Fiche

I. Qu'est-ce qu'un système d'information ?

Dans le monde technologique actuel, il est nécessaire de différencier un « système informatique », par exemple, un ensemble d'ordinateurs, d'écrans, d'imprimantes, et un « système d'information ».
Décomposons le mot « système d'information », SI en abrégé :

• Un système est un ensemble d'éléments organisés qui travaillent ensemble pour atteindre un objectif commun. Par exemple, au collège, la vie scolaire est un système : il y a la ou le CPE, les surveillants, le logiciel d'appel, etc. Tout est organisé pour assurer le suivi des élèves et le bon fonctionnement de l'établissement.

• Une information est soit une donnée brute (par exemple une vidéo ou un numéro de téléphone), soit une organisation d'informations (base de données organisée), soit une connaissance.

Un système d'information est donc un ensemble organisé de ressources permettant de gérer des informations. Il comprend des personnes (utilisateurs, informaticiens), des machines (ordinateurs, serveurs, réseaux), des procédures (méthodes de travail) et des données (textes, images, nombres).
Le rôle principal d'un système d'information est de collecter, stocker, traiter et diffuser des données permettant à une organisation de prendre des décisions.
Voici quelques exemples de SI :

• À l'école : applications de communication pour les familles et les élèves, cahier de texte numérique, bulletins scolaires, espaces de travail partagés.

• Dans le domaine médical : dossiers patients informatisés, suivi à distance des constantes vitales.

• Dans les entreprises : gestion des stocks, des commandes, des plannings ou de la relation client.

• Dans les administrations : démarches en ligne pour les cartes d'identité ou les passeports.

Un bon système d'information permet une prise de décision rapide, une meilleure organisation et une automatisation de certaines tâches. Il améliore aussi la communication entre les personnes ou les services.

II. Usage et impacts du numérique

Le numérique est devenu incontournable dans la vie quotidienne. Il transforme nos manières d'apprendre, de travailler, de communiquer et de consommer. Il est donc essentiel de réfléchir à nos usages pour qu'ils restent responsables et durables. Cette réflexion se fait à l'échelle individuelle, dès le plus jeune âge (encadré par les parents) puis en tant qu'adulte, mais aussi à l'échelle des dirigeants et gouvernements de chaque pays. En effet, selon les usages, les impacts peuvent être positifs ou négatifs.

Impacts positifs :

• Accès instantané à une quantité immense d'informations via Internet ;

• Développement des échanges à distance (visioconférences, réseaux sociaux) ;

• Innovation dans de nombreux domaines : médecine (chirurgie assistée), transports (voitures autonomes), agriculture (robots agricoles), éducation (ENT, classe virtuelle) ;

• Gain de temps et amélioration de la productivité dans les entreprises.

Impacts négatifs :

• Dépendance aux écrans, troubles du sommeil ou baisse de l'attention ;

• Cyberviolence, atteinte à la vie privée, harcèlement en ligne ;

• Usurpation d'identité ;

• Diffusion de fausses informations (*fake news*) ;

• Surconsommation de ressources : fabrication d'appareils numériques gourmande en métaux rares et en énergie, surconsommation d'eau liée à l'utilisation de l'IA qui nécessite des ordinateurs très puissants qu'il faut refroidir avec quatre fois plus d'eau que prévu par l'industrie ;

• Inégalités d'accès : certaines personnes ou régions n'ont pas accès aux outils numériques ou ne savent pas bien les utiliser (fracture numérique) ;

• Non-respect de la propriété intellectuelle (par exemple, en téléchargeant ou regardant illégalement des films, des séries mais aussi de

la musique, alors qu'il s'agit de contenus payants).

III. Cybersécurité

Depuis l'essor du numérique à grande échelle et dans tous les foyers dans les années 2000, nos données personnelles et professionnelles sont de plus en plus stockées en ligne. La cybersécurité est l'ensemble des pratiques et outils mis en place pour protéger les systèmes informatiques contre les attaques ou les pannes. Ces pratiques consistent principalement à protéger les données personnelles, créer des traces numériques (historique de navigation, géolocalisation), identifier, authentifier et respecter la propriété intellectuelle. Ces pratiques sont mises en œuvre par des professionnels mais doivent aussi être adoptées par chacun de nous.
En effet, les menaces sont nombreuses :

• Virus, logiciels espions (*malwares*), rançongiciels (*ransomwares*) ;

• Vol d'identifiants ou de données bancaires ;

• Piratage de comptes ou de serveurs ;

• Escroqueries en ligne (hameçonnage ou *phishing*).

Afin de limiter les risques, il est important, pour chacun de nous, d'adopter de bonnes pratiques :

• Créer des mots de passe complexes et ne pas les réutiliser dans plusieurs applications ou sur plusieurs sites ;

• Ne jamais cliquer sur des liens suspects dans un mail ou un SMS ;

• Mettre à jour régulièrement ses logiciels et utiliser un antivirus ;

• Sauvegarder régulièrement ses données importantes sur plusieurs supports différents.

Enfin, les entreprises et les administrations doivent mettre en place des systèmes de protection avancés, des pare-feux et des formations à la sécurité numérique. La cybersécurité est l'affaire et la responsabilité de tous : élèves, parents, enseignants, professionnels, citoyens.

À retenir :

1. Un système d'information sert à **collecter, organiser, stocker, traiter et partager des données** dans tous les secteurs d'activité.

2. Le numérique offre des **bénéfices importants**, mais il a aussi des **effets négatifs** sur la santé, l'environnement et la société.

3. La cybersécurité permet de se protéger des **menaces en ligne**. Chacun doit adopter des **comportements numériques responsables**.

Définitions importantes :

Système d'information : ensemble organisé de moyens pour gérer des informations.
Numérique : ensemble des technologies liées aux ordinateurs, aux réseaux et aux données.
Fracture numérique : inégalités d'accès ou de maîtrise des outils numériques.
Hameçonnage (ou *phishing*) : tentative de vol d'informations par des messages frauduleux.
Rançongiciel (ou *ransomwares*) : programme malveillant qui bloque un système en échange d'une rançon.
Cybersécurité : ensemble des protections contre les attaques informatiques.