**مقدمة بحث عن اهمية الامن السيبراني**

ظهرت العديد من المصطلحات الجديدة في العصر الحديث والتي واكبت التطورات التي يعيشها الكوكب وخصوصًا مع مطلع القرن الواحد والعشرين، وقد ارتبطت تلك المفاهيم بالتطورات الكبيرة التي حدثت في شتى المجالات وبشكل خاص في مجال التكنولوجيا والاتصالات، فمنذ ظهور الإنترنت والحواسيب والأجهزة الذكية ظهرت آلاف المصطلحات المرافقة لها، فقد تطلبت تلك التكنولوجيا برامج وتطبيقات وأدوات وطرق مختلفة من أجل التعامل معها ومع تقنياتها الحديثة، ومن أهم تلك المفاهيم ظهر مفهوم الأمن السيبراني، وسوف يتم التعرف عليه وعلى أهميته من خلال فقرات بحث عن الأمن السيبراني التعريف والأنواع والأهمية وغير ذلك.

**بحث عن اهمية الامن السيبراني**

في كثير من الأحيان يكلف المعلمون طلابهم بكتابة بحث عن موضوع معين، ويكون ذلك عادةً من أجل إثراء الطلاب والطالبات بالمعلومات المهمة حول ذلك الموضوع الذي وقع اختيار المدرس عليه نظرًا لأهميته من وجهة نظره وارتباطه بالمادة التي يدرسها الطلاب أيضًا، ولا بد أن يتطرق البحث إلى مختلف التفاصيل حول الموضوع سواء كان الموضوع تقنيًا أو سياسيًا أو تاريخيًا أو دينيًا أو اجتماعيًا أو علميًا وغير ذلك، حيث يبدأ البحث بمقدمة تكون تمهيدًا لما سيأتي فيه، وينتهي بخاتمة موجزة تلخص ما ورد فيه، وهذا البحث سوف يتناول الحديث عن أهمية الأمن السيبراني من خلال فقرات عديدة عن هذا الموضوع المهم.

**ما هو الأمن السيبراني‎**

في البداية لا بدَّ من التعرف على تعريف مفهوم الأمن السيبراني، حيث يطلق عليه اسم الأمن السيبراني أو أمن الحاسوب ويسمى باللغة الإنجليزية باسم: cybersecurity or Computer security، ويعتبر أمن الحواسيب أحد فروع التكنولوجيا المهمة جدًا والتي ظهرت في العصر الحديث، والتي يمكن أن تعرف أيضًا باسم أمن المعلومات، ويطبق هذا الأمن على الحواسيب والشبكات بشكل أساسي، ولا بد من القول بأن أمن الحاسوب "الأمن السيبراني" يسعى إلى حماية المعلومات من التلف أو الفساد بسبب الكوارث الطبيعية أو السرقة أو غير ذلك من الأسباب، ويحرص على أن تبقى متوفرة لأصحابها وفي متناول أيديهم كلما احتاجوا إليها، ويمكن تعريف الأمن السيبراني بشكل عام بأنه مجموعة من الآليات والعمليات الجماعية التي يتم من خلالها حماية المعلومات والخدمات الحساسة من العبث أو التلف أو النشر أو الانهيار من قبل الأنشطة غير المرغوب بها وغير المصرح لها من أشخاص غير جديرين بالثقة بالنسبة لأصحاب المعلومات.

**نشأة الأمن السيبراني**

يعتقد البعض أن الأمن السيبراني حديث الظهور، ولكن في الحقيقة يرجع ظهور الأمن السيبراني إلى السبعينيات من القرن العشرين الماضي، ففي ذلك الوقت لم تكن برامج الفيروسات والتجسس والديدان الإلكترونية منتشرة وشائعة، ولكن مع مرور الوقت زاد معدل الهجمات الإلكترونية والجرائم الإلكترونية ما أدى إلى ظهور مثل هذه المصطلحات، ويشار إلى أن الحواسيب وشبكات الإنترنت كانت في مرحلة التطوير في ذلك الوقت، وكان من السهل التعرض لتهديدات عديدة مختلفة، وفي ثمانينات القرن العشرين تم ابتكار أول برنامج فيروسات على يد روبرت تي موريس، وقد حصل وقتها على تغطية إعلامية واسعة بسبب انتشاره بشكل كبير وتعطيل العديد من الأنظمة، وقد حكم عليه بالسجن جراء ذلك، وكانت تلك الحادثة سببًا قويًا ودافعًا لتطوير الأمن السيبراني وأدواته وقوانينه، وفي التسعينيات شهد الأمن السيبراني تطورًا كبيرًا وذلك مع تطور الفيروسات الخبيثة وأساليب الهجمات الإلكترونية المختلفة، ووضعَت بروتوكولات حماية المواقع الإلكترونية مثل: http، وكان إحدى الوسائل التي أتاحت الوصول الآمن إلى شبكة الإنترنت منذ ظهورها.

**أنواع الأمن السيبراني**

توجد أنواع عدة للأمن السيبراني، وتختلف عن بعضها حسب مجال الحماية الذي يعمل عليه النظام، وفيما يأتي سوف يتم إدراج أنواع الأمن السيبراني:

* **أمن الشبكات "Network Security"**: يتم في هذا النوع حماية الحواسيب من القرصنة والهجمات الإلكترونية التي تتعرض لها سواء كان ذلك من داخل الشبكة أو من خارجها، وقد استخدمت فيه تقنيات مختلفة مثل جدار الحماية وغير ذلك.
* **أمن التطبيقات "Application Security"**: يتم في هذا النوع حماية مختلف المعلومات المرتبطة بالتطبيقات والبرامج على الحواسيب، مثل كلمات المرور وعمليات المصادقة وأسئلة الأمان لتحديد هوية المستخدم وما إلى هنالك.
* **الأمن التشغيلي** **"Operational Security"**: يتولى هذا النوع مهمة إدارة المخاطر التي تتعرض لها العمليات الداخلية للأمن السيبراني، ولذلك يتم فيه توظيف خبراء من أجل إيجاد خطط بديلة في حال التعرض لهجمات إلكترونية مباغتة.
* **الأمن السحابي "Cloud Security"**: يشمل هذا النوع البرامج التي تعمل على تخزين المعلومات والبيانات وتحفظها من خلال شبكة الإنترنت، ويتم حفظ البيانات من خلال برامج إلكترونية على شبكة الإنترنت بدلًا من تخزينها محليًا أو على أجهزة قابلة للتلف والفساد، وهذا ما من شأنه أن يوفر حماية تخزين عالية جدًّا.

**مميزات الأمن السيبراني**

يتميز الأمن السيبراني بأنه يمكن المستخدمين من حماية معلوماتهم وبياناتهم المخزنة على أجهزتهم، أو المعلومات الموجودة على البرامج المختلفة، ومن أهم ميزات الأمن السيبراني ما يأتي:

* يعمل على تقييم جميع المخاطر والتهديدات التي قد تهاجم المستخدم.
* يوفر الأمن السيبراني إطارًا فعالًا للعمل وآمنًا في جميع الأوقات.
* يحمي المعلومات والبيانات من جميع المخاطر.
* يمتلك مصادر فعالة من أجل الحماية وتوفر البيئة الآمنة للمستخدمين.

**أهمية الأمن السيبراني**

إنَّ أهمية الأمن السيبراني كبيرة جدًّا في الوقت الحالي، وخصوصًا مع سيطرة التكنولوجيا الحديثة على جميع مفاصل الحياة وفي شتى المناحي، وتكمن أهمية الأمن السيبراني في أهمية البيانات والمعلومات التي يعمل على توفير الحماية لها، ومن أهم فوائد الأمن السيبراني أنه يحمي أمن الحواسيب بيانات الشركات المختلفة والمؤسسات الحكومية وبيانات الأشخاص من الهجمات والغزوات الإلكترونية التي تهدف غالبًا إلى سرقة المعلومات واستغلالها في مكاسب ومصالح وأمور أخرى مختلفة دون إذن ودون شرعية، وربما تكون تلك البيانات متعلقة بالأمن العام للبلاد أو بالصناعة أو بالتجارة أو بمعلومات لها أهمية كبيرة لدى أصحابها سواء كانوا أفرادًا او مؤسسات عامة أو خاصة أو دولية، وفي بعض الأحيان تكون هذه البيانات حكومية ومهمة جدًّا، ومن أجل هذا تزداد أهمية الأمن السيبراني كل يوم بشكل أكبر لحماية هذه البيانات المختلفة.

**ما أهداف الأمن السيبراني**

هنالك أهداف عديدة يحرص الأمن السيبراني على تحقيقها وتوفيرها لجميع الأشخاص والمستخدمين من أفراد ومؤسسات ويعمل على الوصول إليها من قبل جميع مستخدمي شبكة الإنترنت حول العالم، وفيما يأتي سوف يتم إدراج أهم أهداف الأمن السيبراني بشكل عام:

* **تأمين البيانات**: يعني هذا أن الأمن السيبراني يسمح للأشخاص المصرح لهم بالوصول إلى المعلومات والبيانات، ويعمل على تعديلها في الوقت المناسب، ويعني هذا أنه يعمل على وصول البيانات الموثوق، ويمنع الأفراد غير الموثوقين وغير المصرح لهم من الوصول إليها.
* **صحة البيانات**: يعمل على ضمان صحة المعلومات ودقتها كما يريد أصحابها، كما يعمل على حمايتها من أي تعديل أو تحريف غير مسموح به وغير مصرح له، ويهدف هذا النوع من الحماية إلى عدم العبث بالبيانات أو التغيير عليها من قبل المتطفلين والفاسدين واللصوص ويوفر ضمان وجود مصادر موثقة للمعلومات وحقيقية.
* **سرية المعلومات**: يعمل الأمن السيبراني على المحافظة على الخصوصية بشكل كبير، ويحرص على تجنب الكشف غير الموثوق وغير المصرح له عن البيانات والمعلومات إلا لأصحابها فقط، وبهذا يوفر ضمان سرية البيانات بشكل كامل.

**أهم المشاكل التي يواجهها الأمن السيبراني**

رغم كل الفوائد والأهمية التي يحملها الأمن السيبراني إلا أنه يواجه العديد من المشاكل والعقبات في الآونة الأخيرة، ويسعى الخبراء والمختصون إلى تجاوزها باستمرار، وفيما يأتي أهم العقبات التي تواجه الأمن السيبراني بالتفصيل:

* زيادة تعقيد الهجمات والجرائم الإلكترونية باستمرار، حيث يترافق ذلك مع التقدم والتطور الإلكتروني على كافة الأصعدة، وقد ساعد الذكاء الاصطناعي وتعلم الآلة والعملات المشفرة  في زيادة تعقيد تلك البرامج الضارة.
* عدم وجود أعداد كافية من خبراء الأمن السيبراني، إذ يعاني هذا المجال من العمل من نقص كبير في عدد الخبراء.
* إمكانية إخفاء الهوية باستعمال العديد من تقنيات عالم الإنترنت المستخدمة مثل العملات المشفرة إذ يمكن استخدامها من دون الخوف من الكشف عن المستخدم، وهذا يوفر فرصة آمنة للصوص لسرقة ما يريدون من دون أن يكشفوا.
* عدم وجود اتصال آمن على شبكة الإنترنت، وهذا يؤدي إلى انهيار نظام تبادل المعلومات وانتشار البرامج الضارة بشكل أكبر وأسهل.
* تطوير عمليات الاحتيال باستمرار من خلال استهداف واستغلال الأشخاص وخداعهم بطرق عديدة مثل النقر على رابط يؤدي إلى الوصول إلى بياناتهم ومعلوماتهم الشخصية.

**خاتمة بحث عن اهمية الامن السيبراني**

من دون شك يعتبر الأمن السيبراني سلاحًا حديثًا في مواجهة اللصوص والمفسدين الذين يقومون بهجمات للاستيلاء على معلومات وبيانات تكون سرية بهدف السرقة والابتزاز وما شابه ذلك، وهو أحد الطرق المهمة في التعامل مع مشاكل التكنولوجيا وشبكة الإنترنت وعالم الحواسيب، لأنه مع ظهور كل اختراع تظهر العديد من المشاكل التي يجب التصدي لها عبر ابتكار وسائل دفاعية ومقاومة ناجحة، وهنا تكمن أهمية الأمن السيبراني في قدرته على صد تلك الأساليب القذرة التي تسعى إلى ممارسة السرقة والابتزاز والاختلاس عبر وسائل التكنولوجيا الحديثة والدخول إلى خصوصيات المستخدمين والاستيلاء على معلوماتهم وبياناتهم الشخصية.