الجامعة السورية الخاصة
SYRIAN PRIVATE UNIVERSITY

وحدة متطلبات الجامعة

مهارات الحاسوب
Computer Skills
2019

المحاضرة الثانية عشر

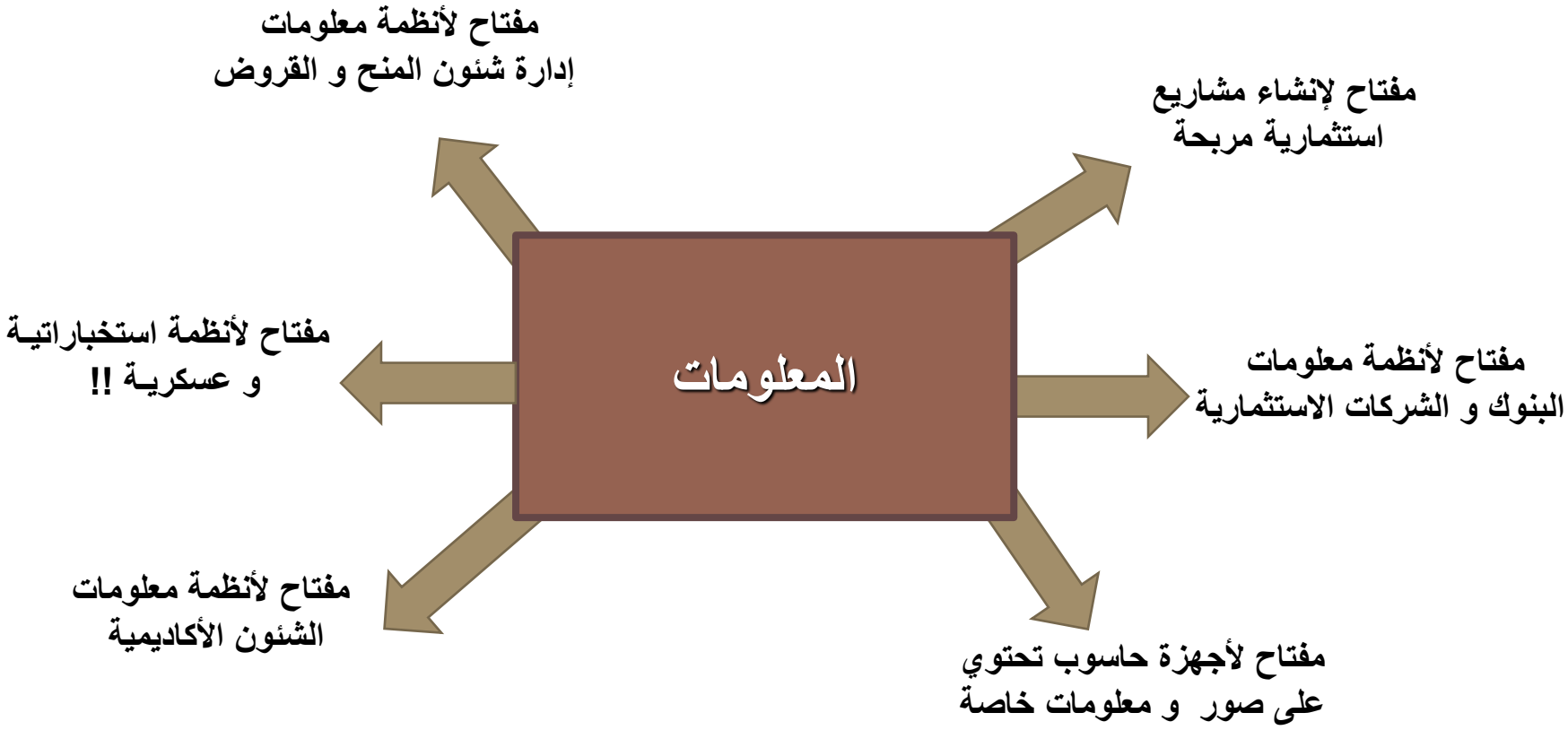
أمن المعلومات
(Information security)

أمن المعلومات

أمن المعلومات:

- هو عملية الحفاظ على المعلومات بشكل آمن، وحمايتها من الوصول الغير المصرح به، وذلك لكي تبقى محمية و آمنة. وأن تكون على علم بالمخاطر المترتبة على السماح لشخص ما بالوصول إلى معلوماتك الخاصة.
- تؤمن المنشأة نفسها والأفراد العاملين فيها وأجهزة الحاسب المستخدمة فيها ووسائط المعلومات التي تحتوي على بيانات المنشأة، وذلك في جميع مراحل تواجد المعلومة (التخزين – النقل – المعالجة).
- حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات في كافة المراحل.

أهمية أمن المعلومات



أهمية أمن المعلومات – ضرورة ملحة:

١. القطاعات الأمنية والعسكرية والاقتصادية تعتمد على صحة ودقة المعلومات.
٢. حاجة الدول لوجود إجراءات أمنية قابلة للتطبيق تغطي المخاطر التي يمكن أن تظهر عند التعامل مع الأطراف الأخرى.
٣. الحاجة المتزايدة لإنشاء **بيئة إلكترونية آمنة** تخدم القطاعين الخاص والعام.
٤. النمو السريع في استخدامات التطبيقات الإلكترونية والتي تتطلب بيئة آمنة.
٥. الحاجة إلى حماية البنية التحتية للشبكة المعلوماتية وذلك من أجل استمرارية الأعمال التجارية.
٦. مع تطور التقنية المعلوماتية وازدهارها توفرت فرصاً **للإجرام الإلكتروني**.

أهداف أمن المعلومات

١) معالجة الأخطاء المتعمدة وغير المتعمدة أثناء تصميم وبناء و تشغيل الأنظمة.

٢) منع سرقة أو اكتشاف المعلومات لغرض تغييرها بشكل غير قانوني.

٣) الحفاظ على المعلومات المتواجدة في اي نظام من الضياع أو التلف و من أخطاء الاستخدام المتعمد أو العفوي والكوارث الطبيعية و أخطاء الأجهزة و أخطاء البرمجيات.

عناصر أمن المعلومات

١. **السرية أو الموثوقية:** وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك .

٢. **الاستمرارية:** التأكد من استمرار عمل النظام ألمعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع.

٣. **التكاملية وسلامة المحتوى:** التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به في أي مرحلة من مراحل المعالجة أو الإرسال والاستقبال.

مقدمة في أمن المعلومات

كلمة المرور (Password)

- هي مجموعة من الرموز التي تسمح للدخول إلى الحاسوب، أو الموارد على شبكة الاتصال أو المعلومات.

فوائد كلمة المرور:

- تسمح للمستخدمين المصرح لهم فقط لدخول النظام.
- إدارة و تحديد هوية الأشخاص بفاعلية و التدقيق في عملية الوصول.
- حفظ و حماية المعلومات.
- حماية المعلومات الشخصية الخاصة بك.

نصائح لإنشاء كلمات المرور

١. يجب أن يكون توقعها صعب.

٢. يجب ألا يكون طولها أقل من (٨) أحرف.

٣. يجب أن تتسم بميزة التعقيد، و التي ينبغي أن تحتوي على خليط من الأرقام و الأحرف و الرموز الخاصة مثل (*/ - @ + $).

٤. يجب أن لا تحتوي على اسم المستخدم.

٥. يجب أن لا تحتوي كلمة المرور على معلومات شخصية مثل رقم الهاتف، أو اسم أحد الأقارب، أو تاريخ الميلاد.

نصائح للاستخدام كلمات المرور

١. لا تفصح عن كلمات المرور لأي شخص.
٢. لا تستخدم نفس كلمة المرور للعمل في مواقع متعددة مثل البريد الإلكتروني أو الحاسب المصرفي.
٣. لا تكتب أو تحفظ كلمة المرور على ورقة أو في رسالة بريد الالكتروني.
٤. لا تستخدم خاصية تذكر كلمة المرور المتوفرة في بعض أنظمة التشغيل.
٥. قم بتغير كلمة المرور بشكل دوري.

البرامج الخبيثة (Malicious Software)

- هي أحد تهديدات الحاسوب في هذا العصر.
- البرمجيات الخبيثة: هي أي برنامج يعطي بعض السيطرة أو السيطرة الكاملة على الحاسوب الخاص بك لمن قام بتصميمه لهذا الغرض.
- الأضرار التي تقوم بها هذه البرامج قد تكون خفيفة كتغيير اسم المؤلف لمستند ما أو كبيرة مثل الوصول الكامل للحاسوب دون المقدرة على تعقبها.

- يمكن تتصنيف أنواع البرمجيات الخبيثة على النحو التالي:

١. الفيروسات (Viruses)
٢. الديدان (Worms)
٣. برامج التجسس (Spywares)
٤. الخداع (Hoax)
٥. عمليات الاحتيال واصطياد الضحايا (Phishing Scam).
٦. أحصنة طروادة (Trojan Horses).

الفيروسات (Viruses)

- فيروسات الكمبيوتر:
  - هي برامج تقوم بمهاجمة وإتلاف برامج معينة.
  - تنتقل الى برامج أخرى عند تشغيل البرامج المصابة.
  - تقوم بالتلاعب بمعلومات الكمبيوتر المخزنة.
- ينتقل الفيروس إلى جهازك عندما تقوم بنقل ملف ملوث بالفيروس إلى جهازك أو عند زيارة احد المواقع المشبوهة أو أثناء تبادل الأقراص أو الفلاشات مع الأصدقاء.
- ينشط الفيروس عند محاولة فتحه ويمكن ان يصلك ايضاً عن طريق البريد الإلكتروني على هيئة مرفقات.

أنواع الفيروسات (Viruses Types)

١. فيروسات التشغيل: (Boot Sector Virus): وهو الذي ينشط في منطقة نظام التشغيل وهو من اخطر أنواع الفيروسات حيث انه يمنعك من تشغيل الجهاز.
٢. فيروسات الماكرو (Macro Virus): وهي من اكثر الفيروسات انتشارا حيث انها تضرب برامج الاوفيس.
٣. فيروسات الملفات (File Virus): وهي تنتشر في الملفات وعند فتح أي ملف يزيد انتشارها.
٤. الفيروسات المخفية (Stealth Virus): وهي التي تحاول أن تختبئ من البرامج المضادة للفيروسات و لكن سهلة الإمساك.
٥. الفيروسات المتحولة (Polymorphic virus): وهي الأصعب على برامج المقاومة حيث انه صعب الإمساك بها وتتغير من جهاز إلي آخر في أوامرها ولكن مكتوبة بمستوى غير تقني فيسهل إزالتها.
٦. فيروسات متعددة الملفات (Multipartite Virus): تصيب ملفات قطاع التشغيل و سريعة الانتشار.
٧. الباتشات (Trojans): الباتش هوعبارة عن برنامج صغير قد يكون مدمج مع ملف آخر للتخفي عندما ينزله شخص و يفتحه يصيب المسجلات و يفتح عندك منافذ مما يجعل جهازك قابل للاختراق بسهوله و هو يعتبر من أذكى البرامج.
   - فمثلا عند عمل سكان (scan)هناك بعض التورجن يفك نفسه على هيئة ملفات غير محدده فيمر عليها السكان دون التعرف علية و من ثم يجمع نفسه مرة ثانية.

الديدان (Worms)

- ديدان الحاسوب هي الفيروسات التي تقوم بإنشاء نسخ من تلقاء نفسها.
- يمكن أن تسبب الضرر بشكل واسع.
- على عكس الفيروسات، التي تتطلب نشر ملفات المضيف المصابة، تعتبر الديدان برنامج مستقل ولا يحتاج إلى برنامج مضيف أو مساعدة أشخاص للنشر.

برامج التجسس (Spywares)

- هي مماثلة لبرامج الإعلانات، ولكن لديها نوايا ضارة. في حالة التجسس، المستخدم يجهل هذا الغزو.
- يمكن لبرامج التجسس جمع ونقل المعلومات الشخصية.
- المعلنين وغيرهم يرغبون في معرفة ماهي المواقع الإلكترونية التي يقوم المستخدمون بزيارتها وما هي عادات وأساليب تصفح الإنترنت لديهم.
- في بعض الأحيان تقوم برامج التجسس بإعادة توجيه مدخلات المتصفح لتوجه المستخدم إلى موقع آخرغير المقصود.
- بسبب ما تقوم به هذه البرامج من نقل للمعلومات دون علم المستخدم، تصنف هذه البرامج على أنها برمجيات مقتحمة للخصوصية

الخدعة (Hoax)

- هو إنذار كاذب عن فيروس في الحاسوب.
- عادة التحذير يصل عن طريق مذكرة البريد الإلكتروني أو يتم توزيعها من خلال مذكرة في الشبكة الداخلية للشركة
- فيروسات الخدعة، عادة ما تكون غير ضارة ولكنها تكون مزعجة باعتبارها خداع وتضيع للوقت وذلك من خلال إعادة توجيه الرسالة.
- هناك عدد من الخداع من خلال تحذير المستخدمين أن ملفات النظام المهمة توجد بها فيروسات وبالتالي تقوم بتشجيع المستخدم عل حذف الملف، مما يسبب إتلاف النظام.

رسائل الاصطياد الخادعة (Phishing Scam)

- التصيد هو محاولة الحصول على معلومات مثل أسماء المستخدمين وكلمات المرور وتفاصيل بطاقة الائتمان من قبل محتالين متنكرين بوصفهم أنهم يعملون في منظمات جديرة بالثقة.
- التصيد هي عملية يحتال فيها المهاجم حيث يرسل رسالة بالبريد الإلكتروني يطلب فيها بطاقات ائتمانية أو بطاقات التجارة الإلكترونية وتكون صالحة وسارية المفعول
- البريد الإلكتروني غالباً ما يستخدم أساليب التخويف في محاولة الإغراء الضحية إلى زيارة مواقع ويب مخادعة. يشعر فيها الضحية بأنها مواقع عامة مثل التجارة الإلكترونية أو الخدمات المصرفية.

أحصنة طروادة (Trojan Horses)

- حصان طروادة من البرمجيات الخبيثة التي تبدو أنها برمجيات سليمة. تقوم بخداع المستخدمين من أجل تحميلها وتطبيقها على أنظمتهم.
- فيتم بذلك تنشيطها، وتبدأ بمهاجمة النظام، فتؤدي إلى بعض الأمور المزعجة للمستخدم أو بعض الأضرار.

أضرار الإصابة بالفيروسات و البرامج الخبيثة

١. تعطيل الحاسوب.
٢. ظهور شاشة الموت الزرقاء.
٣. سرقة النقود إلكترونياً.
٤. بعض الأمور المزعجة للمستخدم مثل تغير سطح المكتب و حذف الملفات.
٥. سرقة البيانات.
٦. إتلاف البرمجيات و التسبب في الحرمان من استخدام بعض الخدمات.
٧. بطئ عمل الحاسب وبطئ الاتصال بالانترنت.

أعراض الإصابة بالفيروسات و البرامج الخبيثة

- تباطؤ أداء الحاسوب.
- زيادة حجم الملفات، أو زيادة زمن تحميلها للذاكرة .
- ظهور رسائل تخريبية على الشاشة، أو الرسوم أو صدور بعض الأصوات الموسيقية.
- حدوث خلل في لوحة المفاتيح كأن تظهر على الشاشة أحرف ورموز غير التي تم ضغطها أو حدوث قفل للوحة المفاتيح .
- ظهور رسالة ذاكرة غير كافية لتحميل برنامج كان يعمل سابقاً بشكل عادي.
- سعة الأقراص أقل من سعتها الحقيقية.

طرق الحماية

- هناك العديد من البرامج التي تقوم بفحص الفيروسات وتقسم إلى نوعين رئيسيين:
  - فاحصات الفيروسات على الحاسب الشخصي،
  - فاحصات الفيروسات على الشبكة،
    - حيث يتم في هذا النوع تنزيل البرنامج الرئيسي على الخادم ومن ثم تحديث تعريفات الفيروسات على أجهزة العميل بشكل آلي من الخادم.
  - يمكن حماية المعلومات على الحاسب بطريقة التشفير، أي ترميز البيانات كي يتعذر قراءتها من أي شخص ليس لديه كلمة مرور لفك شفرة تلك البيانات.

برامج الحماية:

١) برامج مكافحة الفيروسات.

٢) توفير نسخ احتياطية (backup).

٣) جدار الحماية.

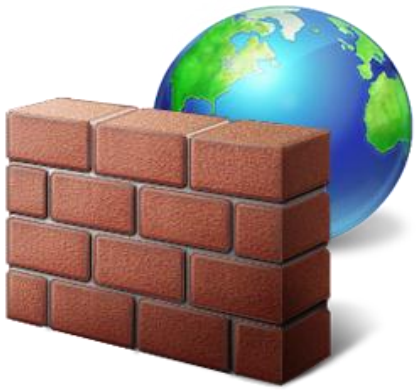
٤) كلمة المرور(Password).

برامج الحماية من الفيروسات

- استخدام البرمجيات المضادة للفيروسات على كافة أجهزة الكمبيوتر المتصلة بالإنترنت وتحديث هذه البرمجيات.
- العديد من برامج مكافحة الفيروسات تدعم التحديثات التلقائية لتعريفات الفيروسات. ومن المستحسن استخدام هذه التحديثات التلقائية عندما تكون متاحة.

الحماية باستخدام جدران الحماية (Firewalls)

- غالباً ما تتم عملية الاختراق من خلال الثغرات الموجودة في المنافذ (Ports) الخاصة بالحاسب الشخصي والتي تعتبر بوابات خروج ودخول البيانات في الحاسب الآلي.
- تعريف الجدار الناري: هو حاجز بين الحاسب الآلي والعالم الخارجي، يقوم بتصفية البيانات القادمة من الخارج بناءً على مقاييس معينة مثل حجم البيانات والعنوان **IP Address** والبروتوكول الذي تم استعماله والمنفذ الذي تستخدمه البيانات للدخول إلى الحاسب الآلي.
- يقوم الجدار الناري Firewall بغلق المنافذ التي لا يحتاج إليها المستخدم أو التطبيق لإستخدامها على الإنترنت وبذلك يمنع الفيروسات والإختراقات من تلك المنافذ.



- أشهر برامج جدران الحماية:

١. Zone Alarm Security Suite
٢. Outpost Firewall
٣. Windows Firewall
٤. Kaspersky Internet Security
٥. Norton 360, Norton IS.

النسخ الاحتياطي (Backup)

- قد نتعرض لفقدان بعض البيانات أو الملفات المهمة أو الضرورية عن طريق:
  - حذفها من غير قصد.
  - تعرضها للعطب.
- لذلك نحتاج لعمل نسخة احتياطية من ملفات النظام، ثم في حالة فقدان أو تلف الملفات يكون باستطاعتنا استعادة الملف المحذوف من النسخة الاحتياطية.

نصائح عند فتح ملحقات البريد الإلكتروني

- ✓ لا تفتح أية ملفات ملحقة ببريد إلكتروني من مصدر غير موثوق.
- ✓ لا تفتح أية ملفات ملحقة ببريد إلكتروني ما لم تعرف محتواها.
- ✓ لا تفتح أية ملفات ملحقة ببريد إلكتروني إذا كان حقل الموضوع مشكوكاً فيها وغير متوقع.
- ✓ احذف سلسلة رسائل البريد الغير هامة وتجنب الرد عليها.
- ✓ لا تقم بتحميل أية ملفات من الغرباء.
- ✓ توخي الحذر عند تحميل الملفات من الانترنت، تحقق من شرعية المصدر وحسن سمعته.

الهدف من إعداد البرامج الخبيثة

- تختلف دوافع إعداد الفيروسات:
  - الدوافع الحسنة،
  - الدوافع المادية،
  - الدوافع الانتقامية.
- بعض الناس يقوم بإعداد الفيروسات للتسلية أو ولإظهار القدرة على البرمجة،
- البعض يعدها بهدف مادي وذلك لضمان تردد المستخدم لمحلات الكمبيوتر للصيانة او التخلص من هذا الفيروس او السطو على حسابات البنوك او المعومات العامة للشركات والمؤسسات الكبرى.
- مهما كان هدف إعداد الفيروس لابد من الوقاية منه لأنه يسبب الكثير من المشاكل والخسائر لمستخدمي الكمبيوتر .

نهاية المحاضرة الثانية عشر