Les dangers en informatique

Discipline : Technologie / Éducation au numérique

---

1. Objectifs du cours

À l'issue de cette séance, les élèves doivent être capables de :

- Identifier les principaux dangers liés à l'usage de l'informatique et d'Internet.
- Comprendre le fonctionnement général des principales menaces numériques.
- Adopter des comportements responsables et sécurisés en ligne.
- Développer un esprit critique face aux messages, fichiers et sites Internet.

---

2. Pourquoi parle-t-on de dangers en informatique ?

L'informatique et Internet sont des outils très utiles pour :

- communiquer,
- apprendre,
- se divertir,
- travailler.

Cependant, comme dans la vie réelle, il existe des **risques**. Certaines personnes ou logiciels malveillants cherchent à :

- voler des informations,
- escroquer,
- espionner,
- bloquer ou détruire des données.

Ces dangers sont appelés **menaces informatiques**.

---

3. Le phishing (ou hameçonnage)

a) Définition

Le **phishing** est une technique d'arnaque qui consiste à se faire passer pour une personne ou un organisme de confiance afin de voler des informations personnelles.

b) Comment cela fonctionne ?

- Réception d’un e-mail, SMS ou message.
- Le message semble venir d’une banque, d’un site connu, d’un jeu, ou d’une administration.
- Il demande de cliquer sur un lien et de saisir :
    - un mot de passe,
    - un numéro de carte bancaire,
    - des informations personnelles.

c) Dangers

- Vol de comptes (réseaux sociaux, jeux, messagerie).
- Vol d’argent.
- Usurpation d’identité.

d) Bonnes pratiques

- Vérifier l’adresse de l’expéditeur.
- Ne jamais cliquer sur un lien douteux.
- Ne jamais donner ses mots de passe.
- Se méfier des messages urgents ou menaçants.

---

4. Le ransomware (rançongiciel)

a) Définition

Un **ransomware** est un logiciel malveillant qui bloque l’accès à un ordinateur ou à des fichiers et demande une rançon pour les débloquer.

b) Comment cela fonctionne ?

- L’utilisateur télécharge un fichier infecté ou clique sur un lien dangereux.
- Le logiciel chiffre (verrouille) les fichiers.
- Un message apparaît demandant de payer pour récupérer les données.

c) Dangers

- Perte totale de documents (photos, devoirs, fichiers personnels).
- Extorsion d’argent.
- Paralysie d’ordinateurs dans des écoles, hôpitaux ou entreprises.

d) Bonnes pratiques

- Ne pas télécharger de fichiers inconnus.
- Faire des sauvegardes régulières.
- Maintenir le système à jour.
- Utiliser un antivirus.

---

5. Le cheval de Troie

a) Définition

Un **cheval de Troie** est un programme qui semble utile ou inoffensif mais qui cache un logiciel malveillant.

b) Comment cela fonctionne ?

- Le programme est présenté comme un jeu, un logiciel gratuit ou une mise à jour.
- Une fois installé, il peut :
  - espionner l'utilisateur,
  - voler des données,
  - installer d'autres virus.

c) Dangers

- Espionnage (caméra, micro, clavier).
- Vol de données personnelles.
- Contrôle à distance de l'ordinateur.

d) Bonnes pratiques

- Télécharger uniquement depuis des sites officiels.
- Lire les autorisations demandées.
- Ne pas installer de logiciels piratés.

---

6. Autres dangers courants

a) Virus informatique

- Programme qui se propage et endommage le système.

b) Spyware (logiciel espion)

- Collecte des informations sans l'accord de l'utilisateur.

c) Mots de passe faibles

- Faciles à deviner (1234, prénom, date de naissance).

d) Réseaux sociaux

- Surpartage d’informations personnelles.
- Risques de cyberharcèlement.

---

7. Les règles essentielles de sécurité numérique

- Utiliser des mots de passe longs et complexes.
- Ne jamais partager ses identifiants.
- Mettre à jour régulièrement les appareils.
- Réfléchir avant de cliquer.
- Demander de l’aide à un adulte en cas de doute.

---

8. Conclusion

L’informatique est un outil puissant, mais il doit être utilisé avec prudence. Connaître les dangers permet de mieux s’en protéger. Être un bon citoyen numérique, c’est adopter des comportements responsables, respectueux et sécurisés.

Vocabulaire à retenir

- Phishing
- Ransomware
- Cheval de Troie
- Virus
- Données personnelles
- Mot de passe