مفهوم الامن:

- هي عملية حماية النظام من الدخول الغير مصرح به للأفراد من خارج المؤسسة او داخلها بدون قصد.
- إبقاء معلوماتك تحت السيطرة الكاملة بمعني عدم إمكانية الوصول لها من قبل أي أي شخص اخر بدون اذن منك.

مخاطر البيئة:

تحدث عندما يتم اختراق النظام لديك، وأكثر المستهدفين هم الأشخاص الذين يقومون بتصفح الانترنت

حيث يسبب الاختراق في مشاكل مثل بطء حركة التصفح وانقطاعه على فترات منتظمة.

تواجد المخاطر:

1- الرؤية: ان يتوفر لدي جميع الدوائر الحكومية قرارات امن المعلومات.
2- الغايات:
   1) تحسين عمليات امن المعلومات
   2) إيجاد هيئة لتمكين الخدمات
   3) تدريب قوي عاملة
   4) المحافظة علي العمليات
   5) المحافظة علي الجاهزية
   6) حماية المعلومات والأصول
   7) نشر عمليات إدارة المخاطر
   8) إيجاد برامج امن المعلومات

امن المعلومات:

ضمان الحفاظ علي السرية والسلامة والتوافر والتي تشمل الأجهزة والبرمجيات.

السرية Confidentiality:

الحفاظ علي القيود المصرح بها للوصول الي المعلومات

لحماية الخصوصية والمعلومات.

السلامة Integrity:

حماية النظام من التلف او التعديل.

التوافر Availability:

ضمان الوصول الي المعلومات واستخدامها في الوقت المناسب.

الأصالة:

خاصية كون الشيء حقيقي وموثوق به، أي الثقة في الارسال.

المساءلة:

الهدف الأمني الذي يفرض متطلبا يشمل إمكانية تتبع أفعال أي كيان.

التهديدات السلبية:

الهكر يأخذ الرسالة ولم يرسلها

التهديدات الإيجابية:

الهكر يأخذ الرسالة ثم يرسلها وهنا الخطر يكون اقل من السلبية.

فيروسات الكمبيوتر:

الأكثر شيوعا من بين مشاكل امن المعلومات التي يتعرض لها الأشخاص والشركات.

هو برنامج يدخل الي الجهاز ويكون غير مرغوب فيه

والفيرس هو احد البرامج الخبيثة او المتطفلة.

والبرامج المتطفلة تسمي الديدان او احصنة طراوده.

برامج الدعاية او التجسس:

هي تنتشر خلف ملف حتي يتم تشغيله تسيطر عليه.

وتتواجد الفيروسات في مكان أساسي في الحاسب كالذاكرة المؤقتة.

كيف تعمل الفيروسات؟

في البداية كانت تعتمد علي الإهمال لكن ما تراها من فيروسات اكثر تعقيدا مثل البرامج الدودية

Worms: يمكن نسخ نفسها والانتقال الي الأجهزة المختلفة.

Trojans: تتخذ هيئة برامج مفيدة حتي يقوم المستخدم بتنزيلها علي جهازه ثم تسيطر عليه.

ابرز المؤشرات لوجود فيروس:

1) بطء عمل نظام التشغيل.
2) السرعة ابطء من الطبيعي.
3) كثرة التوقف عن استجابة الأوامر.
4) تعطل نظام التشغيل عن العمل ثم يعاد تشغيله.
5) الطابعة لا تعمل.
6) اذا ظهر رسائل غير عادية

خطوات التخلص من فيروسات الكمبيوتر:

ثبت جميع التحديثات المتوفرة لنظام التشغيل Operation System Update.

عمل فحص للجهاز بعد التثبيت يمكن ان تكون التحديثات مصابه.

كيف تحمي جهازك من الفيروسات:

لا شيء يضمن امن للموارد بنسبة 100% هو فقط تقليل او تجنب المخاطر.

1) تثبيت جميع تحديثات الأمان.
2) استخدام ال Firewall وهي أداة تحمي من المتسللين.
3) تثبيت برامج لمكافحة الفيروسات والحفاظ علي تحديثها.

الجدار الناري Firewall:

هو جهاز hardware او software يقوم بالتحكم ومرور البيانات في الشبكة والتحكم يكون بالمنع او السماح وغالبا يستخدم في وجود البريد الالكتروني والانترنت مع بروتوكولات TCP/IP

ماذا يستطيع ان يفعل الFirewall :

يعمل علي النظام الخارجي مثل شبكة الانترنت والارسال ولكن النظام الداخلي لا يتعامل معه وهكذا الديدان

تحديات امن الحاسوب:

1) ليس امرا بسيطا.
2) يجب اخد الهجمات بعين الاعتبار.
3) تطوي عمل الخوارزميات والمعلومات السرية.
4) تطلب مراقبة منتظمة.
5) معرقة عقول بين المهاجم ومسؤول النظام.

6) تعتبر عائقا امام استخدام النظام.

أنواع الهجوم:

1- هجوم نشط: محاولة تغير موارد النظام
2- هجوم سلبي: محاولة الحصول علي المعلومات دون التأثير علي الموارد.

تصنيف الهجمات:

1- هجوم داخلي: بواسطة كيان داخل محيط النظام.
2- هجوم خارجي: من خارج محيط الأمان.

الوسائل المستخدمة للتعامل مع الهجمات الأمنية:

1- الوقاية Prevent
2- الكشف Detect
3- الاسترداد Recovery

ملاحظات مهمة:

هذه الإجراءات قد تخلق ثغرات جديدة.

بكون هناك دائما ثغرة متبقية لا يمكن القضاء عليها بالكامل.

الهدف هو تقليل المخاطر.

مصطلح Counterassaults الهجمات المضادة او إجراءات الوقاية:

الإجراءات التي تتخذ لمنع وتخفيف تأثير الهجمات او استغلال الثغرات مثل استخدام جدران الحماية والتحديثات الأمنية وأنظمة كشف التسلل.