م. محمد نصيف مصطفى العاني
خريج كلية الهندسة – الجامعة التكنولوجية
قسم هندسة الحاسبات
ماجستير هندسة حاسبات / تخصص ذكاء اصطناعي – تركيا / أنقرة
دكتوراه حالياً في هندسة الحاسبات / تخصص ذكاء اصطناعي – ماليزيا

Eng. Mohammed Nsaif Mustafa Al-Ani
Bachelor's Degree in Computer Engineering – University of Technology
Master's Degree in Computer Engineering (Artificial Intelligence) – Ankara, Turkey
Ph.D. Candidate in Computer Engineering (Artificial Intelligence) – Malaysia

🎓 سلسلة محاضرات الأمن السيبراني (من البداية إلى الاحتراف)

🔹 **المستوى الأول – الأساسيات (المبتدئ)**

Lecture-1 مقدمة في الأمن السيبراني(Introduction to Cybersecurity)

- مفهوم الأمن السيبراني وأهميته.
- التهديدات والمخاطر في العالم الرقمي.
- مكونات منظومة الأمن.(Confidentiality, Integrity, Availability)
- الفرق بين الأمن المادي والأمن المعلوماتي.

🧠 المحاضرة الأولى: مقدمة في الأمن السيبراني

مفهوم الأمن السيبراني

الأمن السيبراني هو مجموعة من الإجراءات والتقنيات التي تهدف إلى حماية الأنظمة الحاسوبية والشبكات والبيانات من أي نوع من التهديدات الرقمية.
يشمل ذلك منع الهجمات الإلكترونية، والكشف عنها، والاستجابة لها، والتقليل من آثارها على الأفراد والمؤسسات.

🔹 يُعرف أيضًا بأنه:

"حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية التي تهدف إلى الوصول غير المصرح به أو التغيير أو التدمير أو تعطيل الخدمات".

أهمية الأمن السيبراني

1. **حماية المعلومات الحساسة** مثل البيانات الشخصية والمصرفية والطبية.
2. **ضمان استمرارية العمل** في المؤسسات والشركات.
3. **منع الخسائر المالية** الناتجة عن الاختراقات.
4. **الحفاظ على الثقة الرقمية** بين المستخدمين والمؤسسات.
5. **حماية البنية التحتية الحيوية** كشبكات الكهرباء والمياه والمواصلات.

التهديدات السيبرانية

التهديدات السيبرانية تتنوّع حسب هدف المهاجم ونوع النظام المستهدف، وأبرزها:

- **الفيروسات والبرمجيات الخبيثة (Malware):** برامج تُزرع في النظام لتدميره أو سرقة بياناته.
- **هجمات التصيّد (Phishing):** رسائل مزيفة تستدرج المستخدمين لكشف معلوماتهم.
- **الهجمات على كلمات المرور (Password Attacks):** محاولة سرقة أو كسر كلمات المرور.
- **هجمات حجب الخدمة (DoS / DDoS):** إغراق الخوادم بطلبات غير طبيعية لتعطيلها.
- **الهندسة الاجتماعية (Social Engineering):** استغلال الثقة البشرية لخداع الضحية.

مبادئ الأمن الأساسية(CIA Triad)

- **السرية (Confidentiality):** حماية المعلومات من الوصول غير المصرح به.
- **السلامة (Integrity):** التأكد من عدم التلاعب أو التغيير في البيانات.
- **التوافر (Availability):** ضمان أن تكون الأنظمة والخدمات متاحة عند الحاجة إليها.

هذه المبادئ الثلاثة تُعدّ الأساس الذي يُبنى عليه أي نظام أمني ناجح.

مجالات الأمن السيبراني

1. **أمن الشبكات (Network Security):** حماية البنية التحتية من الاختراق.
2. **أمن التطبيقات (Application Security):** حماية البرمجيات من الثغرات.
3. **أمن المعلومات (Information Security):** حماية البيانات من التسريب أو الضياع.
4. **أمن المستخدم (User Security):** تدريب المستخدمين على السلوك الآمن.
5. **أمن السحابة (Cloud Security):** تأمين الخدمات والبيانات على الإنترنت.

التحديات الحديثة

- تطور أدوات الهجوم بسرعة كبيرة.
- نقص الوعي الأمني لدى الأفراد.
- اعتماد المؤسسات على إنترنت الأشياء.(IoT)
- صعوبة اكتشاف الهجمات المتقدمة.(Advanced Persistent Threats)

الخلاصة

الأمن السيبراني لم يعد خيارًا، بل ضرورة لكل شخص ومؤسسة في هذا العصر الرقمي.
كل جهاز متصل بالإنترنت هو هدف محتمل، لذا يجب بناء ثقافة أمنية تبدأ من الفرد وتمتد إلى المجتمع والدولة.