كل شخص تقريبا يشترك في "القيم والخواص الأساسية"

- الحياه
- السعاده
- الاهداف علي تحقيق الاهداف

طريقتان لرؤيه العالم

١-وجهة نظر الأنانية: النظر في الذات فقط وقيمها الأساسية

٢-وجهة نظر أخلاقية: احترام الآخرين وقيمهم الأساسية

المجتمع: رابطة الناس المنظمة بموجب نظام من القواعد

القواعد: تهدف إلى النهوض بخير الأعضاء مع مرور الوقت

قواعد سلوك المجتمع

ما يجب على الناس

لا ينبغي القيام به في حالات مختلفة (شبكة الطرق - جيدة أو سيئة)

الأخلاق (دراسة فلسفية للأخلاق التوجيهية)

١-الفحص العقلاني للأخلاق:

٢- تقييم سلوك الناس.

٣- فالأخلاقيات أوسع من الأخلاق من حيث أنها تشمل الانشطة العليا التي تقيم النظم الأخلاقية وإيجاد طرق جديدة لتقييم المشاكل

النظرية الأخلاقية العملية: تنتج تفسيرات قد تكون مقنعة لجمهور متشكك، ولكن منفت

النسبية: لا توجد معايير عالمية للحق والخطأ

يمكن لشخص واحد أن يقول " Xهو الحق"، وآخر يمكن القول " Xخطأ"، وكلاهما يمكن أن يكون على حق

النسبية الذاتية: كل شخص يقرر الحق والخطأ لنفسه أو نفسها

هناك أربعة مفاهيم أساسية تؤثر في الجوانب الأخلاقية :

* ***امكانية التعرض للمسائلة:***

قبول الالتزامات المحتملة للقرار الذي يتخذه الانسان في حياته الخاصة والمهنية.

* ***المسؤولية والمحاسبة:***

تقييم مستوى الفرد ومحاسبته عن القرار

* ***المسؤولية القانونية:***

تسمح للأفراد بالحصول على تعويض عن الضرر الناتج عن قرار فرد ما

* ***اجراءات مطلوبة أو مستحقة:***

القدرة على الاستئناف لدى السلطات الأعلى

قضايا في نظم المعلومات

: هناك خمسة أبعاد أخلاقية مهمة:

أولا: حقوق المعلومات

أي الحقوق التي يمتلكها الأفراد والمنظمات بما له علاقة بالمعلومات التي تخص أفرادا آخرين.

ثانيا: حقوق الملكية

حماية الملكية الفردية التقليدية في ظل المجتمع الرقمي

ثالثا: المسؤولية والسيطرة

محاسبة ما يقع من تجاوز وأذى الأفراد بمعلوماتهم أو حقوقهم

رابعا: نوعية وجودة النظم

وهي النظم التي ينبغي أن تؤمن لحماية أمن المجتمع

خامسا: نوعية وجودة الحياة

القيم الثقافية والممارسات الواجب حمايتها من التجاوزات في المجتمع

اتجاهات التكنولوجيا وتأثيرها على الموضوعات الأخلاقية

الاتجاه	التأثير
القدرات الحاسوبية تتضاعف كل «18» شهر	اعتماد أكثر من قبل المنظمات على النظم الحاسوبية في عملياتها المهمة والحساسة
انخفاض متواصل وسريع في تكاليف تخزين البيانات	تمكين المنظمات من الاحتفاظ بقواعد بيانات تفصيلية عن الأفراد
تقدم وتطور في مناجم وتحليل البيانات	تمكين المنظمات من تحليل كميات هائلة من بيانات الأفراد وتطوير معلومات أوضح عن سلوكهم
تقدم وميزات في الشبكات والإنترنت	تمكين المنظمات من نسخ بيانات من موقع الى آخر والوصول الى بيانات من مواقع بعيدة بسهولة

المبادئ الأخلاقية في صناعة القرارات

اولا: افعل للآخرين كما تريد أن يفعلوا لك، وذلك لتحقيق شيء من العدالة في صناعة القرار.

ثانيا: إذا كان فعل فرد ما غير صحيح، فهو غير صحيح للأفراد الآخرين في المنظمة.

ثالثا: إذا كان هناك فعل لا يجوز تكراره، إذن لا ينبغي أن تعمله من الأساس.

رابعا: اتخذ خطوات عملية لغرض انجاز المهام، وذلك بوضع قيم لسلم الأولويات من الأعمال.

خامسا: قم بالعمل الذي ينتج عنه أقل الأضرار أو ما تكون كلفته ممكنة.

سادسا: افترض ان كل الأشياء هي مملوكة لشخص آخر ما لم يكن هناك إعلان محدد بخلاف ذلك .

تحديات الانترنت لحماية الحرية الفردية والخصوصية

١ـ المعلومات المرسلة عبر الانترنت تمر من خلال الأنظمة الحاسوبية، و كل منها قادرا على مراقبة وتسجيل هذه المعلومات من دون معرفة الزوار
٢ـ هناك أدوات يمكن استخدامها لمراقبة شبكة الويب لتحديد من قاموا بزيارة الموقع أو مراقبة العاملين بها، لذا فإن الطلب التجاري لمثل هذه المعلومات الشخصية يكون افتراضيا بلا حدود
٣ـ هناك تحديات أخرى مثل الكوكيز بالقرص الثابت
والرصد على الويب المستخدم للمراقبة ونموذج الموافقة وعدم الموافقة .

تأثيرات نظم المعلومات على الحياة اليومية

نظم المعلومات مصدر للإزدهار والثراء، ولكن لها تأثيرات سلبية مثل:

١-الأخطاء في نظم المعلومات العملاقة تجعل من المستحيل استئصالها بالإضافة الى الأخطاء الصغيرة التي تسبب ارباكا في عمل المنظمة.
٢- هناك وظائف يمكن أن تفقد عندما يستعاض عن العاملين بالحواسيب
٣- القدرة على امتلاك الحواسيب ربما يزيد من التفاوت الاجتماعي والاقتصادي
٤- الانتشار الواسع في استخدام الحواسيب يزيد من الجرائم الحاسوبية واساءة الاستخدام
٥- ممكن أن يسبب مشاكل صحية متنوعة كالإجهاد ومشاكل النظر

قواعد السلوك المهني والخصوصية والممارسة المشروعة للمعلومات

قواعد السلوك المهني:

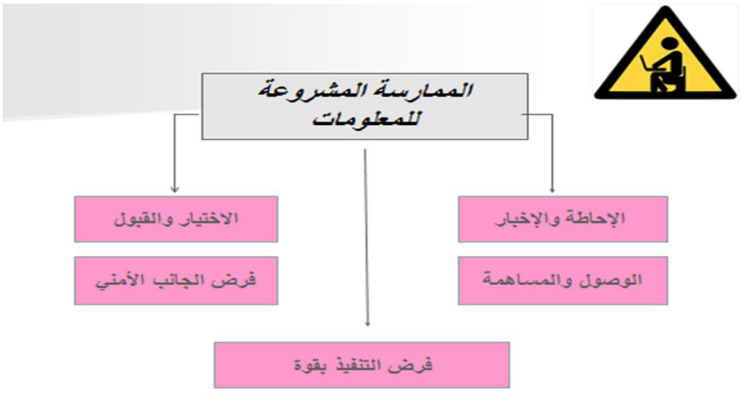
فرضت هذه القواعد بغرض تنظيم دخول المهني الى عالم الكفاءة والمنافسات وتأمين نوع من القواعد الأخلاقية .

الخصوصية وسرية المعلومات:

تعني أن يكون للأفراد الحق بأن يكونوا أحرار من المراقبة من قبل أفراد آخرين أو منظمات.

الممارسة المشروعة للمعلومات:

عبارة عن مجموعة من المبادئ تحكم تجميع واستخدام المعلومات عن الأفراد.



حقوق الملكية الفردية والانترنت

هي حقوق التأليف والنشر الإلكتروني وهي من أهم أشكال الحماية وهذه الحقوق تعطي الحق للناشرين ببيع وتوزيع نسخ من المنتج , اعادة انتاجه, اعداد اعمال مقتبسة منه وهكذا.

ولهذا ان الملكية الفكرية هي موضوع للحماية تحت ثلاث مسميات :

سر التجارة	حقوق التأليف	براءة الاختراع
مفهوم يمثل أي منتج لعمل فكري كالوصفات والمعدات والنماذج أو البيانات المجمعة والمؤلفة	منحة شرعية تعمل على حماية المبدعين من أن ينسخ عملهم بواسطة الآخرين	يمنح مالك براءة الاختراع حق احتكار الأفكار خلف الاختراع لمدة عشرين سنة

الجرائم وإساءة الاستخدام وأمن المعلومات على الانترنت

فيض الرسائل

ارسال أصحاب الأسواق كميات غير مطلوبة لجمهور المستلمين وهذا يسبب المضايقة للعديد منهم

القرصنة

هو الدخول الى البيانات الخاصة عن الزبائن وكلمات المرور.

الشغب

استخدام برامج روتينية لربط المواقع بغرض عدم السماح للزائرين بالوصول اليه

البرنامج الخبيث

استخدام بيانات لنقل الفيروسات يمكن ان تعطل الحاسوب الذي تمت اصابته

التلصص

استراق واختلاس السمع واعتراض المعلومات التي قد تشتمل على أرقام بطاقات ائتمان وغيرها

الخداع

تقديم النفس بشكل غير صحيح بوضع مواقع وهمية لجمع معلومات سرية عن الزوا

الفيروسات: أخطارها وأنواعها

ما هو الفيروس؟؟؟

كلمة فيروس أطلقت مجازا على برنامج حاسوبي يقوم بأعمال تخريبية في برامج الحاسوب والمعلومات المخزنة فيه . كمحتويات القرص الصلب وتغيير نظام تقسيمه، هذا بالإضافة الى تغيير بيانات نظام التشغيل وتخريب الرقائق الخاصة بذلك وبكل التطبيقات.

كيف ينتقل؟؟؟

يمكن أن ينتقل الفيروس عن طريق القرص المرن أو المنتكز أو الصلب أو عن طريق شبكة الانترنت

أنواع الفيروسات

الفيروس	تأثيره
فيروس رئيسي	يؤدي إلى تخريب المعلومات بشكل تدريجي بطيء.
فيروس ثانوي	يسبب تغييرا لواحد أو أكثر من الملفات القابلة للتنفيذ.
فيروس معتدل	يدمر جميع الملفات عن طريق إعادة التهيئة.
فيروس مبتدئ "عادي"	يقوم بالتكاثر ولا يسبب أي تخريبا متعمدا للأقراص.
فيروس غير محدد الضرر	يستهدف شبكات الكومبيوتر لمعرفة كلمة السر للمستخدمين.

حماية الأعمال الالكترونية من الفيروسات

أولا: التشفير:

هو ما يشتمل على استخدام حسابات رياضية أو مفاتيح لتحويل البيانات إلى رموز مجمعة عند إرسالها ومن ثم فك هذه الرموز عند استلامها.. وهذه الوسيلة تسوق وتباع كمنتج مستقل.

ثانيا: رفض أو إعاقة الخدمة:

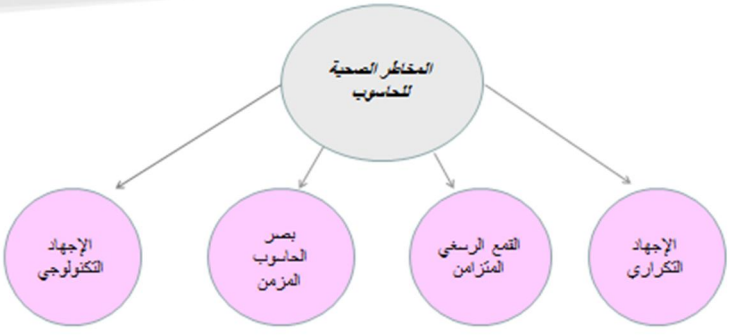
هي عبارة عن خطوات تتبعها المنظمات لغرض حماية نظم معلوماتها من هجمات اعاقة الخدمة من قبل الفيروسات.

ثالثا جدران النار:

هو عبارة عن حارس بوابة يقوم بحماية الانترنت والشبكات الحاسوبية الأخرى من التطفل عن طريق مصفاة أو نقطة نقل آمنة في الوصول من و إلى الانترنت.

المخاطر الصحية من استخدام النظم المحسوبة

ينفق ما يقارب عشرين مليار دولار سنويا لتعويض ومعالجة أمراض ضحايا الوظائف ذات العلاقة بالعمل الحاسوبي !!!



التحديات والحلول للالتزامات الأخلاقية والمتطلبات الاجتماعية لنظم المعلومات

التحديات الإدارية

تفهم المخاطر الأخلاقية للتكنولوجيا الحديثة المتسارعة
وضع سياسات أخلاقية تشمل موضوعات نظم المعلومات

الحلول المقترحة

- **تحديد الأبعاد والمبادئ الرئيسية لمجتمع المعلومات واستخدامها كمؤشرات للقرارات.**
- **تقويم تأثيرات نظم المعلومات والانترنت على حماية الخصوصية والممتلكات الفكرية.**
- **اجراء تقويم لتأثيرات نظم المعلومات على الحياة اليومية.**
- **تحديد التحديات الإدارية الأساسية لنظم المعلومات وتقديم الحلول.**
- **تحليل العلاقات الخاصة بالموضوعات الأخلاقية والاجتماعية والسياسية التي تثيرها نظم المعلومات وتكنولوجياتها.**

حالات دراسية بين الخصوصية والأمنية في نظم المعلومات

لا يزل الجدل محتدم !!!
في وسط محاولات ايجاد التوازن بين السلامة العامة والأمن الوطني من جهة وبين الحرية الفردية أو الخصوصية من جهة أخرى

والأمثلة على ذلك كثيرة في الولايات المتحدة الأمريكية.

**** كاميرات المراقبة :***
في الانفاق والموانئ والحدود والبنوك والمخازن.
*** قواعد البيانات.**
مثل قاعدة بيانات طلبات تأشيرات الدخول وقواعد البيانات الطبية ..
**** الأقمار الصناعية الرقابية:***
كالتي تستخدمها المخابرات الأمريكية CIA لمراقبة الأفراد.
**** صلاحيات المراقبة والتصنت الالكتروني :***
ومن أهمها صلاحيات وكالة التحقيقات الفيدرالية FBI للمراقبة أيضا

تعريفات جرائم الكمبيوتر والانترنت:

الجريمة الإلكترونية هي كل فعل ضار و غيره يأتيه الفرد أو الجماعة عبر استعماله الأجهزة الإلكترونية.

الجريمة الالكترونية عبارة عن نشاط اجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الاجرامي.

الجريمة الإلكترونية لها مسميات عدة منها

1- جرائم الحاسوب والإنترنت
2-جرائم التقنية العالية
3 -الجريمة الإلكترونية
4 -الجريمة السايبرية
5- جرائم أصحاب الياقات البيضاء

أهداف الجرائم الإلكترونية

نستطيع تلخيص بعض أهداف الجرائم الإلكترونية ببضعة نقاط أهمها :

١-التمكن من الوصول الى المعلومات بشكل غير شرعي كسرقة المعلومات او الاطلاع عليها او حذفها او تعديلها بما يحقق هدف المجرم.

٢-التمكن من الوصول عن طريق الشبكة العنكبوتية إلى الأجهزة الخادمة(Servers) المزودة للمعلومات وتعطيلها.

٣-الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالمؤسسات والبنوك والجهات الحكومية والأفراد وابتزازهم بواسطتها

٤- الكسب المادي أو المعنوي أو السياسي غير المشروع عن طريق تقنية المعلومات مثل عمليا ت اختراق وهدم المواقع على الشبكة العنكبوتية وتزوير بطاقات الائتمان وسرقة الحسابات المصرفية

المجرم المعلوماتي

هو شخص يختلف عن المجرم العادي فلا يمكن أن يكون هذا الشخص جاهلا للتقنيات الحديثة المعلوماتية.

هل هناك نموذج محدد للمجرم المعلوماتي ؟؟ لا ولكن

هناك سمات مشتركة بين هؤلاء المجرمين

منها ما يلي:

١. مجرم متخصص: له قدرة فائقة في اختراق الشبكات وكسر كلمات المرور أو الشفرات ويسبح في عالم الشبكات ليحصل على كل غالٍ وثمين من البيانات والمعلومات الموجودة في أجهزة الحواسب ومن خلال الشبكات.
٢. مجرم يعود للإجرام: يعود للجريمة دائمًا فهو يوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به ليحقق جريمة الاختراق بهدف الإيذاء
٣. مجرم محترف: يوظف مهاراته في الاختراق والسرقة والنصب والاعتداء على حقوق الملكية الفكرية وغيرها من الجرائم مقابل المال
٤. مجرم ذكى: يقوم بتعديل وتطوير في الأنظمة الأمنية حتى لا تستطيع أن تلاحقه وتتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب.

الصفات المشتركة بين الكثيرمن المجرمين فيما يلي:

١. عادة ما تتراوح أعمار تلك الفئة من المجرمين ما بين ١٨-٤٥ عامًا.
٢. المهارة والإلمام الكامل والقدرة الفنية الهائلة في مجال نظم المعلومات
٣. الثقة الزائدة بالنفس والإحساس بإمكانية ارتكابهم لجرائمهم دون افتضاح أمرهم.

إلمامه التام بمسرح الجريمة وبأدواته ، وبما يجنبه فجائية المواقف التي قد تؤدي.
إلى إفشال مخططه وافتضاح أمره

تتعدد أنماط الجناة في الجريمة المعلوماتية ، فهناك:

١. الهاكارز " Hackers " أو المتسللون وهم عادةً مجرمون محترفون يستغلون خبراتهم وإمكانياتهم في مجال تقنية المعلومات للتسلل إلى مواقع معينة للحصول على معلومات سرية أو تخريب وإتلاف نظام معين وإلحاق الخسائر به بقصد الانتقام أو الابتزاز.
٢. وهناك الكراكرز" " Crackers " المخترقون" سواء كان من الهواة أو المحترفين وعادةً ما يستخدم مجرمو هذا النمط قدراتهم الفنية في اختراق الأنظمة والأجهزة تحقيقاً لأهداف غير شرعية كالحصول على معلومات سرية أو للقيام بأعمال تخريبية. إلخ

حتى يتمكن القراصنة (Hackers) من تنفيذ جريمتهم الإلكترونية يستلزم ذلك توفر أدوات، ومن أبرزها: ((أدوات الجرائم الالكترونيه))

1- الاتصال بشبكة الإنترنت وتعتبر أداة رئيسية لتنفيذ الجريمة.

2- توفر برمجيات خاصة لنسخ المعلومات المخزنة عند المستخدم على جهاز الحاسوب.

3- وسائل التجسس ومنها ربط الكاميرات بخطوط الاتصال الهاتفي.

4- البار كود وهي عبارة عن أدوات تستخدم لمسح الترميز الرقمي وفك شيفرة الرموز.

5- طابعات.(Printers) - هواتف رقمية ونقالة.

6- برامج ضارة ومنها Trojan horse إذ تتمثل وظيفته بخداع الضحية وتشجيعه على تشغيله فيلحق الضرر الشامل بالحاسوب والملفات الموجودة عليه.

هناك عدد من الأسباب التي يمكن حصرها كأسباب للجريمة الإلكترونية ، منها ما يقع على المستوى الفردي أو على المستوى الكوني، ومنها ما يقع على مستوى مجتمعي، ومنها ما يقع على مستوى شخصي.

أ) أسباب الجريمة على المستوى الفردي:

البحث عن التقدير هناك بعض الجرائم الإلكترونية التي يرتكبها شباب طائش وصغار سن، وذلك من باب التحدي، وحب الظهور في الإعلام.

- الفرصة :(Opportunity) ان تكنولوجيا المعلومات والاتصالات والاستخدام المتزايد للأنترنت قد خلق فرص جديدة للمجرمين نمو الجريمة . ان جرائم الإنترنت تمثل شكلا جديدا ومميزا ضبط الذات المنخفض: إن السلوك الطائش يُعدّ مظهرا من مظاهر الضبط الذاتي المنخفض. لسلوك الطائش يُعدّ عملاً سهلاً وقد يحقق المصالح الخاصة بسرعة مثل (الرشوة، السرقة) ونحوهما من الأعمال الإجرامية

النشاط الروتيني:

ويمكن تفسير زيادة ضحايا الجريمة الإلكترونية من خلال التغييرات في أنشطة الناس الروتينية في الحياة اليومية فمع ظهور شبكة الإنترنت فقد تغيرت طريقة الناس التي يتواصلون فيها أو يتفاعلون مع الآخرين في العلاقات الشخصية والترفيه والتجارة الخ.
ان التغييرات في أنشطة الناس الروتينية مثل استخدام النت وشبكات التفاعل الاجتماعي مثل الفيس بوك و الإيميل والمواقع وغيرها قد خلقت فرصاً للجناة المتحفزين مع وجود أهداف قيمة وسهلة في الحيز الفضائي مع غياب الحراسة.
يري كوهين وفيلسون أنه من المرجح أن تحدث الجريمة عندما تتلاقي ثلاثة عوامل هي: الجاني المتحفز والهدف المناسب وغياب الحراسة

أسباب الجريمة على المستوى المجتمعي:

التحضر *(Urbanization)*

١- عادة يهاجر الشباب غير المتمكنين من الريف إلى المدن وهناك لا يستطيعون مواجهة متطلبات الحياة الحضرية باهضه التكاليف، والتي تتطلب مهارات عالية أحيانا، مما يجعل شرائح كبيرة من المهاجرين غير قادرين على تلبية متطلبات الحياة الحضرية مما يجعلهم يعيشون في مدن الصفيح والأحياء الطرفية والهامشية وكنتيجة يجد الناس انفسهم في تنافس غير قادرين على مجاراته مما يجعلهم يلتفتون إلى الاستثمار في الجريمة الإلكترونية حيث لا تتطلب رأس مال كبير والتي تعرف "أولا الياهو"
٢- وكما يرى ميك فان التحضر سبب رئيسي للجرائم الإلكترونية في نيجيريا وان التحضر بدون الجريمة مستحيل وكنتيجة فان الصفوة بينهم قد وجدوا إن الاستثمار في الجريمة الالكترونية مربحة.

٣- البطالة (Unemployment)
٤- الضغوط العامة (Strains)
٥- البحث عن الثراء (Quest for Wealth
٦- ضعف إنفاذ القانون وتطبيقه في الجريمة الإلكترونية (lack of law enforcement and implementation)

أسباب الجريمة عل المستوى الكوني:

١ - التحول للمجتمع الرقمي:
إن من أهم سمات عصر المعلومات السمات الثلاثة الرئيسة:
١. تغيرات كمية في **مقدار المعلومات المتدفقة** ونوعها،
٢. **إرسال المعلومات إلى العديد من الأطراف** (البشر والمعدات) فالمعلومات توجه الصاروخ والصحفي يرسل التقرير والبث المباشر من مكان الحدث.
٣. **وجود الشبكات حيث يتم تداول المعلومات بين جميع الأطراف مثل البريد الإلكتروني الجوال الخ.**
٤. **لعولمة**
٥. **لترابط الكوني**

أسباب الجريمة عل المستوى الكوني: **تكملة**

٣ - قطاع الطاقة*(Energy)*
وتشمل الصناعات التي تنتج الطاقة وتوزع الطاقة الكهربائية والبترول والغاز الطبيعي.

4-قطاع المال والبنوك*(Banking and Finance)*
وتشمل البنوك، وشركات الخدمات المالية من غير البنوك ونظم الرواتب وشركات الاستثمار والقروض المتبادلة والتبادلات الأمنية والمادية.

5 - قطاع الخدمات الإنسانية الحيوية(Vital Human Services)
وتشمل نظم التزويد بالمياه، وخدمات الطوارئ والخدمات الحكومية (البطالة والضمان الاجتماعي وتعويض الإعاقات و إدارة سجلات المواليد الخ.)·

و- أسباب تتعلق بخصائص الجريمة الإلكترونية نفسها:

- **فيما يلي مجموعة من خصائص الجرائم والتي تؤدي إلى ارتكاب الجريمة الإلكترونية منها:**

1- الازالة *(Removable)* الجريمة الإلكترونية لا تتطلب الإزالة فيمكن نسخها فقط·

- **2 - التوافر *(Available)* المعلومات في كل مكان جاهزة**

3- القيمة *(Valuable)* معلومات بطاقات الائتمان والحسابات المصرفية والتصاميم قيمة·

4- المتعة *(Enjoyable)* كثير من الجرائم الإلكترونية ممتعة من مثل سرقة الموسيقى والمال

٥-الديمومة *(Durable)* المعدات والبرامج المسروقة يمكن أن تستخدم لفترة طويلة·

6 -سرعة التنفيذ لا يتطلب تنفيذ الجريمة الإلكترونية الوقت الكثير وبضغطة واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخر وهذا لا يعنى أنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينه

و- أسباب تتعلق بخصائص الجريمة الإلكترونية نفسها: تكملة

7- التنفيذ عن بعد لا تتطلب الجريمة الإلكترونية في أغلبها (إلا جرائم سرقة معدات الحاسب) وجود الفاعل في مكان الجريمة بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن مكان الجريمة سواء كان من خلال الدخول للشبكة المعنية أو اعتراض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب الخ·

٨ - **إخفاء الجريمة** إن الجرائم التي تقع على الحاسبات الآلية أو بواسطتها (كجرائم الإنترنت) تعد جرائم مخيفة.

١٠ - عابرة للحدود الدولية(Transnational)

١١ - جرائم ناعمة.

١٢ - صعوبة إثباتها والذي يرجع إلى افتقاد وجود الآثار التقليدية للجريمة وغياب الدليل الفيزيقي (بصمات، تخريب، شواهد مادية) وسهولة محو الدليل أو تدميره في زمن متناهي القصر، يضاف إلى ذلك نقص خبرة الشرطة والنظام العدلي وعدم كفاية القوانين القائمة

خصائص الجرائم الإلكترونية

1-تتّسم بسهولة الوقوع في فخها، حيث إنّ غياب الرقابة الأمنية تساهم في انتشارها وتسهيل ذلك·

2-الضرر الناجم من الجرائم الإلكترونية غير قابل للقياس إذ إنّها تحلق أضراراً جسيمة·

3-صعوبة الكشف عن مرتكب الجريمة إلا بأساليب أمنية وتقنية عالية.

4-سلوك خارج عن المألوف وغير أخلاقي مجتمعيّاً.

5-ذات عنف وجهد أقل من الجرائم التقليديّة.

6-جريمة غير مقيّدة بزمان ومكان إذ تمتاز بالتباعد الجغرافيّ وعدم تقيدها بالتوقيت الزمنيّ.

7 -سهولة إخفاء آثار الجريمة والأدلة التي تدلّ على الجاني نظراً للترميز والتشفير الذي يحدث على الرموز المخزّنة على وسائط التخزين الممغنطة.

أهم طرق الجريمة الإلكترونية

١. **تخريب** المعلومات و إساءه استخدامها ويشمل ذلك قواعد معلومات المكتبات.
٢. **رقة المعلومات** ويشمل **بيع المعلومات** كالبحوث أو الد راسات الهامة أو ذات العلاقة بالتطوير التقني أو الصناعي أو العسكري أو تخريبها أو تدميرها. الخ
٣. **تزوير** المعلومات ويشمل الدخول لقواعد في النظام التعليمي وتغيير المعلومات وتحريفها، مثل تغيير علامات الطلاب.
٤. **تزييف** المعلومات وتشمل تغيير في المعلومات على وضع غير حقيقي مثل وضع سجلات شهادات لم تصدر عن النظام التعليمي وإصدارها
٥. **انتهاك** الخصوصية ويشمل نشر معلومات ذات طبيعة خاصة عن الأفراد، أو الدخول لحسابات الأفراد الإلكترونية ونشر معلومات عنهم أو وضع معلومات تخص تاريخ الأفراد ونشرها.
٦. **التنصت** وتشمل الدخول لقواعد المعلومات وسرقة المحادثات عبر الهاتف.
-7 **التجسس** ويشمل اعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد

٨ -التشهير

٩- **الدخول** غير القانوني للشبكات .
١٠- **قرصنة البرمجيات** ويشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى.
١١- **قرصنة البيانات** والمعلومات
١٢- **القنابل البريدية** وتشمل إرسال فيروسات لتدمير البيانات من خلال رسالة إلكترونية.
١٣- **إفشاء الأسرار** وتشمل الحصول على معلومات خاصة جداً ونشرها على الشبكة.
١٤- **الإحتيال** المالي بالبطاقات.
١٥- **سرقة الأرقام** والمتاجرة بها وخاصة أرقام الهواتف السرية.
١٦- المطاردة والملاحقة **والابتزاز** وتشمل ملاحقة الذكور للإناث أو العكس.
١٧- **الإرهاب** الإلكتروني. يشمل جميع المكونات

أنواع الجريمة الإلكترونية

١. جريمة إلكترونية **تستهدف الأفراد** ويُطلق عليها أيضاً مسمى جرائم الإنترنت الشخصية
٢. جريمة إلكترونية **تستهدف الملكيّة** يستهدف هذا النوع من الجريمة الجهات الحكوميّة والخاصة والشخصية ويركّز على تدمير الملفات الهامة

٣. جريمة إلكترونية **تستهدف الحكومات** وهي هجمات يشنّها القراصنة على المواقع الرسميّة الحكومية وأنظمة شبكاتها والتي تركز كل اهتمامها على القضاء على البنية التحتيّة.

٥. **الجرائم السياسية الإلكترونية والتي تركز على استهداف المواقع العسكرية لبعض الدول لسرقة المعلومات التي تتعلّق بأمن الدولة.**

٦. **–سرقة المعلومات الموثّقة إلكترونياً ونشرها بطرق غير شرعيّة**

٧. **جرائم الشتم والسبّ والقدح.** **٨- جرائم التشهير ويكون هدفها الإساءة لسمعة الأفراد .**

٨. **النصب والاحتيال الإلكتروني.**

٩. **جرائم الاعتداء على الأموال أو الابتزاز الإلكتروني.** **١٠ - الوصول إلى مواقع محجوبة.**

١٠. **الإرهاب الإلكتروني.** **-١١- الجرائم الجنسية الإلكترونية.**

١٢. **جرائم الاعتداء علي الاموال (مؤسسات مصرفية ومالية وبنوك)**

مكافحة الجرائم الإلكترونية:

برامج أمنية و قواعد قانونية للحماية من الجرائم الإلكترونية؟

أولا : الجانب الأمني من الحمايـة:

يتعلق هذا الجانب بكل ما هو فني و تقني لحماية شبكة الأنترنت و الكمبيوتر ويتمثل في ثلاث نقاط مسائل تتعلق بأمن المعلومات و مهددات أمن المعلومات و في الأخير الإجراءات الأمنية

مسائل تتعلق بأمن المعلومات:

1 –المسألة الإداريـــة والفنية:

2–المسألة الماليـــة :

3 –المسألة الوظيفية :

4 –المسألة الخصوصية:

5 –مسألة تحديد مخاطر و حوادث الكمبيوتر و الشبكة

لتأمين سلاسة وسهولة تطبيق أمن المعلومات يجب أن تخضع لمتطلبات فنية وإدارية ، ومن أهم المتطلبات الفنية:

الدراسة التحليلية لأمن النظم: إن الدراسة التحليلية لتحديد مناطق التهديد للأمن ومستوى الخطورة في كل موقع ثم تصميم طرق الإنقاذ من كل منطقة من مناطق التهديد لا بد أن تمثل جزءًا أساسيًا للغاية عند تحليل وتصميم النظام الآلي للمعلومات كما أن مستخدم النظام نفسه لا بد أن يوثق الخطوات العملية التي يجب أن يقوم بها في أي حالة من حالات الكوارث في كتيب استخدام النظام.

التوثيق: أكدت الكثير من الدراسات أن التوثيق في الأنظمة الآلية للمعلومات من أضعف الثغرات في أمن تلك الأنظمة، ويهدف إلى جعل الأنظمة مفهومة للمستخدمين والمشغلين ومفهومة للمصممين حتى يمكنهم من الصيانة المستقبلية ، لحماية الأنظمة من الاحتكار. ولكن التوثيق سلاح ذو حدين فيمكن أن يكشف التوثيق الجيد الأنظمة لأشخاص غير مأذون لهم بذلك مما يستوجب عمل حماية خاصة وجيدة لوثائق النظام

أمن البرامج والبيانات: لقد لوحظ أن الكثير من المبرمجين يقومون بعمل الصيانة العادية في البرامج على النسخ الأصلية للنظام ، فإذا حدثت أي مشكلة في برنامج ما يصعب عليهم التعامل معها أو الرجوع عن آخر تعديلات قاموا بها ، لهذا يجب المحافظة على النسخة الأصلية للبرنامج المصدر ، وأن يقوم المبرمجون بعمل التعديلات اللازمة على نسخة أخرى ، وعند الانتهاء وإجازة التعديلات يتم تعديل النسخة الأصلية وتوثيق ذلك التعديل.

أمن التشغيل: يشمل أمن التشغيل التحكم في الإدخال والتعديل والإطلاع في قسم المستخدمين والتنسيق بين قسم المستخدم والحاسب الآلي في توزيع المسؤوليات والتأكد من تشغيل الأعمال والبرامج الصحيحة في قسم الحاسب الآلي وضمان التشغيل المستمر للأجهزة متى طلب ذلك.

نقطة الضعف في التشغيل هي عدم استيعاب المشغلين لظروف التشغيل استيعاباً جيداً أو محاولة إثبات بعضهم عدم قدرة الأخرى أو تغير أوقات الدوام أو ترك العمل. أما نقطة الضعف الأساسية في استمرارية عمل الحاسب الآلي تكمن في عدم التزام الشركات بعقود الصيانة.

برامج أمن النظام: برامج أمن النظام هي برامج مساعدة يتم تصميمها لتمكن من مراقبة أي تغيير في الملفات، سواء كانت برامج أو بيانات، ويتم ذلك بالطريقة الخاملة وهي تسجيل لأي تغيير منذ البداية ليتم مراجعته مؤخراً أو بالطريقة الحية وهي عدم السماح بالتغيير منذ البداية إلا بناء على صلاحية مبرمجة. وكذلك تقوم برامج النظام بتسجيل محاولات لاختراق النظام مثل مسح المعلومات في الملف المخترق ، أو قفل الجهاز إذا حصل اختراق إلكتروني أو عمل تشفير معقد للحماية إذا حدث الاختراق

الأمن في نظم الاتصالات وقواعد البيانات: يشمل الأمن هنا التوثق من الطرفين والمستخدمين وذلك بالتحكم المادي (استخدام المعدات الخاصة) أو التحكم المنطقي (عمل كلمات سر وتغييرها من وقت إلى آخر). كذلك يشمل الأمن في نظم الاتصال تسجيل كل الملاحظات في أي طرف ونوع الاستخدام بالإضافة إلى التعرف على الشخص المستخدم وذلك عن طريق رقم التعريف أو البطاقة الممغنطة أو غيرها وربط ذلك بالصلاحيات الممنوحة لهذا الشخص.

تطوير وتنفيذ النظم: عند تطوير أو تصميم أي نظام يجب اتباع الطرق العلمية الصحيحة في التصميم كما يجب مراجعته جيداً واختباره و التأكد من خلوه من الأخطاء قبل البدء في التنفيذ، كما يجب تدريب موظفي التشغيل والاستخدام تدريباً جيداً عليه.

المتطلبات الإدارية لأمن النظم الآلية للمعلومات:

التنظيم الإداري:

تنظيم إدارة خاصة بأمن النظم والمعلومات يناط بها تحديد سياسة المنشأة والقواعد والأحكام لضمان استمرارية العمل بالكفاءة المطلوبة.

يحدد مشرف للأمن بالحاسب الآلي تقع على عاتقه مسؤولية التأكد من التزام العاملين بالسياسة الأمنية المرسومة وتنسيق التدريب الفني لهذا المجال. أمن المعلومات يجب أن يدعم أهداف ورؤية المؤسسة ، عن طريق شخص مؤهل يحمل اسم *ISSO (Information Systems Security Officer*

التنظيم الإداري:

يحدد مسؤول أمن يمثل المستخدم ويكون مسؤولاً لدى الجهة المستخدمة للنظام من ضمان التزام إدارة الحاسب الآلي بالسياسة الأمنية المحددة وتحديد مستوى الصلاحيات لكل المتعاملين مع النظام.

يحدد قسم للمراجعة (*Auditing*) في إدارة الأمن مهمته عمل وتنفيذ نظام دقيق للمخزون من وسائل التخزين وأي معدات أو مستلزمات تشغيلية. ويقوم بمتابعة الأفراد في المنشأة وضمان التزامهم بالقواعد والأحكام المطبقة

خطط الطوارئ:

لا بد من وضع الخطط لاستمرارية عمل النظام في حالة المشاكل الكبيرة كتعطل الحاسب الآلي تعطلاً طويلاً، أو في غير ذلك من الحالات الطارئة لا بد من قياس المشاكل التي سيواجهها مستخدم النظام في هذه الحالات ووضع البدائل على ضوء ذلك، فمثلاً في النظم المصرفية أو نظم الحجوزات الجوية حيث لا غنى عن الحاسب الآلي ولو لبضع دقائق ، لهذا يستوجب وجود نظام مساند يعمل بطريقة فورية في حالات الطوارئ.

التحكم المادي وصوره

الأمن المادي لمركز المعلومات والحاسب الآلي:

يشمل الأمن المادي لمركز المعلومات والحاسب حمايته من الحريق والسوائل والغبار والكهروستاتيكا، وكذلك ضمان الكهرباء الكافية والمستلزمات البيئية من حرارة ورطوبة موزونة إضافة إلى التحكم في زيارة ودخول الأفراد إلى المبنى أو المكاتب أو إلى مركز المعلومات،

مراقبة الأفراد:

يمثل الأفراد خط الدفاع الرئيسي في أمن المعلومات ، خاصة المتعاملين من الأنظمة بشكل مباشر. فأمن المعلومات يعتمد أولاً وأخيراً على أمانة الأفراد المتعاملين معها، فلا يكفي التأكد من أخلاقيات الموظف وأهليته للعمل عند تعيينه ، بل يجب أن تستمر مراقبته لأن التغيير السلوكي متوقع في أي وقت، كذلك يجب عدم الاعتماد على موظف واحد بأي حال من الأحوال.

الصيانة والتأمين:

تعتبر الصيانة خط الدفاع الثاني في أمن المعلومات، ووجود الصيانة ضمان للتشغيل المستمر للأنظمة كما أن التأمين التجاري يغطي تكلفة إرجاع المعلومات المفقودة وتغطية الخسارة الناتجة عن تعطيل النظام ، إضافة لتغطية الأجهزة إذا لم تغط بواسطة عقود الصيانة.

تقييم الخطط:

إعادة تقييم خطط حماية المعلومات بشكل دوري، لأنه بمرور الوقت يتطور العتاد والبرمجيات التي تحفظ وتعالج المعلومات ، وفي الوقت نفسه يزداد عدد وحجم التهديدات لأمن المعلومات.

الحماية المادية (*Physical Security*):

الحماية المادية هي أول خط دفاع عن أمن المعلومات في أي منشأة ، حيث يتضمن حماية المنشأة ، حماية الأشخاص، وحماية المعدات. هدف الحماية المادية هو الإحالة دون حصول مشاكل في أنظمة الحاسب الآلي، وإذا حدثت فيجب كشف مكان حدوثها وإصلاحه

حماية المنشأة (*Building Security*):

قبل انتشار الشبكات كان المطلوب هو حماية مركز الحاسب الآلي فحسب، أما الآن فيجب حماية كل المواقع التي تحتوي على حاسب آلي أو أي عتاد متصل بالحاسب الآلي. لهذا عند تصميم المواقع يجب الأخذ بعين الاعتبار العوامل البيئية مثل الحرارة والرطوبة والبرودة والإضاءة والطاقة الكهربائية المستخدمة.

فيما يلي بعض النصائح لحماية مواقع استخدام الحاسب الآلي :

- **استخدام أضواء للطوارئ (*Emergency Lights*) ، للإضاءة في حالات الإخلاء عند حدوث أي طارئ.**
- **استخدام حاويات مضادة للحريق ، حيث تحوي وسائل التخزين (القرص الصلب، والقرص الليزري...).**
- **استخدام المعدات بالشكل الصحيح، والتدريب على استخدامها.**
- **استخدام معدات ذات تقنيات عالية ودقة شديدة فيما يتعلق بالطاقة الكهربائية.**
- **استخدام كابينات خاصة لحفظ معدات وكابلات الشبكة ، حيث يكون لها مفتاح خاص ومراوح للتبريد وأبواب تفتح بزاوية ١٨٠° ، وسهلة النقل.**

- عمل صيانة دورية للمعدات.
- مواقع استخدام الحاسب الآلي يجب أن تكون خالية من الغبار ويمنع الأكل والشرب والتدخين فيها.
- وضع إنذار حماية من المياه قرب المعدات لحساسة.
- الكهرباء الساكنة قد تكون خطرة جدًا لبعض المعدات الإلكترونية الدقيقة (الحاسب الآلي) ولمنعها يفضل استخدام معدات مضادة للكهرباء الساكنة وتأريث المعدات ، واستخدام أرضيات ومكاتب مضادة للكهرباء الساكنة.
- الحفاظ على معدل رطوبة معتدل ٤٠ – ٦٠ % .
- نوعية الكابلات المستخدمة: حيث إن النحاس قابل للتأثر بالأمواج الكهرومغناطيسية ، ويمكن إختراقه بسهولة ، أما كابلات الألياف الضوئية فهي أكثر أمناً من الكابلات النحاسية.

مهددات أمن المعلومات:

هي الحالة أو الظرف الذي يؤدي حتما إلى تعطيل الشبكة المعلوماتية و أنواع هذه المهددات:

1- مهددات **طبيعيـــة** : مثل الزلازل التي تؤدي إلى قطع الإتصالات بالشبكة.

2-مهددات **غير مقصـــودة** من طـــرف الإنســـان كسوء إستعمال كلمة السر.

3- مهددات **إنسانيـــة**: وهو ما يقـــوم به المتسللـــون الذيـــن يخترقون المواقع.

ان الثغرات الأمنية يمكن كشفها من طرف الهاكرز خصوصا في الحواسب الشخصية إما على مستوى خطوط الإتصال فهي معرضة المراقبة بالإشعاعات أو التصنت و التجسس لأنه يستخدم للإتصال بشبكة الأنترنت الألياف البصرية و الأقمار الصناعية كما يمكن إعتراض طريق وصل الأسلاك للإستراق عن طريق الشبكة

توجد ثغرات بروتوكولات الإتصالات في شبكة الأنترنت و كذا الثغرات الموجودة في برامج البريد الإلكتروني *e-mail*

حيث لا يوجد مايمنع من إستعمال و تغير محتوى الرسالة بالبرامج الخبيثة، و لها عدة أنواع مثلا:

1 - **الفيروسات و حصان طروادة :** هذا الأخير يمكن أن يفرغ الملفات من محتوياتها.

2- **الباب السري** : يسمح بالدخول دون المرورباجهزة أو برامج الحماية.

3- **الدودة** : برنامج يؤدي إلى تخريب الملفات التي يدخلها.

هذه المهددات و غيرها هي التي تعترض أمن المعلومات و التي لازلت تتطور بتطور العلم.

الإجـــراءات الأمنـيـــة

إستخدام جدار الحماية *fire well* و هو حاجز يوضع بين الشبكة الذاخلي أنترنت و خادم شبكة الأنترنت و من أهم مهامه فحص المعلومات الذاخلة و الخارجة و السماح لها بالمرور في حالة مطابقتها للمواصفات و تقديم تقارير عن التحركات المشبوهة و لكنه يمكن أن يعطل بعض المعلومات و يحدث عطب.

-**التشفير** و هو تحويل المعلومة من نص واضح إلى آخر غير مفهوم و قد أستحسن هذا النوع من النظام لنجاعته في عدم كشف المعلومات على شبكة الأنترنت.

-**التوقيع الرقمي** و هي تقنية تفيد في إمكانية عدم تزوير الرسائل الإلكترونية.

-**إستخدام أنظمة كشف الإختراقات** و وضع حلول للثغرات الأمنية.

-**وضع سياسة أمنية للشبكة** و حشد كل الإمكانيات البشرية و المادية لتطبيقها.

-**الإحتفاظ بنسخ إحتياطية** لكل المعلومات الحساسة في أقراص إضافية ليست مرتبطة. بالشبكة.

الجوانب الأخلاقية التي يجب أن يلتزم بها مهندس البرمجيات؟

- **السرية** : *(Confidentiality)* عليك أن تحترم سرية زبائنك و رؤسائك، سواء كان هناك هناك ميثاق أخلاقي أم لا
- **الكفاءة** : *(Competence)* عليك أن تقر و تعترف بإمكانياتك و معارفك و ألا تدعي علما لا تعلمه أو معرفة تقع خارج مجال اختصاصك.

حقوق الملكية الفردية : **(Intellectual property rights)** عليك أن تكون واعيا لكل القوانين المتعلقة بحقوق الملكية الفكرية مثل براءات إختراع و حقوق النسخ

يتوجب على مهندس البرمجيات الالتزام بإجراء نشاطات :

١. التحليل ، التوصيف ، التصميم ، التطوير ، الاختبار ، الصيانة
وفق أسلوب صحيح و مفيد و يحترم هذه المهنة وبشكل متلائم مع سلامة و صحة و رفاه المجتمع

المبادئ الثمانية التي يجب ان يلتزم بيها مهندسي البرمجيات ؟!((الميثاق الاخلاقي))

١- المجتمع : يلتزم مهندس البرمجيات بالعمل وفق أسلوب يتسق مع المصلحة العامة.

٢- اتخاذ القرارات : يجب أن يحافظ مهندس البرمجيات على قدر واسع من الاستقلالية في إتخاذه لقراراته

٣- الإدارة : يتوجب على مهندس البرمجيات عند توليه منصبا قياديا أو إداريا بأن يرفع من شأن القيم الأخلاقية ضمن المؤسسة في تطوير و صيانة البرمجيات

٤- الزبائن و الرؤساء : CLIENT AND EMPLOYER علي مهندس البرمجيات أن يحترم الزبون و الرئيس بشكل يتفق مع المصلحة العامة

٥- المهنة : يجب ألا يسيء مهندس البرمجيات لسمعة هذه المهنة إطلاقا

٦- المنتج : يتوجب على مهندس البرمجيات أن يضمن بأن منتجه يحترم المعايير المهنية قدر الإمكان.

٧- الزملاء : إتخاذ موقف عادل اتجاه الزملاء دون إفراط أو تفريط

٨- الذات : تنمية الحس الأخلاقي و متابعة آخر التطورات في حقل هندسة البرمجيات.

إن أكبر معضلة يمكن أن يواجهها المهندسون هي العمل مع أرباب العمل الذين لا يسلكون طرقا أخلاقية في عملهم
هب أنك تعمل في شركة لتطوير البرمجيات ، ثم و أثناء تطوير أحد هذه البرامج الحرجة ، و نتيجة الضغط قامت الشركة بتزوير سجلات الأمان لهذه البرمجية. ماذا ستفعل في هذه الحالة ؟ فمن جانب يتوجب عليك أن تحترم سرية الشركة التي تعمل بها ، و من جانب آخر قد يسبب كتمانك للموضوع في حدوث أضرار لا تحمد عقباها .

المشكلات الأخلاقية Ethical dilemmas:

أكبر المعضلات التي يواجهها مهندسي البرمجيات هي:

- خلاف من حيث المبدأ بسياسات الإدارة العليا
- رب العمل يتصرف بطريقة لا أخلاقية و يصدر نظام الأمان الحرج بدون إنهاء اختبار النظام

الاشتراك في تطوير أنظمة الأسلحة العسكرية أو الأنظمة النووية.

Computer Virusتعريف الفيروس:

هو نوع من أنواع البرمجيات التخريبية الخارجية، صُنعت عمداً بغرض تغيير خصائص ملفات النظام. تتكاثر الفيروسات عن طريق توليد نفسها بنسخ شفرتها الأصلية وإعادة توليدها، أو عن طريق إصابة برنامج حاسوبي بتعديل خصائصه.

البرامج الممكن إصابتها تتضمن، ملفات البيانات، أو قطاع البوت Boot في القرص الصلب.

خواص الفيروسات:

- **برنامج قادر على التناسخ *Replication* والانتشار.**
- **الفيروس يربط نفسه ببرنامج أخر يسمى الحاضن *Host*.**
- **لا يمكن أن تنشأ الفيروسات من ذاتها.**

•يمكن أن تنتقل من حاسوب مصاب لآخر سليم.

مكونات الفيروس:

يتكون برنامج الفيروس من أربعة أجزاء رئيسية وهي:

١. **آلية التناسخ** *The Replication Mechanism* وهو الجزء الذي يسمح للفيروس أن ينسخ نفسه.

٢. **آلية التخفي** *The Protection Mechanism* وهو الجزء الذي يخفي الفيروس عن الاكتشاف.

٣. **آلية التنشيط** *The trigger Mechanism* وهو الجزء الذي يسمح للفيروس بالانتشار قبل أن يعرف وجوده كاستخدام توقيت الساعة في الحاسوب كما في فيروس *(Michelangelo)* الذي ينشط في السادس من مارس من كل عام .

٤. **آلية التنفيذ** *The Payload Mechanism* وهو الجزء الذي ينفذه الفيروس عندما يتم تنشيطه

الوقاية من الفيروس:

•استخدام برامج للكشف عن الفيروسات في الجهاز.
•احتفظ بنسخ احتياطية من البرامج والملفات الموجودة على الحاسب.
•إجراء الفحص على البرامج المحملة (المنزلة-*Downloads*) أو المنقولة من شبكة الإنترنت قبل تشغيلها.
•استخدام برمجيات الجدار الناري. *(Firewall)*
•استخدم نظام التشغيل جنوا لينكس فهو يعتبر أكثر أمانا وفيه فيروسات قليلة عكس نظام التشغيل ويندوز.
•لا تشغل أي برنامج أو ملف لا تعرف ما هو بالضبط.
•الحذر من رسائل البريد الإلكتروني غير معروفة المصدر وفحصها قبل الإقدام على فتحها.

اللغات التي يكتب بها الفيروس:

لسهولة الوصول لعتاد الحاسوب وهناك أيضاً اللغات من أهم اللغات التي يكتب بها كود الفيروس هي لغة التجميع أسمبلي الراقية مثل C, C++ Visual C . Visual Basic، ***script viruses Visual Basic Scripting edition (VBS) and the JavaScript programming languages***

طرق انتقال الفيروسات:

فيروس قطاع التمهيد: يصيب قطاع التمهيد من أجهزة الكمبيوتر. أثناء تحميل النظام ، يتم تحميل فيروس قطاع التمهيد في الذاكرة الرئيسية ويدمر البيانات المخزنة في القرص الثابت

فيروس ماكرو يرتبط ببرامج التطبيقات مثل *word* و *excel*. عند فتح المستند المصاب ، يتم تحميل فيروس الماكرو في الذاكرة الرئيسية ويدمر البيانات المخزنة في القرص الثابت

فيروسات البريد الإلكتروني

- يتحرك في رسائل البريد الإلكتروني
- يكرر نفسه عن طريق إرسال نفسه تلقائيًا إلى عشرات الأشخاص في دفتر عناوين البريد الإلكتروني للضحية
- مثال: فيروس ميليسا ، فيروس *ILOVEYOU*

أنواع الملفات التي يمكن أن يصيبها الفيروس

بشكل عام الفيروس يصيب الملفات التنفيذية أو الملفات المشفرة غير النصية مثل:

- الملفات ذاتية التنفيذ مثل ملفات ذات امتداد *(EXE ,·DLL,·COM·)* ضمن أنظمة التشغيل دوس وميكروسفت ويندوز أو *(ELF)* في أنظمة لينكس ·
- سجلات الملفات والبيانات *(VOLUME BOOT RECORD)* في الأقراص المرنة والصلبة والسجل رقم (٠) في القرص الصلب ·*MASTER BOOT*
- ملفات الأغراض العامة مثل ملفات *Batch* والسكريبت في ويندوز.
- ملفات الاستخدام المكتبي مثل مايكروسوفت ورد وإكسل و أكسس.
- قواعد البيانات وملفات *Outlook* لما تحويه من عناوين ·*E-mail*
- الملفات من النوع *(HTML)* والتي تستخدم في تصميم صفحات ومواقع الويب.
- الملفات المضغوطة مثل *ZIP* ملفات *MP3*

أعراض الإصابة

- تكرار رسائل الخطأ في أكثر من برنامج·
- ظهور رسالة تعذر الحفظ لعدم كفاية المساحة·
- تكرار اختفاء بعض الملفات التنفيذية·
- حدوث بطء شديد في بدء تشغيل [نظام التشغيل] أو تنفيذ بعض التطبيقات·
- رفض بعض التطبيقات للتنفيذ

أولاً: من حيث السرية

أنواع الفيروسات ثلاثة: (الفيروس والدودة وحصان طروادة):

١. الفيروس :هو برنامج تنفيذي له امتداد (.com, .exe ,.bat,.pif,.scr) ويعمل بشكل منفصل ويهدف إلى إحداث خلل في نظام الحاسوب.

٢. الدودة/ ديدان الحاسب :هي فيروس ينتشر فقط عبر الشبكات والإنترنت ويعمل على الانتشار على الشبكات عن طريق عناوين البريد الإلكتروني،

فمثلا عند إصابة الجهاز يبحث البرنامج الخبيث عن عناوين الأشخاص المسجلين في دفتر العناوين ويرسل نفسه إلى كل شخص وهكذا. مما يؤدي إلى انتشاره بسرعة عبر الشبكة

الدودة/ ديدان الحاسب

الدوده لاتنفذ أي عمل مؤذي، إنما تنتشر فقط مما يؤدي إلى إشغال موارد الشبكة بشكل كبير. ومع التطور الحاصل في ميدان الحوسبة أصبح بإمكان المبرمجين الخبيثين إضافة سطر برمجي لملف الدودة بحيث تؤدي عمل معين بعد انتشارها،

- (مثلا بعد الانتشار إلى عدد ٥٠٠٠٠ جهاز يتم تخريب الأنظمة في هذه الأجهزة) أو أي شيء آخر (مثلا في يوم معين أو ساعة أو تاريخ...الخ) وأصبحت الديدان من أشهر الفيروسات على الشبكة العالمية وأشهر عملياتها التخريبية وأخطرها تلك التي يكون هدفها حجب الخدمة مما يسبب توقف السيرفر عن العمل. وهذه الديدان استهدفت مواقع لكثير من الشركات العالمية أشهرها مايكروسوفت.

فيروس دودة

الدودة هي أيضا برنامج مدمر يملأ نظام حاسوبي بمعلومات ذاتية النسخ ، مما يؤدي إلى انسداد النظام بحيث يتم إبطاء عملياته أو إيقافه

حصان طروادة

حصان طروادة هو برنامج مدمر. يتظاهر عادة بألعاب الكمبيوتر أو برامج التطبيقات. إذا تم تنفيذه ، فسيتعرض نظام الكمبيوتر للتلف

حصان طروادة :Trojan Horse سمي هذا الفيروس بحصان طروادة لأنه يذكر بالقصة الشهيرة لحصان طروادة حيث اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طرواده والتغلب على جيشها، وهكذا تكون آلية عمل هذا الفيروس حيث يكون مرفقا مع أحد البرامج، أي يكون جزءا من برنامج دون أن يعلم المستخدم. وعندما يبدأ البرنامج تنفيذ عمله ويصل إلى مرحلة ما ينشط ويقوم بعمله التخريبي.

يأتي حصان طروادة عادةً مع أدوات مراقبة وأجهزة تسجيل رئيسية

إجراءات لمنع الإصابة بالفيروس

- قم دائما بتحديث برنامج مكافحة الفيروسات الخاص بك على الأقل أسبوعيا.

- قم بعمل نسخ احتياطية من ملفاتك المهمة وتأكد من إمكانية استعادتها.
- قم بتغيير تتابع بدء تشغيل الكمبيوتر لبدء تشغيل الكمبيوتر من محرك الأقراص الثابت الخاص به
- لا تشارك Drive C: بدون كلمة مرور وبدون قيود للقراءة فقط.
- محركات الأقراص المرنة الفارغة من الأقراص قبل تشغيل أجهزة الكمبيوتر ، وخاصة أجهزة الكمبيوتر المحمولة.
- نسيان فتح مرفقات البريد الإلكتروني غير المتوقعة ، حتى لو كانوا من الأصدقاء
- احصل على التدريب على برنامج مكافحة الفيروسات الخاص بجهاز الكمبيوتر الخاص بك واستخدامه.
- لديك نسخ احتياطية متعددة من الملفات الهامة. هذا يقلل من فرصة أن جميع المصابين.
- قم بتثبيت تحديثات الأمان لنظام التشغيل والبرامج الخاصة بك في أقرب وقت ممكن.
- القفز على فرصة لمعرفة المزيد عن جهاز الكمبيوتر الخاص بك. سيساعدك هذا في تحديد الفيروسات.

الأمن المعلوماتي (المفاهيم والمصطلحات

أمن المعلومات: هو حماية وتأمين المعلومات والموارد المستخدمة كافة لمعالجة المعلومات ، بحيث تتضمن الأمن المادي للمنشأة والأفراد العاملين فيها ، وأمن الحاسبات ووسائط نقل المعلومات والشبكات ، وذلك عن طريق اتباع إجراءات ووسائل حماية تضمن في النهاية سلامة المعلومات.

المعلومات نوعان :

- **معلومات إلكترونية (Electronic Form Information)**
- **تحفظ باستخدام التكنولوجيا الإلكترونية (مثل الحاسب الآلي).**
- **معلومات تقليدية (Traditional Form Information)**
- **تحفظ باستخدام الوسائل التقليدية(مثل الورق).**

المعلومات الإلكترونية معرضة للعطب والهجوم أكثر من المعلومات التقليدية للأسباب التالية:

- **إمكانية تسرب المعلومات الإلكترونية.**
- **المعلومات الإلكترونية غير ظاهرة للعين.**
- **المعلومات قد تحفظ باستخدام وسائل صغيرة الحجم.**
- **صعوبة التخلص من المعلومات.**
- **صعوبة التعامل مع الحاسب الآلي**
- **تزايد الاتصالات والشبكات**

الصور التي تتنقل فيها المعلومات:

- **عبر وسائط التخزين (القرص الصلب ، القرص المرن ،القرص المضغوط ...)**
- **عبر الأسلاك (الشبكات ، الهاتف ...)**
- **لاسلكي(الأمواج الكهرومغناطيسية ، الأشعة تحت الحمراء...)**

كيفية تأمين أمن المعلومات:

- إذا طبقت الكثير من نظم الأمان، سيصعب عليك استخدام المعلومات التي تقوم بحمايتها ، فبإحكامك نظم الأمان، إنك بالوقت نفسه تقوم بإبطاء معدل نقل المعلومات ومن ثم يقل معدل الإنتاجية، وعلى الرغم من ذلك إذا كنت متحرراً جداً ولا تقوم باستخدام أي نظم أمان، سيتمكن منافسوك من معرفة خططك المستقبلية واختراق وتدمير البيانات ، لهذا يجب التوازن في تطبيق الأمن

أمثلة على جرائم الحاسب الآلي:

تهديد من قبل الفيروسات:

- فيروس (*Sobig Virus*): حيث يعد من أكبر التهديدات في سنة ٢٠٠٣ ، واعتمد على أكثر من طريقة لنشر نفسه عبر أجهزة الحاسب الآلي ، استطاع أن ينسخ نفسه على الأقراص المشارك بها عبر الشبكات ، واستطاع أن يخترق دفتر العناوين في أوتلوك وإرسال نفسه في بريد إلكتروني باسمك إلى أي بريد شخص آخر موجود في دفتر العناوين الخاص بك.

Exchange Server 2003

تجسس صناعي:

- شركة VIA Technology : في سنة ٢٠٠٣ ، تم ادانة مدير الموظفين في الشركة بسرقة تكنولوجيا من أحد زبائنها، حيث إن أحد المهندسين في شركة {VIA) خرج منها ليعمل في شركة أخرى وأحد زبائن VIA وهي شركة D-Link. لعدة أشهر مع استمراره بالحصول على راتب من شركة VIA، ثم استقال منها ورجع إلى VIA، وتبين أنه قد سرق أحد برامج المحاكاة

- إرهاب إلكتروني:

- حيث إن استخدام الإنترنت من قبل مجموعات متطرفة، تقوم بالدعوة إلى التطرف والتدريب على كيفية صنع الأسلحة الفتاكة، هو مثال على الإرهاب الإلكتروني.

التزوير الإلكتروني وانتحال الشخصية والاحتيال هم من أفضل الأمثلة على جرائم الإنترنت. حيث استطاع مخترق (Hacker) الوصول إلى قاعدة بيانات شركة تعالج بطاقات الائتمان، حيث تمكن الشخص من الوصول إلى معلومات ٥.٦ مليون بطاقة ائتمان.

مفهوم التهديد الأمني للمعلومات (*Information Threats*):

- تقدير المعلومات يختلف من منشأة إلى أخرى، حيث أنه في بعض المنشآت تكون الخصوصية هي أهم عوامل المعلومات (مثل المنشآت العسكرية)، وأخرى تهتم أكثر بسلامة المعلومة (مثل المنشآت التجارية والصناعية).

تهديد أمن المعلومة يعني التأثير في أحد العوامل التالية :

- السلامة (Integrity).
- إمكانية الوصول للمعلومة (Availability).
- الخصوصية (Confidentiality)

أهداف التهديد الأمني ودوافعه (*Motives*):

أهداف التهديد الأمني ودوافعه متعددة من أهمها الدافع المادي ، حيث إن الإغراءات المالية قد تؤدي بالشخص إلى سرقة أو تزوير معلومات معينة. أو الدافع السياسي والعسكري من أجل الحصول على معلومات عن نشاطات وخطط الدول الأخرى المستقبلية والمالية ومن ثم محاولة إيقافها أو منافستها . أو الدافع التجاري والاقتصادي حيث تجري حرب قوية بين الشركات التجارية الكبرى لكسب أكبر عدد ممكن من العملاء، ومن ثم الحصول عن طريق الاختراق على معلومات عنها . أو الدافع الفردي . حيث تكون مجموعات التباهي بالنجاح والتحدي من طلاب الجامعات أو الأندية أو العاطلين عن العمل هدفها إما واختراق أجهزة الأصدقاء، وإما التخريب في أنظمة الشركات والمؤسسات التي قامت بفصل بعض من عمالها أو موظفيها.

أنواع التهديد الأمني (جرائم الحاسب)

١. تهديد غير مقصود لأمن أنظمة الحاسب (*Accidental Threats*):
   - تعطل العتاد في الحاسب الآلي (Hardware Failure) .
   - أخطاء المستخدمين (Human Errors) .
   - خطأ في البرمجيات (Software Errors) .
   - المياه والكهرباء والحريق
٢. كوارث طبيعية (Natural Hazards): حيث يحصل تهديد مادي، وأنواع التهديدات المادية:
   - الحرارة العالية والرطوبة.
   - الغبار والدخان.
   - الزلازل والبراكين والأعاصير والطوفان والصواعق... .
   - و هذا النوع من الحوادث لا يزيد عن ٥% من جملة التهديدات الأمنية الأخرى.

٣. تهديدات من قبل أشخاص (*Human Threats*):
   - السرقة Theft.
   - التهديد باختراق البيانات (Hacking & Interception).
   - هندسة العلاقات (Social Engineering) .
   - الاقتحام العشوائي .
   - حرب القيادة (War-Driving) .
   - التنصت وأنواعه (Sniffing , Spoofing and Eavesdropping) .

- التهديد بإعطاب وتغيير البيانات (Fabrication & Denial of Service) .
-

التحكم المادي وصوره

لتأمين سلاسة وسهولة تطبيق أمن المعلومات يجب أن تخضع لمتطلبات فنية وإدارية ، ومن أهم المتطلبات الفنية:

- **الدراسة التحليلية لأمن النظم: إن الدراسة التحليلية لتحديد مناطق التهديد للأمن ومستوى الخطورة في كل موقع ثم تصميم طرق الإنقاذ من كل منطقة من مناطق التهديد لا بد أن تمثل جزءًا أساسيًا للغاية عند تحليل وتصميم النظام الآلي للمعلومات كما أن مستخدم النظام نفسه لا بد أن يوثق الخطوات العملية التي يجب أن يقوم بها في أي حالة من حالات الكوارث في كتيب استخدام النظام.**

- **التوثيق: أكدت الكثير من الدراسات أن التوثيق في الأنظمة الآلية للمعلومات من أضعف الثغرات في أمن تلك الأنظمة، ويهدف إلى جعل الأنظمة مفهومة للمستخدمين والمشغلين ومفهومة للمصممين حتى يمكنهم من الصيانة المستقبلية ، لحماية الأنظمة من الاحتكار. ولكن التوثيق سلاح ذو حدين فيمكن أن يكشف التوثيق الجيد الأنظمة لأشخاص غير مأذون لهم بذلك مما يستوجب عمل حماية خاصة وجيدة لوثائق النظام.**

- **أمن البرامج والبيانات: لقد لوحظ أن الكثير من المبرمجين يقومون بعمل الصيانة العادية في البرامج على النسخ الأصلية للنظام ، فإذا حدثت أي مشكلة في برنامج ما يصعب عليهم التعامل معها أو الرجوع عن آخر تعديلات قاموا بها ، لهذا يجب المحافظة على النسخة الأصلية للبرنامج المصدر ، وأن يقوم المبرمجون بعمل التعديلات اللازمة على نسخة أخرى ، وعند الانتهاء وإجازة التعديلات يتم تعديل النسخة الأصلية وتوثيق ذلك التعديل.**

- **أمن التشغيل: يشمل أمن التشغيل التحكم في الإدخال والتعديل والإطلاع في قسم المستخدمين والتنسيق بين قسم المستخدم والحاسب الآلي في توزيع المسؤوليات والتأكد من تشغيل الأعمال والبرامج الصحيحة في قسم الحاسب الآلي وضمان التشغيل المستمر للأجهزة متى طلب ذلك. نقطة الضعف في التشغيل هي عدم استيعاب المشغلين لظروف التشغيل استيعاباً جيداً**

- **برامج أمن النظام: برامج أمن النظام هي برامج مساعدة يتم تصميمها لتمكن من مراقبة أي تغيير في الملفات، ويتم ذلك بالطريقة الخاملة وهي تسجيل لأي تغيير منذ البداية ليتم مراجعته مؤخراً أو بالطريقة الحية وهي عدم السماح بالتغيير منذ البداية إلا بناء على صلاحية مبرمجة. وكذلك تقوم برامج النظام بتسجيل محاولات لاختراق النظام مثل مسح المعلومات في الملف المخترق ، أو قفل الجهاز إذا حصل اختراق إلكتروني أو عمل تشفير معقد للحماية إذا حدث الاختراق.**

- **الأمن في نظم الاتصالات وقواعد البيانات: يشمل الأمن هنا التوثق من الطرفين والمستخدمين وذلك بالتحكم المادي (استخدام المعدات الخاصة) أو التحكم المنطقي (عمل كلمات سر وتغييرها من وقت إلى آخر). كذلك يشمل الأمن في نظم الاتصال تسجيل كل الملاحظات في أي طرف ونوع الاستخدام بالإضافة إلى التعرف على الشخص المستخدم وذلك عن طريق رقم التعريف أو البطاقة الممغنطة أو غيرها وربط ذلك بالصلاحيات الممنوحة لهذا الشخص.**

- **تطوير وتنفيذ النظم: عند تطوير أو تصميم أي نظام يجب اتباع الطرق العلمية الصحيحة في التصميم كما يجب مراجعته جيداً واختباره و التأكد من خلوه من الأخطاء قبل البدء في التنفيذ، كما يجب تدريب موظفي التشغيل والاستخدام تدريباً جيداً عليه.**

المتطلبات الإدارية لأمن النظم الآلية للمعلومات:

التنظيم الإداري:

- **تنظيم إدارة خاصة بأمن النظم والمعلومات يناط بها تحديد سياسة المنشأة والقواعد والأحكام لضمان استمرارية العمل بالكفاءة المطلوبة.**
- **يحدد مشرف للأمن بالحاسب الآلي تقع على عاتقه مسؤولية التأكد من التزام العاملين بالسياسة الأمنية المرسومة وتنسيق التدريب الفني لهذا المجال. أمن المعلومات يجب أن يدعم أهداف ورؤية المؤسسة ، عن طريق شخص مؤهل يحمل اسم ISSO (Information Systems Security Officer).**
- **يحدد مسؤول أمن يمثل المستخدم ويكون مسؤولاً لدى الجهة المستخدمة للنظام من ضمان التزام إدارة الحاسب الآلي بالسياسة الأمنية المحددة وتحديد مستوى الصلاحيات لكل المتعاملين مع النظام.**
- **يحدد قسم للمراجعة (Auditing) في إدارة الأمن مهمته عمل وتنفيذ نظام دقيق للمخزون من وسائل التخزين وأي معدات أو مستلزمات تشغيلية. ويقوم بمتابعة الأفراد في المنشأة وضمان التزامهم بالقواعد والأحكام المطبقة.**

خطط الطوارئ:

لا بد من وضع الخطط لاستمرارية عمل النظام في حالة المشاكل الكبيرة كتعطل الحاسب الآلي تعطلاً طويلاً، أو في غير ذلك من الحالات الطارئة لا بد من قياس المشاكل التي سيواجهها مستخدم النظام في هذه الحالات ووضع البدائل على ضوء ذلك، فمثلاً في النظم المصرفية أو نظم الحجوزات الجوية حيث لا غنى عن الحاسب الآلي ولو لبضع دقائق ، لهذا يستوجب **وجود نظام مساند يعمل بطريقة فورية في حالات الطوارئ.**

الأمن المادي لمركز المعلومات والحاسب الآلي:

يشمل الأمن المادي لمركز المعلومات والحاسب حمايته من الحريق والسوائل والغبار والكهروستاتيكا، وكذلك ضمان الكهرباء الكافية والمستلزمات البيئية من حرارة ورطوبة موزونة إضافة إلى التحكم في زيارة ودخول الأفراد إلى المبنى أو المكاتب أو إلى مركز المعلومات،

مراقبة الأفراد:

يمثل الأفراد خط الدفاع الرئيسي في أمن المعلومات ، خاصة المتعاملين من الأنظمة بشكل مباشر. فأمن المعلومات يعتمد أولاً وأخيراً على أمانة الأفراد المتعاملين معها، فلا يكفي التأكد من أخلاقيات الموظف وأهليته للعمل عند تعيينه ، بل يجب أن تستمر مراقبته لأن التغيير السلوكي متوقع في أي وقت

الصيانة والتأمين:

تعتبر الصيانة خط الدفاع الثاني في أمن المعلومات، ووجود الصيانة ضمان للتشغيل المستمر للأنظمة

تقييم الخطط

إعادة تقييم خطط حماية المعلومات بشكل دوري، لأنه بمرور الوقت يتطور العتاد والبرمجيات التي تحفظ وتعالج المعلومات.

الحماية المادية Physical Security

الحماية المادية هي أول خط دفاع عن أمن المعلومات في أي منشأة ، حيث يتضمن حماية المنشأة ، حماية الأشخاص، وحماية المعدات. هدف الحماية المادية هو الإحالة دون حصول مشاكل في أنظمة الحاسب الآلي،

حماية المنشأة Building Secur

يجب حماية كل المواقع التي تحتوي على حاسب آلي أو أي عتاد متصل بالحاسب الآلي. لهذا عند تصميم المواقع يجب الأخذ بعين الاعتبار العوامل البيئة مثل الحرارة والرطوبة والبرودة والإضاءة والطاقة الكهربائية المستخدمة.

حماية وسائط المعلومات (Media Security):

إذا كانت المعلومات هي الكنز الثمين الذي يجب على المؤسسة الحفاظ عليه، فإن الوسائط التي تستخدم لتخزين المعلومات هي التي يجب الاهتمام بها.

حماية الاتصالات والشبكات (Networks &Communication Security):

أدى التقاء تقنية الحاسب الآلي بتقنية الاتصالات إلى اتساع مجال استخدام الحاسب الآلي، وأصبحت المعلومات تنقل عبر الهواء إلى جميع أنحاء العالم مما أدى إلى ظهور مشاكل سرقة المعلومات من خلال نظم الاتصالات التي تربط الحاسبات بعضها ببعض.

حماية التطبيقات (Applications Security):

لا بد من وجود أسس وقواعد تبنى عليها أمن التطبيقات وتحمى من خلالها البيانات من الفقد أو التلف أو سوء الاستخدام، كما يؤخذ في عين الاعتبار القدرة على استعادة هذه البيانات إذا مافشلت إجراءات حمايتها لسبب أو لآخر، أي إننا نتحدث عن **شق الوقاية وشق العلاج** معاً. وهذا لن يتم إلا من خلال خطة متكاملة لتأمين التطبيقات وما يرتبط بها من بيانات

التوثيق

هي عبارة عن وسيلة اتصال مكتوبة، حيث يلعب توثيق الأنظمة دوراً مهماً جداً في دورة حياة إنشاء الأنظمة . فالتوثيق مهم لأي تعديلات أو تحسينات مستقبلية قد يتطلبها النظام. وحماية التوثيق المصاحب لإعداد أي نظام لا يقل أهمية عن مراحله المختلفة. والكم الكبير جداً من الوثائق سواء المطبوع منها على ورق أو المخزنة على وسائل تخزين ممغنطة يجب أن تكون على سرية تامة وبعيدة عن التداول أو السرقة أو الاستنساخ

قوانين وأحكام للحماية

الأحكام والقوانين (Security Policy):

أهم عناصر بنائية أمن المعلومات هي الأحكام والقوانين (Policies) ، كل منشأة بحاجة إلى قوانين وأحكام لتعريف الحدود المقبولة للسلوك في العمل وكيفية الرد على أي مخالفة تحدث. وبالطبع تختلف القوانين والأحكام من منشأة إلى أخرى ، حسب احتياجات كل منشأة ، ومن الأمثلة على بعض هذه القوانين والأحكام:

- **منع استخدام ألعاب الكمبيوتر على أجهزة الحاسب في المنشأة.**
- **منع إرسال رسائل إلكترونية بحجم أكبر من ٢ ميجابايت.**
- **عدم استخدام أي برامج مقرصنة.**

هناك وظيفتان رئيسيتان للقواعد والأحكام (Policies) :

١. **داخلية (Internal Policies): حيث يذكر فيها ما هو المطلوب من الموظفين وكيفية جزائهم على الأعمال التي يقومون بها.**
٢. **خارجية (External Policies): حيث يتم تذكير العالم خارج المنشأة عن كيفية عملها ، وأن هناك أحكاماً وقواعد لحمايتها.**

النسخ الاحتياطي وحماية الملفات (Backup & File Protection):

من أهم وسائل حماية المعلومات وجود إستراتيجية للنسخ الاحتياطي للعتاد والبرمجيات والمعلومات والتوثيقات ، ويجب تحديد هذه الإستراتيجية في القواعد والأحكام الخاصة في النسخ الاحتياطي (Backup Policy) ، حيث يتم ذكر الإجراءات والخطوات اللازمة لعمل النسخ الاحتياطية وذكر الجدول الزمني لكل منها.

الحماية حسب صلاحيات المستخدم (User Privileges):

- حيث يجب تحديد الصلاحيات لكل مجموعة من مجموعات المستخدمين من قبل مشرفي الحاسب الآلي، الذين يمكن تصنيفهم على النحو التالي:
- المستفيدون :
  - الإدارة العليا.
  - مديرو الإدارات.
  - الموظفون المسؤولون عن إدخال البيانات وتحديثها.
  - الموظفون الذين يستخدمون البيانات.

- جمهور المتعاملين مع المؤسسة.

متخصصون في الحاسب الآلي:

- مدير النظام.
- مدير قاعدة البيانات.
- مدير أمن النظام.
- المبرمجون.
- المشغلون.

التحقق من الشخصية والصلاحيات (Authentication & Authorization):

التحقق من الشخصية يعني ربط الشخص مع صلاحياته ، حيث إنه يجب تقديم بيانات تمكن النظام من التأكد من شخصية المستخدم ، هذه البيانات قد تأتي من إحدى الأمور التالية:

١. بيانات مقدمة من قبل المستخدم (كلمة السر).
٢. ماذا بحوزة المستخدم؟ (كارت رقمي).
٣. هوية المستخدم (بصمة الاصبع).
٤. شكل المستخدم (*Face or Eye Recognition*).
٥. صوت المستخدم (*Voice Recognition*).

استخدام كلمات المرور (Passwords):

- **يعتبر هذا هو خط الدفاع الأول للتأكد من صلاحية المستخدم في بث البيانات. وهذا هو أسهل أسلوب وأرخص أسلوب كذلك ، ولكي يحقق هذا الأسلوب النجاح يجب توعية المستخدمين بعدم التخلي عن كلمة المرور لأي شخص، وأن يفرض عليهم تغييرها بصفة دورية. يجب كذلك تشفير كلمات المرور في الملفات المستخدمة لحفظها في الحاسب**

- **ومن عيوب هذا الأسلوب أنه يمكن كسره بسهولة بواسطة برامج تقوم بعمل عدد لا نهائي من المحاولات حتى تتوصل إلى الكلمة الصحيحة، ولذلك يجب تحديد عدد المحاولات الفاشلة التي يتم بعدها فصل الحاسب الشخصي عن الشبكة وإيقافه عن العمل تماماً.**

وسائل أخرى للتحقق من الشخصية(Other Methods of Authentication):

الملامح الفيزيائية للفرد (Biometric): حيث تستخدم هذه التقنية أدوات وأجهزة للتعرف على الشخص عن طريق ملامحه الفيزيائية التي تختلف من شخص لآخر ، وهناك عدة أنواع :

١) بصمة الصوت (*Voice Print*).
٢) بصمة الأصبع (*Finger Print*).
٣) التعرف على الوجه (*Face Recognition*).
٤) التعرف على القزحية(*Iris Recognition*).

مفهوم التوقيع الرقمي:

طريقة تشفير إلكترونية تعمل على توثيق المعاملات التي تتم عبر الشبكات (الإنترنت). وهناك عنصران أساسيان في أي توقيع بشكل عام:

١) مصداقية الموقع: حيث يشير التوقيع إلى الشخص الذي قام بتوقيع الوثيقة.

٢) **مصداقية المعلومات: حيث إنه يجب أن يتم التأكد من أن المعلومات المرسلة لم يتم العبث بها.**

مفهوم الشهادات الرقمية وسلطات منحها(Certifications Authorities):

قد ينكر الشخص المستقبل أن المرسل قد أرسل إليه المفتاح العام لسبب ما، لهذا من الضروري وجود إستراتيجية مقنعة لكي يتم ربط سلطة ما بالمفتاح العام. الحل هو استخدام طرف ثالث يكون محل للثقة لكي يربط المرسل مع المفتاح العام الخاص به، ويسمى هذا الطرف بسلطة المصادقة (**Certifications Authorities**)، ومن هنا ظهر مصطلح الشهادات الرقمية (**Digital Certificates**) ، **وهي سجل إلكتروني يذكر فيه المفتاح العام على أنه موضوع الشهادة،** ويؤكد أن الموقع المعرف عنه في الشهادة يحمل المفتاح الخاص ، وهكذا يمكن للمستلم أن يستخدم المفتاح العام المذكور في الشهادة ، وهذا يؤدي إلى الثقة والأمان بين المرسل والمستقبل

استخدامات الشهادات الرقمية:

تستخدم الشهادات الرقمية في المنشآت الكبيرة ، التي تتضمن إرسال وثائق رسمية داخل المنشأة وخارجها، حيث تكون سلطات المصادقة منظمة في هيكل هرمي شبيه بالشجرة، حيث يتم وضع المفتاح العام والتعريف بكل عميل في شهادة رقمية وتقوم سلطة المصادقة بالتوقيع رقمياً عليها وتكون الشهادات متوافرة لكل الموظفين ، وتقوم سلطة المصادقة التي على رأس الهرم بتوقيع شهادات سلطات الصادقة التابعة لها وهكذا.

الجدار الناري هو حاجز بين الحاسب الآلي والعالم الخارجي وفي أقله سوف يقوم بتصفية البيانات القادمة من الخارج بناءا على مقاييس معينة مثل حجم البيانات ورقم الآيبي *IP Address* والبروتوكول الذي تم استعماله والمنفذ الذي تستخدمه البيانات للدخول إلى الحاسب الآلي

التشفير (Encryption)

ما هو التشفير أو التعمية (Cryptography) :

التشفير هو العلم الذي يستخدم الرياضيات للتشفير وفك تشفير البيانات. التشفير يُمكّنُك من تخزين المعلومات الحساسة أو نقلها عبر الشبكات غير الآمنة- مثل الإنترنت- وعليه لا يمكن قراءتها من قبل أي شخص ما عدا الشخص المرسل لـه. وحيث أن التشفير هو العلم المستخدم لحفظ أمن وسرية المعلومات، فإن تحليل وفك التشفير (**Cryptanalysis**) هو علم لكسر و خرق الاتصالات الآمنة. أي باختصار:

التشفير هو تحويل المعلومات المهمة أو التي لا تريد أن يطلع عليها أحد إلى نص مخفي أي لا يمكن فهمه.

أهداف التشفير:

يوجد أربعة أهداف رئيسية وراء استخدام علم التشفير وهي كالتالي:

١. **السرية أو الخصوصية (Confidentiality) :**
هي خدمة تستخدم لحفظ محتوى المعلومات من جميع الأشخاص ما عدا الذي قد صرح لهم الإطلاع عليها.

٢.**تكامل البيانات (Integrity) :**
وهي خدمة تستخدم لحفظ المعلومات من التغيير (حذف أو إضافة أو تعديل) من قبل الأشخاص الغير مصرح لهم بذلك.

٣.**إثبات الهوية (Authentication) :**
وهي خدمة تستخدم لإثبات هوية التعامل مع البيانات (المصرح لهم).

٤.**عدم الجحود (Non-repudiation) :**

وهي خدمة تستخدم لمنع الشخص من إنكاره القيام بعمل ما.
إذاً الهدف الأساسي من التشفير هو توفير هذه الخدمات للأشخاص ليتم الحفاظ على أمن معلوماتهم.

أنواع التشفير :

حالياً يوجد نوعان من التشفير وهما كالتالي :

١. **التشفير التقليدي**. (**Conventional Cryptography**).
٢. **تشفير المفتاح العام**. (**Public Key Cryptography**)

عملية التشفير: هي عملية تغيير المعلومة إلى شكل آخر غير مفهوم، حيث يمكن استخدام التشفير عند إرسال معلومات أو رسائل من شخص إلى آخر بحيث يخشى وقوع المعلومات في يد طرف ثالث لا ينبغي أن يطلع عليها، ثم العبث بها. وتعتمد قوة هذه المفاتيح على صيغ رياضية معقدة (خوارزميات) وعلى طول المفتاح مقدراً بالبت (Bit).

- أهمية التشفير:

- تنبع أهمية التشفير من مفهومها، يمكن استخدام التشفير في التوقيع الإلكتروني أو في تشفير المكالمات الهاتفية أو في المراسلات الحساسة داخل أو خارج المنشآت ، حيث معظم تطبيقات التشفير تستخدم في النواحي الأمنية والعسكرية.

- هدف التشفير هو ليس إخفاء الرسالة بل إخفاء معنى الرسالة ، حيث يتم استخدام خوارزميات Algorithms متفق عليها من قبل المرسل والمستقبل لترميز الرسالة وتسمى (Encryption) ،

أساسيات تشفير البيانات

١)
الإزاحة (Transposition) .
٢) تحديد سايفر البديل (Substitution Cipher).
- التوسيع
- الضغط

- تقسيم الكتل

استبدال الحروف المتعدد (Multiple Substitution Cipher).

مثال :

ع = س + ١٣ أي كلما أعطينا قيمة لي س نجد قيمة ع

قيم س	1	2	3	4
قيم ع	14	15	16	17

السؤال المطروح ماهي فائدة المعادلة في التشفير ...؟؟

الجواب : تخيل أن الحروف هي عبارة عن أرقام هدا ليس خيال بل حقيقة عند جهاز الكمبيوتر.

مثلا :

1= A	8= H	15= O	22= V
2= B	9= I	16= P	23= W
3= C	10= J	17= Q	24= X
4= D	11= K	18= R	25= Y
5= E	12= L	19= S	26= Z
6= F	13= M	20= T	
7= G	14= N	21= U	

مجال الحروف [Z....A] ومجال الأرقام [26....1]

الآن نعود إلى المعادلة السابقة :

ع = س + ١٣

قيم س	A	B	C	D
قيم ع	N	O	P	Q

الشرح : أي عندما أعطينا لي س القيمة A تحصلنا على قيمة ع وهي N

س : يمثل الحرف الأصلي

ع : يمثل الحرف المشفر

أي الحرف A يصبح N بعد عملية التشفير

ع = س + ١٣

13 + A = N

١٣ + ١ =١٤

اضمن أن الجميع فهم فائدة المعادلة في التشفير :

ألان نريد تشفير كلمة ABDELMALEK باستعمال المعادلة السابقة :

عندما نعطي لي س الحرف A نجد أن ع تصبح قيمتها N

عندما نعطي لي س الحرف B نجد أن ع تصبح قيمتها O

عندما نعطي لي س الحرف D نجد أن ع تصبح قيمتها Q

عندما نعطي لي س الحرف E نجد أن ع تصبح قيمتها R

عندما نعطي لي س الحرف L نجد أن ع تصبح قيمتها Y

عندما نعطي لي س الحرف M نجد أن ع تصبح قيمتها Z

عندما نعطي لي س الحرف A نجد أن ع تصبح قيمتها N

عندما نعطي لي س الحرف L نجد أن ع تصبح قيمتها Y

عندما نعطي لي س الحرف E نجد أن ع تصبح قيمتها R

عندما نعطي لي س الحرف K نجد أن ع تصبح قيمتها X

أي عند تشفير كلمة ABDELMALEK بمعادلة السابقة نجد NOQRYZNYRX

ملاحظة هامة

فك التشفير يكون بإدخال النص المشفر إلى المعادلة س = ع – ١٣

وعملياتا التشفير وفك التشفير كالتالي:

- طريقة Caesar
- طريقة Monoalphabetic
- طريقة plyfair
- طريقة vigenere

١. طريقة Caesar:

تعتبر الطريقة السابق ذكرها وإعطاء مثال عليها هي من أبسط طرق التشفير والمسماه بطريقة Caesar (قيصر)

عيوب هذه الطريقة:

1.لو نظرنا إلى هذه الطريقة من جانب أمني لرأينا أنها سهلة الكسر لدينا 26 احتمالية (عدد الحروف الانجليزية) أو بالأصح 25 احتمالية لأن الحرف لا يساوي نفسه .
ولنأخذ على سبيل المثال الحرف A لكسره نجرب كل الحروف ماعدا الحرف نفسه وهذه طريقة معروفه لكسر التشفير وتسمى البحث الشامل Brute force Search .

2. لا يوجد مفتاح Key، وسوف نرى في الطرق الأخرى فائدة المفتاح أي أن هذه الطريقة ثابتة.(نقوم بإرسال النص المشفر فقط).

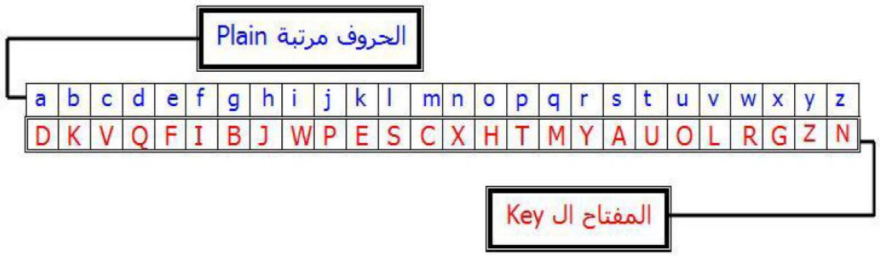
٢ . طريقة Monoalphabetic

• طريقة Monoalphabetic :

فكرة هذه الطريقة أن يكون لدينا مفتاح Key ونقوم بتبديل النص الأصلي بالمفتاح Key.وهي أفضل من طريقة Caesar لأن المفتاح متغير :

الشرح:

- لدينا الأحرف من a-z:



سؤال: لماذا قمنا باختيار هذا المفتاح (DKVQFIBJWPESCXHTMYAUOLRGZN) هل له قاعدة ؟
الجواب: نحاول أن نختار المفتاح عشوائيا، و ليس له قاعدة قمنا باختياره عشوائيا ونحاول أن نوزع الحروف بشكل متباعد.

والآن وبعد أن وضعنا المفتاح ال Key ونريد تشفير رسالتنا بذلك المفتاح ولنفرض أن الرسالة plaintext التي لدينا هي : "C for Arab" .

ولتشفيرها : نبدأ بحرف C ننظر إلى الحروف Plain ونبحث عن الC و نرى ماذا يقابله (في الجدول السابق) ، ويقابله حرف الـV . ثم نأتي للحرف التالي وهو ال f وننظر لمقابلة في الجدول وهو حرف الـ I .... وهكذا إلى أن نحصل على النص المشفر Cipher text :

"V IHY DYDK"

طريقة plyfair

• طريقة Playfair :

أخترع هذه الطريقة العالم Charles Wheatstone في عام 1854م ولكنها سميت بعد ذلك بأسم صديقة Baron Playfair، وكانت هذه الطريقة تستخدم لعدة سنين بين(US & British) في الحرب العالمية الأولى (WW1).

وفكرة هذه الطريقة أن يكون لدينا مصفوفة من نوع x55، أي تكون المصفوفة مكونة من 25 عنصر ، ولكن الحروف الانجليزية تساوي 26 !!!

ولهذا السبب جعل Charles حرفي الـ I و J متساويان، أي(I,J=>I).

الشرح:

1. نختار مفتاح Key ولنفترض "COMPUTER".

2. نقوم بتعبئة المصفوفة ونبدأ بالمفتاح Key أولا .

3. بعد ذلك نكتب الحروف بعد المفتاح Key.

4. نبدأ بحرف ال A بعد كتابة المفتاح Key وبعده ال B ثم حرف ال C ولكن حرف ال C موجود في ال key ولذلك لا نكتب ال C بل نذهب إلى الحرف الذي بعده وهكذا إلى أن نصل إلى ال Z.

1. نأخذ حرفين في كل مرة وإذا تشابه الحرفين نضع 'X' ، مثلا "balloon" تصبح كالتالي "ba lx lo on".

2. إذا جاء حرفين في نفس الصف مثلا "AR" (في الجدول السابق) نبدله مع الأيمن منه إلى "RM" وهنا وقعت في طرف الجدول أخذنا "R" ونرجع إلى بداية الصف ونأخذ ال "M". ولو جاء في الوسط مثلا : "ON" تصبح "NA" .

3. إذا جاء حرفين في نفس العمود ، نبدله مع الأسفل منه ، مثال "MU" يشفر إلى "CM" .

4. معادا ذلك (أي إذا وقعت الحروف غير المكان السابق) كل حرف يبدل مع الحرف الواقع في نفس العمود وعلى صف الحرف الأخر،مثال "HS" يشفر إلى "EA" , "BP" يشفر إلى "MZ", "IM" إلى "RU" وهكذا ..

ولفك التشفير نقوم بعكس الخطوات السابقة.

ونصبح المصفوفة Matrix كما يلي :

C	O	M	P	U
T	E	R	A	B
D	F	G	H	I
K	L	N	Q	S
V	W	X	Y	Z

مفهوم المصنف الرقمي

قد تعاملت النظم القانونية مع مصنفات المعلوماتية بوصفها تنتمي إلى بيئة الكمبيوتر، وقد شملت هذه المصنفات ابتداء من منتصف السبعينات وحتى وقتنا الحاضر ثلاثة أنواع من المصنفات

١. **البرمجيات ، وقواعد البيانات والدوائر المتكاملة.**

هي مصنفات جاءت وليدة علوم الحوسبة ، ومع ظهور شبكات المعلومات ، ظهرت أنماط جديدة من المصنفات تثير مسألة الحاجة إلى الحماية القانونية وهي:

٢. **أسماء النطاقات أو الميادين أو المواقع على الشبكة Domain Names ، وعناوين البريد الالكتروني ، وقواعد البيانات على الخط التي تضمها مواقع الانترنت** ، وهو تطور لمفهوم قواعد البيانات السائدة قبل انتشار الشبكات التي كان مفهوما أنها مخزنة داخل النظام أو تنقل على واسطة مادية تحتويها . و محتوى موقع الانترنت، من نصوص ورسوم وأصوات) يطلق على المؤثرات الصوتية والحركية لوسائط المتعددة.(Multimedia –

وترى هذه النظم القانونية، أن المصنف الرقمي يشمل كافة المصنفات المتقدمة ، فبرنامج الكمبيوتر من حيث البناء والأداء مصنف رقمي ، وقاعدة البيانات من حيث آلية ترتيبها وتبويبها، والأوامر التي تتحكم بذلك تنتمي إلى البيئة الرقمية ، وذات القول يرد بالنسبة لكافة العناصر المتقدمة ، وبالتالي نرى أن أي مصنف إبداعي عقلي، ينتمي إلى بيئة تقنية المعلومات يعد مصنفا رقميا.

٣. وتتمثل المصنفات الرقمية ببرامج الحاسوب (الكمبيوتر) وبقواعد البيانات وبالدوائر المتكاملة ، أما في بيئة الانترنت فتتمثل بأسماء نطاقات أو مواقع الانترنت ، وبمحتوى المواقع من مواد النشر الالكتروني نصوصا وصورا ومواد سمعية ومرئية (الوسائط المتعددة).

حماية الملكية الفكرية:

تشير الملكية الفكرية إلى إبداعات العقل من اختراعات، ومصنفات أدبية، وفنية، وتصاميم وشعارات وأسماء وصور مستخدمة في التجارة،والملكية الفكرية محمية قانونا، بحقوق منها مثلا: البراءات، وحق المؤلف والعلامات التجارية، التي تمكّن الأشخاص من كسب الاعتراف، أو فائدة مالية من ابتكارهم أو اختراعهم، ويرمي نظام الملكية الفكرية، من خلال إرساء توازن سليم بين مصالح المبتكرين ومصالح الجمهور العام، إلى إتاحة بيئة تساعد على ازدهار الإبداع والابتكار.

المنظمة العالمية للملكية الفكرية . WIPO

الملكية الفكرية في العصر الرقمي

من أهم المعلومات عندما تعمل عبر الإنترنت هي ما يلي:

حق المؤلف مصطلح قانوني يصف الحقوق الممنوحة للمبدعين فيما يخص مصنفاتهم الأدبية والفنية. ويغطي حق المؤلف طائفة مصنفات واسعة، من الكتب والموسيقى واللوحات الزيتية والمنحوتات والأفلام إلى البرامج الحاسوبية وقواعد البيانات والإعلانات والخرائط الجغرافية والرسوم التقنية.

ما معنى "ترخيص" المصنفات وكيف يمكنك القيام بذلك؟

انتج مصنفاً أو شارك في إنتاجه ولك حقوق عليه. ويمكنك، بصفتك أحد أصحاب حق المؤلف، أن تقرر السماح للغير باستخدام هذا المصنف أو الانتفاع به. وتُبرم هذه الترتيبات عادة في إطار ترخيص.

وإذا كنت تود ترخيص مصنفك لهيئة بث أو ناشر موسيقى أو حانة أو ملهى ليلي، فعليك الانضمام إلى: منظمة إدارة جماعية. إذ تعمل هذه المنظمات على رصد استخدام مصنفك ومصنفات المبدعين والناشرين الآخرين، وتتولى مسؤولية التفاوض على التراخيص مع المستخدمين وتحصيل الإتاوات عن استخدامها. وتعدُّ منظمات الإدارة الجماعية مفيدة بخاصة للموسيقيين والمؤلفين في الحالات التي يستخدم فيها العديد من الناس مصنفاً واحداً عدة مرات.

إذا وجدت قطعة موسيقية أو مصنفاً فنياً أعجبني على الإنترنت، فهل يجب الحصول على إذن لاستخدامه؟

تتمتع عادة المصنفات المنشورة على الإنترنت، سواء على صفحة شبكية أم على منصة تواصل اجتماعي، بالحماية بموجب حق المؤلف و/أو الحقوق المجاورة؛ فيتعين عليك عامةً أن تحصل على إذن صاحب الحق قبل استخدام مصنفه.

أما إذا كان المصنف مدرجاً في الملك العام – أي بعد انقضاء مدة الحماية بموجب حق المؤلف – فلك مطلق الحرية في استخدامه. ولكن تأكد أولاً من عدم خضوع هذا المصنف لأي حقوق أخرى.

فعلى سبيل المثال، لوحة موناليزا لدا فينشي مدرجة في الملك العالم، ولكن إذا وجدت صورة لهذه اللوحة على الإنترنت، فقد يمتلك المصور حقوقاً على هذه الصورة؛ وعليه يتعين عليك أن تتصل بالمصور للحصول على إذنه قبل استخدامها.

وإذا كنت صاحب شركة صغيرة وأردت تحميل واستخدام تسجيل أو أي مصنف آخر محمي بموجب حق المؤلف في إطار حملة إعلامية مثلاً، فيجب عليك أن تحصل على إذن صاحب أو أصحاب الحقوق قبل القيام بذلك.

.

هل أسماء الأغاني محمية بموجب حق المؤلف؟

من غير المرجح أن تستوفي أسماء الأغاني شروط الإبداع والأصالة اللازمة للحصول على الحماية بموجب حق المؤلف. أما العناوين والشعارات الرمزية والكتابية فتُحمى غالباً بموجب العلامات التجارية.

هل يمكنني حماية موقعي الإلكتروني بموجب حق المؤلف؟

تجوز الحماية بموجب حق المؤلف لأي مضمون أصلي – من نص أو رسم أو صورة أو مقطع مصور – تنتجه وتنشره على موقعك الإلكتروني. وعليه، ينبغي زيارة الموقع الإلكترون(**للمكتب الوطني لحق المؤلف**) في بلدك للاطلاع على الإجراءات المحددة التي تتيح لك تسجيل موقعك الإلكتروني طوعاً.

هل اسم نطاق موقعي الإلكتروني محمي بموجب حق المؤلف؟

لا يشمل قانون حق المؤلف أسماء النطاقات. وإنما تتولى شركة الإنترنت للأسماء والأرقام المخصصة (الآيكان) وضع وإدارة القواعد التي تنظم استخدام أسماء النطاقات و/أو انتهاكها. ويعدُّ مركز الويبو للتحكيم والوساطة مزوداً رائداً **لخدمات تسوية المنازعات** في إطار سياسة الآيكان الموحدة لتسوية منازعات أسماء الحقول.

هل يمكنني حماية برمجية أو تطبيق محمول؟

إن البرمجيات الحاسوبية وغيرها من البرمجيات مثل التطبيقات المحمولة (مثل واتس آب وكاندي كراش) محمية بوصفها مصنفات أدبية في إطار حق المؤلف. وعليه، فإنها **تُمنح الحماية تلقائياً لدى إصدارها وليس من الإلزامي تسجيلها رسمياً.** أما في بعض البلدان، فقد تختلف إجراءات التسجيل الطوعي للبرمجيات عن تسجيل المصنفات الإبداعية الأخرى.

لدي حساب على تويتر. فهل تغريداتي مؤهلة للحماية بموجب حق المؤلف؟

إن طول التغريدة محدود بمئة وأربعين رمزاً؛ وعليه فمن غير المرجح أن تستوفي التغريدات شرط الإبداع اللازم للحصول على الحماية بموجب حق المؤلف؛ ولكن توجد استثناءات. ويرجى مراعاة **أن الصور المدرجة في تغريداتك قد تكون محمية بموجب حق المؤلف.**

ما هي إدارة الحقوق الرقمية ؟

يستخدم أصحاب الحقوق مجموعة من التكنولوجيات الرقمية لحماية مصنفاتهم من الانتهاك. إذ تحمي هذه التكنولوجيات المصنفات من أي تغيير غير مصرح به ، وقد تفرض قيوداً على عدد النسخ التي يمكن إصدارها، وعلى نوع أجهزة عرض المصنف. ووفقاً للقانون الدولي، لا يجوز إزالة أو تغيير أو تجاوز حماية إدارة الحقوق الرقمية.

ما هي الإجراءات العملية التي يجب أن اتخذها لنشر مصنفي عبر الإنترنت؟

يمكنك، كمؤلف، أن تتيح مصنفاتك للغير من خلال نشرها عبر الإنترنت مع الحفاظ على حقوقك عليها. ويمكنك الإشارة إلى ذلك:

١- **بوضع رمز (@) بجوار اسمك وسنة إنتاج المصنف.** وقد تود أيضاً :

٢ - **إدراج قسم "شروط الاستخدام" في موقعك الإلكتروني تحدد فيه طرائق الاستخدام المسموح بها.** فيمكنك مثلاً أن تسمح للزائرين بطباعة نسخة من أعمالك الشعرية أو رسوماتك لاستخدامهم الشخصي مع حظر بيع هذه الأعمال دون الحصول على موافقتك المسبقة.

وعندما ترفع أي مادة جديدة وأصلية على الموقع الإلكتروني، :

٣ - لا تنسى الاحتفاظ بنسخة مطبوعة تظهر تاريخ النشر في سجلاتك لإثبات أنك أول شخص رفع هذا المضمون على الإنترنت عند الاقتضاء.

ماذا عن حق المؤلف وشبكات التواصل الاجتماعي؟

عندما تتسجل لاستخدام شبكة اجتماعية أو أي منصة رقمية أخرى، فإنك ملزم بشروط وأحكام الاستخدام. وينطوي ذلك غالباً على منح المنصة أو الخدمة ترخيص غير حصري باستخدام مضامينك وإن احتفظت ببعض الحقوق على المضامين التي تنشرها. فبعبارة أخرى، يجوز للمنصات، بحسب شروطها، أن تستخدم المضامين التي ألفتها أو تنشرها. انظر مثلاً

تطبيقات وخوارزميات التنقيب في قواعد البيانات في المجال المني والستخباراتي

التقنيات الحديثة للتنقيب في قواعد البيانات

١ . الجار الاقرب

٢ . التجزئة العنقودية

٣ . شجر القرار

٤ . الشبكات العصبيه

٥ . استقراء القاعده

١ . خوارزميه الجار الاقرب

وهي من تقنيات التنقيب عي قواعد البيانات التي تستخدم في المجال الامني للكشف عن مرتكبي جريمة ما وذلك بأن يتم استخدام المعلومات الخاصة بالجرائم الشبيهة التي تم ارتكابه ا س ابقاً بهدف تحديد هوية مرتكب الجريمة الحالية عن طريق تحديد عدد من السجلات التجريبية ثم استخدامها بهدف التنبؤ بالقيمة المطلوبة.

فمثلا إذا كان لدين ا مجموعة من الجرائم ذات طابع الخوارزمية سيكون بأن يتم بحث حالة الجوار لطبيعة معي ن والتي تم ارتكابه ا سابقاً فإن استخدام هذه المجرمين الذين ارتكبوا تلك الجرائم

١٠الجوار في هذه الحالة هو الصفات السياسية لاولئك المجرمين، كالعم ر والمس توى التعليم ي والوضع أنه يمكن أن يتم اكتشاف صفة أو طبيعة جوار محددة الاجتماعي بالضافة لدوافع ارتكابها، ولكن هذا لينفي ولم تكن بالحس بان بحي ث تؤدي إلى كشف المجرم المطلوب.

٣ . التحليل بالتجزئة العنقودية

هي عملية تجميع السجلات المتشابهة في مجموعات، ويتم ذلك بهدف الاستكشاف عالي المستوى لما يجري داخل

قاعدة البيانات • .ففي مجال المن عادة ما يستخدم التحليل العنقودي في تجزئة الشخاص، أو السكان بشكل عام، إلى مجموعات يمكن دراستها بشكل مباشر ومحدد • .كذل ك يمكن استخدامها ف ي تجزئة مجموعة من الشخاص المرتبطين بقضية التي يمكن أن يستفاد منها في فك رموز معين ة بهدف استكشاف الروابط والفوارق القضية.

•وبشكل عام، تهدف التجزئة العنقودية إلى وضع العنا ر المتجانسة في مجموعات منفصلة • .ويتم ضم أي عنصر في مجموعة بناءا على أن يكون هذا العنصر مائلً للتشابه بعنصر منها أكثر من أن يكون شبيهاً لعنصر من مجموعة أخرى.

٣ . شجر القرار

شجرة القرار هي نموذج استكشافي يظهر على شكل شجرة. ويمثل كل فرع من فروعها سؤالً تص نيفياً وتمثل أوراقها أجزاءاً من قاعدة البيانات تنتمي للتصنيفات التي تم بنائها.

استخدام شجرة القرار فى التنبؤ

ومن المهم جداً عن بناء خوارزمية شجرة القرار أ ن يؤخذ بعين الأعتبار أن تكون قابلة للتطبيق بقدر المكان وبشك ل مثال ي عل ى ك ل البيانات المتوفرة • .القاعدة الس اسية في بناء شجرة القرار هي إيجاد أفضل سؤال عند كل فرع م ن فروع الشجرة بحي ث يقسم هذا السؤال ال بيانات إل ى قسمين، القسم الأول منها ينطبق عليهم السؤال والقسم الثان يل ينطبق

الفرق بين شجر ة القرار والتجزئة العنقودية

•تهدف تقنية شجرة القرار إلى تقسيم قاعدة البيانات بهدف معي نسبق وأن تم تحديده • .قد تكون شجرة القرار أكثر تعقيداً من التجزئة العنقودي ة ولكنه ا تؤدي إلى نتائج يمكن إظهاره بشك لمبسط وفائدة عالية المستوى.

٤ . الشبكات العصبية

•تعتبر الشبكات العصبية هي وأشجار القرار من أه م تقنيات التنقيب ف ي البيانات، نظراً للنتائج الدقيق ة التي يتم التوصل إليها باستخدام هذه الخوارزميات ولمكانية تطبيقهم ا في حل العديد من المشاكل وبكاف ة الأنواع، هذا بالرغم من صعوبتهما والتي أدت لعدم انتشار بشكل واسع لهما.

• خوارزمية الشبكة العصبية تشبه في تركيبتها تركيب مخ الانسان ، فهي تعمل بنفس الطريقة كم يعمل المخ ف ي نقل ومعالج ة المعلومات والتوصل إلى الاستنتاجات واكتشاف النماط والتنبؤات