وزارة التعليم العالي والبحث العلمي

كلية المستقبل الجامعة

قسم ادارة الاعمال

المرحلة: الاولى

المادة: برمجة الحاسوب

اسم التدريسي: م. م هبه علي حسن

امان الحاسوب وتراخيص البرامج

مقدمه

يتم استخدام الحواسيب في جميع المجالات للتعامل مع البنوك والتسوق والاتصال مع الاخرين عبر الرسائل الالكترونية او برامج المحادثة. ومن المهم المحافظة على الرسائل الخاصة والبيانات الشخصية ومحتويات الحاسوب . لذا يجب الاهتمام بالأمن وحماية الحاسوب . ان التطورات الحديثة في انظمة شبكات الحاسوب وتقنيات المعلومات احدثت تغييرات مستمرة في اساليب العمل والميادين كافة , اذ اصبحت عملية انتقال المعلومات عبر الشبكات المحلية والدولية واجهزة الحاسوب من الامور الروتينية في يومنا هذا , واحدى عالمات العصر المميزة التي يمكن الاستغناء عنها لتأثيرها الواضح في تسهيل متطلبات الحياة العصرية من خلال تقليل حجم الاعمار وتطوير اساليب خزن وتوفير المعلومات , اذ ان انتشار انظمة المعلومات المحوسبة ادى الى ان تكون عرضة لاختراق. لذلك اصبحت هذه التقنية سلاحا ذو حدين تحرص المنظمات على اقتناءه وتوفير سبل الحماية له, والهدف من امن الحاسوب يتضمن حماية المعلومات والممتلكات من الاختراقات والسرقة والفساد او الكوارث الطبيعية وفي نفس الوقت يسمح للمعلومات والممتلكات ان تبقى منتجة وفي متناول مستخدميها .الاختراقات هي محاولة الدخول على جهاز او شبكة حاسوب الي من قبل شخص غير مصرح له بالدخول الى الجهاز او الشبكة وذلك بغرض الاطلاع او السرقة او التخريب او التعطيل.

امن الحاسوب Security Computer

يعد امن الحاسوب جزء من امن المنظومة المعلوماتية والتي بدورها جزء من الامن العام Cyber Security والهدف من امن الحاسوب يتضمن حماية المعلومات والممتلكات من السرقة والفساد او الكوارث الطبيعية .وبعبارة اخرى هي عملية منع واكتشاف استعمال الحاسوب الي شخص غير مسموح له مخترق (وهي اجراءات تساعد على منع المستخدمين غير المسموح لهم بالدخول واستعمال ملفاته).

- **خصوصية الحاسوب Privacy Computer**

يستخدم هذا المصطلح ليشير الى الحق القانوني في الحفاظ على خصوصية البيانات المخزنة على الحاسوب او الملفات المشتركة . وتظهر حساسية مسالة خصوصية الحاسوب او البيانات الخاصة عندما يتعلق الامر ببيانات التعريف الشخصية المحفوظة في اي جهاز رقمي سواء كلن حاسوب او غيره وان عدم القدرة على التحكم بأخفاء هذه البيانات هو ما يؤدي الى تهديد خصوصية البيانات في الغالب

تراخيص برامج الحاسوب

وهو ما يعرف (ب رخصة او تراخيص البرامجيات) : وهي وثيقة قانونية تحكم استعمال او اعادة توزيع البرامجيات المحمية بحقوق النسخ . اذ يخضع استخدام برامج الحاسوب لاتفاقية التراخيص التي هي بمثابة عقد بين المستخدم وبين الجهة المنتجة للبرامج. وتسمح اتفاقية التراخيص باستخدام البرنامج كما انها تمنح حقوق اخرى وتفرض بعض القيود ايضا . وغالبا ماتوجد اتفاقية التراخيص على المنتج بشكل :

- مطبوعة على ورقة مستقلة مرفقة مع المنتج.
- مطبوعة في دليل الاستخدام وغالبا ما يكون ذلك على ورقة الغلاف من الداخل.

وتنص اتفاقية التراخيص في ضرورة الحصول على ترخيص مستقل لكل نسخة من كل برنامج يتم استخدامه على الحاسوب , فلكل اتفاقية ترخيص تمنح الحق في استخدام نسخة واحدة من البرنامج على الحاسوب

انواع التراخيص

1 : **اتفاقية الترخيص للمستخدم** : التطبيقات وانظمة التشغيل, وتتمثل في منح ترخيص استخدام المنتج على جهاز حاسوب واحد باستخدام مفتاح التفعيل لكل حاسوب

2 : **التراخيص الجماعية** : تختلف من منتج الى اخر , وهي تسمح باستخدام البرنامج على عدد معين من اجهزة الحاسوب , وهي غالبا ما توفر مزايا سعرية كما يسهل الاحتفاظ بها , وتختلف عن النوع الاول باستخدام مفتاح تفعيل واحد لكل الحواسيب او لمجموعة بين الحواسيب

الاختراق الأكتروني Intrusion Electronic

هو قيام شخص غير مخول او اكثر بمحاولة الدخول الوصول الكترونيا الى الحاسوب او الشبكة عن طريق شبكة الانترنت وذلك بغرض الاطلاع, والسرقة , التخريب , والتعطيل باستخدام برامج متخصصة

انواع الاختراق الالكتروني

يمكن تقسيم الاختراق من حيث الطريقة المستخدمة الى ثلاثة اقسام :::

1- المزودات او اجهزة الرئيسية للشركات والمؤسسات او الجهات الحكومية : وذلك باختراق الجدار الناري Firewallوالتي توضع لحمايتها يتم ذلك باستخدام المحاكاة لغرض الخداع وهو مصطلح يطلق على عملية انتحال شخصية للدخول الى النظام

2- الاجهزة الشخصية : والعبث بما فيها من معلومات وتعد من الطرق الشائعة لقلة خبرة اغلب مستخدمي هذه الاجهزة من جانب ولسهولة تعلم برامجيات الاختراق وتعددها من جانب اخر

3- .البيانات : من خلال التعرض والتعرف على البيانات اثناء انتقالها ومحاولة فتح التشفير اذا كانت البيانات مشفرة وتستخدم هذه الطريقة في كشف ارقام بطاقات الائتمان وكشف الارقام السرية لبطاقات البنوك.

مصادر الاختراق االلكتروني:

***مصادر متعمدة**

ويكون مصدرها جهات خارجية تحاول الدخول الى الجهاز بصورة غير مشروعة بغرض قد يختلف حسب الجهاز المستهدف.

- ومن الامثلة على المصادر المتعمدة الاختراق :
- الالكتروني المحترفون والهواة لغرض التجسس دون الاضرار بالحاسوب
- اختراق شبكات الاتصال والاجهزة الخاصة بالاتصال للتنصت او الاتصال المجاني
- اختراق لنشر برنامج معين او لكسر برنامج او لفك شفرتها المصدرية– (.)Crackers
- اعداء خارجيون وجهات منافسة .
- مجرمون محترفون في مجال الحاسوب والانترنت.

***مصادر غير متعمدة**

وهي تنشا بسبب ثغرات موجودة في برامجيات الحاسوب والتي قد تؤدي الى تعريض الجهاز الى نفس المشاكل التي تنتج عن الاخطار المتعمدة

ما هو الأمن السيبراني

يحتوي نهج الأمن السيبراني الناجح على طبقات متعددة من الحماية تنتشر عبر أجهزة الكمبيوتر أو الشبكات أو البرامج أو البيانات التي يرغب المرء في الحفاظ عليها. بالنسبة للأشخاص والعمليات والتكنولوجيا، يجب أن يكمل كل منها الآخر داخل المؤسسة لإنشاء دفاع فعال في مواجهة الهجمات Cisco أتمتة عمليات التكامل على مستوى منتجات السيبرانية يمكن لنظام إدارة التهديدات الموحد .المحددة وتسريع وظائف عمليات الأمان الرئيسية: الاكتشاف والتحقيق والمعالجة Security

الأشخاص

يجب على المستخدمين فهم المبادئ الأساسية لأمان البيانات والامتثال إليها مثل اختيار كلمات مرور قوية والحذر من المرفقات الموجودة ضمن البريد الإلكتروني والنسخ الاحتياطي للبيانات

التقنية

توفير التكنولوجيا هو أمر ضروري لمنح المؤسسات والأفراد أدوات الأمن السيبراني اللازمة لحماية أنفسهم من الهجمات السيبرانية. يجب حماية ثلاثة كيانات رئيسية: الأجهزة الطرفية مثل أجهزة الكمبيوتر والأجهزة الذكية والموجّهات والشبكات والسحابة. تتضمن أشكال التكنولوجيا والحماية DNS الشائعة المستخدمة لحماية هذه الكيانات، الجيل التالي من الجدران النارية وتصفية ضد البرامج الضارة وبرامج مكافحة الفيروسات وحلول أمان البريد الإلكتروني

أنواع تهديدات الأمن السيبراني

1. **تصيد المعلومات** هو عملية إرسال رسائل بريد إلكتروني احتيالية تشبه رسائل البريد الإلكتروني من المصادر الموثوقة. والهدف هو سرقة المعلومات الحساسة مثل أرقام بطاقة الائتمان ومعلومات تسجيل الدخول. وهو أكثر أنواع الهجمات الإلكترونية شيوعًا. يمكنك المساعدة في حماية نفسك من خلال التثقيف أو استخدام الحلول التقنية التي تعمل على تصفية رسائل البريد الإلكتروني الضارة.
2. **برامج الفدية** هي نوع من البرامج الضارة. وهي مصممة بهدف ابتزاز المال عن طريق منع الوصول إلى الملفات أو نظام الكمبيوتر حتى يتم دفع الفدية.

ولا يضمن دفع الفدية استرداد الملفات أو استعادة النظام

3. **البرامج الضارة** هي نوع من البرامج المصممة للوصول غير المصرح به إلى جهاز الكمبيوتر أو إلحاق الضرر به .