مقدمة في الأمن السيبراني

جيهان تركي نصرالدين

الامن السيبراني

الامن السيبراني :

حماية الشبكات وأنظمة المعلومات و الاجهزة والبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق او تعطيل او تعديل او استخدام او استغلال غير مشروع.

أهمية الامن السيبراني:

يحافظ على امان الدول

يحارب الجرائم الالكترونية والاختراق والاحتيال والتصدي للحروب السيبرانية .

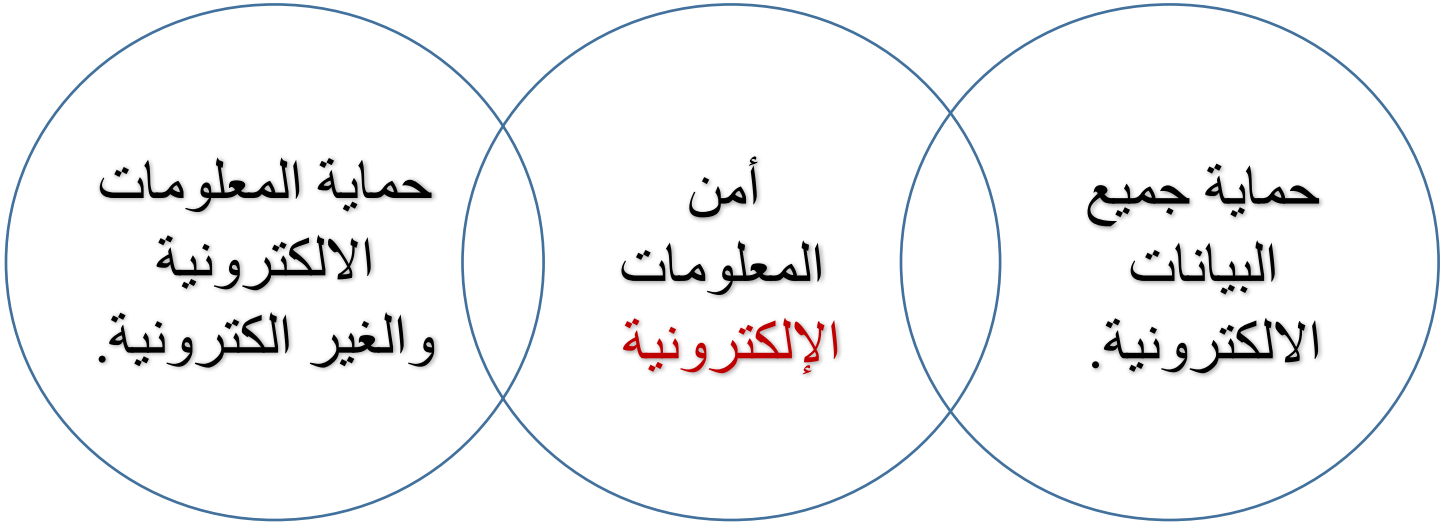
اعداد جيهان نصرالدين

اهتمام المملكة العربية السعودية بالأمن السيبراني

- **الهيئة الوطنية للأمن السيبراني**
- هي هيئة حكومية مختصة في الأمن السيبراني في السعودية، مهتمة في شؤونه، وفي زيادة عدد الكوادر الوطنية المؤهلة لتشغيله،
- لها شخصية مستقلة، وترتبط مباشرة بالملك سلمان بن عبدالعزيز آل سعود، ويرأس مجلس إدارتها وزير الدولة الدكتور مساعد العيبان.
- تأسست بأمر ملكي في عام 2017.
- **الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز**
- هي مؤسسة وطنية تحت مظلة اللجنة الأولمبية السعودية

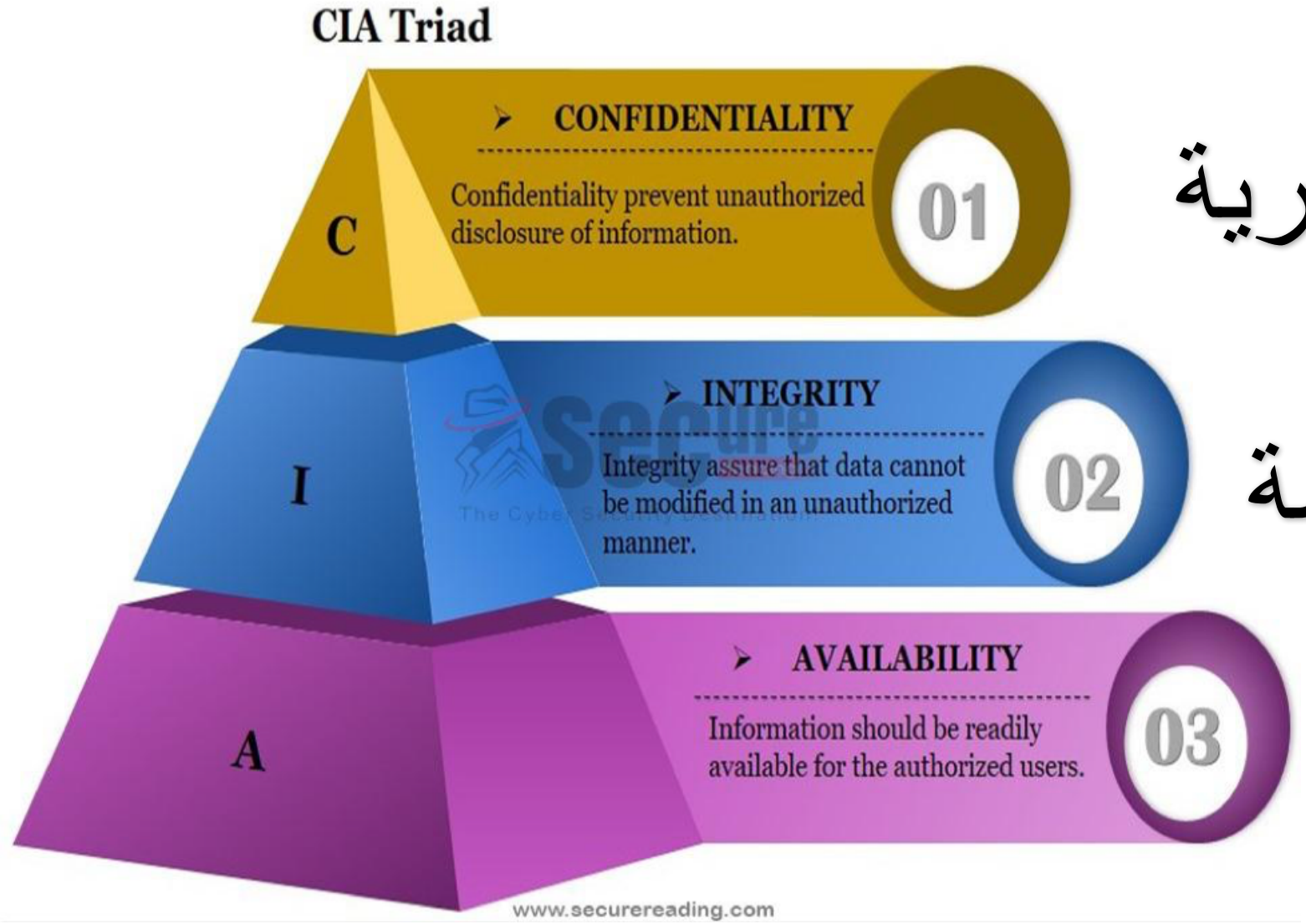
امن المعلومات و الامن السيبراني

- **امن المعلومات :** يهتم بحماية البيانات في جميع اشكالها " ورقية و الكترونية "
- **الامن السيبراني :** يشمل حماية البيانات الالكترونية



اعداد جيهان نصرالدين

اهداف الامن السيبراني



السرية

السلامة

الاتاحة

الهندسة الاجتماعية و التصيد

- **الهندسة الاجتماعية**

مهاجم يحاول التلاعب بالأفراد في القيام بأعمال أو إفشاء معلومات سرية.

- **التصيد الاحتيالي**

هو جريمة إلكترونية يتم فيها الاتصال بالهدف عن طريق البريد الإلكتروني أو الهاتف أو رسالة نصية من قبل شخص يمثل مؤسسة شرعية لجذب الأفراد إلى توفير بيانات حساسة مثل معلومات التعريف الشخصية وتفاصيل البطاقات المصرفية وبطاقات الائتمان وكلمات المرور.

اشكال الاحتيال

- ❖وجود أخطاء إملائية و أيضا أخطاء في تركيب الجملة.
- ❖السؤال عن معلومات شخصية.
- مثل السؤال عن رقم بطاقة حسابك البنكي أو كلمة المرور الخاصة بك. فالبنك الخاص بك على علم برقم حسابك فهو ليس في حاجة إلى مثل هذه المعلومات.
- ❖تحتوي الرسالة على تهديدات قد تكون غير منطقية غالباً.
- ❖ارتباطات مزيفة ، مثل رابط يوجهك لموقع اخر غير المكتوب

البرمجيات الضارة

البرمجيات الضارة :

برنامجٌ يُصيب الأنظمة بطريقة خفية (في الغالب) لانتهاك سرية او سلامة ودقة او توافر البيانات او التطبيقات او نظم التشغيل.

- برامج التجسس مصممة لتتبع وتجسس على المستخدم.
- برامج الإعلانات مصممة لتقديم الإعلانات تلقائيًا .
- برامج الرعب مصممة لإقناع المستخدم باتخاذ إجراء محدد بناءً على الخوف.
- الفدية مصممة لتشفير بيانات الكمبيوتر حتى يتم الدفع مقابلها .
- الفايروسات و الديدان وحصان الطروادة و روتكيت .

أعراض الإصابة بالبرمجيات الضارة

- زيادة في استخدام المعالج
- انخفاض في سرعة الكمبيوتر
- توقف عمل الكمبيوتر
- انخفاض في سرعة التصفح
- مشاكل غير مفهومة عند الاتصال بالشبكة
- ملفات محذوفة او معدلة
- ظهور ملفات ، برامج و ايقونات على سطح المكتب غير معروفة
- القيام بإجراءات غير معروفة
- اغلاق البرامج لنفسها

هجمات حجب الخدمة ، هجمات حجب الخدمة الموزعة

- وفيها يتم اغارق الخادم بالطلبات بقصد شُغل الخادم وتعطيله عن التجاوب مع المستخدمين الأبرياء. ونتيجة لعملية الإغراق تتوقف الشبكة عن العمل بسبب زيادة الزحام المروري للبيانات فتتوقف الخدمات ويتعطل التواصل مع الأجهزة والتطبيقات الشبكية.
- تحدث هجمات قطع الخدمة ضرر كبير في نظام الاتصالات وتخسر المؤسسة المال والوقت في محاولة للتعافي من تلك الهجمات. وهذه الهجمات سهلة التنفيذ حتى من قبل اشخاص قليلو الخبرة.
- تتشابه هجمات حجب الخدمة الموزعة مع هدف هجمات حجب الخدمة ولكن تختلف في انها تحدث من اكثر من جهاز بقص شُغل الخادم.

حماية اجهزتك!

- شغل جدار الحماية
- استخدام برامج الكشف عن الفايروسات
- حدث نظام تشغيل الكمبيوتر
- احمِ الأجهزة باستخدام كلمات المرور
- عمل نسخة احتياطية للبيانات
- شفر بياناتك
- استخدم التصفح امخفي

الجدار الناري و مكافح الفايروسات و امن الانترنت

- مكافح الفايروسات : برنامج مصمم لحماية النظام من البرمجيات المدمرة مثل الفايروسات الموجودة في النظام
- الجدار الناري : هو برنامج يتحكم في الاتصالات الداخلة والخارجة والمسموح منها والغير مسموح
- مجموعات أمان الإنترنت : عادة من أكثر من تطبيق واحد يتم تجميعه في واجهة واحدة.

القضايا الأخلاقية في الأمن السيبراني

- الحفاظ على السرية التامة للملكية أو المعلومات الحساسة الأخرى التي تتم مواجهتها في سياق الأنشطة المهنية
- الامتناع عن أي أنشطة قد تشكل تضارباً في المصالح أو الإضرار بسمعة أو ضرر لأصحاب العمل أو مهنة أمن المعلومات أو الجمعية
- لا تعمد إصابة أو استهانة السمعة المهنية للمنظمة او زملائك.