

"الفيروسات الحاسوبية: المفهوم، الأنواع، والحماية منها" مادة الحاسوب – المرحلة الثانية – قسم القانون

أهداف المحاضرة:

1. تعريف الفيروسات الحاسوبية.
2. التعرف على أنواع الفيروسات الشائعة.
3. فهم آلية عمل الفيروسات.
4. طرق انتشارها.
5. الأساليب المستخدمة للحماية منها.
6. العلاقة بين الفيروسات والجوانب القانونية.

أولاً: ما هو الفيروس الحاسوبي؟

هو برنامج خبيث يُصمَّم للتسلل إلى الحواسيب دون علم المستخدم.

يُعدّل الملفات أو يتلف البيانات أو يعطل النظام.

يشبه الفيروس البيولوجي من حيث القدرة على الانتشار والتخريب.

ثانياً: أنواع الفيروسات الشائعة:

1. فيروس الملفات: يصيب الملفات القابلة للتنفيذ (.exe) ويُعد الأخطر.

2. فيروس قطاع الإقلاع (Boot Sector Virus): يصيب بداية التشغيل في الجهاز.

3. الفيروسات المتعددة الأشكال (Polymorphic): يتغير شكله ليتجنب برامج الحماية.

4. فيروسات الديدان (Worms): تنتشر عبر الشبكة بشكل تلقائي.

5. أحصنة طروادة (Trojans): تظهر كبرامج شرعية لكنها تقوم بمهام خبيثة.

6. **Spyware و Adware:** تنجسس على المستخدم أو تعرض إعلانات مزعجة.

ثالثاً: كيف تنتشر الفيروسات؟

من خلال:

تحميل برامج غير موثوقة.

فتح مرفقات بريد إلكتروني مشبوهة.

استخدام فلاش ميموري أو أقراص ملوثة.

الدخول لمواقع غير آمنة.

رابعاً: آثار الفيروسات:

حذف أو تلف البيانات.

إبطاء الجهاز أو تعطيله.

سرقة معلومات خاصة (مثل كلمات المرور).

التجسس أو فتح الجهاز عن بُعد.

خامساً: الحماية من الفيروسات:

1. استخدام برنامج مكافحة الفيروسات وتحديثه دورياً.

2. عدم تحميل البرامج من مصادر مجهولة.

3. الحذر من الروابط في البريد الإلكتروني.

4. تفعيل الجدار الناري (Firewall).

5. التحديث الدائم لنظام التشغيل.

سادساً: الجانب القانوني للفيروسات:

تعتبر الفيروسات أداة للجرائم الإلكترونية.

القوانين تجرّم:

نشر أو تطوير البرمجيات الخبيثة.

التعدي على الخصوصية أو سرقة البيانات.

اختراق الأنظمة بدون إذن.

أمثلة:

قوانين الجرائم المعلوماتية في العراق (أو بلدك).

عقوبات تصل إلى السجن والغرامة.