

محاضرة أساسيات الحاسوب: الشبكات وأمن المعلومات

الوحدة الأكاديمية الثالثة

المحاضرة الثالثة — معمارية الشبكات، أنظمة القياس، والأمان الرقمي

1. قياس البيانات والنظام الثنائي (Binary System)

يعتمد الحاسوب في تمثيل ومعالجة البيانات على النظام الثنائي (Binary System) المكون من رقمين فقط (0 و 1) للتعبير عن الحالات الكهربائية (On/Off).

الوحدة	الرمز	القيمة الحسابية / التكافؤ	التوضيح والاستخدام
Bit	bit	إما 0 أو 1	أصغر وحدة بناء تخزينية داخل الحاسوب
Byte	B	Bits 8	يمثل حرفاً أو رمزاً واحداً (تشفير ASCII/Unicode)
Kilobyte	KB	Bytes (2 ¹⁰) 1,024	تخزين المستندات النصية الصغيرة
Megabyte	MB	KB 1,024	تخزين الصور، ملفات الصوت والصوتيات
Gigabyte	GB	MB 1,024	تخزين البرمجيات والأفلام عالية الدقة
Terabyte	TB	GB 1,024	سعات الأقراص الصلبة الحديثة وقواعد البيانات

2. شبكات الحاسوب (Computer Networks)

شبكة الحاسوب هي نظام لربط جهازين أو أكثر من خلال وسائط نقل (سلكية أو لاسلكية) بهدف مشاركة الموارد (كالمطابعات والملفات) والبيانات.

الشبكة الواسعة (WAN)

تغطي مساحات جغرافية شاسعة بين مدن ودول مختلفة. وتعتبر شبكة الإنترنت العالمية أشهر مثال على شبكات WAN.

الشبكة المحلية (LAN)

تغطي نطاقاً جغرافياً محدوداً مثل غرفة، منزل، أو مبنى مكتبي. تتميز بسرعات نقل عالية جداً وزمن تأخير منخفض.

3. وسائط ونموذج نقل البيانات

- وسائط سلكية: الكوابل المزدوجة المجدولة (UTP/STP)، الكوابل المحورية (Coaxial)، وألياف الضوء (Fiber Optics) التي تمتاز بسرعات فائقة.
- وسائط لاسلكية: أمواج الراديو (Wi-Fi)، البلوتوث (Bluetooth)، وشبكات الخليوي (4G/5G).
- نموذج العميل/الخادم (Client/Server): حيث يطلب الجهاز العميل الموارد من جهاز خادم مركزي يمتلك صلاحيات ومعالجة أعلى.

4. أساسيات أمن المعلومات (Cybersecurity Fundamentals)

يهدف أمن المعلومات إلى حماية الأنظمة والبيانات والشبكات من الهجمات الرقمية وعمليات الوصول غير المصرح بها.

مثلث الحماية الأساسي (CIA Triad):

- السرية (Confidentiality): ضمان عدم الاطلاع على البيانات إلا من قبل الأشخاص المصرح لهم.
- النزاهة والسلامة (Integrity): حماية البيانات من التعديل أو التغيير غير المصرح به أثناء النقل أو التخزين.
- التوافر (Availability): ضمان وصول المستخدمين المصرح لهم للخدمات والبيانات عند الحاجة إليها.

5. أشكال التهديدات البرمجية والشائعة

برمجيات الفدية (Ransomware)

تشفير ملفات المستخدم بشكل كامل والمطالبة بمبالغ مالية مقابل إعطاء مفتاح التشفير.

الفيروسات والبرمجيات الخبيثة

برامج صُممت لإلحاق الضرر بالنظام، التجسس، أو نسخ نفسها وتخريب الملفات (Viruses, Worms, Trojans).

الهندسة الاجتماعية (Social Eng)

التلاعب النفسي بالأفراد لدفعهم إلى كشف معلومات سرية أو إعطاء صلاحيات وصول.

التصيد الإلكتروني (Phishing)

استخدام رسائل أو مواقع مزيفة شبيحة بالمؤسسات الرسمية لخدع المستخدم وسرقة بياناته الحساسة.

6. إرشادات وقواعد الأمان الرقمي المستمر

- اعتماد **كلمات مرور معقدة** وفريدة لكل حساب، مع استخدام مدير كلمات المرور.
- تفعيل **المصادقة المتعددة العوامل (MFA / 2FA)** لتأمين تسجيل الدخول.
- إجراء **نسخ احتياطي دوري (Backup)** وفق قاعدة (1-2-3) على وسائط منفصلة أو سحابية.
- تحديث نظام التشغيل والتطبيقات بانتظام لسد الثغرات الأمنية (Patch Management).