**المحاضرة الثامنة: الأمن السيبراني**

**أولا- مفهوم الفضاء السيبراني:**

 يقصد بالفضاء السيبراني ذلك الوسط الذي تتواجد فيه شبكات الحاسوب ويحصل من خلالها التواصل الإلكتروني . وبمفهوم أشمل يعرف بأنه مجال مركب مادي وغير مادي يشمل مجموعة من العناصر هي: أجهزة الكمبيوتر، أنظمة الشبكات والبرمجيات ، حوسبة المعلومات ، نقل وتخزين البيانات ومستخدمي كل هذه العناصر .

كما يمكن تعريف الفضاء السيبراني على أنه:

 مصطلح لوصف الأنظمة والخدمات المتصلة إما بشكل مباشر أو بشكل غير مباشر إلى شبكة الانترنت والاتصالات السلكية واللاسلكية وشبكات الكمبيوتر.

يتضح من خلال التعاريف السابقة أن الفضاء السيبراني يشمل العناصر الرئيسية التالية:

 **الشكل رقم (01) يوضح العناصر الأساسية للفضاء السيبراني:**

**الفضاء السيبراني**

**شبكة الحواسيب**

**البرمجيات**

**كائنات**

**المعلومات**

**التقنيات**

**الأطياف الكهرومغناطيسية**

**البنية التحتية**

**المكونات الرقمية الأساسية**

**الالكترونيات**

الأشخاص

**وحدات التحكم**

**الإنترنت**

**ثانيا: تعريف الجريمة السيبرانية:** يشار إلى إساءة استخدام تكنولوجيا المعلومات والاتصالات من قبل المجرمين بالتبادل على أنها جرائم الانترنت أو إساءة استخدام الكمبيوتر والجريمة المرتبطة بالحاسب الآلي ، جريمة التكنولوجيا المالية، والجريمة الالكترونية والجريمة الالكترونية كما عرفتها رابطة كبار ضباط الشرطة تنطوي على استخدام الكمبيوتر أو الانترنت شبكات تكنولوجيا لارتكاب أو تسهيل ارتكاب الجريمة ، أما المعهد الاسترالي لعلم الإجرام فيرى بأنها " تسمية عامة لجرائم ارتكبت باستخدام تخزين البيانات الإلكترونية أو جهاز الاتصالات "

**ثالثا:تعريف الأمن السيبيراني:**

عرف الأمنالسيبراني بأنه " عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة"

كما عرفبأنه" وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات ، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ، وتوفير الاتصالات المشفرة.......إلخ .

كما يعني الأمن الالكتروني أي أداة أو تقنية أو علمية مستخدمة لتحمي أصول المعلومات لنظام الأمن الإلكتروني ، حيث يتيح الأمن الإلكتروني ويضيف قيم الشبكات وموجه للبنية الأساسية المرنة والصلبة والمكونات البنية الأساسية الصلبة تعني الأجهزة الصلبة hardware والبرمجيات software المطلوبة لحماية النظام والبيانات من التهديدات والأمن من خارج أو داخل النظام ، أما المكونات البنية الأساسية المرنة تعني السياسات والعمليات والبروتوكولات ، والتوجيهات التي تحمي النظام والبيانات من مصادرها المختلفة.

 ويقصد أيضا بالأمن السيبراني بأنه الحالة المرغوب فيها لعمل أنظمة المعلومات والاتصالات والتي تمنحها القدرة على المقاومة والتصدي لكل ما ينجم عن الفضاء السيبراني ، والذي من شانه أن يعرض المعلومات المخزنة أو المعالجة او المنقولة للتلف أو التغيير أو التجسس.

**رابعا:عناصر الأمن السيبراني:**

لتحقيق الأمن السيبراني تحتاج الدولة الى تنسيق جهودها في جميع أنحاء نظام المعلومات الخاص بها ، وتشمل هذه الجهود عناصر الأمن السيبراني مايلي:

**\* أمن الشبكة:** وهي إجراءات تستخدمها الشركات والأفراد لحماية شبكة المؤسسات من الاختراق.

**\* أمن التطبيقات:** وهي وضع تدابير لحماية البرامج من الفيروسات الضارة وعدم سرقة المعلومات السرية.

\* **أمن المعلومات:** عبارة عن الضوابط التي تضمن خصوصية المعلومات وحمايتها والوصول بسهولة لها عند الحاجة سواء نقلها أو تخزينها.

\* **الأمن التشغيلي:** هي عمليات لحماية المعلومات ومعالجتها وتخزين البيانات.

**\* التعافي من الكوارث:** مجموعة خطوات تستخدمها الشركات للحد من التهديدات أو فقدان المعلومات

\* **استمرارية العمل:** خطة تتبعها الشركات لمواصلة العمل أثناء خرق المعلومات رغم الموارد المتأثرة إن التحدي الأكثر صعوبة في الأمن السيبراني التطور المستمر لمخاطر الأمن نفسها باستمرار .

.لذلك يجب إتباع نهج أكثر فعالية في مجال الأمن السيبراني من خلال دراسة المخاطر المحتملة واتخاذ إجراءات وقائية لتجنب حدوثها ، ووضع خطة للتعافي من الكوارث في حال وقوعها لتقليل الخسائر والتعافي بسرعة.

**خامسا:هدف وأهمية الأمن السيبراني :**

إن هدف الأمن السيبراني هو المساعدة على حماية الأصول وموارد المنظمات من النواحي التنظيمية والبشرية، والمالية، والتقنية ، والمعلوماتية بحيث يسمح لها بمواصلة مهمتها ، والهدف النهائي هو ضمان عدم تضررها ضررا دائما وهذا يتألف من التقليل احتمالات تجسد أي تهديد ، والحد من الضرر الناجم أو سوء الأداء ، وضمان استعادة العمليات العادية لحالتها السابقة خلال إطار زمني مقبول وبتكلفة مقبولة ، في أعقاب وقوع حادث أمني ، وتستغرق عملية الأمن السيبراني المجتمع بأسره ، من حيث يكون فرد فيه معنيا بتنفيذها ، ويمكن دعم ذلك بتطوير مدونة سلوك سيبرانية لأجل الاستخدام السليم لتكنولوجيات المعلومات والاتصالات ، وإعلان سياسات أمن حقيقية تفنن المعايير التي يكون متوقعا من مستخدمي الأمن السيبراني ( الكيانات والشركاء والموردون) الوفاء بها.

**سادسا: أبعاد الأمن السيبراني:**

**1 - البعد العسكري.**

**2- البعد الاقتصادي .**

**3 – البعد الاجتماعي.**

**4 – البعد القانوني.**

**5 – البعد السياسي.**

**سابعا: مشاكل الأمن السيبراني:**

 تواجه النظام الأمني السيبراني الكثير من المشاكل والتحديات وهو أمر طبيعي ، فلا بد من وجود بعض الثغرات في تطبيقات الحماية ، ومن أهم المشاكل نذكر الأتي :

\* زيادة وتطور الهجمات الإلكترونية على البيانات.

\* انتشار عمليات الاحتيال من خلال إخفاء هوية المستخدمين.

\* نقص الخبراء والمطورين في قطاع الأمن السيبراني .

\* انهيار أنظمة الحماية بسبب استخدام الاتصال غير الأمن بالإنترنت .

\* كثرة عمليات الاحتيال والسرقة الإلكترونية والخداع وتطورها .

\* استخدام مواقع التواصل الاجتماعي التي تتيح الدخول إلى معلومات المستخدم بكل سهولة .

**ثامنا : أهمية الأمن السيبراني في القطاع المالي المصرفي:**

- الحفاظ على سمعة البنوك والشركات.

- الإبقاء على درجة نزاهة وثقة مرتفعة.

- تجنب عقوبات عدم الامتثال .

- الحفاظ على بيانات العملاء من الاختراق والسرقة.

- منع الخسائر المالية.

**تاسعا: تحديات الأمن السيبراني في القطاع المصرفي:**

- نقص الوعي .

- الميزانيات غير الكافية والافتقار إلى الإدارة.

- ضعف أمن هوية الدخول والوصول إلى الشبكات.

- زيادة برامج الفدية (Ransomware) .

- الأجهزة المحمولة والتطبيقات.

- وسائل التواصل الاجتماعي.

**- عاشرا: إستراتيجيات تقوية الأمن السيبراني لتحسين الاستقرار المالي والمصرفي:**

سوف نحاول ذكر بعض الإستراتجيات الأساسية والتي من شأنها أن تساهم في تقوية الأمن السيبراني بدرجة كبيرة وتحسين الاستقرار المالي والمصرفي و المتمثلة في:

- إعداد الخرائط السيبرانية والتحديد الكمي للمخاطر.

- تقارب القواعد التنظيمية.

- القدرة على الاستجابة.

- الرغبة في العمل المشترك.

- استحداث سبل ردع أقوى .

- تنمية القدرات و المهارات .