الأمن المعلوماتي

في عالمنا الرقمي المتسارع، لم يعد أمن المعلومات مجرد تخصص تقني، بل أصبح ضرورة حتمية لحماية أصولنا الرقمية، والحفاظ على خصوصيتنا، وضمان استمرارية أعمالنا.

يشهد العالم تحولًا رقميًا غير مسبوق، حيث تعتمد المؤسسات والأفراد على التكنولوجيا في كل جانب من جوانب الحياة. هذا الاعتماد المتزايد على الأنظمة الرقمية جعل المعلومات والأصول الرقمية عرضة لتهديدات متنوعة ومتطورة. من هنا، تبرز أهمية أمن المعلومات كمجال يهدف إلى حماية هذه الأصول من المخاطر التي تهددها.

تهدف هذه المحاضرة إلى تحقيق مجموعة من الأهداف الرئيسية، وهي:

1. **التعريف بمفهوم أمن المعلومات:** سنقوم بتوضيح المبادئ الأساسية لأمن المعلومات، مع التركيز على أبعادها الثلاثة: السرية، والنزاهة، والتوافر.
2. **التعرف على تهديدات أمن المعلومات:** سنتناول مجموعة واسعة من التهديدات التي تواجه الأنظمة الرقمية، بدءًا من البرمجيات الخبيثة وصولًا إلى الهجمات الإلكترونية المعقدة.
3. **استراتيجيات مواجهة التهديدات:** سنستعرض مجموعة من الاستراتيجيات والتقنيات التي يمكن للمؤسسات والأفراد استخدامها لتعزيز مستوى الأمان وحماية أصولهم الرقمية.
4. **التعرف على الأمن السيبراني:** سنوضح العلاقة بين أمن المعلومات والأمن السيبراني، مع التركيز على دور الأمن السيبراني في حماية البنية التحتية الرقمية الحيوية.

أولاً: مفهوم أمن المعلومات:

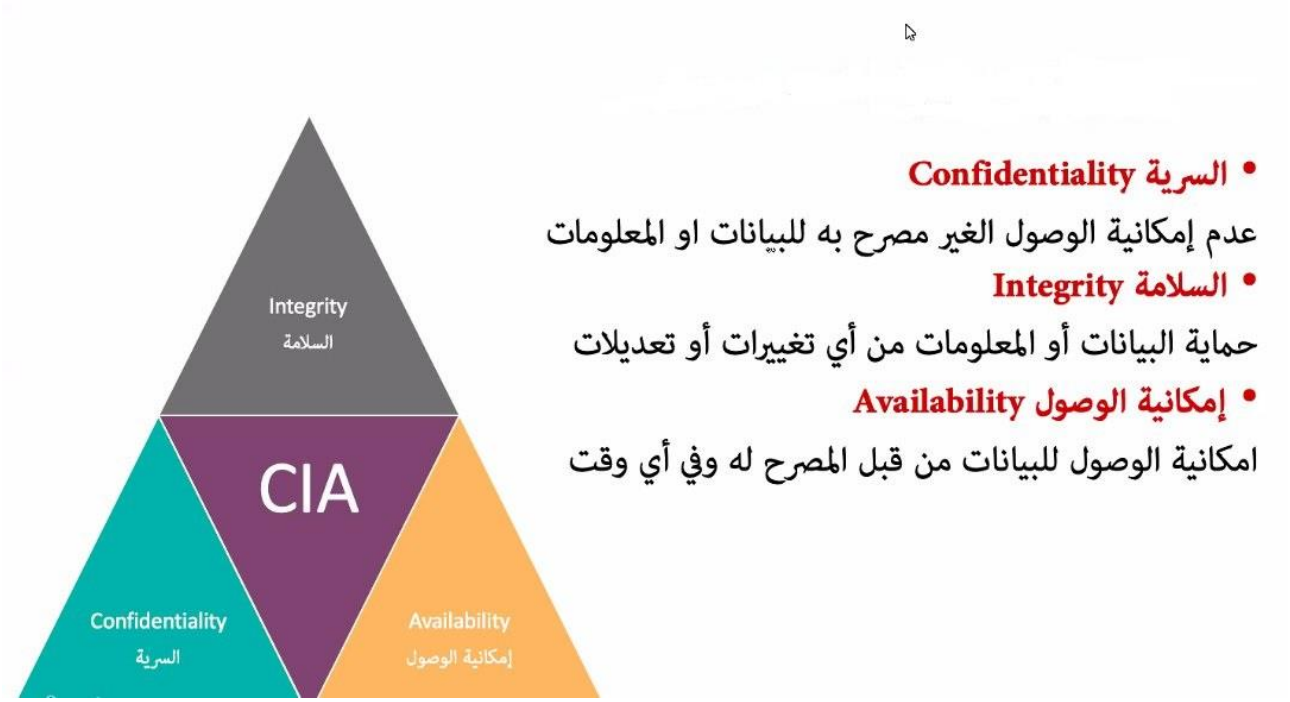
يمكن تعريف أمن المعلومات بأنه مجموعة من الإجراءات والتقنيات التي تهدف إلى حماية المعلومات من الوصول غير المصرح به، أو الاستخدام غير المصرح به، أو الكشف، أو التعطيل، أو التعديل، أو التدمير.

ويقوم أمن المعلومات على ثلاثة أبعاد رئيسية، يشار إليها غالبًا باسم– **ثلاثية CIA:**

- **السرية – الخصوصية (Confidentiality):** ضمان عدم إتاحة المعلومات إلا للأشخاص المصرح لهم بالوصول إليها.
- **السلامة – النزاهة (Integrity) :** ضمان دقة واكتمال المعلومات، وحمايتها من التعديل غير المصرح به.

- **إمكانية الوصول –التوافر (Availability):** ضمان إمكانية الوصول إلى المعلومات والأنظمة عند الحاجة إليها من قبل المستخدمين المصرح لهم.

الشكل (): مثلث الأمن المعلوماتي **CIA Triad**



ثانياً: تهديدات أمن المعلومات:

تواجه الأنظمة الرقمية مجموعة واسعة من التهديدات، التي يمكن أن تتسبب في أضرار جسيمة للمؤسسات والأفراد. ومن أبرز هذه التهديدات:

- **البرمجيات الخبيثة (Malware)**: وتشمل الفيروسات، والديدان، وأحصنة طروادة، وبرامج التجسس، وبرامج الفدية، وغيرها، وتهدف إلى السيطرة على الجهاز وتمكين المخترقين من الوصول إلى المعلومات بسهولة، أو تدمير الجهاز وإتلاف محتوياته وملفاته وبرامج تشغيله. تم التفصيل فيها أكثر في العرض التقديمي للمحاضرة يرجي الإطلاع.
- **التصيد الاحتيالي (Phishing)**: وهو محاولة للحصول على معلومات حساسة عن طريق انتحال شخصية جهة موثوقة.
- **هجمات الحرمان من الخدمة (Denial-of-Service Attacks)** : وتهدف إلى تعطيل عمل نظام أو شبكة عن طريق إغراقها بكميات كبيرة من حركة المرور.
- **هجمات الوسيط (Man-in-the-Middle Attacks)**: وفيها يقوم المهاجم باعتراض الاتصال بين طرفين وتبادل المعلومات بينهما دون علمهما.
- **التهديدات الداخلية (Insider Threats)**: وتشمل التهديدات التي تأتي من داخل المؤسسة، سواء من قبل موظفين حاليين أو سابقين.
- **الاختراق الأمني**: هو عملية اقتحام الأنظمة أو الشبكات الخاصة بأفراد أو منظمات خاصة أو حكومية بمساعدة بعض البرامج المتخصصة في فك وسرقة كلمات السر وتصريحات الدخول بهدف الاطلاع على المعلومات، أو تخريبها، أو سرقتها.
- **الاحتيال المالي**: ويتضمن الاحتيال واستعمال أجهزة الصرف الآلي، وبطاقات وحسابات مزورة وسرقة البيانات وسرقة بطاقات الائتمان، ويتضمن أيضًا الجرائم الناتجة عن السرقات والتعديات المالية على حسابات البنوك ومراكز التعامل المالي من خلال اختراق أنظمتها وتحويل الحسابات والأرصدة للمخترقين.
- **غسيل الأموال – تبيض الأموال**: وهو عملية تحويل الأموال المتحصلة من أنشطة إجرامية بهدف إخفاء أو إنكار المصدر غير الشرعي والمحظور لهذه الأموال أو مساعدة شخص ارتكب جرمًا ليتجنب المسؤولية القانونية عن الاحتفاظ بمتحصلات هذا الجرم.
- **الكوارث**: وهي الحوادث التي تؤثر على نظم المعلومات، وتنقسم إلى كوارث طبيعية مثل الزلازل والأعاصير والفيضانات والحرائق، وكوارث ناتجة عن أسباب تقنية كانقطاع التيار الكهربائي، أو حدوث

عطل في أحد أجهزة الحاسب الآلي أو برمجياته، بالإضافة إلى الأعمال التخريبية التي تشمل جميع الأعمال التي تؤدي إلى تعطل الجهاز بشكل متعمد، وتدخل في إطارها الأعمال الإرهابية التي تؤدي إلى توقف الجهاز عن العمل جزئيًا أو كليًا. وتخريب وسرقة قواعد البيانات.

ثالثاً: طرق مواجهة التهديدات:

لمواجهة هذه التهديدات المتزايدة، يمكن للمؤسسات والأفراد إتباع مجموعة من الاستراتيجيات والتقنيات، ومن أهمها:

- **تطبيق مبدأ أقل الامتياز (Principle of Least Privilege)** : ويعني منح المستخدمين الحد الأدنى من الصلاحيات اللازمة لأداء مهامهم.
- **استخدام المصادقة متعددة العوامل (Multi-Factor Authentication)** : ويتطلب من المستخدمين تقديم أكثر من دليل واحد للتحقق من هويتهم.
- **تشفير البيانات (Data Encryption)**: ويحول البيانات إلى صيغة غير قابلة للقراءة إلا باستخدام مفتاح التشفير المناسب.
- **الجدران النارية (Firewalls)**: وهي أنظمة تعمل كحاجز بين الشبكة الداخلية والشبكات الخارجية، وتقوم بفحص حركة المرور ومنع الوصول غير المصرح به.
- **أنظمة كشف ومنع الاختراق(Intrusion Detection and Prevention Systems)** : وهي أنظمة تقوم بمراقبة الشبكة والأنظمة بحثًا عن أي نشاط مشبوه، وتقوم باتخاذ إجراءات لمنع وقوع الهجمات.
- **التوعية والتدريب:** تدريب الموظفين على أفضل ممارسات أمن المعلومات، مثل كيفية التعرف على رسائل التصيد الاحتيالي، وكيفية إنشاء كلمات مرور قوية.
- **اختيار موقع مناسب للأجهزة وتوفير مصدر احتياطي للطاقة الكهربائية:** لحماية الأجهزة من الكوارث.
- **استخدام وسائل التحقق من الشخصية:** كجزء من طرق المصادقة متعددة العوامل.
- **برامج مكافحة الفيروسات:** لحماية الأنظمة من البرمجيات الخبيثة.

رابعاً: الأمن السيبراني:

غالبًا ما يستخدم مصطلحا "أمن المعلومات" و"الأمن السيبراني" بالتبادل، ولكن هناك فرق دقيق بينهما. يشير أمن المعلومات إلى حماية المعلومات بجميع أشكالها، سواء كانت رقمية أو غير رقمية، بينما يركز الأمن السيبراني بشكل خاص على حماية الأنظمة الرقمية المتصلة بالإنترنت، مثل أجهزة الكمبيوتر، والشبكات، والبرمجيات، والبيانات.

الأمن الحاسوبي أو الأمن السيبراني –أمن السايبر Cyber Security: مجموعة من الممارسات والتقنيات المصممة لحماية **أنظمة المعلومات والشبكات والبيانات** من **الهجمات الإلكترونية**، بهدف ضمان **السرية والنزاهة والتوفر** للمعلومات الرقمية ووسائلها.

وبالتالي، فإن الأمن السيبراني هو جزء من أمن المعلومات، ولكنه يركز على التهديدات والمخاطر التي تنشأ في الفضاء السيبراني. ونظرًا لاعتمادنا المتزايد على الأنظمة الرقمية المتصلة بالإنترنت، فقد أصبح الأمن السيبراني ذا أهمية بالغة لحماية البنية التحتية الحيوية، وضمان استمرارية الأعمال، والحفاظ على الأمن القومي.

في ختام هذه المحاضرة، ندرك أن أمن المعلومات لم يعد ترفًا، بل ضرورة ملحة في عالمنا الرقمي. إن التهديدات تتطور باستمرار، وتتطلب منا يقظة دائمة وتحديثًا مستمرًا لمعرفتنا واستراتيجياتنا. يتضح من المحاضرة أن هناك العديد من التهديدات التي تواجه أمن المعلومات، بدءًا من البرمجيات الخبيثة والاختراق وصولًا إلى الكوارث الطبيعية والأخطاء البشرية. ولمواجهة هذه التهديدات، يجب على المؤسسات والأفراد تطبيق استراتيجيات فعالة، مثل تطبيق مبدأ أقل الامتياز، واستخدام المصادقة متعددة العوامل، وتشفير البيانات، وتوعية الموظفين. ومن خلال تطبيق المبادئ الأساسية لأمن المعلومات، واعتماد أفضل الممارسات، والتعاون بين المؤسسات والأفراد، يمكننا بناء فضاء رقمي أكثر أمانًا وموثوقية.