1️⃣ C’est quoi la cybersécurité ?

La **cybersécurité** est l’ensemble des techniques et règles utilisées pour **protéger les systèmes informatiques, les réseaux, les données et les utilisateurs** contre :

- le piratage
- les virus
- le vol de données
- les attaques informatiques

👉 Objectif principal : **assurer la confidentialité, l’intégrité et la disponibilité des données**

2️⃣ Les 3 piliers fondamentaux (CIA)

On appelle ça la **triade CIA** :

🔒 Confidentialité

➡️ Seules les personnes autorisées peuvent accéder aux données
Exemple : mot de passe, chiffrement

🛡️ Intégrité

➡️ Les données ne doivent pas être modifiées sans autorisation
Exemple : empêcher qu’un fichier soit falsifié

⚙️ Disponibilité

➡️ Les services doivent rester accessibles
Exemple : un site qui ne tombe pas à cause d’une attaque

3️⃣ Les principales menaces

🦠 Malware

Logiciels malveillants :

- Virus
- Trojan (cheval de Troie)
- Ransomware (bloque les fichiers contre de l’argent)
- Spyware (espionnage)

🎣 **Phishing**

➡️ Faux emails / SMS / sites pour voler :

- mots de passe
- informations bancaires

💣 **Attaques réseau**

- **DDoS** : surcharge un serveur pour le rendre indisponible
- **Man-in-the-Middle** : intercepter une communication

🥷 **Ingénierie sociale**

➡️ Manipulation psychologique
Exemple : “Je suis de l’administration, donne-moi ton mot de passe”

🛂 **Types de cybersécurité**

🖥️ **Sécurité des systèmes**

- Antivirus
- Mises à jour
- Permissions utilisateur

🌐 **Sécurité réseau**

- Firewall
- IDS / IPS
- VPN

🔐 **Sécurité des données**

- Chiffrement
- Sauvegardes
- Gestion des accès

☁️ **Sécurité Cloud**

- Protection des données stockées en ligne
- Authentification forte

🧱 Sécurité applicative

- Corriger les failles dans les applications
- Sécurité web (XSS, SQL Injection...)

5️⃣ Notions techniques importantes

🔑 Authentification

- Mot de passe
- Double authentification (2FA)
- Biométrie

🔐 Chiffrement

➡️ Transformer les données en code illisible
Exemples :

- HTTPS
- AES
- RSA

🔍 Logs et audit

➡️ Tracer les actions pour détecter les attaques

6️⃣ Sécurité Web (très important)

Failles courantes :

- **SQL Injection**
- **XSS (Cross-Site Scripting)**
- **CSRF**

Bonnes pratiques :

- Valider les entrées utilisateur
- Utiliser HTTPS
- Ne jamais stocker les mots de passe en clair

7️⃣ Rôles et métiers en cybersécurité

- 🔐 Analyste sécurité
- 🧪 Pentester (tests d'intrusion)
- 👨‍💻 SOC Analyst
- 🏗️ Architecte sécurité
- 📊 RSSI (Responsable sécurité)

8️⃣ Bonnes pratiques pour tout le monde

✔️ Mots de passe forts
✔️ Ne jamais cliquer sur des liens suspects
✔️ Mettre à jour ses logiciels
✔️ Sauvegarder ses données
✔️ Ne pas partager ses infos personnelles

9️⃣ Comment apprendre la cybersécurité ?

Bases

- Réseaux (TCP/IP, DNS, HTTP)
- Systèmes (Linux, Windows)
- Programmation (Python, JS)

Pratique

- Machines virtuelles
- Laboratoires (CTF)
- Simulations d'attaques **légales**

Mentalité

➡️ Toujours penser :
"Et si quelqu'un essayait d'abuser de ce système ?"

🔟 Cybersécurité ≠ Piratage illégal

⚠️ Très important :
La cybersécurité sert à **protéger**, pas à nuire.
Tout test se fait **avec autorisation**.