des publicités intrusives et non désirées.

Comment se fait l'infection ?

Lien ou pièce jointe infectée (e-mail) → Téléchargement d'un fichier ou d'un logiciel non fiable → Exécution du programme malveillant → Propagation et infection du système et des fichiers

Objectifs des malwares

- Dérober des informations (mots de passe, données personnelles).
- Prendre le contrôle du système (à distance).
- Chiffrer les fichiers pour exiger une rançon.
- Perturber ou rendre le système inutilisable.

Conséquences d'une infection



- Perte ou chiffrement des données.
- Vol d'informations sensibles (comptes, mots de passe, ...).
- Ralentissement et instabilité du système.
- Accès non autorisé par un pirate.
- Coûts de récupération et de réparation.

Bonnes pratiques de protection

- Utiliser un antivirus à jour.
- Mettre à jour régulièrement le système et les logiciels.
- Éviter les pièces jointes et les liens suspects.
- Télécharger uniquement depuis des sources fiables (sites officiels).
- Sauvegarder régulièrement ses données.



À retenir

Un virus est un logiciel malveillant qui se propage et peut nuire au système. Il existe plusieurs types de malwares (virus, ver, cheval de Troie, ...). La prévention repose sur un antivirus à jour, les mises à jour, la prudence et la sauvegarde régulière des données.

Le phishing (hameçonnage) et les arnaques en ligne

Définition

Le phishing (hameçonnage) est une technique d'arnaque qui consiste à se faire passer pour un organisme de confiance (banque, administration, service en ligne, etc.) afin de voler des informations sensibles (identifiant, mot de passe, données bancaires, ...).

Principe du phishing



1. Un pirate envoie un message trompeur (e-mail, SMS, etc.).
2. L'utilisateur clique sur un lien et saisit ses informations.
3. Le pirate récupère les données et les utilise à des fins frauduleuses.

Signes d'un message de phishing

- Expéditeur inconnu ou adresse suspecte.
- Message urgent ou menaçant (ex. : « votre compte sera bloqué »).
- Lien vers un site non officiel (adresse étrange ou mal orthographiée).
- Fautes d'orthographe et mise en page douteuse.
- Demande de données sensibles (mot de passe, code bancaire, ...).



Exemples d'arnaques en ligne

Fausse banque	Faux colis	Faux gain	Faux site de vente	Arnaque aux comptes
Demande de mise à jour de vos coordonnées bancaires.	Message sur un colis à récupérer avec un lien frauduleux.	Annonce d'un gain (téléphone, voyage, ...) contre vos données.	Produits très bon marché (paiement sans livraison).	Usurpation d'identité (réseaux sociaux, services en ligne).

Conséquences possibles



- Vol de données personnelles et bancaires.
- Accès non autorisé à vos comptes (e-mail, réseaux sociaux, ...).
- Pertes financières.
- Usurpation d'identité.
- Installation de logiciels malveillants.

Bonnes pratiques de prévention

- Vérifier l'identité de l'expéditeur.
- Ne pas cliquer sur des liens suspects.
- Saisir l'adresse du site manuellement (ex. : www.sonelgaz.dz)
- Utiliser l'authentification à deux facteurs (2FA).
- Mettre à jour l'antivirus et le navigateur.
- Être vigilant face aux offres trop alléchantes.

À retenir

Le phishing est une arnaque en ligne qui vise à voler vos informations. Pour se protéger, il faut rester vigilant, vérifier les sources et ne jamais communiquer ses données sensibles.

Les mots de passe : création et gestion sécurisées

Définition

Un mot de passe est une combinaison secrète de caractères qui permet d'authentifier un utilisateur et de protéger l'accès à un compte, à un appareil ou à un service en ligne.

Comment créer un mot de passe robuste ?

- Utiliser au moins 12 caractères.
- Mélanger des majuscules (A–Z), minuscules (a–z), chiffres (0–9) et caractères spéciaux (! @ # $ % ...).
- Éviter les mots du dictionnaire, les informations personnelles (nom, date de naissance, ...).
- Utiliser une phrase de passe (suite de mots) facile à retenir mais difficile à deviner.



Exemples de mots de passe

Faibles (à éviter)	Robustes (recommandés)
123456	A!7kPz$9mQ2v
password	Bio_TIC@2026!
azerty	Université#34Cloud
Ali2025	Soleil*Vert9Bf!
19900101	Etude2026_**Sécu

Gestion des mots de passe

- Utiliser un gestionnaire de mots de passe (ex. : Bitwarden, KeePass, 1Password).
- Générer des mots de passe forts et uniques.
- Les stocker de manière chiffrée et les synchroniser en toute sécurité.



Pourquoi c'est important ?

- Empêcher les accès non autorisés.
- Protéger les données personnelles et sensibles.
- Éviter le piratage et l'usurpation d'identité.

Bonnes pratiques

- Utiliser un mot de passe différent pour chaque compte.
- Changer régulièrement ses mots de passe (ex. : tous les 3 à 6 mois).
- Activer l'authentification à deux facteurs (2FA) (code par SMS, application ou clé de sécurité).
- Ne jamais partager son mot de passe.



À retenir

Un bon mot de passe est long, complexe, unique et régulièrement mis à jour. Pour une sécurité renforcée, il est recommandé d'utiliser un gestionnaire de mots de passe et la 2FA.

Les réseaux Wi-Fi publics et les risques de sécurité

Définition

Un réseau Wi-Fi public est un accès sans fil à Internet, souvent gratuit, disponible dans des lieux publics (café, aéroport, hôtel, bibliothèque, université, ...).

Exemples de réseaux Wi-Fi publics

Café / Restaurant | Aéroport | Hôtel | Bibliothèque / Université



Principaux risques

- **Interception des données** (mots de passe, identifiants, messages, ...).
- **Faux point d'accès** (hotspot malveillant imitant un réseau officiel).
- **Infection par des logiciels malveillants** (virus, spyware, ...).
- **Vol d'informations personnelles** (usurpation d'identité).

Pourquoi est-ce risqué ?



- Les communications peuvent être non chiffrées et lisibles par un tiers.
- Un attaquant sur le même réseau peut surveiller et intercepter vos échanges.

Bonnes pratiques de sécurité

- Éviter les opérations sensibles (banque, achats, ...).
- Utiliser un VPN pour chiffrer la connexion.
- Vérifier le nom exact du réseau (ex. : « Universite-Guest »).
- Activer le pare-feu et l'antivirus.
- Utiliser des sites en HTTPS (cadenas 🔒 dans le navigateur).

Wi-Fi public vs Wi-Fi privé

Critère	Wi-Fi public	Wi-Fi privé (maison, bureau)
Sécurité	Faible	Élevée
Confidentialité	Risque d'interception	Données mieux protégées
Utilisateurs	Multiples et inconnus	Limités et contrôlés
Contrôle	Aucun (réseau ouvert)	Paramétrable (mot de passe, chiffrement WPA2/WPA3)

Solutions recommandées

- **VPN** — Utiliser un VPN (réseau privé virtuel).
- **https://** — Privilégier les sites sécurisés (HTTPS).
- Désactiver le partage de fichiers sur le réseau.

À retenir

Les réseaux Wi-Fi publics sont pratiques mais peu sécurisés. Il faut rester prudent, protéger ses données (VPN, HTTPS) et éviter toute opération sensible sur ces réseaux.

Les mises à jour, antivirus et pare-feu

Définition générale

Ce sont des mécanismes de protection complémentaires qui permettent de corriger les failles, détecter et bloquer les menaces et contrôler les accès au système et au réseau.

Les mises à jour (Updates)



- Corrigent les failles de sécurité (vulnérabilités).
- Améliorent la stabilité et les performances.
- Ajoutent de nouvelles fonctionnalités.

L'antivirus



- Détecte les logiciels malveillants (virus, vers, logiciels espions, ...).
- Bloque et supprime les menaces.
- Protège en temps réel le système et les fichiers.

Le pare-feu (Firewall)



- Contrôle les connexions entrantes et sortantes.
- Bloque les accès non autorisés.
- Filtre le trafic réseau selon des règles de sécurité.

Exemples

Mises à jour	Antivirus	Pare-feu
Windows Update	Windows Defender	Pare-feu Windows (Windows Firewall)
Mises à jour des logiciels (navigateur, Office, ...)	Kaspersky	Pare-feu matériel (routeur, box Internet)
	Avast	
	Bitdefender	

Pourquoi sont-ils importants ?



- Réduire le risque d'infection et de piratage.
- Protéger les données personnelles et professionnelles.
- Assurer la stabilité et la continuité du système.
- Prévenir les accès non autorisés au réseau.

Bonnes pratiques



- Activer les mises à jour automatiques.
- Utiliser un antivirus fiable et le maintenir à jour.
- Activer et configurer le pare-feu.
- Vérifier régulièrement les alertes de sécurité.
- Ne pas désactiver ces protections sauf raison légitime.

À retenir

Les mises à jour, l'antivirus et le pare-feu sont trois protections essentielles : les mises à jour corrigent les failles, l'antivirus détecte et élimine les menaces et le pare-feu contrôle les accès au réseau.

La sauvegarde des données et la récupération après incident

Définition

La sauvegarde (backup) consiste à créer une **copie des données importantes** afin de les protéger contre la perte, la coruption ou un incident (panne, virus, erreur, vol, ...).

Pourquoi sauvegarder ?



- Prévenir la perte de données (panne, virus, ransomware).
- Assurer la continuité du travail (projets, cours, recherches, ...).
- Pouvoir restaurer rapidement les données en cas d'incident.
- Protéger les données sensibles et importantes.

Types de sauvegarde

- **Complète :** copie de toutes les données (plus longue, plus d'espace).
- **Incrémentielle :** seules les nouvelles données ou les données modifiées.
- **Différentielle :** les données modifiées depuis la dernière sauvegarde complète.

Où sauvegarder ses données ?

- Disque dur externe (simple et grande capacité).
- Clé USB (pratique et portable).
- Cloud (Google Drive, OneDrive, Dropbox, ...) (accès partout et sauvegarde automatique).
- NAS (serveur de stockage réseau) (pour un usage professionnel).

Comment restaurer les données ?

1. Choisir la sauvegarde appropriée (date, version).
2. Lancer la restauration (récupération des fichiers).
3. Vérifier l'intégrité des données restaurées.

Stratégie de sauvegarde (règle 3-2-1)

3-2-1

- **3** — 3 copies des données (originale + 2 sauvegardes).
- **2** — Sur 2 supports différents (ex. : disque dur et cloud).
- **1** — 1 copie hors site (à distance, ex. : cloud) pour plus de sécurité.

Bonnes pratiques

- Sauvegarder régulièrement et automatiquement.
- Conserver plusieurs versions des fichiers.
- Tester périodiquement la restauration.
- Chiffrer les sauvegardes pour les données sensibles.
- Utiliser une solution de cloud fiable et sécurisée.



À retenir

La **sauvegarde** est une mesure essentielle pour **protéger ses données** et assurer leur **récupération rapide** en cas d'incident. La **règle 3-2-1** (3 copies, 2 supports, 1 copie hors site) est une bonne pratique.

La protection des données personnelles et la vie privée

Définition

Les **données personnelles** sont toute information qui permet d'identifier directement ou indirectement une personne (nom, photo, e-mail, numéro de téléphone, localisation, ...).

Exemples de données personnelles



- Nom et prénom
- Numéro de téléphone
- Adresse e-mail
- Localisation (GPS)
- Photo / vidéo
- Numéro d'identité (CNI, passeport)
- Données de santé
- Données bancaires

Principaux risques



- Vol d'identité (usurpation).
- Collecte et utilisation abusive des données.
- Profilage et suivi en ligne (traçage).
- Phishing et arnaques ciblées.

Cadre et droits

- Règlement Général sur la Protection des Données (RGPD, UE).
- Loi algérienne relative à la protection des données à caractère personnel.
- Des droits pour l'utilisateur : accès, rectification, suppression et opposition au traitement.

Bonnes pratiques pour protéger sa vie privée

- Limiter les informations personnelles partagées en ligne.
- Configurer les paramètres de confidentialité (réseaux sociaux, applications, navigateur).
- Utiliser des mots de passe forts et la double authentification.
- Contrôler les autorisations des applications (caméra, micro, localisation, ...).
- Être vigilant face aux liens et pièces jointes suspects (phishing).

Outils et réglages utiles



- **VPN** (masquer son adresse IP et sécuriser la connexion).
- **HTTPS** (chiffrement des échanges sur les sites web).
- **Gestion des cookies** (accepter, refuser ou personnaliser leur utilisation).

Les bonnes attitudes en ligne



- Lire les politiques de confidentialité.
- Éviter les sites non fiables.
- Supprimer régulièrement les données inutiles.
- Maîtriser son empreinte numérique (informations laissées sur Internet).

À retenir

Protéger ses **données personnelles**, c'est **maîtriser** les informations que l'on partage, **limiter leur collecte** et leurs usages, et **faire valoir ses droits** à la vie privée.

Les bonnes pratiques pour un usage responsable et sécurisé d'Internet

Sécurité de base

- Utiliser des mots de passe robustes et uniques.
- Activer l'authentification à deux facteurs (2FA).
- Mettre à jour le système et les applications.
- Utiliser un antivirus et un pare-feu.





Vérification de l'information

- Vérifier la fiabilité de la source (site officiel, auteur, date).
- Croiser l'information avec plusieurs sources.
- Se méfier des fausses informations (rumeurs, canulars).



Comportement responsable

- Respecter les autres en ligne (netiquette).
- Éviter le cyberharcèlement.
- Respecter le droit d'auteur et citer ses sources.
- Utiliser Internet à des fins éducatives et productives.



Protection de la confidentialité

- Limiter les informations personnelles partagées (adresse, localisation, ...).
- Gérer les paramètres de confidentialité sur les réseaux sociaux.
- Contrôler les autorisations des applications (caméra, micro, contacts, ...).



Usage sain et durable

- Gérer son temps de connexion (éviter l'usage excessif).
- Privilégier des contenus utiles et de qualité.
- Adopter un usage écoresponsable (réduire le stockage inutile, limiter la consommation de données).



À retenir

Un **usage d'Internet responsable et sécurisé**, c'est **s'informer**, se **protéger**, **respecter les autres** et adopter de **bonnes habitudes** pour un environnement numérique sûr, éthique et durable.

Synthèse générale et conclusion de la séance

Objectifs de la séance (rappel)

- Comprendre les concepts clés de l'Internet, du Web et du Cloud.
- Identifier les principaux services et navigateurs.
- Connaître les risques et les menaces en ligne.
- Adopter les bonnes pratiques de sécurité et d'usage responsable.

Principaux acquis

- **Internet :** réseau mondial d'échange d'informations.
- **Web :** service d'accès aux contenus et services en ligne.
- **Cloud :** stockage et services à distance.
- **Sécurité :** protection des données, des systèmes et de la vie privée.
- **Usage responsable :** un Internet utile, sûr, éthique et durable.

Messages clés

- Protéger ses données et sa vie privée.
- Se méfier des menaces (virus, phishing, ...).
- Utiliser des mots de passe robustes et uniques.
- Maintenir ses logiciels à jour et utiliser un antivirus.
- Sauvegarder régulièrement ses données.
- Vérifier la fiabilité des informations en ligne.
- Adopter un comportement responsable et respectueux.

Conclusion

Cette séance a permis d'acquérir une vision globale des **usages**, des **opportunités** et des **risques** liés à l'Internet, au Web et au Cloud, ainsi que des moyens de **sécuriser** ses données et de naviguer de manière **responsable**.



À retenir (l'essentiel)

- Internet relie les personnes, les informations et les services.
- Le Web facilite l'accès aux contenus.
- Le Cloud offre des services flexibles et accessibles.
- La sécurité et la responsabilité sont indispensables pour un usage sûr et efficace.

Merci pour votre attention !

EXERCICES D'APPLICATION (Évaluation)

Exercice 1 : QCM

Cocher la bonne réponse.

1) Internet est :

- ☐ a) Un logiciel de navigation
- ☑ b) Un réseau mondial d'ordinateurs
- ☐ c) Un service de stockage en ligne

2) Le Cloud permet :

- ☐ a) De naviguer plus vite
- ☑ b) De stocker et partager des données
- ☐ c) De protéger l'ordinateur d'un virus

Exercice 2 : Vrai / Faux

Indiquer V (vrai) ou F (faux).

1	Le Web est un service d'Internet.	V
2	Un mot de passe fort améliore la sécurité.	V
3	Le Wi-Fi public est toujours sûr.	F
4	Le pare-feu bloque les accès non autorisés.	V
5	Le Cloud permet d'accéder aux données à distance.	V

Exercice 3 : Questions courtes

Répondre brièvement.

1. Citer deux menaces en ligne.
2. Donner deux bonnes pratiques de sécurité.
3. Quelle est l'utilité d'une sauvegarde ?
4. Qu'est-ce que le phishing ?
5. Citer un exemple de service Cloud.

Exercice 4 : Mise en situation

Vous recevez un e-mail vous informant que votre compte universitaire sera suspendu. Le message contient un lien pour "confirmer vos informations".

- Identifier le type de menace.
- Indiquer les actions à adopter.



Exercice 5 : Mini-projet

Proposer un plan simple pour sécuriser un ordinateur personnel (3 à 5 étapes). (Ex. : mises à jour, antivirus, pare-feu, sauvegarde, mot de passe, ...)



Objectif de l'évaluation

Vérifier la compréhension des notions essentielles et la capacité à les appliquer dans des situations concrètes.

Correction des exercices 3, 4 et 5

Correction – Exercice 3 (Questions courtes)



1. Citer deux menaces en ligne. → Virus (logiciel malveillant) et phishing (hameçonnage).
2. Donner deux bonnes pratiques de sécurité. → Utiliser un mot de passe robuste et maintenir les logiciels à jour.
3. Quelle est l'utilité d'une sauvegarde ? → Conserver une copie des données pour les récupérer en cas de panne, perte ou attaque.
4. Qu'est-ce que le phishing ? → Une tentative de fraude qui usurpe l'identité d'un service de confiance pour voler des informations personnelles (mots de passe, données bancaires, ...).
5. Citer un exemple de service Cloud. → Google Drive, OneDrive, Dropbox ou iCloud.

Correction – Exercice 4 (Mise en situation)



1) Identification du type de menace

Type : Phishing (hameçonnage).

2) Indices de fraude (justification)

- Expéditeur suspect ou non officiel.
- Message incitant à "confirmer des informations".
- Lien vers un site douteux (URL non officielle).
- Ton urgent ou menaçant (suspension du compte).

3) Actions à adopter

- Ne pas cliquer sur le lien et ne pas saisir ses informations.
- Vérifier l'expéditeur et l'URL officielle du service.
- Signaler l'e-mail comme phishing (spam).
- Supprimer le message.
- Changer le mot de passe et activer la double authentification (si nécessaire).

Correction – Exercice 5 (Mini-projet)



Plan simple pour sécuriser un ordinateur personnel (exemple en 5 étapes)

1. **Mises à jour** — Installer régulièrement les mises à jour du système et des logiciels.
2. **Antivirus** — Utiliser un antivirus fiable et le maintenir à jour.
3. **Pare-feu** — Activer et configurer le pare-feu (Windows Defender ou équivalent).
4. **Sauvegarde** — Mettre en place une sauvegarde régulière (sur disque externe ou Cloud).
5. **Mot de passe** — Utiliser un mot de passe robuste et unique et activer la double authentification (2FA).