



الكلية : الاداب

القسم او الفرع : الترجمة

المرحلة: الاولى

أستاذ المادة : م.م سهر يوسف محمد

اسم المادة باللغة العربية :حاسبات

اسم المادة باللغة الإنكليزية :

اسم المحاضرة التاسعة باللغة العربية: الفيروسات في الحاسوب: ماهيتها وتأثيرها على الأنظمة الإلكترونية

اسم المحاضرة التاسعة باللغة الإنكليزية : **The Role of Viruses in Modern Technology and**

Their Impact on Cybersecurity

The Role of Viruses in Modern Technology and Their Impact on Cybersecurity

دور الفيروسات في التكنولوجيا الحديثة وتأثيرها على الأمن السيبراني

مع تزايد الاعتماد على التكنولوجيا الحديثة في الحياة اليومية والعملية، أصبح خطر الفيروسات الإلكترونية واحدًا من أكبر التحديات التي تواجه الأفراد والشركات على حد سواء. في هذه المحاضرة، سنتناول كيف تؤثر الفيروسات على التكنولوجيا الحديثة والأمن السيبراني، وما هي الاستراتيجيات المتبعة لمواجهة هذه التهديدات الرقمية.

تأثير الفيروسات على التكنولوجيا الحديثة

مع تطور التكنولوجيا الحديثة، ازدادت تعقيد الفيروسات وأساليبها في الهجوم. في السابق، كانت الفيروسات الحاسوبية بسيطة إلى حد كبير، ولكن مع تقدم البرمجيات والشبكات، بات بإمكان المهاجمين تطوير فيروسات متقدمة للغاية تستغل نقاط الضعف في الأنظمة. هذه الفيروسات قادرة على التسلل إلى الأجهزة الذكية، الشبكات المنزلية، وحتى البنية التحتية الحيوية مثل محطات توليد الطاقة والمستشفيات.

تطور هجمات الفيروسات

مع استخدام الحوسبة السحابية، إنترنت الأشياء (IoT)، والذكاء الاصطناعي، أصبحت الهجمات الفيروسية أكثر ذكاءً وتكيفًا مع البيئة الرقمية المتغيرة. على سبيل المثال، تنتشر الفيروسات الآن ليس فقط من خلال البرمجيات التقليدية، بل أيضًا عبر الأجهزة الذكية المتصلة بالإنترنت، مما يعزز الحاجة إلى تعزيز حماية الأمن السيبراني.

تأثير الفيروسات على الأمن السيبراني

يعد الأمن السيبراني أحد المجالات الأكثر تأثرًا بالفيروسات. إذ يمكن للفيروسات اختراق أنظمة الشركات والمؤسسات الكبيرة مما يعرض بيانات حساسة للخطر، مثل معلومات العملاء، الخطط الاستراتيجية، وأسرار الشركة. هذا قد يؤدي إلى خسائر مالية ضخمة، فضلًا عن تأثيره السلبي على سمعة المؤسسة. الهجمات الفيروسية مثل هجمات الفدية (Ransomware) تمثل تهديدًا حقيقيًا حيث يجبر المهاجمون الضحايا على دفع مبالغ مالية لاستعادة الوصول إلى بياناتهم.

استراتيجيات مواجهة الفيروسات

لحماية الأنظمة من الفيروسات، يعتمد الأمن السيبراني على مجموعة متنوعة من الأساليب التي تتراوح بين الإجراءات الوقائية والتقنيات المتقدمة. من بين هذه الاستراتيجيات:

- برامج مكافحة الفيروسات: برامج متخصصة في اكتشاف وإزالة الفيروسات قبل أن تسبب أضرارًا.
- تحديث الأنظمة بانتظام: من المهم إجراء التحديثات الأمنية اللازمة لسد الثغرات التي قد يستغلها الفيروس.
- التوعية الأمنية: توعية الموظفين والمستخدمين حول كيفية التعامل مع البريد الإلكتروني المشبوه والبرامج غير المعروفة.
- النسخ الاحتياطية: الاحتفاظ بنسخ احتياطية من البيانات المهمة للحماية من فقدان البيانات في حال وقوع هجوم فيروسي.

أمثلة على الهجمات الحديثة

1. **هجوم "SolarWinds"** أثر هذا الهجوم الفيروسي الذي استهدف شركة SolarWinds على العديد من المؤسسات الحكومية والخاصة في عام 2020.
2. **هجمات "Ransomware"** تشمل هجمات فدية تستهدف الشركات والمستشفيات وتجبرها على دفع أموال لاستعادة الوصول إلى بياناتها.
3. **Stuxnet** صُمم لاستهداف الأنظمة الصناعية وتم استخدامه كأداة في الحروب السيبرانية.