Initiation à la Cybersécurité

KBU

VITA VERITAS

Objectifs pédagogiques

À la fin du cours, l'apprenant sera capable de :

- Comprendre ce qu'est la cybersécurité
- Identifier les principales menaces numériques
- Reconnaître une attaque simple (phishing, virus…)
- Appliquer des bonnes pratiques de sécurité au quotidien

I – Introduction à la cybersécurité

1.1 Définition

La **cybersécurité** est l'ensemble des méthodes ou moyens utilisés pour :

- ✓ Protéger les ordinateurs / téléphones
- ✓ Protéger les réseaux
- ✓ Protéger les données personnelles

contre les attaques sur internet.

En résumé : la cybersécurité sert à se protéger quand on utilise Internet.

1.2 Pourquoi la cybersécurité est importante ?

La cybersécurité est essentielle car elle protège les **réseaux, appareils, programmes et données** contre les **cyberattaques** menées par des cybercriminels.

Ces attaques visent à obtenir un accès non autorisé, voler ou modifier des informations, interrompre les opérations d’entreprise, extorquer de l’argent ou réaliser le vol d’informations importantes.

Exemples concrets :

- protéger ton téléphone
- protéger tes photos
- protéger ton compte Facebook / WhatsApp
- éviter les arnaques
- piratage de comptes bancaires

Tout le monde est concerné,
pas seulement les informaticiens.

La cybersécurité est bien au-delà du domaine informatique et concerne chaque individu, organisation et État.
Les attaques ciblent désormais toutes les structures, qu’elles soient grandes entreprises, collectivités locales, associations ou particuliers, car **tout système connecté est une cible potentielle**. Les cybercriminels exploitent souvent l’erreur humaine, comme dans les cas de hameçonnage ou de mauvaises pratiques de gestion des accès, ce qui rend chaque collaborateur un acteur clé de la sécurité.

La cybersécurité est l'affaire de tous

Le facteur humain est crucial : même avec des outils technologiques avancés, la faille la plus fréquente reste l'humain.

C'est pourquoi la formation continue, la sensibilisation et la mise en place d'une culture de la sécurité sont essentielles. Des initiatives comme le modèle **« zéro confiance »** ou la **gouvernance partagée** permettent de renforcer la capacité à se protéger et à réagir.

En résumé**, la cybersécurité est l'affaire de tous** – du simple utilisateur lambda au PDG, quelques soient nos domaines d'expertises.

II - Les principaux dangers sur internet

2.1 Les virus informatiques

Un **virus informatique** est un programme malveillant conçu pour se propager d'un ordinateur à un autre en s'insérant dans des fichiers ou logiciels légitimes, sans le savoir de l'utilisateur.

Il peut perturber le fonctionnement de l'appareil, corrompre des données, voler des informations ou même provoquer une panne complète. Son fonctionnement repose sur une analogie avec les virus biologiques : il **s'attache à un hôte** (comme un fichier exécutable), se réplique lorsqu'il est activé, et se propage via des réseaux, clés USB, e-mails ou téléchargements.

2.2 Le phishing (hameçonnage)

Le phishing, aussi appelé hameçonnage, est une escroquerie en ligne où un cybercriminel se fait passer pour une entité de confiance (banque, administration, réseau social, etc.) pour tromper sa victime. L'objectif est de voler des informations personnelles sensibles comme des mots de passe, des numéros de carte bancaire ou des identifiants de connexion.

2.3 Le piratage de mots de passe

Le piratage de mot de passe est une attaque informatique visant à obtenir un accès non autorisé à un compte ou un système en déchiffrant ou en devinant le mot de passe d’un utilisateur. Cela peut se faire par des méthodes simples comme deviner un mot de passe faible, ou par des techniques plus sophistiquées comme le phishing, l’attaque par force brute, le credential stuffing (utilisation de mots de passe volés sur plusieurs sites) ou encore l’installation de logiciels malveillants voleurs de mots de passe.

III – Les attaques courantes

3.1 Attaque par mots de passe faible

Une attaque par mot de passe simple est une méthode utilisée par les cybercriminels pour accéder à un compte en devinant ou en testant systématiquement des mots de passe faibles ou courants. Elle repose sur le fait que beaucoup d'utilisateurs choisissent des mots de passe faciles à retenir, comme « 123456 », « motdepasse », des noms de familles ou des dates de naissance, ce qui les rend vulnérables.

3.1 Wi-Fi public non sécurisé

Les réseaux Wi-Fi publics (cafés, écoles, aéroports) sont souvent :

- ✓ non sécurisés
- ✓ accessibles à tout le monde

Cela signifie que :

- ➢ tes données peuvent être espionnées
- ➢ tes mots de passe peuvent être volés

Conseil : Tous les réseaux Wi-Fi publics (aéroports, cafés, hôtels) doivent être considérés comme non sécurisés, même s’ils semblent légitimes. Évite de te connecter à tes comptes importants sur un Wi-Fi public.

3.2 Applications et sites non fiables

Les **applications et sites non fiables** présentent des risques importants pour votre sécurité numérique, vos données personnelles et votre confidentialité.

➢ Signes suspects :

- pas de cadenas 🔒 dans la barre d’adresse
- offres trop belles pour être vraies
- fautes d’orthographe
- demande trop d’informations personnelles
- **Sites malveillants** : Hébergent des logiciels malveillants (malware, ransomware) qui infectent votre appareil.
- **Sites de désinformation** : Propagent des fausses informations, souvent dans un but politique ou économique.

- URL suspecte (ex. : paypa1.securite.com au lieu de paypal.com)
- Absence de **HTTPS** (cadenas dans la barre d’adresse)
- Design bas de gamme, erreurs de frappe, contenu mal rédigé
- Aucune information d’entreprise (adresse, téléphone, mentions légales)

Applications non fiables

Applications espionnes : Collectent vos données personnelles sans consentement

Jeux frauduleux : Envoient les utilisateurs vers des sites d’arnaques

Applications malveillantes : Contiennent des logiciels malveillants cachés.

Applications avec trop de permissions : Demande d’accès à vos contacts, caméra, localisation sans justification

IV – Les bonnes pratiques de Cybersécurité

4.1 Créer un bon mot de passe

Un bon mot de passe :

Minimum 8 caractères

Majuscules + minuscules

Chiffres + symboles

Exemple :Pa@2O26CyBer!

4.2 Ne jamais cliquer sans réfléchir

Avant de cliquer sur un lien, pose-toi ces questions :

- Qui m’envoie ce message ?
- Est-ce logique ?
- Est-ce urgent sans raison ?

En cas de doute : **ne clique pas**.

4.3 Faire les mises à jour

- Téléphone : mises à jours constructeurs
- Ordinateur : mises à jours Systèmes d’Exploitation
- Applications : mises à jours officielles

Les mises à jour corrigent des failles de sécurité.

V – Conclusion

Adopter un comportement numérique responsable en cybersécurité repose sur l'application de bonnes pratiques quotidiennes et la mise en place d'une culture de la vigilance.

À retenir absolument :
Protège tes mots de passe
Méfie-toi des messages suspects
Fais les mises à jour
Réfléchis avant de publier ou de cliquer

La cybersécurité commence par ton comportement.