المحور الثالث: الأمن المعلوماتي

مع تطور العلم والتكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة ونقل البيانات عبر الشبكات من موقع لآخر أصبح النظر إلى أمن تلك البيانات والمعلومات مهم للغاية مع العمل على توفير حمايتها من المخاطر التي تهددها.

أولا: مفهوم الأمن المعلوماتي

يعني أمن المعلومات إبقاء معلوماتك تحت سيطرتك المباشرة والكاملة، أي بمعنى عدم إمكانية الوصول لها من قبل أي شخص أو طرف آخر دون إذن منك، وان تكون على علم بالمخاطر المترتبة عن السماح لشخص ما بالوصول الى معلوماتك. بمعنى ، منع الافراد غير المصرح لهم، منع تعديل البيانات، منع أخذ المعلومات.

ثانيا: عناصر الأمن المعلومات

1- سرية المعلومة

2- سلامة المعلومة

3- توافر وإتاحة المعلومة

ثالثا: التهديدات المحتملة لأمن المعلومات (المشاكل الأمنية)

المشاكل الأمنية أو التهديدات عبارة عن أي حدث أو فعل من المحتمل أن ينتج انتهاك للسياسات والإجراءات الأمنية سواء كان مقصود أو غير قصود، ولقد تنوعت أشكال التهديدات المحتملة لأمن المعلومات التي يترتب عليها آثارا اقتصادية واجتماعية سلبية، وأهم هذه الأشكال ما يلي:

1- الاختراق:

الاختراق هي 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. ومن أهم الجرائم التقنية الناتجة عن عمليات الاختراق ما يلي:

- **الاختراق والتعدي ودخول الحواسيب غير المصرحة:** تهدف لقراءة البيانات أو نسخها أو الاستيلاء عليها أو اتلافها أو مسحها، وهذه الجرائم في ازدياد مستمر من طرف الهاكرز أو قراصنة الحاسب الآلي والانترنيت، حيث يقومون باختراق أنظمة وقواعد المعلومات وسرقتها أو العبث بها، وترتكب

جرائم الحاسب الآلي من طرف الأشخاص العاديين أكثر مما ترتكب من قبل العاملين في مجال الحاسب الآلي.

- **الاحتيال المالي:** تتضمن الجرائم من هذا النوع الاحتيال واستعمال أجهزة الصرف الآلي، وبطاقات وحسابات مزورة وسرقة البيانات وسرقة بطاقات الائتمان ، وتتضمن أيضا الجرائم الناتجة عن السرقات والتعديات المالية على حسابات البنوك ومراكز التعامل المالي من خلال اختراق أنظمتها وتحويل الحسابات لأرصدة المخترقين.
- **غسيل الأموال:** عبارة عن عملية تحويل الأموال المتحصلة من أنشطة إجرامية بهدف إخفاء أو انكار المصدر غير الشرعي والمحظور لهذه الأموال أو مساعدة شخص ارتكب جرما ليتجنب المسؤولية القانونية عن الاحتفاظ بمتحصلات هذا الجرم. وفي هذا الصدد يتم استخدام التقنية في عمليات التحويل للأرصدة أو شراء منتجات بواسطة الانترنيت بهدف اظهار المال الناتج عن جرائم جنائية (كترويج المخدرات، أو الإرهاب...) بصورة أموال لها مصدر مشروع. وفي غالبية هذه الحالات يقوم المجرمون بتصميم برامج تقوم بمسح المعلومات الموجودة في الجهاز بمجرد الوصول اليها بطريقة غير مباشرة، وفي بعض الحالات يدمرون جميع وسائل حفظ المعلومات ذات العلاقة كالأقراص وخلافه للتخلص من الأدلة التي تدينهم.

2- الفيروسات:

من أخطر المشكلات التي تهدد أمن المعلومات، حيث تهدف إلى السيطرة على الجهاز وتمكن المخترقين من الوصول للمعلومات بسهولة، أو تدمير الجهاز واتلاف محتوياته وملفاته وبرامج تشغيله.

الفيروس عبارة عن برنامج صغير مثل أي برنامج تطبيقي مكتوب بإحدى اللغات، يتم برمجته من قبل المبرمجين أو الشركات ويتم تصميمه بشكل متعمد ومتقن، حيث يعمل المبرمجون على برمجة الفيروسات وذلك لاهداف عديدة اقتصادية وسياسية وعسكرية، فبعض المبرمجين الهواة يعتبرون ان عمل الفيروس فن وهواية، في حين ان بعض المبرمجين والشركات تسعى من وراء انتاج هذه الفيروسات الى تحقيق أهداف تجارية من خلال بيع برامج مضادات الفيروسات.

ان الفيروسات ذات هدف تخريبي تنتشر ذاتيا وبسهولة من حاسوب لآخر وتستطيع أن تصيب وتفسد الأجهزة والبرامج والشبكات المتصلة معها بشكل جزئي أو كلي، وأهم طرق انتقال الفيروسات هي الشبكة العنكبوتية ووسائط التخزين مثل الفلاش والأقراص. وللفيروس ثلاث خواص: التضاعف، التخفي، والحاق الأذى. ومن أكثر أنواع الفيروسات انتشارا: **حصان طروادة، ديدان الحواسيب، القنابل الموقوتة.**

3- الكوارث:

الكارثة هي حادثة محددة زمنيا ومكانيا ينجم عنها تعرض مجتمع بأكمله أو جزء من مجتمع إلى أخطار شديدة مادية، وخسائر في أفراده تؤثر على البناء الاجتماعي بارباك حياته وتوقف توفير المستلزمات الضرورية لاستمرارها، اما بالنسبة الى الكوارث التي تؤثر على نظم الحاسوب يمكن تقسيمها إلى:

- **الكوارث الطبيعية:** كالزلازل، الأعاصير، الفيضانات والنيران.
- **الكوارث الناتجة عن أسباب تقنية:** كانقطاع التيار الكهربائي، أو حدوث عطل في أحد أجهزة الحاسب الآلي أو برمجياته.
- **الأعمال التخريبية:** تتضمن جميع الأعمال التي تؤدي إلى تعطل الجهاز بشكل متعمد، وتدخل في إطارها الأعمال الإرهابية التي تؤدي إلى توقف الجهاز عن العمل جزئيا او كليا.

رابعا: طرق مواجهة مهددات أمن المعلومات

1- اختيار موقع مناسب للأجهزة:

2- توفير مصدر احتياطي للطاقة الكهربائية

3- استخدام وسائل التحقق من الشخصية

4- جدران الحماية

5- برامج مكافحة الفيروسات

6- التشفير او التعمية