



# امنية تكنولوجيا المعلومات

## المحاضرة : 1

عنوان المحاضرة : امن الحاسوب و المعلومات

اعداد : أ. سالمة علي القجامية



# محتوى المحاضرة

- المقدمة
- طرق وأدوات حماية امن المعلومات
- المصطلحات الأمنية المستخدمة لامن المعلومات
- سياسات المعلومات
- سياسات الاستخدام
- المخاطر و الاعتداءات في بيئة المعلومات
- العمليات الرئيسية المتصلة بأمن المعلومات





# أمن الحاسوب والمعلومات

## Computer and Information Security


أمن الحاسوب هو فرع من فروع التكنولوجيا المعروفة باسم أمن المعلومات، كما هي مطبقة على الحاسوب والشبكات. والهدف من أمن الحاسوب يتضمن حماية المعلومات والممتلكات من السرقة والفساد، أو الكوارث الطبيعية، بينما يسمح للمعلومات والممتلكات أن تبقى منتجة وفي متناول مستخدميها المستهدفين.

مصطلحات أمن نظام الحاسوب، تعني العمليات والآليات الجماعية التي من خلالها تحمي المعلومات والخدمات الحساسة من النشر، والعبث بها أو الانهيار الذي تسببه الأنشطة غير المأذون بها أو الأفراد غير الجديرين بالثقة، والأحداث غير المخطط لها على التوالي.



ما هو أمن المعلومات؟ يعني إبقاء معلوماتك تحت سيطرتك المباشرة والكاملة، أي بمعنى عدم إمكانية الوصول لها من قبل أي شخص آخر دون إذن منك، وان تكون على علم بالمخاطر المترتبة عن السماح لشخص ما بالوصول إلى معلوماتك الخاصة. أنت بالتأكيد لا ترغب أن يكون للآخرين مدخل لمعلوماتك الخاصة ومن الواضح أن معظم الأشخاص يرغبون في الحفاظ على خصوصية معلوماتهم الحساسة مثل كلمات المرور ومعلومات البطاقة الائتمانية وعدم تمكن الآخرين من الوصول إليها، والكثير من الأشخاص لا يدركون بأن بعض المعلومات التي قد تبدو تافهة أو لا معنى لها بالنسبة لهم فإنها قد تعني الكثير لناس آخرين وخصوصا إذا ما تم تجميعها مع أجزاء أخرى من المعلومات فعلى سبيل المثال لا يمكن للشركة الراغبة في الحصول على معلومات شخصية عنك للاغراض التسويقية أن تشتري هذه المعلومات من شخص يقوم بتجميعها من خلال الوصول إلى جهاز كمبيوترك بشكل غير شرعي.





**أمن المعلومات** ، **من زاوية أكاديمية** : هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها .

**ومن زاوية تقنية** : هو الوسائل والادوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية .

**ومن زاوية قانونية** : فان أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها او استغلال نظمها في ارتكاب الجريمة ، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها ( جرائم الكمبيوتر والإنترنت ) .

ان اغراض ابحاث واستراتيجيات ووسائل أمن المعلومات سواء من الناحية التقنية او الادارية , وكذلك هدف التدابير التشريعية في هذا الحقل ، ضمان توفر **العناصر** التالية لأية **معلومات** يراد توفير الحماية الكافية لها :-



## □ السرية أو الموثوقية CONFIDENTIALITY

وتعني التأكد من ان المعلومات لا تكشف ولا يطلع عليها من قبل اشخاص غير مخولين بذلك .

## □ التكاملية وسلامة المحتوى INTEGRITY

التأكد من ان محتوى المعلومات صحيح ولم يتم تعديله او العبث به وبشكل خاص لن يتم تدمير المحتوى او تغييره او العبث به في اية مرحلة من مراحل المعالجة او التبادل سواء في مرحلة التعامل الداخلي مع المعلومات او عن طريق تدخل غير مشروع

## □ استمرارية توفر المعلومات او الخدمة AVAILABILITY

التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وان مستخدم المعلومات لن يتعرض الى منع استخدامه لها او دخوله اليها .



## ❑ عدم إنكار التصرف المرتبط بالمعلومات ممن قام به

ويقصد به ضمان عدم انكار الشخص الذي قام بتصرف ما متصل بالمعلومات او مواقعها انكار انه هو الذي قام بهذا التصرف ، بحيث تتوفر قدرة اثبات ان تصرفا ما قد تم من شخص ما في وقت معين .

وقد يعتقد البعض أن الحلول التقنية الأمنية وحدها كفيلة بتأمين جانب الحماية للمعلومات، وهذا بالطبع اعتقاد خاطئ. إذ أن حماية المعلومات تركز على ثلاثة عناصر أساسية مكملة لبعضها البعض وهي

العنصر البشري

الحلول التقنية

السياسات الأمنية للمعلومات ، والتي بدورها تحكم وتنظم كيفية تعامل العنصر البشري مع المعلومات بشكل سليم للوصول إلى الهدف المنشود.



## طرق وأدوات حماية امن المعلومات

1. التأمين المادي للأجهزة والمعدات.
2. تركيب مضاد فيروسات قوي وتحديثه بشكل دوري.
3. تركيب أنظمة كشف الاختراق وتحديثها.
4. تركيب أنظمة مراقبة الشبكة للتنبيه عن نقاط الضعف التأمينية.
5. عمل سياسة للنسخ الاحتياطي.
6. استخدام أنظمة قوية لتشفير المعلومات المرسلة.
7. دعم أجهزة عدم انقطاع التيار.
8. نشر التعليم والوعي الامني.





# المصطلحات الأمنية المستخدمة لامن المعلومات

## 1. التحقق من الهوية

التأكد من صحة الهوية الخاصة بأحد المستخدمين أو العمليات أو الأجهزة، و تلزم المصادقة التحقق من امتلاكه صالحة الوصول إلى النظام أو الموارد من خلال إنشاء الثقة اللازمة للتحقق من الهوية و تشمل التحقق من صحة الهوية و التحقق من مصدر الرسالة و محتواها.

## 2. التصريح

إذن يمنح بالوصول إلى النظام أو الموارد ، و هي تمنح بعد تخطي مرحلة المصادقة المخصصة للتحقق من هوية المستخدم للوصول إلى الانظمة المعلوماتية.



### 3. التشفير

عملية تحويل النص الواضح إلى نص مشفر باستعمال خوارزميات وذلك لجعل المعلومات سرية.

### 4. شهادة رقمية

معلومات رقمية مشفرة تستعمل للتحقق من إن طالب المعلومات حقيقي وغير مزور. يستعمل الشخص الذي يريد إرسال معلومات مشفرة هذا التصديق أما الشخص المتلقي للرسالة المشفرة، فانه يستعمل مفتاحا للوصول إلى المعلومات، و تحوي هذه الشهادة على المعلومات التالية:

أ- تحديد هيئة التوثيق التي أصدرت الشهادة.

ب - أسماء المشتركين فيها.

ج - المفتاح العام الخاص بالمشارك.





## 5. التوقيع الرقمي

إصدار رقمي للتوقيع، يستعمل لمصادقة ومطابقة مرسل المعلومات . هدفه منع التزوير باستخدام الشهادات الرقمية و توقيع البيانات رقمياً .

## 6. الرسائل الغير مرغوب فيها

تكاثر إرسال رسائل لا قيمة لها وغير مرغوب فيها بشكل هائل تحتوي على محتويات تجارية أو مرفوضة يتم إرسالها دون موافقة مسبقة عبر وسائل الاتصالات المختلفة، بما في ذلك، خدمات البريد الالكتروني، ورسائل الجوال، والفاكس، والبلوتوث، والرسائل الفورية. و أغراضها إما إعلانية أو الحجب / منع الوصول بشكل مؤقت.

## 7. برامج التجسس :

جمع المعلومات عن المستخدمين بدون علمهم أو موافقتهم مثل معلومات الدخول أو كلمات السر، الخ. و يعتبر أحد انواع الاكواد الخبيثة.



## 8. الانتحال

تزيف هوية مستخدم ما للحصول على ميزة الوصول الخاصة به بهدف الدخول إلى النظام بامتيازات المستخدم الاساس، و لها القدرة على:

- أ- استقبال رسالة من خلال التكر كما لو كان هو مقر الوصول الشرعي للتسليم.
- ب- التكر كما لو كان الجهاز يرسل رسالة إلى أحد جهات الاستلام

## 9. الاصطياد الالكتروني

انتحال شخصية أو مؤسسة موثوقة للحصول على معلومات حساسة ذات قيمة لغرض سرقة الهوية من خلال وسائل خداع تعتمد على الحاسوب.

## 10. البرامج الخبيثة

برنامج يتم إدخاله إلى أحد الانظمة - عادة ما يتم ذلك خفية - الانتهاك نواحي السرية و التكاملية و الاتاحة الخاصة ببيانات الضحية أو تطبيقاته أو نظام التشغيل الخاص به أو مضايقة الضحية أو إحداث خلل لديه.



# السياسات الأمنية للمعلومات Information Security Policy

سياسات المعلومات (Information Policies) هي مجموعة من القواعد والإرشادات التي تحدد كيفية إدارة واستخدام المعلومات في مؤسسة معينة. تهدف هذه السياسات إلى حماية المعلومات الحساسة، وضمان سلامتها وسريتها، وتحديد الوصول إليها واستخدامها بشكل ملائم وفقًا لأهداف المؤسسة والتشريعات القانونية ذات الصلة. من بين العناصر الرئيسية لسياسات المعلومات:

- **سياسات الوصول والاستخدام:** تحدد من يمكنه الوصول إلى المعلومات وكيفية استخدامها، وتنظم الصلاحيات والتصاريح المطلوبة للوصول إلى المعلومات الحساسة.
- **سياسات الحفظ والتخزين:** تحدد كيفية تخزين المعلومات وحفظها، بما في ذلك استخدام التشفير وإجراءات النسخ الاحتياطي والاحتفاظ بالسجلات.

سياسات الحماية والأمان: توضح الإجراءات والتقنيات اللازمة لحماية المعلومات من التهديدات الداخلية والخارجية، مثل الاختراقات الإلكترونية والفيروسات وسرقة البيانات.

سياسات المشاركة والتبادل: تحدد كيفية مشاركة المعلومات داخل المؤسسة ومع أطراف خارجية، وتنظم الاتفاقيات والعقود الخاصة بالمشاركة والتبادل.

سياسات الاستبعاد والتدمير: توضح كيفية التخلص من المعلومات التي لم تعد مطلوبة أو غير صالحة، بما في ذلك إجراءات التدمير الآمنة لمنع الوصول غير المصرح به.

سياسات التدريب والتوعية: تحدد كيفية توعية الموظفين بأهمية حماية المعلومات والالتزام بسياسات المعلومات، وتوفير التدريب اللازم لذلك. ومنظم.



❑ الثقة بجميع البرامج الملتزمة بسياسة الأمن ولكن يكون البرنامج ليس جديرا بالثقة (وهذا هو انعدام أمن الحاسوب).

❑ الثقة بجميع البرامج الملتزمة بسياسة الأمن والبرمجيات صدّق على أنها جديرة بالثقة.

❑ عدم الثقة بأي برمجيات ولكن فرض سياسة أمنية مع آليات ليست جديرة بالثقة (مرة أخرى هذا هو انعدام أمن الحاسوب).

❑ عدم الثقة بأي برمجيات ولكن فرض سياسة أمنية مع آليات جديرة بالثقة.

هناك استراتيجيات وتقنيات مختلفة مستخدمة في تصميم أنظمة الأمن. ومع ذلك فهناك عدد قليل، إن وجد، من الاستراتيجيات الفعالة لتعزيز الأمن بعد التصميم. أحد الأساليب يفرض مبدأ الامتيازات الأقل إلى الحد الأعلى، حيث يمتلك الكيان الامتيازات المحتاجة لوظيفته فقط. وبهذه الطريقة حتى لو استطاع المهاجم الوصول إلى جزء من النظام، فالأمن الجيد يضمن انه من الصعب عليهم الوصول إلى باقي الأجزاء.



# سياسات المعلومات Information Policies

تلك السياسات التي تشير إلى الجوانب المختلفة لأمن المعلومات , وهي تتضمن سياسات ( الوصول إلى , التصنيف , التأشير عليها , التخزين , الإرسال , تدمير ) المعلومات الحساسة . إن تطوير الـ Information Policies هو عملية هامة جداً ودرجة لعنصر الأمان . حيث أن البيانات لها مستويات مختلفة في عملية التصنيف . وهي غالباً ما تشبه التصنيف التالي :

❑ عام ( Public ) ... وهي المعلومات التي تكون متاحة للجمهور المتعاملين . مثل

المعلومات المنشورة على الـ Web





- ☐ داخلي ... المعلومات الموجودة على الشبكة الداخلية للشركة .
- ☐ خاصة ... السجلات الشخصية , بيانات العملاء , وهكذا
- ☐ سرية ... مثل معلومات الـ Public Key Infrastructure PKI , أى معلومات أخرى تكون مقصورة على أشخاص معينين يجب أن يعرفوها .



# سياسات الاستخدام Usage Policies

تقوم سياسات الاستعمال بتغطية " كيفية استخدام (المعلومات , المصادر). و ستحتاج إلى أن تشرح للمستخدمين (كيفية استخدام هذه المصادر , لأي غرض يتم استخدامها) . فهذه السياسات تفرض قانون حول استخدام أجهزة الكمبيوتر .

- ❖ وهي تتضمن تعبيرات بخصوص (السرية , الملكية , نتائج الأفعال الغير صحيحة)
- ❖ يجب لتلك السياسات أن تحدد وبشكل واضح توقعات الاستعمال بخصوص ( الإنترنت , الوصول عن بعد , البريد الإلكتروني) فمثلاً تشير إلى أن استخدام الإنترنت لأغراض العمل وليست لأغراض شخصية .





- ❖ تخاطب تلك السياسات المستخدمين وتعرفهم ( كيفية معالجة الحوادث من يتصلون إذا وقعت شيء مشبوه).
- ❖ يجب أن توضح تلك السياسة للمستخدمين بأن هناك مراقبة ويجب موافقتهم عليها.
- ❖ يجب أن تذكر نتائج سوء الاستعمال بشكل حاد وقاطع.



# المخاطر والاعتداءات في بيئة المعلومات

## □ الأجهزة Devices

وهي كافة المعدات والادوات المادية التي يتكون منها النظم ، كالشاشات والطابعات ومكوناتها الداخلية ووسائل التخزين المادية وغيرها

## □ البرامج Software

وهي الاوامر المرتبة في نسق معين لانجاز الاعمال ، وهي اما مستقلة عن النظام او مخزنة فيه .



## □ المعطيات Requirements

انها الدم الحي للأنظمة ، وما سيكون محلا لجرائم الكمبيوتر ، وتشمل كافة البيانات المدخلة والمعلومات المستخرجة عقب معالجتها ، وتمتد بمعناها الواسع للبرمجيات المخزنة داخل النظم والمعطيات قد تكون في طور الادخال او الاخراج او التخزين او التبادل بين النظم عبر الشبكات ، وقد تخزن داخل النظم او على وسائط التخزين خارجه

## □ الاتصالات Communication

وتشمل شبكات الاتصال التي تربط اجهزة التقنية بعضها بعض محليا ونطاقيا ودوليا ، وتتيح فرصة اختراق النظم عبرها كما انها بذاتها محل للاعتداء وموطن من مواطن الخطر الحقيقي. ومحور الخطر الانسان ، سواء المستخدم او الشخص المناط به مهام تقنية معينة تتصل بالنظام ، فادراك هذا الشخص حدود صلاحياته ، وادراكه اليات التعامل مع الخطر ، وسلامة الرقابة على انشطته في حدود احترام حقوقه القانونية ، مسائل رئيسة يعنى بها نظام الأمن الشامل ، تحديدا في بيئة العمل المرتكزة على نظم الكمبيوتر وقواعد البيانات



# العمليات الرئيسة المتصلة بأمن المعلومات

تتعدد عمليات التعامل مع المعلومات في بيئة النظم وتقنيات المعالجة والاتصال وتبادل البيانات ، ولكن يمكن بوجه عام تحديد العمليات الرئيسة التالية :-

## ➤ تصنيف المعلومات Information classification

وهي عملية اساسية لدى بناء أي نظام او في بيئة أي نشاط يتعلق بالمعلومات وتختلف التصنيفات حسب المنشأة مدار البحث ، فمثلا قد تصنف المعلومات الى معلومات متاحة ، وموثوقة ، وسرية ، وسرية للغاية او قد تكون معلومات متاح الوصول اليها واخرى محظور التوصل اليها وهكذا.



## التوثيق Documentation ➤

وتتطلب عمليات تأمين المعلومات اساسا اتباع نظام توثيق خطي لتوثيق بناء النظام وكافة وسائل المعالجة والتبادل ومكوناتها . وبشكل رئيس فان التوثيق لازم وضروري لنظام التعريف والتحويل ، وتصنيف المعلومات ، والانظمة التطبيقية . وفي اطار الأمن ، فان التوثيق يتطلب ان تكون استراتيجية او سياسة الأمن موثقة ومكتوبة وان تكون إجراءاتها ومكوناتها كاملة محل توثيق ، اضافة الى **خطط التعامل مع المخاطر والحوادث** ، والجهات المسؤولة ومسؤولياتها وخطط التعافي وادارة الازمات وخطط الطوارئ المرتبطة بالنظام عند حدوث الخطر.

## ➤ سجل الأداء

تحتوى مختلف أنواع الكمبيوترات نوعا ما من السجلات التي تكشف استخدامات الجهاز وبرمجياته والنفاز اليه ، وهي ما يعرف بسجلات الأداء او سجلات النفاز الى النظام ، تتخذ سجلات الأداء اهمية استثنائية في حال تعدد المستخدمين وتحديدا في حالة شبكات الكمبيوتر التي يستخدم مكوناتها اكثر من شخص ، وفي هذه الحالة تحديدا ، أي شبكات المستخدمين ، فان هناك اكثر من نوع من أنواع سجلات الأداء وتوثيق الاستخدامات ، كما ان سجلات الأداء تتباين من حيث نوعها وطبيعتها وغرضها ، فهناك سجلات الأداء التاريخية والسجلات المؤقتة ، وسجلات التبادل وسجلات النظام وسجلات الأمن وسجلات قواعد البيانات والتطبيقات وسجلات الصيانة او ما يعرف بسجلات الأمور التقنية وغيرها . وبشكل عام فان سجلات الأداء منوط بها ان تحدد المستخدم ووقت الاستخدام ، ومكانه ، وطبيعة الاستخدام ( محتواه ) واية معلومات إضافية أخرى تبعا للنشاط ذاته.





## ➤ عمليات الحفظ Back-up

عمليات الحفظ تتعلق بعمل نسخة إضافية من المواد المخزنة على إحدى وسائط التخزين سواء داخل النظام أو خارجه ، وتخضع عمليات الحفظ لقواعد يتعين ان تكون محددة سلفا وموثقة ومكتوبة ويجري الالتزام بها لضمان توحيد معايير الحفظ وحماية النسخ الاحتياطية

## ➤ وسائل التعريف والتوثيق من المستخدمين وحدود صلاحيات الاستخدام

ان الدخول الى أنظمة الكمبيوتر وقواعد البيانات ومواقع المعلوماتية عموما ، يمكن تقييده بالعديد من وسائل التعرف على شخصية المستخدم وتحديد نطاق الاستخدام ، وهو ما يعرف بأنظمة التعريف والتحويل . والتعريف او الهوية مسألة تتكون من خطوتين ، الأولى وسيلة التعريف على شخص المستخدم ، والثانية قبول وسيلة التعريف او ما يسمى التوثق من صحة الهوية المقدمة .



ووسائل التعريف تختلف تبعا للتقنية المستخدمة ، وهي نفسها وسائل أمن الوصول الى المعلومات او الخدمات في قطاعات استخدام النظم او الشبكات أو قطاعات الاعمال الإلكترونية ، وبشكل عام ، فان هذه الوسائل تتوزع الى ثلاثة أنواع :-

- 1) شئ ما يملكه الشخص مثل البطاقة البلاستيكية او غير ذلك
- 2) شئ ما يعرفه الشخص مثل كلمات السر او الرمز او الرقم الشخصي غير ذلك
- 3) شئ ما يرتبط بذات الشخص او موجود فيه مثل بصمة الاصبع او بصمة العين والصوت وغيرها .

وتعد وسائل التعريف والتوثق الاقوى ، تلك الوسائل التي تجمع بين هذه الوسائل جميعا على نحو لا يؤثر على سهولة التعريف وفعاليتها في ذات الوقت .  
وايا كانت وسيلة التعريف التي سيتبعها توثق من قبل النظام ، فانها بذاتها وبما ستصل باستخدامها تخضع لنظام أمن وارشادات امنية يتعين مراعاتها