قوانين وأخلاقيات الحاسوب

Computer ethics and law

م. عمرو أحمد الهمزة

العقود (Contracts)

العقد هو : اتفاق مكتوب بين فريقين يكون العقد بينهما ساريا إذا كان صالحا بموجب قانون مكان إقامة الفريق الذي يرغب بتنفيذ العقد.

العقود الإلكترونية: هي العقود التي يتم إبرامها عبر شبكة الإنترنت.

أو : هو خلاصة التجارة الإلكترونية التي تعرف على انها انشطة يتم تنفيذها عبر شكل من اشكال الشبكة الالكترونية كالانترنت او الشبكات المغلقة المستعملة في تبادل البيانات الالكترونية مهما كانت تلك الأنشطة.

عقود استخدام البرامج (Software License Agreement): عقود **Shrink warp**.

قبل أن يكون هناك صفحات إنترنت **web pages** ،كان هناك البرمجيات ، وتماما كما اصبح لصفحات الويب ، عقود ويب (**web wrap agreements**) فقد كان للبرمجيات الجاهزة (**software**) عقودا مشابهة سميت (**shrink wrap agreement**) وعقود (**shrink wrap agreement**) ، هي اتفاقيات الرخص (النقل) الرخص التي ترافق البرامج ، **وهي على شكلين:**

١) الأول التي تظهر على الشاشة أثناء عملية تنزيل البرنامج على الجهاز ، وعادة لا يقرؤها المستخدم ، بل يكتفي بمجرد الضغط (أنا اقبل **I agree**) أو (**I accept**) ، إنها العقد الإلكتروني الذي يوجد في واجهة أي برنامج ويسبق عملية التنزيل (**Install**) .

٢) الصورة الثانية ، وهي السبب في أخذها هذا الاسم (الذي يعني رخصة فض العبوة) فإنها الرخص التي تكون مع حزمة البرنامج المعروضة للبيع في محلات بيع البرمجيات ، وعادة تظهر هذه الرخصة تحت الغلاف البلاستيكي على الحزمة وعادة تبدا بعبارة (بمجرد فض هذه العبوة فانك توافق على الشروط الواردة في الرخصة) ومن هنا شاع تعبير (رخصة فض العبوة) .

أنواع العقود الإلكترونية:

١) عقود تتم بمجرد الضغط على ايقونة (مربع/ مستطيل) وتسمى (**Icon Clicking**).

٢) عقود تتم بطباعة العبارة التي تفيد القبول (**Click & Type**).

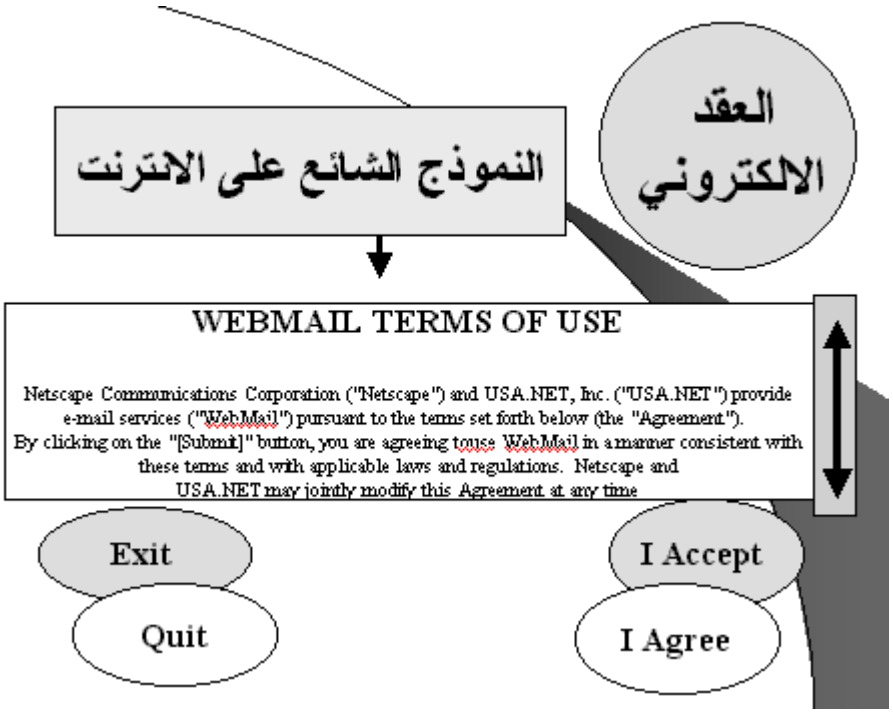
الهدف من عقد التراخيص:

١) منح المستخدم إذناً باستخدام البرنامج إستخداماً قانونياً.

٢) وضع ضوابط وشروط وحدود مدة الإستخدم.

٣) تحديد المقابل المادي للترخيص بالاستعمال.

نموذج ايضاحي للعقد الالكتروني على الانترنت



شروط صحة القعد الإلكتروني:

١) أن يكون متاحاً وميسراً قراءة الشروط والإطلاع عليها.

٢) توفر خيارات القبول والرفض.

٣) اعتماد وسائل التعريف بشخصية بالمستخدم.

٤) توفر وسائل الأمان.

مزايا العقود الإلكترونية:

١) السرعةيتم تبادل المعلومات بسرعة كبيرة لايمكن ان تقاس بمثيلها (البريد العادي).

٢) الدقة فعند كتابة البيانات الخاصة بالعقود تكون بعد تدقيقها صحيحة ولامجال لاعادة كتابتها مرة اخرى عند الزوم وهذا يقلل الخطا الى درجة كبيرة.

٣) كلفة اقل ان التعامل بين الدول على شبكة الانترنت اقل كلفة بكثير من التعامل الورقي او التعامل عبر الفاكس او البريد العادي.

٤) السرية ان اتمام المعاملات عبر الشبكة الالكترونية تعطي حيزا كبيرا من الامان عنه في طرق الاتصال العادية حيث لامجال لتسرب المعاملات او العقود نظراً لحمايتها.

﴿ التجارة الإلكترونية (Electronic Commerce) ﴾

تمهيد:

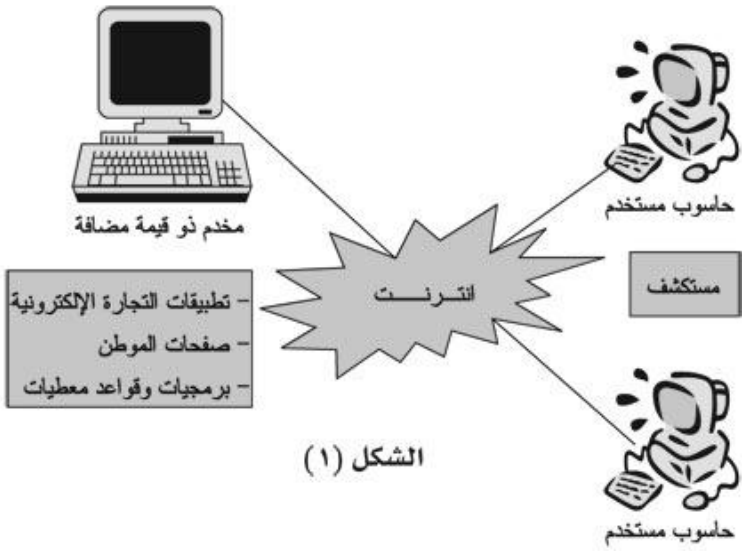
في هذا العصر الرقمي الذي تنتشر فيه الإنترنت انتشاراً هائلاً، شاع مفهوم التجارة الإلكترونية التي تتيح العديد من المزايا، فبالنسبة لرجال الأعمال، أصبح من الممكن تجنب مشقة السفر للقاء شركائهم وعملائهم، وأصبح بمقدورهم الحد من الوقت والمال للترويج لبضائعهم وعرضها في الأسواق. أما بالنسبة للزبائن فليس عليهم التنقل كثيراً للحصول على ما يريدونه، أو الوقوف في طابور طويل، أو حتى استخدام النقود التقليدية، إذ يكفي اقتناء جهاز كمبيوتر، وبرنامج مستعرض للإنترنت، واشتراك بالإنترنت.

ولا تقتصر التجارة الإلكترونية **(E-Commerce)** كما يظن البعض- على عمليات بيع وشراء السِلَع والخدمات عبر الإنترنت، إذ إن التجارة الإلكترونية- منذ انطلاقتها -كانت تتضمَّن دائما معالجة حركات البيع والشراء وإرسال التحويلات المالية عبر شبكة الإنترنت، ولكن التجارة الإلكترونية في حقيقة الأمر تنطوي على ما هو أكثر من ذلك بكثير، فقد توسَّعت حتى أصبحت تشمل عمليات بيع وشراء المعلومات نفسها جنبا إلى جنب مع السِلَع والخدمات، ولا تقف التجارة الإلكترونية عند هذا الحد، إذ إن الآفاق التي تفتحها التجارة الإلكترونية أمام الشركات والمؤسسات والأفراد لا تقف عند حد .

ماهي التجارة الإلكترونية؟

التجارة الإلكترونية هي: نظام يُتيح عبر الإنترنت حركات بيع وشراء السِلع والخدمات والمعلومات.

كما يُتيح أيضا الحركات الإلكترونية التي تدعم توليد العوائد مثل عمليات تعزيز الطلب على تلك السِلع والخدمات والمعلومات، حيث إن التجارة الإلكترونية تُتيح عبر الإنترنت عمليات دعم المبيعات وخدمة العملاء. ويمكن تشبيه التجارة الإلكترونية بسوق إلكتروني يتواصل فيه البائعون (موردون، أو شركات، أو محلات) والوسطاء (السماسرة) والمشترون، وتُقدَّم فيه المنتجات والخدمات في صيغة افتراضية أو رقمية، كما يُدفَع ثمنها بالنقود الإلكترونية والشكل رقم (١) يبين البنية التحتية العامة لتطبيقات التجارة الإلكترونية على الإنترنت.



الشكل (١)

أنواع التجارة الإلكترونية:

١) تجارة إلكترونية من الشركات إلى الزبائن الأفراد **(Business-to-Consumer)** : ويُشار إليها اختصارا بالمصطلح **B2C** ، وهي تمثِّل التبادل التجاري بين الشركات من جهة والزبائن الأفراد من جهة أخرى .

٢) تجارة إلكترونية من الشركات إلى الشركات **(Business-to-Business)** : ويُشار إليها اختصارا بالرمز **B2B** ؛ وهي تمثِّل التبادل التجاري الإلكتروني بين شركة وأخرى والشكل التالي يبين البنية التحتية لتطبيقات التجارة الإلكترونية في مجال الأعمال المهنية **B2B**.

فوائد التجارة الإلكترونية للشركات:

١) **تسويق أكثر فعالية، وأرباح أكثر**: إن اعتماد الشركات على الإنترنت في التسويق، يتيح لها عرض منتجاتها وخدماتها في مختلف أصقاع العالم دون انقطاع –طيلة ساعات اليوم وطيلة أيام السنة– مما يوفِّر لهذه الشركات فرصة أكبر لجني الأرباح، إضافة إلى وصولها إلى المزيد من الزبائن .

٢) **تخفيض مصاريف الشركات** : تُعَدّ عملية إعداد وصيانة مواقع التجارة الإلكترونية على الويب أكثر اقتصادية من بناء أسواق التجزئة أو صيانة المكاتب. ولا تحتاج الشركات إلى الإنفاق الكبير على الأمور الترويجية، أو تركيب تجهيزات باهظة الثمن تُستخدَم في خدمة الزبائن. ولا تبدو هناك حاجة في الشركة لاستخدام عدد كبير من الموظفين للقيام بعمليات الجرد والأعمال الإدارية، إذ توجد قواعد بيانات على الإنترنت تحتفظ بتاريخ عمليات البيع في الشركة وأسماء الزبائن، ويتيح ذلك لشخص بمفرده استرجاع المعلومات الموجودة في قاعدة البيانات لتفحص تواريخ عمليات البيع بسهولة .

٣) **تواصل فعال مع الشركاء والعملاء** : تطوي التجارة الإلكترونية المسافات وتعبر الحدود، مما يوفّر طريقة فعالة لتبادل المعلومات مع الشركاء. وتوفِّر التجارة الإلكترونية فرصة جيدة للشركات للاستفادة من البضائع والخدمات المقدَّمة من الشركات الأخرى (أي الموردين)، فيما يُدعى التجارة الإلكترونية من الشركات إلى الشركات **(Business-to-Business)**.

الفوائد التجارية للزبائن:

١) **توفير الوقت والجهد**: تُفتَح الأسواق الإلكترونية **(e-market)** بشكل دائم (طيلة اليوم ودون أي عطلة)، ولا يحتاج الزبائن للسفر أو الانتظار في طابور لشراء منتج معين، كما ليس عليهم نقل هذا المنتج إلى البيت. ولا يتطلب شراء أحد المنتجات أكثر من النقر على المنتَج، وإدخال بعض المعلومات عن البطاقة الائتمانية. ويوجد بالإضافة إلى البطاقات الائتمانية العديد من أنظمة الدفع الملائمة مثل استخدام النقود الإلكترونية **(E-money)** .

٢) **حرية الاختيار**: توفِّر التجارة الإلكترونية فرصة رائعة لزيارة مختلف أنواع المحلات على الإنترنت، وبالإضافة إلى ذلك، فهي تزوِّد الزبائن بالمعلومات الكاملة عن المنتجات. ويتم كل ذلك بدون أي ضغوط من الباعة .

٣) **خفض الأسعار**: يوجد على الإنترنت العديد من الشركات التي تبيع السلع بأسعار أخفض مقارنة بالمتاجر التقليدية، وذلك لأن التسوق على الإنترنت يوفر الكثير من التكاليف المنفَقة في التسوق العادي، مما يصب في مصلحة الزبائن .

٤) **نيل رضا المستخدم**: توفِّر الإنترنت اتصالات تفاعلية مباشرة، مما يتيح للشركات الموجودة في السوق الإلكتروني **(e-market)** الاستفادة من هذه الميزات للإجابة على استفسارات الزبائن بسرعة، مما يوفِّر خدمات أفضل للزبائن ويستحوذ على رضاهم.

مخاطر التجارة الإلكترونية:

١) سرقة كلمات المرور الخاصة بالمستخدم.
٢) سرقة معلومات بطاقات الإئتمان.
٣) عمليات النصب والإحتيال المختلفة.

طرق الحماية أثناء التعامل مع التجارة الإلكترونية:

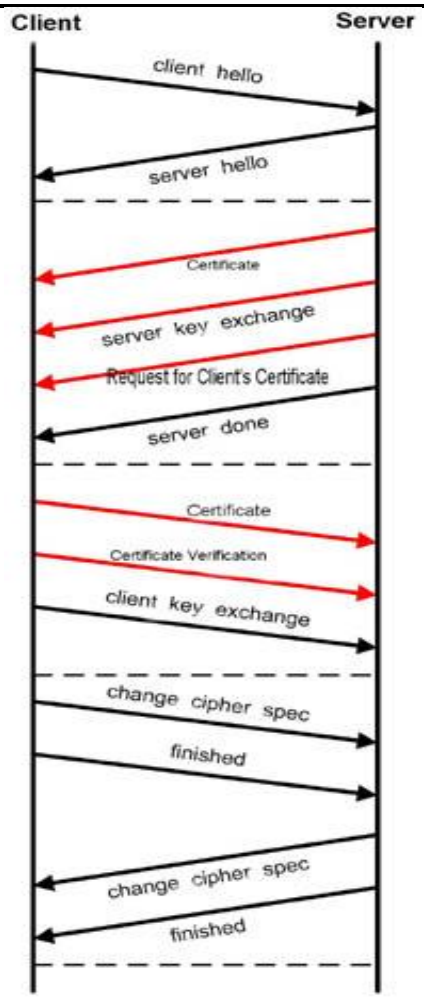
١) تحديث مستعرض الإنترنت.
٢) تعطيل الكوكيز وإعدادات الجافا أو مسحها بعد الإنتهاء من العملية.
٣) تفريغ الذاكرة المؤقتة للمستعرض .
٤) عدم تفعيل خاصية الدخول التلقائي للموقع.

سرية وأمن المعلومات:

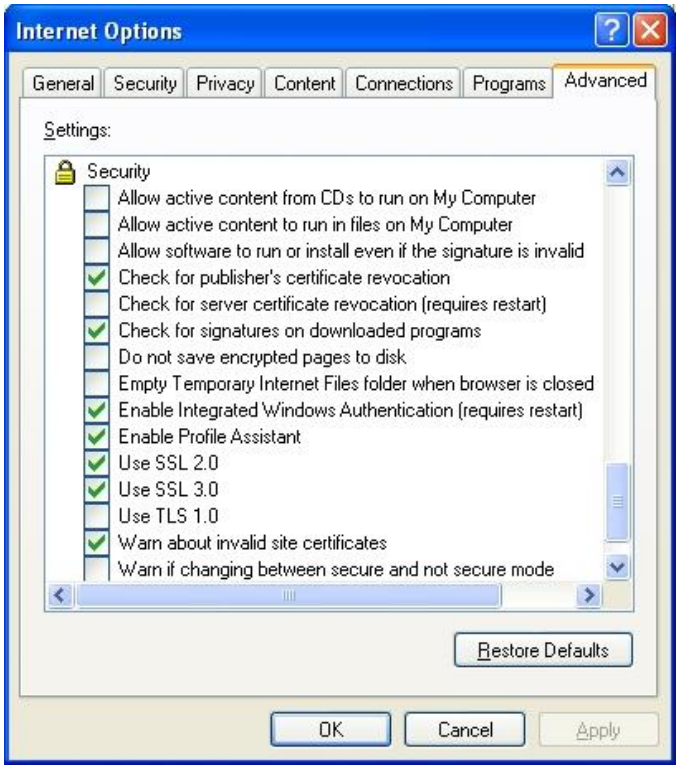
توجد عدة تقنييات لحماية لتعاملات الإلكترونية ومنها:

- **بروتوكول الطبقات الآمنة (SSL:Secure Socket Layers)**: وهي عبارة عن تقنية تستخدم لحماية المواقع ، فعند زيارتك لموقع يستخدم هذه التقنية تلاحظ ظهور أيقونة **(PADLOCK ICON)** في الشريط اسفل المتصفح يختلف شكلها ولونها حسب المتصفح الذي تستخدمه ، فقد تكون عبارة عن علامة X حمراء أو علامة تعجب ! صفراء كما يمكن ان تظهر بأشكال أخرى وتعمل بالشكل التالي:
يقوم بروتوكول **SSL** بإنشاء طبقة إرسال خاصة بدلاً من استخدام بروتوكول**HTTP** ، مما يعني أن بمقدور النظام العمل مع أي من بروتوكولات الانترنيت، بما في ذلك **HTTP** و **FTP** و **Telnet** و **Gopher** يعمل بروتوكول **SSL** من خلال تأسيس قناة اتصال آمنة ومنفصلة لكافة الرسائل التي تستخدم بروتوكول **HTTP** ويتم إعداد هذه القناة الآمنة على المخدم وعلى المتصفح بواسطة برمجيات **SSL** خاصة تتم بعض عمليات تبادل المعلومات المعهودة باستخدام بروتوكولات **SSL** على الشكل التالي:
  - تؤمن تقنية **SSL** التعرف بهوية المتصل بالموقع قبل تبادل أي معلومات بين المتصفح والموقع وخاصة عند وجود الشهادات الرقمية **(Digital Certificates)**.
  - تقوم تقنية **SSL** بتحويل المعلومات إلى صيغ غير مقروءة **(UNREADABLE FORMAT)** تقوم بتشفيرها خلال إنتقالها عبر شبكات غير آمنة مثل الإنترنت.

الشكل التالي يبين كيفية التخاطب بين الـ **server** والـ **client** باستخدام الـ **SSL**



و في هذا الشكل يبين إمكانية تفعيل عمل هذا البروتوكول أو إلغاءه من خلال متصفح الويب



*** ملاحظة / مهمة بروتوكول SSL هي تأمين اتصال آمن فقط، على أنه لايقوم بحماية المعلومات بعد تخزينها على المخدم.**

يوفر **SSL** السمات التالية لضمان سرية المعلومات على الإنترنت:

أ- الثوثيق.

ب- سلامة البيانات.

ت- سرية البيانات عن طريق التشفير.

عملية سرقة معلومات بطاقات الإتمان :

تتم عملية سرقة معلومات بطاقات الإتمان من الزبائن بالطريقة التالية:

لنفرض ان شخصاً يقوم بالاتصال بأحد البنوك التي تستخدم نظام الشهادات الرقمية وتقنية **SSL** ، تتم سرقة المعلومات الخاصة بالزبون عندما يطلب موقع البنك على الانترنت ، يكون أحد ال **(Hacker)** قد قام مسبقاً ببناء موقع مطابق تماماً لموقع البنك ولا يختلف عنه سوى عدم استخدامه لنظام **SSL** ، فبعد كتابة الاسم وكلمة السر والرقم السري ورقم بطاقة الإتمان وعند ضغط الشخص على مفتاح **(Enter)** للقيام بعملية التحويل لا يحصل شئ سوى ظهورهذه الرسالة:

("there was a technical problem with the site and "please try again later")

أي انه يوجد مشكلة في المخدم الذي تتصل به يرجى المحاولة مرة أخرى .

وفي هذه اللحظة يكون ال **(hacker)** قد أخذ المعلومات التي قام بإدخالها هذا الشخص وقام بإستخدامها في موقع البنك الحقيقي لتحويل المبالغ التي يريد دون أن يشعر أحد وباستخدم اسم وكلمة سر وبطاقة إتمان حقيقية .

والفريق بين الموقع الاساسي للبنك وموقع الهاكرز هو أيقونة (**Pad lock Icon**) تظهر في أسفل المتصفح تبين استخدام الموقع لنظام **SSL** ، فإذا لم تظهر الأيقونة ، فهذا يعني أن الموقع مزيف .

- **بروتوكول الحركات المالية الآمنة (SET: Secure Electronic Transaction).**

﴿الشهادات الرقمية (Digital Certificates)﴾

يستخدم الشهادات الرقمية الحكومات والبنوك والشركات الكبرى وهي عبارة عن بروتكول يستطيع تحديد والتعرف على أي شخص أو موقع ضمن نظام متكامل مثل الأنترنت ، والأنترنت هو نظام مفتوح لايمكن التعرف على كل الاشخاص داخل هذا النظام ، لذلك من الضروري على جهات مثل الحكومات والبنوك وغيرها استخدام نظام الشهادات الرقمية للتعرف على الاشخاص بشكل كامل وتأمين اتصال آمن بينها وبين زبائنها عن طرق الإنترنت .

لكل جهه تستخدم بروتكول الشهادات الرقمية **(Digital Certificates)** مفاتيح تشفير خاصة به **(Public Encryption Key)** ، ويكون استخدام نظام الشهادات الرقمية موجود لدى المخدم ويعمل ضمن نظام **SSL** ويسمح المخدم الذي يملك نظام الشهادات الرقمية للزبائن بالتسجيل لديه وتشفير بياناتهم وتأمينها ، حيث تتم عملية الاتصال بهذه المواقع بعد ذلك بشكل آمن دون الخوف على بيانات المستخدمين .

ان استخدام بروتوكول الشهادات الرقمية يسمح لنظام الـ **SSL** بإعطاء الوثوقية للمستخدم ،أي يؤكد له ان الموقع الذي يتصل به هو فعلاً الموقع المقصود وتسمى هذه العملية التي يقوم بها نظام الـ **SSL** لصالح المستخدم بـ **(Authentication)** ، وهذه العملية مهمة جداً بالنسبة للمستخدم خاصة اذا اراد استخدام بطاقة الإتمان خاصته **(Credit Card) .**

﴿التوقيع الرقمي (Digital Signature)﴾

التوقيع الرقمي هو : عبارة عن جزء صغير مشفر من بيانات يضاف الى رسالة إلكترونية كالبريد الإلكتروني أو العقد الإلكتروني.

وثمة خلط كبير في مفهوم التوقيع الرقمي ، حيث يظن البعض انه أرقام ورموز أو صورة للتوقيع العادي . وهو ليس كذلك ، إذ لا تعد صورة التوقيع العادي بواسطة السكانر (الماسحة الضوئية) توقيعا إلكترونيا.

فالتوقيع الإلكتروني على رسالة ما عبارة عن بيانات مجتزأة من الرسالة ذاتها (جزء صغير من البيانات) يجري تشفيره وإرساله مع الرسالة. بحيث يتم التوثق من صحة الرسالة من الشخص عند فك التشفير وانطباق محتوى التوقيع على الرسالة.

ويتم التوقيع الإلكتروني (الرقمي) بواسطة برنامج كمبيوتر خاص لهذه الغاية وباستعماله فان الشخص يكون قد وقع على رسالته تماما كما يوقع ماديا (في عالم الأوراق والوثائق الورقية) ، ويستخدم التوقيع الرقمي على كافة الرسائل الإلكترونية والعقود الإلكترونية .

أما وظيفة التوقيع الرقمي ، فيمكن من الوجهة القانونية تبين وظائف رئيسة لها هي :-

١- التوقيع الرقمي يثبت الشخص الذي وقع الوثيقة.

٢- يحدد التوقيع الرقمي الشيء (الوثيقة) التي تم توقيعها بشكل لا يحتمل التغيير .

هل يحقق التوقيع الرقمي الوظيفة التي يحققها التوقيع العادي ؟

متى ما كان للتوقيع الرقمي القدرة على إثبات الشخص الذي وقع الوثيقة ، فانه يحقق وظيفة التوقيع العادي التقليدي أو المادي (**Traditional Penned Signature**).

والحقيقة أن التوقيع الرقمي يفضل التوقيع العادي من زوايا متعددة !! كيف ؟

ان التوقيع العادي عبارة عن رسم يقوم به الشخص ، انه فنا وليس علما ، ومن هنا يسهل تزويره أو تقليده ، أما التوقيع الرقمي ، فهو من حيث الأصل وفي حدود أمن استخدام برنامجه من قبل صاحب البرنامج ، علم وليس فنا ، وبالتالي يصعب تزويره ، وان كان هذا لا يعني انه يمكن عند اختلال معايير الامن المعلوماتي قد يتم استخدام توقيع الغير الالكتروني ، وتكمن صعوبة (التزوير) في اختيار اجزاء من الوثيقة المرسلة ذاتها ومن ثم تشفير هذه الاجزاء ، وهو ما يقوم به برنامج الكمبيوتر وليس الشخص ، وتحصين التوقيع الرقمي رهن بحماية سرية كلمة السر ومفتاح التشفير .

وفي بيئة التوقيع العادي على الأوراق أو المحررات ، يمكن اقتطاع الوثيقة عن التوقيع الوارد عنها أو اقتطاع جزء منها واستبداله ، في حين ذلك ليس أمرا متاحا في الوثيقة الإلكترونية الموقعة رقميا ، فالتوقيع الرقمي لا يثبت الشخص منظم الوثيقة فقط ، بل يثبت بشكل محدد الوثيقة محل هذا التوقيع ، أنه جزء منها ورموز مقتطعة ومشفرة ، ولدى فك التشفير يتعين أن ينطبق التوقيع ذاته على الوثيقة . إنها مسالة أشبه بنموذج التثقيب الذي يستخدم لمعرفة صحة الإجابات النموذجية في امتحانات الخيارات المتعددة ، انك تضع الكرت المثقب على الإجابة فتحدد فورا الصواب والخطا . وهنا يتعين أن ينطبق النموذج (التوقيع) على الرسالة فإذا تخلف ذلك كانت الوثيقة غير المرسلة وكان ثمة تلاعب بالمحتوى . ومن هنا أيضا يفضل التوقيع الرقمي التوقيع العادي.

﴿قانون حقوق النسخ (Copyright Law)﴾

منظمة الملكية الفكرية العالمية (World Intellectual Property Organization): أو ويبو (**WIPO**)، منظمة دولية تابعة للأمم المتحدة، تعمل من أجل حماية الحقوق الملكية الفردية للأفراد. ظهرت في سنة ١٩٦٧ وتأسست سنة ١٩٧٤. انطلقت بعد انعقاد مؤتمر باريس للملكية الصناعية في ١٨٣٣ بيرن و مؤتمر حماية المصنفات الأدبية والفنية، الموقّع في سنة ١٨٨٦م ، مهمتها فرض الاحترام للخصوصية الفكرية في العالم بأسره، إظافة إلى حماية حقوق الفرد الملكية(صور، أغاني، فنون...). تستمد الويبو نحو ٨٥ بالمائة من ميزانيتها السنوية من أنشطة التسجيل والنشر الدولية المنتفع بها على نطاق واسع. ويتأتى الجزء الباقي من اشتراكات الدول الأعضاء فيها. وتبلغ ميزانية الويبو السنوية ما يناهز ٢٠٠ مليون فرنك سويسري.

الدول الأعضاء:١٧٧ دولة الهيئات الرئيسية صاحبة القرار للدول الأعضاء:الجمعية العامة والمؤتمر ولجنة التنسيق.

عدد موظفي الأمانة:٨٢٣ موظفا من ٨٥ بلدا

ميزانية الويبو:٦٧٨ مليون فرنك سويسري (لسنتي ٢٠٠٢ و٢٠٠٣)

عدد المعاهدات الدولية التي تديرها الويبو:٢٣ معاهدة منها ١٦ معاهدة بشأن الملكية الصناعية و٦ معاهدات بشأن حق المؤلف، بالإضافة إلى اتفاقية إنشاء الويبو.

عدد المنظمات غير الحكومية التي تتمتع بصفة مراقب:١٦١ منظمة.

حقوق الملكية الفكرية:

١. حق المؤلف، حقوق النسخ (**Copyright**) .
٢. براءة الإختراع (**Patents**).

إلى أي فئة تنتمي البرمجيات؟

إن البرمجيات الحاسوبية هي خليط من الفكرة والتعبير، فلا تعبير بدون فكرة. وعليه فالبرمجيات تنتمي إلى فئتَي الحماية المذكورتين. فما يحمي البرمجيات في الوقت الحالي بصفة عامة هو حق المؤلف. ولكن البرمجيات المتطورة وأساليب البرمجة يمكن حيازة براءة اختراع لها، بسبب الابتكار الذي تنطوي عليه.

حقوق النسخ والتأليف (Copyright):

(بالإنجليزية: Copyright، بالفرنسية Droit d'auteur) مجموعة من الحقوق الحصرية (exclusive rights) التي تنظم استعمال النصوص أو أي تعبير عملي (فني ، أدبي ، أكاديمي) عن فكرة أو معلومة ما . أي انه "حقوق نسخ و استخدام" عمل إبداعي جديد .
تشكل هذه الحقوق نوع من الحماية للمبدع ليتقاضى أجرا عن إبداعه لفترة محددة تختلف حسب البلد .
تعمل حقوق المؤلف على حماية البرمجيات، فنسخ كتاب مثلاً يستغرق وقتاً طويلاً، وقد يتعين على المرء أن يطبع كل صفحة على حدة حتى يحصل على نسخة منها، أو على الأقل أن يستخرج نسخة فوتوغرافية أو يمسح كل صفحة. ومن المحتمل أن يستغرق الأمر وقتاً أطول مما يستحق الكتاب، أما عملية نسخ برنامج حاسوبي فقد لا تستغرق سوى ثوانٍ معدودة .

تَسمح براءات الاختراع لشركات البرمجيات الصغيرة بحماية اختراعاتها والاستفادة من رسوم براءة الاختراع المرتفعة. وإذا وَجد مطور ما طريقةً جديدة لتحقيق هدف مشابه، ولكن ببرمجيات مختلفة تماماً، فإنه سيخرق براءة اختراع موجودة. وقد يتوصل مطوران مستقلان فيما بينهما، إلى طريقتين مختلفتين تماماً لتوليد نتيجة واحدة. ولكن إذا حصل أحدهما على براءة اختراع قبل الآخر، فإن عَمَلَ الآخر سيعدّ خرقاً لها.

إذن التعامل مع البرمجيات الحاسوبية ليس بالأمر السهل. فالطباعة على الحاسوب مثلاً تعد ضرباً من الكتابة، ذلك أن هذه الطباعة تتألف في الأصل من كلمات وأرقام. ولكن عندما يعمل الحاسوب على تنفيذها، تتحول وظيفتها إلى وظيفة الاختراع، بحيث تعمل على أداء مهمة بعينها أملاها عليها المستخدم. وطبعاً إعادة اكتشاف أشياء متماثلة هي شيئ شائع كثيراً في وسط آلاف المطورين الذين يعملون في قطاع البرمجيات.

ومثال آخر هو برنامج الرسم الهندسي. فبرنامج الرسم الذي يحتوي على مادة محمية بحقوق المؤلف، هو برنامج له القدرة على كتابة برنامج شبيه ببرنامج شركةٍ أخرى، ما دام رماز البرمجية (software code) مُلك للشركة، وليس مستعاراً من الآخرين. إن هذا الأسلوب يبقي على حالة التنافس في هذا المجال، ويؤدي إلى نشوء برمجيات ذات مستوى أفضل.

قوانين حقوق النسخ والتأليف:

١. **القانون الأنجلو–سكسوني** : مصطلح "حقوق النسخ" يعود في أصله إلى القانون الأنجلو–سكسوني، ولذلك فهو السائد في البلاد الناطقة بالإنجليزية مثل الولايات المتحدة. وهو لا يقيم اعتباراً خاصاً لحقوق المؤلف في (العزو*) أو حقه في عدم تشويه أو تغيير عمله، لأن قانون حقوق النسخ في تلك البلدان نشأ وتطور بضغط من الناشرين وليس من المؤلفين.
٢. **القانوني الأوروبي** : أما ما يقابل حقوق النسخ في التراث القانوني الأوروبي (وخصوصاً الفرنسي)، فيسمى بحقوق التأليف (أو "حقوق المؤلفين" droit d'auteur)، ويعكس حرصاً على حماية حقوق المؤلف في أن ينسب عمله إليه وأن لا يستغل بغير إذنه ("حقوق أخلاقية" Moral Rights).

*__حق العزو__: العزو في قوانين حقوق النشر هو الاعتراف بعمل شخص آخر يستخدم في عمل آخر، والعزو مطلوب قانونيا في أغلب رخص حقوق النشر ومنها رخصة جنو للوثائق الحرة ورخصة التشارك الإبداعي.

إن العزو غالبا هو أول متطلبات الترخيص، فهو يسمح للمؤلف بالحصول على سمعة جيدة مما يعود بالنفع له ويمنع الآخرين من سرقة أعماله. وهو أيضا نوع من احترام صانع العمل وشكر له، لكن يمكن بالحصول على رخصة من صاحب العمل التخلص من هذا المطلب.

لا تطلب قوانين الولايات المتحدة العزو إلا في الأعمال المرئية (الرسوم والصور)، وإنما تترك العزو للمتعاقدين، لكن أغلب القوانين الأوروبية تستوجب العزو في الاعمال المحمية، كما تنصح بعزو العمل حتى لو انتهت فعالية الرخصة كدليل على احترامها.

__معاهدة بيرن__: وهي الاتفاقية الدولية الرئيسية المعنية بحقوق النسخ عام ١٨٨٦م ، قد نشأت في أوروبا ولم تنضم إليها الولايات المتحدة إلا في وقت متأخر، فإن تلك الاتفاقيات تحتم على الدول المتعاهدة احترام حقوق المؤلفين الأخلاقية (مثل حق العزو). وقد رفضت الولايات المتحدة عند انضمامها لمعاهدة بيرن أن تعدل قانون حقوق النسخ لديها ليشمل الحقوق الأخلاقية، بحجة أن تلك الحقوق محمية أصلاً في القانون الأمريكي بطرق أخرى.

__مجال الحماية__ :

كان مفهوم حقوق النسخ أو التأليف في بداياته معنياً بحماية حقوق مؤلفي الأعمال الأدبية والفكرية (أي حقوق الكتّاب)، لكنه الآن يستوعب مجالات أخرى واسعة. فمعظم الدول تعطي حقوق النسخ في الأعمال الموسيقية والدرامية والسينمائية والفوتوغرافية، وكذلك الفنون الجميلة من رسوم ونحوت، والأعمال المعمارية (من الجانب الفني أو الجمالي فقط)، وبرامج الكمبيوتر وتصاميم الأزياء.

من أهم مبادئ حقوق النسخ أنها لا تحمي الأفكار وإنما تحمي تعبير المؤلف عن الأفكار. فمثلاً لو اكتشف أحدهم نظرية فيزيائية، فإنه لا يستطيع أن يخضع النظرية لحقوق النسخ، لكن لو ألف مقالاً أو كتاباً يشرح فيه النظرية، فإن نص المقال أو الكتاب يصبح خاضعاً لحقوق النسخ.

وكذلك لا تحمي حقوق النسخ الجوانب العملية أو العلمية وإنما تحمي الجانب الفني أو الجمالي، أو طريقة التعبير. وتأتي أهمية ذلك في مجال برامج الكمبيوتر والهندسة المعمارية والتصنيع. لو اخترع مهندس جهازاً ما فلا يمكنه يحمي اختراعه بحقوق النسخ (وإنما عليه أن يلجأ إلى براءة الاختراع)، ولكن لو قام بتصنيع

اختراعه بشكل ما، فإن الجوانب الجمالية التي لا علاقة لها بعمل الجهاز قد تخضع لحقوق النسخ. أيضاً لو كتب أحدهم برنامج معالج نصوص، فإن الخوارزمية لا تخضع لحقوق النسخ ولا يمكنه الحصول على حقوق النسخ في برامج معالجات النصوص عموماً، لكن التصميم العام واختيار الألوان وغيرها من الأمور التي تخضع للذوق الشخصي وما شابه قد تصبح محمية بحقوق النسخ.

الحقوق الحصرية:

١. **النسخ (أو حق إعادة الإنتاج)**: وهو لا يقتصر على إعادة نسخ أو إنتاج كامل العمل، وإنما يكفي لخرق هذا الحق نسخ أو اقتباس جزء صغير جداً من العمل في بعض الأحيان في القانون الأمريكي يسمح بنسخ جزء من العمل تحت ضوابط معينة.
٢. **حق الاشتقاق (أو حق التكييف)**: ويعني ذلك إنتاج عمل جديد مبني على العمل.
٣. **حق النشر أو التوزيع**: أي بيع نسخ من العمل بشكل تجاري أو توزيعها على العامة بشكل غير تجاري وهذا هو الغالب على برمجيات الحاسب.
٤. **الحقوق الأخلاقية (أو حقوق التأليف)**: وتعني حق المؤلف في أن يوضع اسمه على العمل، وأن لا ينسب العمل إلى مؤلف آخر، وأن لا يتعرض العمل للتشويه أو التغيير. وهو من العلامات الفارقة بين قوانين الملكية الفكرية الأوروبية ونظيرتها الأمريكية، إذ لا تعترف الحكومة الأمريكية بمثل هذه الحقوق ضمن قانون حقوق النسخ إلا في مجال الصور والرسوم، ولكن القانون الأمريكي يحمي هذه الحقوق من خلال قوانين أخرى كقوانين المنافسة التجارية.

الخرق والتعدي على حقوق النسخ (Infringement):

وعادةً ما يسمى التعدي على حقوق النسخ بالخرق، ويسمى أيضاً التعدي أو التجاوز (**Infringement**) وتتم معالجة الخرق باللجوء إلى القضاء المدني في الأغلب، فإما أن يمنع القضاء الشخص المتعدي من مواصلة المخالفة، أو أن يفرض عليه تعويضات مالية يؤديها إلى صاحب الحقوق، أو الاثنين معاً. في السنين الأخيرة تمت إضافة العقوبات الجنائية إلى قانون حقوق النسخ.

ويشترط في الخرق أو التعدي حصول نوع من النسخ الفعلي، بمعنى لو وصل شخصان إلى نفس التعبير بشكل مستقل، فلن يوجد خرق ما دام ليس هناك ما يثبت أن أحدهما رأى عمل الشخص الآخر. ولكن هذا لا يعني اشتراط النية أو العلم لحدوث التجاوز، فاستعمال نسخة غير مرخصة من برنامج كمبيوتر دون علم بمخالفتها لحقوق النسخ لا يعني بالضرورة حصانة المستخدم من التبعات القانونية ، يوجد في القانون الأمريكي مفهوم "المتعدي البريء،" لكنه لا ينطبق إلا في حال أهمل صاحب العمل وضع إخطار بحقوق النسخ على أعماله.

مدة حقوق النسخ:

١. **الأفراد**: تتفاوت المدة حسب الدولة، ولكن الاتجاه العام هو إلى توحيد المدة من خلال اتفاقيات منظمة التجارة العالمية ، حالياً تنص الاتفاقيات على أن لا تقل مدة الحماية في الدول الأعضاء عن حياة المؤلف وخمسين عاماً بعدها ،وفي بعض الدول تكون مدة الحماية عبارة عن حياة المؤلف وسبعين عاماً بعدها.
٢. **الشركات والأشخاص المجهولين**: تصبح المدة ٩٥ عاماً بعد النشر أو ١٢٠ عاماً بعد الإنتاج، أيهما أقل.

﴿ قوانين براءة الاختراع (Patents Law) ﴾

أتفاقية تريبس (TRIPS):

- تشكل هذه الاتفاقية جزءاً من اتفاقيات منظمة التجارة العالمية (**WTO :World Trade Organization**).
- يمثل التوقيع على هذه الاتفاقية شرطاً من شروط الانضمام الى منظمة التجارة العالمية.
- تضع هذه الاتفاقية المبادئ الأساسية في كل مجالات الملكية الفكرية (حقوق المؤلف والحقوق المجاورة، العلامات التجارية، البراءات) والتي على الدول المشاركة العمل على تطبيقها.
- تترك المنظمة الحرية لكل دولة لإيجاد الطريقة المثلى لتطبيق هذه المعاهدة على أن تقدم الدولة تقارير دورية للجهات المختصة في المنظمة.

تاريخ إنظمام بعض الدول العربية إلى الإتفاقيات العالمية

Countries	Paris Convention	Berne Convention	WIPO Agreement	WTO member
Egypt	1951	1977	1975	1995
Saudi Arabia	2004	2004	1982	2005
Tunisia	1984	1987	1975	1995
Syria	1924	2004	2004	Non member
Sudan	1984	2000	1974	Observing member
UAE	1996	2004	1974	1996
Yemen	2006	Non member	1979	Observing member
Bahrain	1997	1997	1995	1995
Lebanon	1924	1947	1986	2000
Libya	1976	1976	1976	Non member
Jordan	1972	1999	1972	2000
Kuwait	Non member	Non member	1998	1995
Morocco	1917	1917	1971	1995
Oman	1999	1999	1996	2000

تعريف: هي مجموعة من الحقوق الخاصة تمنح بشكل رسمي للمخترع لفترة زمنية محددة.

وظيفة براءة الاختراع: تكفل البراءة لمالكها حماية اختراعه لفترة محدودة.

نوع الحماية التي توفرها براءة الاختراع:

المراد بالحماية بموجب البراءة أن الاختراع لا يمكن استغلاله لأغراض تجارية (صناعته، واستيراده وعرضه للبيع، واستعماله وتخزينه بهدف بيعه أو عرضه للبيع) دون موافقة مالك البراءة، ويجوز لمالك البراءة أن يرخص لغيره في القيام بجميع أعمال الاستغلال أو بعضها.

مدة الحماية: تمتد مدة لحماية لبراءة الإختراع ٢٠عاماً من تاريخ إيداع الطلب

.

من يمنح براءة الاختراع:

١. المكتب الوطني لبراءات الاختراع : وهو خاص بالبلد ذاته ولا يتعداه إلى بلدن أخرى.

٢. أو المكتب الاقليمي الذي يعمل لصالح عدة دول مثل:

- مكتب براءات الاختراع لمجلس التعاون لدول الخليج العربية.
- المكتب الأوروبي لبراءات الاختراع.
- المنظمة الاقليمية الأفريقية للملكية الصناعية.

موضوع الإختراع: منتج جديد ، طريقة جديدة ، تحسين منتج ، تحسين طريقة.

شروط منح براءة الاختراع:

١. **جديداً** : يكون الاختراع جديدا إذ لم يسبق من حيث التقنية الصناعية السابقة، ويقصد بالتقنية الصناعية السابقة في هذا المجال كل ما تحقق الكشف عنه للجمهور في أي مكان أو زمان بالوصف المكتوب، أو الشفوي، أو بطريق ا لاستعمال، أو بأي وسيلة أخرى من الوسائل التي يتحقق بها العلم بالاختراع، وذلك قبل تاريخ تقديم طلب البراءة أو طلب الأسبقية المدعى بها نظاما.

٢. **ابتكارياً**: يكون الاختراع منطويا على خطوة ابتكاريه إذا لم يتيسر لرجل المهنة العادي التوصل إليه بصورة بديهية نتيجة التقنية الصناعية السابقة المتصلة بطلب البراءة.

٣. **قابل للتطبيق الصناعي أو وينتج عنه حل لمشكلة معينة في مجال التقنية بطريقة عملية.**

﴿الملكية الفكرية وحماية برامجيات الحاسب﴾

تمهيد:

لقد تزايدت أهمية البرمجيات الحاسوبية بدءاً من أول جهاز حاسوب كان معروفاً ، وأدت أجهزة الحاسوب دوراً حيوياً في حياتنا، من تسهيل الرياضيات بواسطة الآلات الحاسبة، إلى تفعيل حركة المال عن طريق أجهزة الصرف الآلي. لكن ومع كل العون الذي أصبح في متناول أيدينا، فإننا لم نفعل ما هو في مصلحة هذه البرامج ولا مؤلفيها، فالبرمجيات تتعرض للهجوم، لأنها ملكية فكرية، وهي ليست كياناً مادياً ملموساً، ولهذا فإنه من السهل نسخها. والبرامج المنسوخة لا تدر أموالاً على مبتكريها، فهم يتقاضون أموالاً أكثر على البرامج غير المنسوخة.

يشمل مصطلح "البرمجيات الحاسوبية" برامج الحاسوب، وقواعد المعطيات، والملفات الحاسوبية، واللوازم التحضيرية للتصميم، وجميع أساليب العمل المخزنة رقمياً التي يمكن النفاذ إليها بواسطة الحاسوب، والوثائق المطبوعة المرافقة مثل أدلة المستخدم.

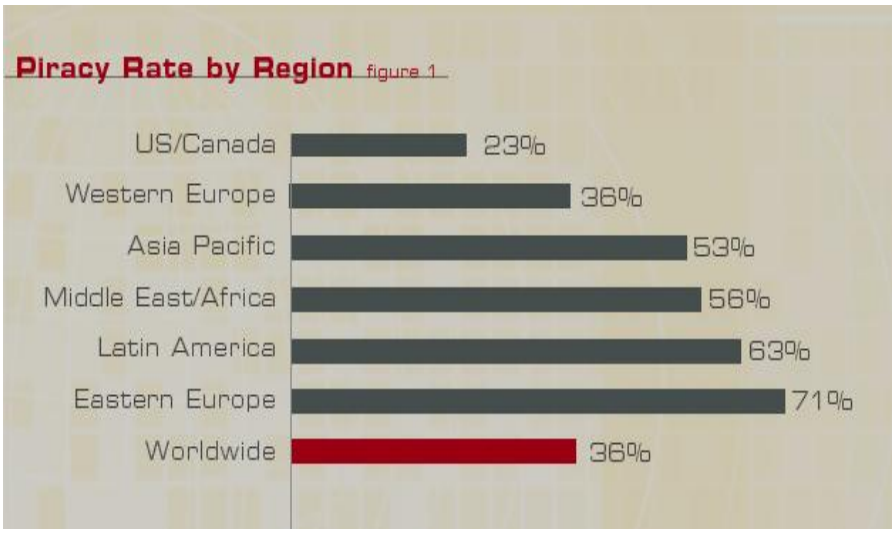
وتمر صناعة البرمجيات بمأزق مزدوج،فمستخدمو الحواسيب يلجؤون إلى قرصنة البرامج بسبب ارتفاع أسعارها، بينما يعمد منتجوها إلى المغالاة في الأسعار لأنها عرضة للقرصنة فقد تجاوزت نسبة النسخ المقرصنة ثلث إجمالي البرامج المثبتة على الحواسيب في العام الماضي.

كذلك لاحظت الدراسة أن البلاد التي يغلب عليها نمط مؤسسات الأعمال الصغيرة ولديها سوق واسعة لمستخدمي الحاسوب الشخصي مرشحة أكثر من غيرها لقرصنة البرمجيات.

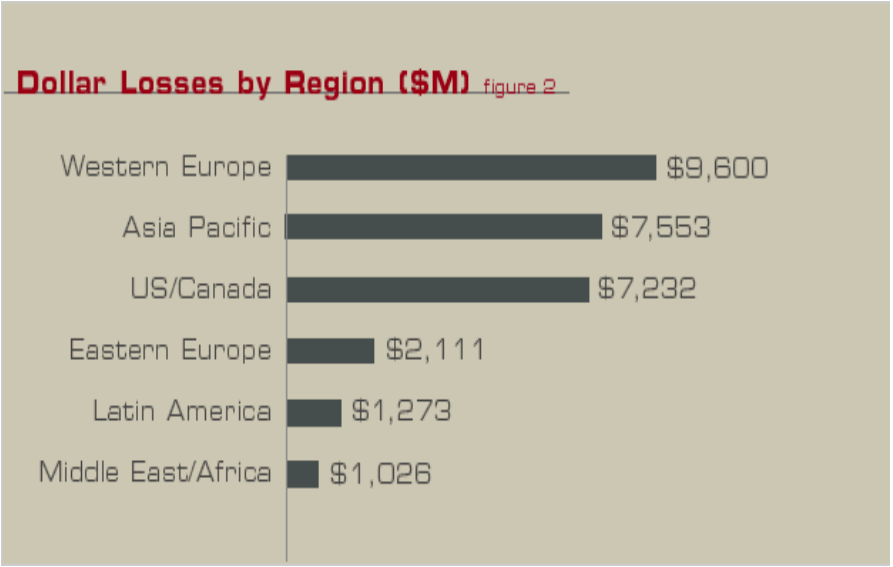
لذلك قامت كل دولة على حدة بتنظيم حماية البرامج طبقاً لقانونها الداخلي ، إلا انه مع بدايةلتسعينات ومع قيام منظمة التجارة العالمية WTO ودخول اتفاقية التريبس حيز التنفيذ فان الاحكام الواردة في الاتفاقية بالنسبة لبرامج الحاسب الآلي تعبر هي الحد الادنى للحماية وقصد نصت الاتفاقية بشكل واضح وصريح على حماية برامج الحاسب سواء في صورة برنمج المصدر أو برنامج الهدف.

في ما يلي رسوم بيانية توضح حجم القرصنة في العالم وكذلك حجم الخسائر المترتبه على ذلك:

الرسم البياني التالي يوضح حجم القرصنة في مختلف أرجاء العالم



الرسم البياني التالي يوضح حجم الخسائر الناتجة من عمليات قرصنة برامج الحاسب الآلي



الـ Program & Software؟

يعد مصطلح البرمجيات **Software** أعم وأشمل من مصطلح البرنامج **Program** إذ يدخل في مفهوم البرمجيات أمور أخرى اضافة إلى البرنامج ذاته وعلى سبيل المثال لا الحصر:

١. المواد التي تسبق إنتاج البرنامج والتي تعبر عن مكوناته مثل الخوارزميات والرسوم والخرائط البيانية.
٢. الوثائق والمستندات والمواد المساندة **Supporting Material** وهي مواد مكتوبه في صورة كتيبات مهمتها شرح البرنامج ويطلق عليها احياناً كتيب الإرشادات **User Manual**.
٣. وصف البرنامج **Program description**.
٤. كافة المواد والوثائق التي تصدر بعد الإنتهاء من تنفيذ البرنامج وبمناسبة الترخيص باستعماله أو استغلاله مثل رخص الاستخدام.

وكل ماسبق محمي الحماية القانونية وفقاً لقوانين حماية الملكية الفكرية وكذلك المعاهدت الدولية.

أما البرنامج فهو: مجموعة من الأوامر والإرشادات التي تحدد للكمبيوتر العمليات التي يقوم بتنفيذها بتسلسل وخطوات محددة.

أو هو : جميع المكونات غير المادية لنظام الحاسب ويشمل برامج النظام وهي اللازمة لتشغيل الحاسب ، وبرامج التطبيقات وهي البرامج الخاصة بالمستخدم.

ومن الناحية القانونية تعددت تعاريف البرنامج ومنها:

تعريف منظمة الملكية الفكرية (WIPO): مجموعة تعليمات يمكنها إذا ما نقلت على ركيزة تستوعبها الآلة أن تساعد في الوصول إلى خاصية ما أو هدف أو نتيجة خاصة بوسطة آلة يمكنها التعامل مع المعلومة.

القانون الأمريكي: مجموعة توجيهات أو تعليمات يمكن للحاسب إستخدامها بشكل مباشر أو غير مباشر بالوصول إلى نتيجة معينة.

القانون الفرنسي: مجموعة الخطوات والإجراءات بالإضافة إلى الوثائق المتعلقة بها التي تهدف إلى تشغيل نظام معالجة البيانات وتوظيفها وفقاً للغرض المنشود.

وهناك الكثير غيرها من التعاريف المتعددة والمختلفة لبرامج الحاسب.

والبرنامج ينقسم إلى قسمين:

١. **البرنامج المصدر(Source Program)**: هو البرنامج المكتوب باللغة التي يفهمها الإنسان أي الكود الذي نكتبة نحن أثناء عملية البرمجة.
٢. **والبرنامج الهدف(Target Or Object Program)**: هو البرنامج المكتوب بلغة الآلة (أي البرنامج التنفيذي الذي نقوم بتثبيته على جهاز الحاسب).

تتفاوت معدلات وأنماط قرصنة البرمجيات من مكان إلى آخر حول العالم تبعا لعوامل مثل:

١. مستويات أسعار البرامج مقارنة مع متوسط الدخل.

٢. توافر البرمجيات المقرصنة.
٣. السمات الثقافية.
٤. قوة قوانين الملكية الفكرية.

أنواع التعدي على البرمجيات:

١. **القرصنة من خلال اعادة البيع (Reseller Piracy)**: يتم التعدي من خلال نسخ البرنامج على أقراص وبيعها مع اطلاع المشتري بأنها نسخ غير أصلية أو نسخ البرنامج على أقراص مع تغليفها وبيعها كنسخ أصلية (التزوير **counterfeit**).
٢. **تحميل البرامج على أجهزة الحاسب (Reseller Piracy – Hard Disk Loading)**: يتم التعدي من خلال تحميل برنامج معين على أجهزة الحاسب المختلفة التي تباع للمشتري. وبالتالي، لا يقوم المشتري بدفع قيمة تلك البرامج أو بدفع ثمن بخس، ويتم بيع الجهاز له متضمناً برامج غير مرخصة)
٣. **التعدي من قبل المستخدم النهائي (End User Piracy)**: شراء نسخة أصلية واحدة من البرنامج واستخدامها على أكثر من حاسب واحد في مؤسسة ما أو نسخها على أقراص تستخدم من قبل العاملين في المؤسسة. حيث أن التعدي هو استخدام البرنامج لعدة مرات دون الحصول على رخصة باستخدامه لأكثر من مرة واحدة.
٤. **التعدي من خلال شبكة الانترنت(Internet Piracy)** : أحدث نوع تعدٍ هو من خلال شبكة الانترنت. تقوم بعض مواقع الويب بإتاحة برامج الحاسب لنسخها دون ترخيص ومن ثم يقوم مستخدم الشبكة بنسخ برامج الحاسب وتحميلها على جهازه. تتجسد خطورة هذا الأسلوب في أن شبكة الإنترنت تتيح لأي شخص الحصول على عدد غير محدود من النسخ وتوزيعها حول العالم خلال دقائق بغاية السهولة والسرعة.
٥. **تعدي المثل للمثل (Peer To Peer Software Provider)**: وهي تستخدم غالباً في الشركات من خلال الشبكة المحلية الخاصة بالشركة حيث يقوم احد الافراد بنسخ برنامج معين على جهازة ثم يقوم بقية أفراد الشبكة باستعمالة او تثبيته على اجهزتم من خلال الشبكة وبدون ترخيص.

مستويات مختلفة لقرصنة البرمجيات:

١. النسخ (**Copyright**).
٢. ستخدام الكتل البرمجية او ما يسمى بالنسخة المصدرية (**Source Copy**).
٣. استخدام التصاميم (**Design Used**).
٤. المفاهيم النظرية أو براءات الإختراع (**Patents**).

آثار القرصنة على صناعة البرمجيات:

١. ضياع فرص ربح
٢. عدم القدرة على استرجاع الاستثمار
٣. عدم وجود حافز لتوسيع الاستثمار
٤. ضعف تقني (هجرة الكوادر – محدودية في التدريب)
٥. ضعف الانتاج الرقمي المحلي .

آثار القرصنة على المستهلك:

١. إهمال الدراسات (كلفة البرمجيات منخفضة مما يسمح بالتجريب) .
٢. عدم الاهتمام بالصيانة (٥٥% من الكلفة الأصلية وليس المقرصنة) .
٣. عدم تحديث النسخة .
٤. عدم الاستفادة من الدعم الفني (محدودية في الاستفادة من المزايا المتقدمة للبرمجيات).

إيجابيات حقوق الملكية الفكرية لبرمجيات الحاسب:

١. تحقيق التقدم.
٢. بناء كوادر وطنية قادرة ومؤهلة.
٣. اثراء المعرفة في المجالات المختلفة.
٤. تشجيع الإبتكار بكل صورة.

سلبيات حقوق الملكية الفكرية على برمجيات الحاسب:

١) **قد تعمل على اعاقة التقدم التقني** : تهدف حقوق المؤلف وبراءات الاختراع إلى حماية الوسائط التي تحميها، ولكن فيما يختص بمجال التقانة، فقد تعمل على إعاقة التقدم التقني. كذلك فإن الأساليب الحالية لحماية البرمجيات من النسخ تعد معوقاً لصناعة البرمجيات. شركة صخر على سبيل المثال كان لها نظام تشغيل خاص في نهاية الثمانينيات من القرن المنصرم، ولكنها بسبب خوفها على برمجياتها من النسخ غير الشرعي، اقتصرتْ على نشر منتجاتها على نطاق ضيق وبأسعار خيالية لا يستطيع المستخدم العربي العادي أن يتحملها.

٢) **انحصار البرنامج على شركة واحدة فقط** : قد تبرز مشاكل جديدة خطيرة بعد الحصول على براءة اختراع لبرمجيات جديدة غير مشهورة، وهذا يعني أنه لن يُسمح لنا باستخدام سوى برنامج واحد من شركة واحدة، وسيتعين على غيرها من الشركات التي تود استخدام البرامج تسديد قدر كبير من المال للحصول على حقوق المؤلف.

٣) **تؤدي إلى كساد صناعة البرمجيات** : وما دامت جلسات استماع براءة الاختراع تجري على مدار أكثر من سنة في سرية تامة، فقد تعمد شركة أولى إلى ابتكار حزمة برامج ثم تتقدم بطلب براءة اختراع لها، وقد تصنع شركة ثانية في أثناء ذلك برنامجاً أفضل، وقد تحرز نجاحاً باهراً، وفجأة تنتقل براءة الاختراع إلى الشركة الأولى التي تسعى لمقاضاة الشركة الثانية. إن هذا الموقف يؤدي إلى كساد صناعة البرمجيات.

ومثال على ذلك برامج شركة لوتس، فقد جرت عادة هذه الشركة على ابتكار برامج لإدارة المعطيات وتنظيمها، واعتقد البعض أن الشركة قد هجرت عملها، ذلك أننا لم نسمع بأي جديد عنهم ، فعندما أصبحت براءة الاختراع بالنسبة إلى البرمجيات مقبولة في بداية تسعينيات القرن العشرين، أغلقت الشركة أقسام الأبحاث والتطوير واستدعت مجموعة من المحاميين للحصول على براءات اختراع لجميع تقنيات البرمجة الخاصة بها، وحتى هذه اللحظة كانت هذه الشركة تبيع الحقوق على أنها عملها الأساسي في المقام الأول.

براءات الإختراع للبرمجيات بين المنح والمنع :

مما سبق يتبين أن منح براءات الاختراع على البرمجيات يضر بالدرجة الأولى بقطاع البرمجيات. وتنص قوانين براءات الاختراع والرسوم الصناعية والدوائر المتكاملة لبعض الدول العربية على عدم منح براءات اختراع عن برمجيات الحاسوب.

وفي أوربة حيث تنتشر شركات البرمجيات الصغرى والمتوسطة، فإن مكتب براءات الاختراعات الأوروبي **(European Patent Convention)** واتفاقية **TRIPS** (الجوانب التجارية المتعلقة بحقوق الملكية الفكرية) التابعة لمنظمة التجارة العالمية **(WTO)** ينصان صراحة على أن البرمجيات والأعمال الأدبية يجب أن تُحمى بحقوق المؤلف **(Copyright)** ، لا ببراءات اختراع.

أما في أمريكا فالوضع مختلف فقد فُتح المجال للحصول على براءات الاختراع للبرمجيات في الولايات المتحدة الأمريكية منذ منتصف التسعينيات فعمالقة صناعة البرمجيات هناك قد ضمنوا لأنفسهم مكانا متقدماً في السباق التقني المحموم ، ورؤوس أموالهم الضخمة كافية للتكفل بمصاريف ملاحقة أي شركة تحاول التعدي على حقوقها الملكية والفكرية.

إن البرمجيات الحاسوبية محمية سلفاً بحق المؤلف فإذا أراد منافس أن يُنتِج برمجية تؤدي نفس الشيئ الذي يقدمه برنامج آخر متاح، فيجب عليه إعادة البرمجة من الصفر إن صاحب الفكرة الأصلي قد حصل سلفاً على مكافأته وعلى ميزات تنافسية أيضاً ، فحق المؤلف كفيل بحماية البرمجيات وتعزيز الإبتكار والمبدعين في هذا القطاع الواسع ، أما براءة الاختراع فيمكن أن تكون سبباً في إعاقة الابتكار والحد من المنافسة في مجال صناعة البرمجيات.

﴿ قانون العلامات التجارية (Trademarks Law)﴾

تعريف: هي الرمز أو الشعار الذي تستعمله الشركات لتمييز منتجاتها عن المنتجات الأخرى من ذات الصنف.

أشكال العلامة التجارية:العلامة التجارة قد تكون أسماً أو كلمة أوحروفاً أوأرقاماً أوأشكالاً ومجموعات ألوان أو أى مزيج من هذه العلامات، مؤهلة للتسجيل كعلامات تجارية.

شروط العلامة التجارية:

١) **أن تكون جديدة:** لم يسبق استعمالها من قبل على ذات السلعة أو المنتج أو الخدمة المراد وضع العلامة عليها.

٢) **أن تكون مميزة** : لها ذاتية خاصة عن غيرها من العلامات التي يُمكن أن تتشابه معها.

٣) **أن تكون مشروعة:** لا تخالف أحكام الشريعة الإسلامية والنظام العام والآداب العامة.

شطب العلامة التجارية:

لا يجوز إلغاء العلامة على أساس عدم الاستخدام إلا بعد انقضاء مدة لا تقل عن ثلاث سنوات متواصلة من عدم الاستخدام، ما لم يثبت صاحب العلامة وجود أسباب وجيهة تستند إلى وجود عقبات تحول دون استخدامها.

مدة الحماية للعلامة التجارية:

تبلغ مدة الحماية الخاصة بالعلامة التجارة مدة (٧) سنوات على الأقل قابلة للتجديد.

سرقة العلامات التجارية من الإنترنت:

لم تكن العلامة التجارية في أي يوم من الأيام مجرد اسم أو رسم خاص بشركة ما، ولكنه شعار للثقة المتبادلة بين الشركة وزبائنها، ومع بدئ الأعمال التجارية عبر الإنترنت أصبح الشعار أكثر أهمية، وذلك كون الثقة بالشراء عبر الإنترنت مازالت محدودة، وبينما هناك مواقع تغطي الجزء المتعلق بالثقة بإتمام عملية البيع والشراء بشكل سليم، فإن الجزء الخاص بمدى جودة المنتج أو الخدمة المقدمة مازال يعتمد بشكل رئيس على العلامة التجارية.

يبدو أن المحتالين عبر الإنترنت **Online scammers** قد أدركوا هذه الحقيقة، ولذلك تركزت عملياتهم على سرقة العلامات التجارية واستخدامها بشكل غير سليم، مما أدى لتشوية كبير لهذه العلامات ولضعف ثقة المستهلك بها.

في دراسة أجرتها **Mark Monitor** مؤخراً بينت ازدياداً كبيراً في عمليات اختطاف العلامات التجارية عبر الإنترنت، وقد بينت الدارسة أن عدد حالات إساءة استخدام العلامات التجارية عبر الإنترنت يصل إلى نصف مليون حالة أسبوعياً، وتتركز عمليات الإساءة على تسجيل أسماء نطاقات بأسماء مشابهة لشعارات أو علامات تجارية معروفة، وقد ازدادت هذه الحالات بمقدار ٤٠% في الربع الأول من عام ٢٠٠٨. وقد توزعت حالات الإساءة وفق النسب التالية: ٦٦% للمواقع المستضافة في الولايات المتحدة تليها ٧% لمواقع مستضافة في ألمانيا ومن ثم ٦% للمواقع المستضافة في المملكة المتحدة، ومن ثم ٤% للمواقع المستضافة في كندا.

وتعتبر عملية اختطاف العلامات التجارية عبر الإنترنت واحدة من عمليات الخداع عبر الإيحاء للمستخدم بأن الموقع الذي يزوره هو موقع شرعي، وبهذا يتم ربط هذا الموقع بأحد الشعارات التجارية الرائدة، وهذا الإجراء يعتبر خرقاً لحقوق المستهلك، وقد يؤدي أحياناً إلى سرقة معلوماته الخاصة والمالية.

نزاعات اسم الملكية (Domain Name Disputes):

تعريف (Domain Name): هو عنوان على الإنترنت يتم تصميه لتمكين مستخدمي الشبكة من إيجاد موقع الكتروني بسهولة.

مستويات أسماء النطاق:

كل إسم نطاق يتكون من ثلاثة مستويات مثلاً العنوان "**WWW.NAME.COM**" مستوياته هي:

1. **"COM" is the Top Level Domain (TLD).**
2. **"NAME" is called the Second Level Domain (SLD).**
3. **"WWW" is the host.**

أنواع أسماء النطاق أو أنواع (TLD):

١) **Com**: شركة ربحية (**Profit Corporation**).
٢) **Org**: شركة أو منظمة غير ربحية (**Nonprofit Corporation**).
٣) **Edu**: تعليمي(**Educational**) مثل المعاهد والجامعات.
٤) **Gov**: حكومي (**Government**).
٥) **Mil**: عسكري (**Military**).
٦) **Net**: إدارة الإنترنت (**Internet administration**) أو موزعي الخدمة المعتمدين.

أنواع الإعتداء على سماء النطاق (Domain Name):

١) **Cyber Squatting**:

a. يعتمد هذا النوع من الاحتيال على أن عملية تسجيل أسماء نطاقات عبر الإنترنت تتم بشكل آلي ولايوجد أي عمليات تدقيق لها، وبالتالي يمكن شراء أسماء نطاقات توحي بأنها لشركة مشهورة، وبهذا يتعامل متصفح الموقع معها على هذا الأساس. و هناك العديد من الحالات التي تم فيها إنشاء مواقع مزورة ادعت أنها شركات البرامج الأمنية الشهيرة مثل (**Panda security, McAfee , Symantec).**

b. أن يقوم شخص أو جهة بتسجيل اسم موقع لعلامة تجارية معينة ليست مملوكة له أصلاً بهدف بيعها.

٢) **Metatages** : اثناء البحث على موقع الكتروني معين يظهر موقع الكتروني آخر بقصد المنافسة.
٣) **Word Stuffing:** محاولة أو مسح بعض المعلومات الواردة على موقع الكتروني معين من قبل شخص غير مالك لذلك الموقع.
٤) **الارتباطات المزورة (False Association) :**تلجأ بعض المواقع إلى تضمين موقعها ارتباطات إلى مواقع متخصصة بتصنيف مصداقية المواقع، ولهذا تعمل المواقع التي تحاول الاحتيال على وضع صور لشعارات مشابهة لتلك الموجودة في المواقع الأصلية، مع فارق وحيد أن هذه الصور لا يمكنك الضغط عليها للوصول للمواقع الأصلية.

الفرق بين العلامة التجارية وإسم الموقع

Domain Name	Trademarks
لا يمكن وجودة إلا دوليا.	يمكن وجودة محلياً أو دولياً.
قد يتم تسجيل الموقع لأسباب مختلفة.	تسجيل العلامة التجارية يتم لغايات تجارية.
لا يتم إخضاع تسجيل الموقع تحت إي صنف.	يتم تسجيلها تحت أصناف معينة.
لا يمكن إيجاد أكثر من اسم واحد للموقع.	من الممكن تسجيل نفس العلامة لأنواع مختلفة من البضائع والخدمات.

﴿ قانون المسؤولية التقصيرية (Tort Law) ﴾

التشهير (Defamation):

مقدمة:

إن جريمة التشهير من الجرائم التي لها الأثر البالغ سلباً على شخص الإنسان فهي من الجرائم الماسة بالشرف وقد عالجتها التشريعات الوضعية بأحكام خاصة سواء من حيث الإثبات أو من حيث العقوبة إن هذه التشريعات وضعت لمعالجة وقائع محصورة نسبياً في كيان مادي قريب ، سواء وقع هذا التشهير أمام مجموعة أفراد أو في إحدى وسائل الإعلام التقليدية (ما قبل النت) والتي يكون فيها التشهير محدوداً إلى حد ما ، كما يسهل فيها الإثبات ويصعب على الجاني الإفلات ، أما بعد ظهور الإنترنت فإن الأمر بات جد خطير، حيث يكون التشهير أمام البلايين كما يصعب فيه الإثبات ويسهل للجاني الإفلات .

تعريف: إصدار عبارات علنية شفهية أو كتابية من شأنها على الأرجح أن تسيء إلى سمعة الشخص، أو اسمه أو تحط من مقامه في نظر المجتمع ككل.

التشهير عبر الإنترنت (Defamation On the Internet):

مقدمة:

المضيء الملتبس دائما بسلبيات تشكل الجانب الآخر المظلم من هذا الجديد وهذا ما ينطبق على ثورة الاتصالات العولمية وعلى رأسها شبكة الإنترنت التي ساهمت في كل جوانب الحياة اتصالا و تطويرا إلا أن سلبياتها و أهمها التشهير بالناس و إساءة سمعتهم قد استدعت وقفة للتصدي لهذا الجانب السيئ من تلك الشبكة العنكبوتية العملاقة التي ما زالت تتطور نحو الأحسن.

للإنترنت إيجابياتها الكثيرة التي تشمل البريد الإلكتروني و البحث عن المعلومات والاتصال الإلكتروني والتعارف الذي قد يقود إلى صداقة أو زواج. لكل هذه الأسباب وغيرها فقد أقبل الناس على الإنترنت وأكثر الذين يستخدمون الإنترنت هم فئة الشباب وهؤلاء يضعون في هذا العالم السايبري صورهم و قليل أو كثير من معلوماتهم الشخصية.

ومن بين هذه الصور والمعلومات الشخصية التي يضعها المواطنون في فضاء الإنترنت تنبثق السلبيات المزعجة التي منها التشهير بالناس وإساءة سمعتهم. وأصبح التصدي لهذا التشهير أمرا ضروريا والتصدي للتشهير وإساءة السمعة قد يكون قانونياً بتفعيل القوانين العادية لتعمل في هذا المجال أو بإصدار قوانين خاصة بمخالفة النشر في الإنترنت كما حصل في بعض البلاد العربية وقد يكون التصدي للتشهير من داخل الإنترنت ذاتها بإنشاء موقع فيها لتوعية ضحاياها أي ضحايا الإنترنت بكيفية التعامل مع هذه الحالات المزعجة .

حيث تعتبر ظاهرة التشهير عبر الإنترنت من أبرز سلبيات الشبكة العنكبوتية، فلقد كثرت المهازل التي بتداولها « خفافيش الانترنت » عن أفراد من المجتمع، بغرض التشهير بهم، وهز صورتهم أمام الآخرين، وأصبح كل من لديه حقد، أو ثأر على أحد المسئولين، أو أحد مشاهير الكتاب، أو الدعاة، أو الإعلاميين، يستخدمه كخميرة دسمة لدسائس وأكاذيب يعجنها أحدهم بماء الكذب والبهتان، ويخبزها بأفران المنتديات على الملأ، ثم يوزعها زاعماً أن صنيعه هذا من باب النصيحة والغيرة العامة على الأخلاق والدين كما شملت هذه الظاهرة أيضاً نشر المعلومات شديدة الخصوصية عن الأفراد والمؤسسات، أو نشر ما يدعى أنه أسرار شركة ما، واتهام بعض الشخصيات المعروفة، أو نشر قصص عنهم تحتمل الصدق أو الكذب، أو " فضح " ممارسة مسئول، أو إدارة ما. أو نشر هواتف، أو عناوين البعض، والتشنيع عليهم، وقد يصل ذلك إلى ما في حكم قذف المحصنات الغافلات.

أحكام التشهير عبر الإنترنت:

إن التشهير بالناس عبر الإنترنت ممنوع شرعاً من عدة أبواب منها: باب الغيبة، والنميمة، والبهتان، وكلها محرمة ومن جانب آخر فإن التشهير محرم من باب إشاعة الفاحشة بالمجتمع الإنساني، والفاحشة ليست مقصورة على الأعمال بل الأقوال أيضاً التي توصف بالفحش إذا جاوزت الأعراف والآداب العامة و هناك جانباً ثالثاً أسود للتشهير، فهو يعتبر من عوامل الإفساد بين الناس وهذا محرم، الأمر الرابع أن هذا التشهير يعتبر حراماً من باب أي الفرقة وأحكام التشهير العادية المتداولة تنطبق على التشهير عبر الإنترنت من الناحية القانونية والجنائية.

من أسباب انتشار ظاهرة التشهير عبر الإنترنت:

١. سهولة نشر المعلومات والوصول إلى أعداد كبيرة من الناس.

٢. صعوبة التعرف على ناشر المعلومة أو منعه من نشرها.
٣. اختلاف قوانين الدول وتعدد الأماكن التي فيها التشهير.
٤. عالمية الإنترنت حيث لا فريق معيّنٍ يمتلكها أو يتحكّم بها.

أسباب التشهير:

١. التشويه: حيث من لدية حقد أو ضغينة ضد شخص معين يسعى إلى تشويه سمعته عبر الإنترنت أمام المجتمع والناس.
٢. المنافسة : حيث غالباً ما تنشأ المنافسة بين الشركات التي تعمل في نفس المجال وتنتج نفس المنتجات.
٣. الاستغلال : حيث يهدف الشخص من وراء عملية التشهير إلى ابتزاز الشخص المشهر به وإستغلالة بجميع طرق الاستغلال.

كيف نحمي أنفسنا من عملية التشهير:

هناك بعض الاحتياطات التي يتوجب علينا فعلها لنحمي أنفسنا من خطر التشهير ومنها على سبيل المثل لا الحصر:

١. ترسيخ القيم الإسلامية في المجتمع.
٢. يرى علم النفس أن الشخصية التي تشهر بزملاء العمل أو بمنافسين شخصية سيكوباتية (الشخصية الناقمة على المجتمع) تعمل ضد القيم الاجتماعية والأخلاقية؛ لأنها تعاني من بعض العقد النفسية التي ربما تكونت منذ الطفولة نتيجة أساليب تربوية خاطئة أدت إلى الشعور بالنقص والدونية أمام الآخرين، وبأنه أقل منهم جهداً وخبرة، وعملاً وإخلاصاً، ويعتقد أنه لو فعل ذلك وشهر بغيره أو بمنافسه استطاع أن يكسب الأصوات. ولا يعلم أنه بذلك يكون قد خسر نفسه؛ لأنه بهذا العمل شوه سمعة وسيرة من يشهر بهم وقد يكونوا أبرياء. وبالتالي فهناك ضرورة لإيجاد واستحداث مواد تربوية في المدارس مثلا « التربية الاجتماعية » حيث يتم عن طريقها إيصال الرسائل الهادفة للتلاميذ، لاسيما في ظل القصور الواضح في أدوار الأسرة التربوية والاجتماعية داخل المجتمع الذي قد يكون له دورٌ في انتشارا مثل هذه الظواهر السلبية.
٣. الابتعاد عن موطن التشهير والابتعاد عن الشبهات.
٤. عدم إعطاء الصور الشخصية مهما كانت صغيرة إلى أشخاص لا تثق فيهم ثقة تامة، والامتناع عن إرسال الصور الشخصية إلى أي موقع إنترنت، حتى لو كان موقعاً للتعارف، أو الصداقة، أو الدردشة.
٥. يجب الحذر عند منح الأشخاص الغرباء أرقام الهواتف الخاصة؛ لأنهم قد يضعوها بسهولة تامة في مواقع " الشات ".

﴿جرائم الحاسب (Computer crimes)﴾

مقدمة:

الجريمة المعلوماتية هي : الابن غير الشرعي .. الذي جاء نتيجة للتزاوج بين ... ثورة تكنولوجيا المعلومات .. مع العولمة .

وفي الحقيقة أن الجرائم المعلوماتية هي ثمرة من ثمار التقدم السريع في شتى المجالات العلمية الذي يتميز به عصرنا الحاضر ؛ فهناك ثورة في مجال الجينات والصبغيات نتيجة للتقدم في فرع الهندسة الوراثية ؛ وهناك ثورة في مجال وسائل الاتصال والمعلومات Information Revolution ترجع إلى استخدام الكمبيوتر (الحاسوب) ... الخ .

ولقد صاحب هذا التقدم السريع في مجال العلوم والتقنية واستخداماتها لخير البشرية ؛ تقدم آخر مواز في مجال الجريمة ؛ فلم تصبح الجريمة مقصورة على طبقة معينة من طبقات المجتمع دون أخرى ؛ وذلك لوضوح إجرام الفساد الذي يتورط فيه كبار المسئولين في الدول المختلفة ؛ علاوة على إجرام ذوي الياقات البيضاء ؛ الذي يتورط فيه كبار المسئولين في الشركات العملاقة ؛ وإجرام الاتجار بالمخدرات .

ثورة الاتصال والمعلومات وخير البشرية :

وعلي مستوى ثورة الاتصال والمعلومات نجد أن الصراع مستمر بين جانبي الخير والشر في هذه الثورة ؛ ففي جانب الخير نجد أن هذه الثورة ساعدت على عولمة المعلومات ؛ وتسهيل كثير من الخدمات والأعمال ؛ فقد توصلت البشرية إلى السيطرة على المعلومات من خلال استخدام الحاسب الآلي computer لتخزين ومعالجة واسترجاع المعلومات ؛ فضلا عن استخدامه في عمليات التصميم والتصنيع والتعليم والإدارة ؛ ناهيك عن تطوير تطبيقاته لتشمل أداء خدمات عديدة مثل التعليم والتشخيص والخدمات التمريضية وتسهيل المعاملات والخدمات البنكية والحجز الآلي لنقل الأشخاص وإدارة المكاتب الحديثة وقيادة المعارك ؛ وعلى وجه العموم دخل الحاسب الآلي في شتى نواحي الحياة الإنسانية .

فضلا عن أنه جعل المعلومات في متناول الجميع من خلال شبكات الإنترنت ؛ أي شبكات المعلومات المحلية والإقليمية والعالمية ؛ وأصبح العالم بذلك مزدهرا بكم هائل من المعلومات لا تعرف الحواجز الجغرافية ولا المسافات ؛ بصورة يمكن معها القول بأن العالم صار أشبه بمجتمع كبير تترابط فيه الحاسبات و شبكات المعلومات ؛ لتعلن بزوغ فجر ثورة جديدة هي الثورة المعلوماتية La revolution information أو الثورة الصناعية الثالثة التي تدفع بالإنسانية إلى عصر جديد هو عصر أو مجتمع المعلومات .

تعريف جرائم الحاسب: فعل أو امتناع عمدي ينشأ عن نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة في الحاسب ، أو التي تحوَل عن طريقه.

الاستخدام غير المصرح به (Unauthorized Use):

يقصد بالاستخدام الغير مصرح به: الوصول إلى موارد أو شبكات أو أنظمة لحاسب الآلي من قبل أشخاص غير مخولين أو لا يملكون الحق في الوصول أو استخدام تلك الموارد أو الأنظمة أو الأجهزة ومن أمثلة ذلك:

- الالتقاط الغير مشروع للمعلومات أو البيانات .
- الدخول الغير مشروع على أنظمة الحاسب الآلي .
- التجسس والتصنت على البيانات والمعلومات .
- انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم وتزوير البيانات او الوثائق المبرمجة أيا كان شكلها .
- إتلاف وتغيير ومحو البيانات والمعلومات .
- جمع المعلومات والبيانات وإعادة استخدامها .
- تسريب المعلومات والبيانات .

هجمات الحرمان من الخدمة على الموقع (Denial of Service Attacks on Web Site):

مقدمة:

أكدت العديد من التقارير تزايد عدد الهجمات من خلال شبكة الإنترنت العملاقة وازدياد شدتها وتأثيرها التدميري عامًا بعد الآخر وتأثيرها على مبيعات المواقع والخدمات عبر الإنترنت.ويرجع ذلك إلى عده أسباب من أخطرها ما يعرف ب" هجمات الحرمان من الخدمات" أو "هجمات حجب الخدمة " (Denial of Service Attacks) ملاحظة (DoS) هنا لا نقصد بها نظام التشغيل المشهور و لكنها اختصار للعبارة Denial-of-Service و هي تعني حجب أو منع ألخدمة.

هي هجمات تتم عن طريق إغراق المواقع بسيل من البيانات غير اللازمة يتم إرسالها عن طريق أجهزة مصابة ببرامج(في هذه الحالة تسمى DDOS Attacks) تعمل نشر هذه الهجمات بحيث يتحكم فيها القراصنة والعابثين الإلكترونيين لمهاجمة المواقع الإنترنت عن بعد لإرسال تلك البيانات إلى المواقع بشكل كثيف مما يسبب بطء الخدمات أو زحامًا مروريًا بهذه المواقع ويسبب صعوبة وصول المستخدمين لها نظرًا لهذا الزحام. ، خصوصا وأنه يبدو، وباعتراف الكثير من خبراء الأمن على إنترنت، وكأنه لا يوجد علاج في الوقت الحالي لهذا الأسلوب في الهجوم على مواقع إنترنت، وعلى هذا الأساس فإن هذا النوع من الهجمات يُدعى في بعض الأوساط " بإيدز الإنترنت".ويتم هذا الهجوم بدون كسر ملفات كلمات السر أو سرقة البيانات السرية، هجمات حجب الخدمة تتم ببساطه بان يقوم المهاجم بإطلاق أحد البرامج التي تزحم المرور للموقع الخاص بك و بالتالي تمنع أي مستخدم آخر من الوصول إليه. وبشكل عام تتواجد مثل هذه الهجمات منذ أعوام إلا أن قوتها الآن أصبحت أكبر من أي فترة مضت، كما أنها وصلت إلى مرحلة من النضج بحيث تستهدف أهدافًا محددة ومقصودة لأغراض تجارية.

تعريف: إغراق الأجهزة المزودة بسيل من الطلبات والأوامر التي تفوق قدرة الجهاز المزود على المعالجة.

أنواع (طرق) هجمات الحرمان من الخدمة:

١. الهجمات التي تستغل خطأ برمجي Bug في بناء TCP/IP .
٢. الهجمات التي تستغل تقصير في مواصفات TCP/IP .
٣. الهجمات التي تعيق المرور في شبكتك حتى لا تستطيع أي بيانات أن تصل إليها أو تغادرها .

كيفية عمل هجوم حجب الخدمة الموزعة ؟

تعتبر هجمات حجب الخدمة الموزعة DDoS (Distributed Denial of Service)، نوعاً جديداً من هجمات حجب الخدمة العادية التي تعتمد على استخدام برامج معينة في الهجوم. وهذا النوع من الهجمات، هو الذي استخدم في الهجوم على كبرى مواقع إنترنت، مثل Yahoo! ZDNet، eBay، Amazon، CNN، وغيرها. وتعتمد هذه الهجمات على تجنيد أجهزة كمبيوتر متصلة بإنترنت، بدون علم مالكيها ، وتوجيهها إلى بث الرزم الشبكية إلى مزود معين، بهدف إيقافه عن العمل، نتيجة ضغط البيانات المستقبلة. ويعتمد هذا النوع من الهجمات على وضع برنامج خبيث خاص، من نوع "حصان طروادة " (Trojan horse)، في كل كمبيوتر متصل بإنترنت يمكن الوصول إليه، عن طريق إرسال البرنامج بواسطة البريد الإلكتروني، مثلاً، وتفعيله على هذه الأجهزة، لتعمل كأجهزة بث للرزم الشبكية، عند تلقيها الأمر بذلك من برنامج محدد يقبع على جهاز أحد المخترقين. ومن أشهر البرامج المستخدمة في إجراء هذه الهجمات: TRINOO stacheldraht. & Tribe Flood Net & TFN2K، يعتبر هذا النوع من هجمات حجب الخدمة، أكثر الأنواع خطورة، حيث يمكن أن يشكل خطراً على شبكة إنترنت كلها، وليس على بعض المواقع فقط.

ويتفق الخبراء اليوم على أنه لا سبيل لعلاج الهجمات الموزعة أو تفاديها. ورغم أن البعض يقترحون استخدام أساليب التحقق من الهوية والتشفير لمعالجة حزم المعلومات المتناقلة، فإنهم يتفقون أيضا على أن هذه الطرق غير عملية لمعالجة المشكلة على إنترنت. وهنالك اقتراحات أخرى بتضمين المعالجات إرشادات يمكنها تمييز هجمات الحرمان من الخدمات وفلترتها قبل أن تؤثر على نظام التشغيل، وهو حل تعمل على تطويره العديد من الشركات المنتجة لبرمجيات مكافحة هجمات الحرمان من الخدمات اليوم.

حقائق حول هجمات حجب الخدمة:

ومع أن هجمات حجب الخدمة تبدو بسيطة وتافهة أحيانا بنظر المبتدئين ممن يديرون سيرفراتهم الخاصة ولكن يبقى هذا الهجوم من اخطر أعمال الهكرز ، فالاختراق يوقف الموقع بتغيير الواجهة الرئيسية مثلا ، ويوقف السيرفر بعمل فورمات أو حتى الجهاز الشخصي ، وتتم إعادة نسخة احتياطية محفوظة وبسرعة ، بينما هجوم حجب الخدمة قد يوقف عمل سيرفر ويب لفترات طويلة وقد تقطع مصالح وأعمال وقد تعرضت مواقع كبيرة لشبح هذا الهجوم الفتاك وهذا الهجوم لا يقف عند حد معين أو يستهدف منفذ معين أو خدمة معينة ، لكن لكل خدمة هجوم وحتى تكرار تصفح الموقع بعمل تحديث أو الدخول عليه أكثر من مرة من آلاف الأجهزة هجون على المنفذ "٨٠" أو محاولة الاتصال بمئات المستخدمين على منفذ ftp وكلما طال الهجوم وكثر الطلب على الخدمة زاد الخطر وقد تدمر عتاد الكمبيوتر بالضغط واستهلاك موارد النظام ، والحماية الفعلية لا تكمن في الجدار الناري لان الجدار الناري ربما يزيد في خطورة إذا كان مبرمج على طريقة عرض رسالة أو إرسال رسالة عند تلقي هجوم فيزيد من الضغط على موارد النظام الفعلية CPU ، يجب على مدير الشبكة أو السيرفر مراقبة البيانات وإغلاق الخدمة التي تتعرض للهجوم مؤقتا حتى تجد حلا لها ويكون بتغيير IP مؤقتا لكي لا ينقطع عملك ، هذا جزء من الأجزاء لهذا الهجوم الجبار ، وللأسف جهل الكثيرين بطريقة الوقاية منه ووقوع الكثير من مدراء السيرفرات تحت هجمات بسيطة ولكن لم يستطيعوا حلها وأدت لمشاكل أكبر.

الحماية من هجمات الحرمان من الخدمة

يتم الحماية من هذه الهجمات بعدة طرق ولكنها تختلف في مدى تأثيرها ومن هذه الطرق ما يعرف بنظام Dos.deny.

ما هو نظام (Dos.deny) ؟

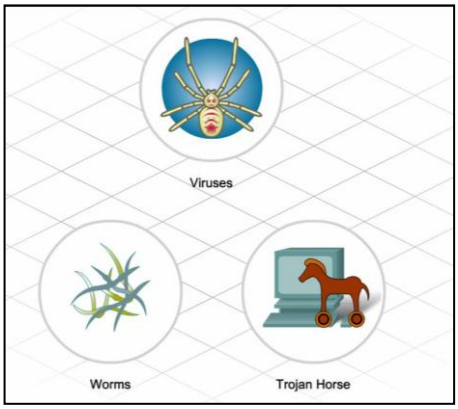
نظام الحماية Dos.deny هو نظام مخصص لاكتشاف هجمات الحرمان من الخدمة DOS و التصدي لها و منعها من التأثير على أداء السيرفرات أو المواقع التي تستعمل هذا النظام ، و لمن لا يعرف ما هي عمليات الحرمان من الخدمة ، فهي قيام شخص باستهداف موقع ما و ذلك بإرسال كم هائل من طلبات التصفح HTTP Request بغرض منع الموقع من العمل بشكل سليم أو إبطاء عمل الموقع ، أو حتى الإطاحة بشكل كامل بسيرفر الموقع بحيث يقف نظام السيرفر (Apache / IIS...) عن العمل نهائيا جراء الكم الهائل من أوامر التصفح .

كيف يعمل نظام Dos.deny ؟

عن طريق إضافة سطر واحد إلى ملفات موقعك ، سيكون بإمكان النظام قراءة رقم (IP) لكل زائر ، و عن طريق تخزين هذه الأرقام و تتبعها وفقاً لخوارزمية معينه سيكون بمقدور النظام اكتشاف عمليات الحرمان من الخدمة و ذلك بضوابط يمكن لمدير الموقع التحكم بها من خلال لوحة التحكم ، بمعنى أنه يمكنك تحديد كم عدد المحاولات و الفترة التي تقع فيها هذه المحاولات ، و التي على أساسها يمكن الحكم أن هذا (IP)يقوم بهجمة للحرمان من الخدمة عندها سيقوم النظام بالكتابة في ملفات من نوع .htaccess و ذلك لمنع ذلك IP من الوصول إلى موقعك (أو أجزاء من موقعك تستطيع تحديدها أيضا).

هل يدعم هذا النظام هجمات الحرمان من الخدمة الموزعة (DDOS) ؟

ليس بشكل كامل .. لن يستطيع هذا النظام الحماية من هجمات الحرمان من الخدمة الموزعة DDOS إذا كانت الهجمات تتم عن طريق عدد كبير جدا من أرقام IP ، أما إذا كانت الهجمة تتم عن طريق عدد محدود من أرقام IP ، فمن خلال ضبط الإعدادات بشكل أكثر صرامة سيكون بمقدورك إيقاف أو الحد من هذه العمليات بشكل كبير.



برامج الحاسب الخبيثة (malicious software):

وتعني البرمجية الماكرة أو الخبيثة، وهي برنامج مخصص للتسلل إلى نظام الحاسب أو تدميره بدون رضا المالك. وما إن تم تثبيت البرمجية الخبيثة فإنه من الصعب جداً إزالتها. وبحسب درجة البرمجية

من الممكن أن يتراوح أذاها من إزعاج بسيط (بعض النوافذ الإعلانية الغير مرغوب بها خلال عمل المستخدم على الحاسب متصلاً أم غير متصلا بالشبكة) إلى أذىً غير قابل للإصلاح يتطلب إعادة تهيئة القرص الصلب وهي عدة أنواع منها:

- الفيروسات (Virus): الفيروس هو مجموعة من التعليمات البرمجية التي ترفق نفسها ببرنامج أو ملف لتتمكن من الانتشار من كمبيوتر إلى آخر.

الفيروس يلحق نفسه ببرنامج أو ملف وينتشر من جهاز إلى جهاز مثل انتشار مرض الإنسان الفيروسات تختلف من نوع إلى آخر بعضها قد يؤدي إلى بعض الأعطال البسيطة وبعضها قد يسبب تلف الهاردوير أو البرامج لديك وحتى ملفاتك المهمة وهناك عدة أنواع من الفيروسات منها:

١. فيروسات بدء التشغيل (Boot Sector Virus): هذا النوع من الفيروسات يصيب قطاع الإقلاع في الجهاز و هو المكان المخصص الذي يتجه إليه الكمبيوتر في بداية تشغيل الجهاز. و هذا النوع من الفيروسات قد يمنع المستخدم من الوصول إلى النظام ويمنعه من إقلاع الجهاز.
٢. فيروس الملفات (File Virus):يصيب البرامج عادة و ينتشر بين الملفات الأخرى و البرامج الأخرى عند تشغيله.
٣. فيروس الماكرو (Macro Virus): هذه الفيروسات تصيب برامج الميكروسوفت أوفيس مثل الوورد و الإكسل، و تعتبر ذات انتشار واسع جدا تقدر ب 75% من عدد الفيروسات الموجودة. يقوم هذا النوع من الفيروسات بتغيير بعض المستندات الموجودة في القرص الصلب و خصوصا الوورد , قد تجد بعض التصرفات الغير منطقية في بعض الأحيان مثل طلب باسوورد لفتح ملف تعرف انك لم تضع عليه باسوورد ، و أيضاً تجد بعض الكلمات قد تغير مكانها و أضيفت كلمات جديدة لا علاقة لها بالموضوع . هي أساساً ليست ضارة، لكنها مزعجة نوعاً ما و قد تكون مدمرة أحياناً.
٤. الفيروس المتعدد الأجزاء (Multipartite Virus): هو الذي يقوم بإصابة الملفات مع قطاع الإقلاع في نفس الوقت و يكون مدمراً في كثير من الأحيان إذا لم تتم الوقاية منه.
٥. الفيروس المتطور (Polymorphic Virus) : هي فيروسات متطورة نوعا ما حيث أنها تغير الشفرة كلما انتقلت من جهاز إلى آخر.
٦. الفيروس المختفي (Stealth Virus):تخفي نفسها بان تجعل الملف المصاب سليما و تخدع مضادات الفيروسات بان الملف سليم و ليس مصاباً بفيروس. مع تطور مضادات الفيروسات أصبح من السهل كشف هذا النوع.

ويتميز الفيروس بعدد من الصفات منها:

١. تأتي على شكل ملف تنفيذي exe في أغلب الأحيان.
٢. لا تنتقل إلا بتدخل الإنسان (تشغيلها أو إرسالها) وأحياناً يستخدم المبرمج مؤقت وتاريخ جهاز المستخدم.
٣. لا تقوم بنسخ نفسها أكثر من مرة.
٤. يلحق نفسه ببرنامج أو ملف وينتشر من جهاز إلى جهاز آخر.

- الديدان (Worm): برامج صغيرة قائمة بذاتها غير معتمدة على غيرها صنعت للقيام بأعمال تدميريه أو لغرض سرقة بعض البيانات الخاصة ببعض المستخدمين أثناء تصفحهم للإنترنت أو إلحاق الضرر بهم أو بالمتصلين بهم، تمتاز بسرعة الانتشار ويصعب التخلص منها نظراً لقدرتها الفائقة على التلون والتناسخ والمراوغة.

آلية عملها:

تصيب الدودة الكمبيوترات الموصلة بالشبكة بشكل أوتوماتيكي، ومن غير تدخل الإنسان وهذا الأمر يجعلها تنتشر بشكل أوسع وأسرع عن الفيروسات. الفرق بينهم هو أن الديدان لا تقوم بحذف أو تغيير الملفات بل تقوم باستهلاك موارد الجهاز واستخدام الذاكرة بشكل فظيع مما يؤدي إلى بطء ملحوظ جدًا للجهاز.

تختلف الديدان في عملها من نوع لآخر، فبعضها يقوم بالتناسخ داخل الجهاز إلى أعداد هائلة، بينما نجد بعضها يتخصص في البريد الإلكتروني بحيث تقوم بإرسال نفسها برسائل إلى جميع الموجودين بدفتر العناوين، بل أن البعض منها يقوم بإرسال رسائل قذرة لعدد عشوائي من المقيدين بسجل العناوين باسم مالك البريد مما يوقعه بالكثير من الحرج.

خطورتها:

تكمن خطورة الديدان باستقلاليتها وعدم اعتمادها على برامج أخرى تلتحق بها مما يعطيها حرية كاملة في الانتشار السريع، وبلا شك أن هناك أنواعا منها غاية في الخطورة، حتى أصبح بعضها كابوساً مرعباً يلازم كل مستخدم للشبكة.

أنواعها:

١. ديدان البريد : وتكون مرفقة في محتوى الرسالة وأغلب الأنواع من هذه الديدان تتطلب من المستخدم أن يقوم بفتح الملف المرفق لكي تصيب الجهاز وأنواع أخرى تكون تحتوي على رابط خارجي وبعد أن تصيب الجهاز تقوم بإرسال نسخ منها إلى جميع المضافين في القائمة البريدية باستعمال برتوكول SMTP.

٢. ديدان المراسلة الفورية : وهذا النوع من الديدان يقوم باستخدام أحد برامج المراسلة الفورية للانتشار وذلك عن طريق إرسال الرسائل إلى جميع المتواجدين.

٣. ديدان آي ار سي (IRC) : وتقوم بالانتشار عن طريق نسخ نفسها في القنوات وإرسال روابط إلى العنوان المصاب بالدودة.

٤. ديدان برامج مشاركة الملفات : وتنتشر عن طريق وضع نفسها قي مجلدات المشاركة حتى تنتشر بين المستخدمين الآخرين.

٥. ديدان الإنترنت: وتقوم بالانتقال عن طريق بروتوكول TCP/IP مباشرة دون الحاجة إلى مستوى أعلى مثل البريد الالكتروني أو برامج تشارك ملفات، ومن الأمثلة عليها هو دودة بلاستر التي تقوم عشوائياً بالانتشار عن طريق البحث عن عناوين يكون المنفذ رقم ١٣٥ مفتوحا لتقوم باستغلاله و إصابة جهاز الضحية.

ومن مميزات الديدان ما يلي:

١. تنتشر بدون التدخل البشري حيث تنتقل من جهاز إلى آخر بدون عمل أي إجراء.

٢. نسخ نفسها في جهازك بعدة أشكال وبذلك يتم إرسالها بدلا من مرة وحدة سترسل آلافاً من النسخ للأجهزة الأخرى.

٣. آثارها الدودة عادة هي زيادة في استخدام مصادر الجهاز فيحصل في الجهاز تعليق بسبب قله الرام المتوفر وأيضا تسبب الدودة في توقف عمل الخوادم.

٤. لا تلحق نفسها بأي برنامج أو ملف وإنما تنتقل تلقائياً.

➢ أحصنة طروادة (Trojan Hours): برنامج كمبيوتر يبدو أنه مفيد ولكنه في الحقيقة يسبب الأضرار.

صمم لكي يكون مزعجاً أكثر من كونه مؤذياً مثل الفيروسات وعندما تقوم بزيارة احد المواقع المشبوهة أحيانا يطلب منك تحميل برنامج معين ، الزائر قد ينخدع في ذلك فيعتقد انه برنامج وهو في الحقيقة تروجان يقوم التروجان في بعض الأحيان بمسح بعض الأيقونات على سطح المكتب. مسح بعض ملفات النظام. مسح بعض بياناتك المهمة. تغير الصفحة الرئيسية للإنترنت إكسبلورر. عدم قدرتك على تصفح الانترنت. وأيضا عرف عن التروجانات أنها تقوم بوضع باكدور في جهازك من ما يسمح بنقل بياناتك الخاصة إلى الطرف الآخر بدون علمك وهذا هو الخطير في الأمر.

لماذا سميت بحصان طروادة ؟

في الأسطورة الإغريقية قام الآخيون بقيادة آغاممنون شقيق مينالاوس بحصار طروادة لاستعادة هيلين زوجة مينالاوس ملك إسبارطة كان باريس قد اختطف هيلين أثناء زيارته إلى إسبارطة وأخذها إلى طروادة. استمر الحصار لعشر سنين فدب القنوط في نفوس الإغريق وأيقنوا أنهم لن يتمكنوا من الاستيلاء على المدينة عندئذ ارتأى أوليس اللجوء إلى الحيلة فتظاهر الإغريق بأنهم على وشك إنهاء الحصار ومغادرة المكان .وكانت بعض سفنهم قد أبحرت لكنها توارت خلف جزيرة قريبة بعد ذلك قام الإغريق ببناء حصان خشبي عملاق وأعلنوا أنه سيكون تقدمة إلى الإلهة مينيرفا ولكن بالحقيقة كان الحصان مملوءا بالجنود. أما بقية الإغريق فقد تركوا مواقعهم وأبحروا تاركين الحصان الكبير خارج أسوار المدينة فرح الطرواديون وتهللوا لِما اعتبروه مغادرة الإغريق لمحيط مدينتهم ففتحوا بوابات المدينة وخرجوا منها مبتهجين. وقد أثار الحصان الخشبي فضولهم وأراد بعضهم سحبه إلى داخل أسوار المدينة، في حين كان آخرون متخوفين منها لكن كاهن معبد نبتيون فقد نصح الطرواديين كي يأخذوا حذرهم و يحترسوا من الإغريق وكان الناس على وشك تدمير الحصان عندما جيء بأحد السجناء الإغريق

إلى وجهاء المدينة وكان يرتجف خوفاً فقال لهم أنه إغريقي واسمه سينون تركه محاصرو المدينة خلفهم بأمر من أوليس وقال لهم أيضاً أن الحصان الخشبي صُنع بتلك الضخامة للحيلولة دون أخذه إلى المدينة من قِبل الطرواديين. وما أن سمعوا ذلك حتى تضاعفت رغبتهم في إدخاله إلى المدينة عندئذ نقلوه إلى داخل المدينة بطقوس رائعة وفرح كبير عند حلول الظلام قام سينون بمساعدة الإغريق المسلحين على الخروج من جسم الحصان ففتحوا بوابات المدينة ليسمحوا لإخوانهم الإغريق – الذين عادوا في الظلام – بالدخول إليها عندئذ أحرقت المدينة وأعمل الإغريق السيوف في الطرواديين وكانت تلك نهاية حروب طروادة قد لا يكون حصان طروادة صُنع أو استُعمل على الإطلاق ولا توجد براهين تؤكد وجود ذلك الحصان باستثناء إشارات أدبية تم تدوينها بعد الحادثة بفترة طويلة كانت مدينة طروادة القديمة تقع بالقرب من مضيق الدردنيل، وفي الخمسينيات من القرن الماضي تم بناء متحف يضم ضمن مقتنياته آثاراً للمدينة مع حصان خشبي في حديقة المتحف يمثل حصان طروادة الأسطوري من هذه الأسطورة استُنبط المصطلح (حصان طروادة) للدلالة على ما هو ظاهره نافع مفيد وباطنه ضرر أكيد.

صمم لكي يكون مزعجاً أكثر من كونه مؤذياً مثل الفيروسات.عندما تقوم بزيارة احد المواقع المشبوهة أحيانا يطلب منك تحميل برنامج معين. الزائر قد ينخدع في ذلك فيعتقد انه برنامج وهو في الحقيقة تروجان يقوم التروجان في بعض الأحيان بمسح بعض الأيقونات على سطح المكتب. مسح بعض ملفات النظام. مسح بعض بياناتك المهمة. تغير الصفحة الرئيسية للإنترنت إكسبلورر. عدم قدرتك على تصفح الانترنت. وأيضا عرف عن التروجانات أنها تقوم بوضع باكدور في جهازك من ما يسمح بنقل بياناتك الخاصة إلى الطرف الآخر بدون علمك.

من مميزات الترجان:

١. لا يتكاثر مثل الدودة.
٢. لا يلحق نفسه بأي برنامج مثل الفيروس.
٣. يستخدم لزرع ملفات التجسس في جهازك مما يسمح بنقل بياناتك إلى الطرف الآخر.

- برامج التجسس(Spy ware) : وهو من الأنواع الغير خطرة و لكن المزعجة و التي تتسبب في بطء الجهاز و سرقة بياناته ، و لكن لا تسبب ضرر للجهاز.

وبرامج التجسس هي البرامج التي لها القدرة لمسْح الأنظمة و مراقبة نشاطهاً ونقل المعلومات إلى حاسبات أَو مواقع أخرى عن طريق الإنترنت. يمكن أنت تكون هذه البيانات أو المعلومات : كلمات السر، أرقام حسابات، معلومات شخصية، ملفات فردية أَو وثائق شخصية أخرى. طبعاً تعطى هذه البيانات إلى شركات تستخدمها لتقديم دعاية للضحية عن منتجاتها ، و الهدف الأول هو مواقع أل Https و هي المواقع التي تستخدم لإدخال أرقام بطاقات الائتمان وهي أخطر المشاكل التي يمكن مواجهتها عند الإصابة بهذا النوع من الفيروسات (ملفات التجسس) ملفات التجسس تعمل على جمع و توزيع معلومات تتعلق بحاسوب المستعمل، كالتطبيقات أو البرامج التي تستخدم على جهاز الحاسوب الخاص بالضحية، استخدامات متصفح الإنترنت أَو عادات استعمال الحاسب ملفات التجسس تحاول دوماً البَقاء متخفية و غير ملحوظة . ولكن يمكن للمستخدم ملاحظة وجودها وذلك إذا أحس ببطء شديد في سرعة الجهاز ملفات التجسس يمكن أَن تدخل إلى جهازك من مواقعِ الويب (كمثال برامج أل shareware أَو ما يعرف بالبرامج المجانية)، أو عن طريق بالبريد الإلكتروني الرسائل.

بعض العلامات الشائعة لوجود برامج خبيثة في جهازك:

١. بطء الجهاز الشديد، بما لا يتناسب مع عدد البرامج التي تعمل في نفس الوقت.
٢. امتلاء القرص بما لا يتناسب مع عدد و حجم الملفات الموجودة عليه.
٣. ظهور مربّعات حوار غريبة أثناء العمل على الجهاز.
٤. إضاءة لمبة القرص الصلب أو القرص المرن، دون أن تقوم بعملية فتح أو حفظ ملف.

لابد أن تعرف أن هذه العلامات لا تعني بالضرورة وجود فيروس، فقد يكون بعضها بسبب مشكلة في عتاد الجهاز مثلاً.

بعض طرق الحماية من برمجيات الحاسب الخبيثة:

١. عدم استخدام برامج لا تعرف مصدرها خاصة البرامج المجانية.

٢. عدم فتح ايميلات لا تعرف المرسل حتى لو كان العنوان مبروك لقد ربحت مليون دولار.
٣. استخدام برامج الحماية من الفيروسات و البرامج المتخصصة لمكافحة ملفات التجسس .
٤. لابد أن تقوم بتحديثه بشكل دوري، وإلا فلا فائدة من وجوده.
٥. لا تقم بفتح المرفقات في إيميلات أصدقائك إذا وجدتها تنتهي بـ exe أو bat أو أي امتداد لا تعرفه .
٦. احرص على فحص جميع البرامج من النت أو السيديهات.

جذب الضحايا على شبكة الإنترنت(Attracting Victims on The Internet):

مقدمة:

منذ انتشار شبكة الإنترنت، والجدل قائم حول مخاطرها الكثيرة على الناشئين خصوصاً في البلدان والمجتمعات المحافظة. فالرقابة عليها، مهما كانت دقيقة، لا يمكن لها أن تكون شاملة. وهناك دائماً ثغرات يستغلها بعض مريدي السوء لتحقيق غاياتهم ونشر أفكار يرفضها الدين والمجتمع، تخالف مبادئ التربية السليمة وتتعدى كل الخطوط الحمراء. لهذا السبب، لا بد من التقيد ببعض الإرشادات والتوجيهات لمنع حصول استغلال، أو للكشف عن احتمال حدوثه مع قريب أو صديق أو ابن، ومنع تكراره، أو الوقاية منه فالتطورات في المعلوماتية وتكنولوجيا الإنترنت التي تسمح باكتساب مصادر جديدة للعلم والتثقيف، هي نفسها تعرض المستخدمين، لا سيما الصغار بالسن منهم، لأشكال عديدة من الاستغلال والسوء. انطلاقاً من هذه النقطة، نشر مكتب التحقيقات الفيدرالي لائحة بالتوصيات والإرشادات التي يمكن الارتكاز عليها لحماية مستخدِمي الإنترنت من أي «شرّ» محتمل. وعلماً أن التقرير انطلق من حالات حصلت في أميركا، وبني على شهادات لضحايا ولعاملين على إنفاذ القوانين لبسوا أدوار أطفال للكشف عن الاستغلال عبر الإنترنت، فإن الوقائع قد لا تنطبق حرفياً على كل المجتمعات، لا سيما العربية منها، لأن الرقابة الرسمية والمنزلية على محتويات الصفحات الإلكترونية هي شديدة وأكثر فعالية مما هو الوضع عليه في البلدان الغربية، لا يمنع أن أي حالة استغلال أينما حصلت في العالم قد تؤخذ منها العبر ويُستفاد منها في محاربة ظاهرة باتت تهدد القاصرين بشكل جدي.

جذ ب الضحايا:

بلا شك أن استخدام الإنترنت يساعد الطلاب على توسيع آفاقهم والاحتكاك بثقافات جديدة وطرق مختلفة في التفكير والعيش، إنما هذا يعرضهم أيضاً لمخاطر كثيرة. فهناك أشخاص يستخدمون شبكة الإنترنت لاستغلال الأطفال والقاصرين، ويعتمدون أسلوباً مدروساً لجذب ضحاياهم، كإظهار الاهتمام، العاطفة، اللطف، وحتى إرسال الهدايا.. وهؤلاء الناس مستعدون أحياناً لتكريس الكثير من الوقت والمال والطاقة لتحقيق غاياتهم، أينما كانت ضحيتهم. وليتمكنوا من الإيقاع منها، يكونون عادةً على اطلاع بتوجهات الموسيقى الحديثة، وهوايات الصغار والشباب واهتماماتهم.. وبعد أن تقع الضحية في فخ الكلام الجميل، ينتقل الحديث إلى أطر لا أخلاقية، ويصبح الأبناء عرضة للاستغلال ولو بطريقة غير مباشرة، أو دون أن يعوا لذلك، عن طريق الحوارات المباشرة التي تتيحها بعض برامج المعلوماتية وغرف الـ«شات» وهذه المشكلة تبرز بشكل خاص مع المراهقين. فهؤلاء الآخرون يعيشون سن التمرّد وإثبات الذات من خلال بحثهم عن بناء علاقات جديدة خارج العائلة. وقد يدفعهم فضولهم إلى إنشاء جسور تواصل مع أصدقاء جدد مجهولي الهوية يقابلونهم عبر الإنترنت، مما قد يعرضهم لخطر الوقوع تحت تأثير أشخاص لا يعرفون أصلهم وفصلهم، مع الإشارة إلى أن من يسعى لاستغلال المراهقين يصبح خبيراً في الكشف عن «حاجات» الضحية في مرحلة المراهقة. وللأسف، إن الأولاد والمراهقين لا يعون دائماً للمخاطر التي يتعرضون إليها من جراء تحدثهم لأشخاص يجهلون كل المعلومات عنهم وعن أخلاقهم «علامات»الخطر وبصورة عامة، إن معظم الأطفال الذين يقعون ضحية الاستغلال عبر الإنترنت يمضون أوقاتاً طويلة أمام الكمبيوتر، خصوصاً في مواقع الـ «شات»، وفي الأوقات المسائية أو عطلات نهاية الأسبوع، وينشغلون بالتحاور مع أصدقاء قدامى أو جدد، وبناء علاقات جديدة مع أشخاص حول العالم.. وعلماً أن المعرفة والخبرة المكتسبة من هذه الممارسات قد تكون مفيدة، يبقى على الأهالي مراقبة الوقت الذي يمضيه الأولاد على الإنترنت. والأوقات التي تعتبر الأكثر خطورة هي في المساء، لأن مريدي السوء، وإن كانوا متصلين بالشبكة على مدار الساعة، يعملون في النهار ويمضون ساعات الليل على الإنترنت محاولين إيجاد ضحايا جدد فضلاً عن ذلك، غالباً ما يقوم أصحاب النوايا السيئة بإرسال ملفات منافية للأخلاق لضحاياهم من الأطفال والمراهقين لذا على الأهالي أن يراقبوا محتويات جهاز الكمبيوتر، وأن ينتبهوا لأمر هام وهو أن الأولاد يحاولون إخفاء الملفات من هذا النوع على أسطوانات مدمجة بعيداً عن الجهاز الرئيسي. وفي حال العثور على ملفات منافية للأخلاق أو تتعارض مع العادات والدين، هذا يعني أن الأبناء قد يكونون عرضة للاستغلال عبر الإنترنت.هناك أيضاً علامة هامة، وهي تلقي اتصالات من أرقام غريبة، غالباً ما تأتي من خارج البلاد. فمريدو السوء لا يكتفون أحياناً بالحوارات الإلكترونية المباشرة في غرف الـ «شات»، بل يحاولون التقرب أكثر من الضحية باستخدام الهاتف. حتى إنه في بعض الأحيان، يبدأ الأولاد بتلقي رسائل أو هدايا من أشخاص لا يعرفهم الأهالي وهذا يعتبر جزءا من عملية «جذب» الضحية.

ومن العلامات الواضحة عن وجود خلل ما في استخدام الأبناء لتكنولوجيا الإنترنت، إقدامهم على إطفاء الشاشة عند دخول أي شخص إلى الغرفة. فحتى لو كان الأطفال هم مجرد ضحايا، ولا ذنب لهم في القضية، فغالباً ما يشعرون بالسوء والحرج عندما يتعرضون للاستغلال ويخرج الموضوع عن الإطار الصحيح. ويسعى «الأشرار» عادةً إلى إحداث فجوة بين الأهالي والأبناء وتعميقها من خلال تضخيم المشاكل التي تطرحها الضحايا على من يستمع إليها.التعاطي مع المشكلة ولعل أول ما يمكن القيام به عند الشك بأن الطفل هو عرضة للاستغلال عبر الإنترنت، هو التحدث معه حول الموضوع، وتوضيح مخاطر هذه الأمور. كما يجب مراجعة الملفات الموجودة في جهاز الكمبيوتر. وإذا كان الأهالي لا يحسنون التعاطي مع تكنولوجيا المعلوماتية،يمكنهم الاستعانة بصديق أو زميل أو

جار.. ومن الضروري أيضاً الانتباه لمصادر الاتصالات الواردة للأبناء، خصوصاً إذا كانت من خارج البلاد، في حال الشك بوجود استغلال. هذا مع الأخذ بالاعتبار أن التواصل الصوتي أصبح ممكناً وسهلاً من خلال العديد من مواقع الإنترنت، خصوصا غرف الـ«شات»التي غالباً ما تكون الوسيلة المستخدمة للإيقاع بالضحية.

وعلى الأهالي أن يقضوا بعض الوقت مع أبنائهم أمام الكمبيوتر، والطلب منهم أن يعرفوهم على المواقع التي يزورونها باستمرار. ومن الهام أن يبقى جهاز الكمبيوتر في صالة مشتركة داخل البيت، وليس في غرفة النوم الخاصة، لكي تكون الشاشة على مرأى من الجميع. ويمكن الاستعانة بخبراء المعلوماتية لوقف تشغيل أي برنامج مشتبه به أو قد يستخدمه المستغلون للتواصل مع الضحية. وفي حين أن غرف الـ «شات» تشكل فرصة هامة للتواصل مع الناس والأصدقاء ومناقشة مواضيع كثيرة ذات جدوى، من الضروري أن تبقى تحت مراقبة الأهالي لأنها الوسيلة المفضلة لدى الباحثين عن ضحايا. وإذا كان لا بد للأهالي من مراقبة البريد الإلكتروني الخاص لأولادهم، عليهم أن يفسروا لهم الأسباب الداعية لذلك.

وفي شتى الأحوال، على الراشدين أن يبقوا في بالهم فكرة هامة وهي أن الأبناء، إذا تعرضوا للاستغلال، ليسوا شركاء، بل ضحايا، وليس لديهم أي ذنب في ذلك. ومن يعمد إلى استغلال القاصرين يتحمل كل المسؤولية في هذه القضية.

توصيات أخيرة:

من الضروري الحرص على الأمور التالية:

١. عدم تسهيل حدوث أي لقاء بين القاصر وشخص آخر تعرف إليه عبر الشبكة.
٢. عدم السماح للأولاد بنشر صور لهم على مواقع عامة أو غير موثوق بها.
٣. توصية الأبناء بعدم إعطاء معلومات شخصية مثل الاسم، رقم الهاتف، العنوان، اسم المدرسة.
٤. الحرص على ألا يعمد الأولاد إلى تحميل صور من مواقع مجهولة.

ومهما كان الخطر كبيراً، لا يُنصح بمنع الأولاد من دخول الإنترنت. فالمخاطر لا تنحصر بالشبكة العنكبوتية. ولا شك أن اتخاذ الخطوات المناسبة لحماية الأبناء من خلال تثقيفهم وتنويرهم حول هذه المخاطر، يساعد على تجنيبهم الوقوع في الفخ، دون حرمانهم من الاستفادة من المزايا التي توفرها التكنولوجيا، وتحديداً الإنترنت الذي يعتبر مخزناً غير محدود للمعلومات.

﴿قانون الاتصالات (Telecommunication Law)﴾

يقصد بقانون الاتصالات الاتفاقيات التي تحكم الطرفين المستخدم والمزود سوءاً كان مزود للاتصالات السلكية أو اللاسلكية أو الاتصال عبر الإنترنت.

مزودي خدمة المعطيات (DSP) :

مزود خدمة المعطيات يعني الشركات والمؤسسات المرخص لها من قبل هيئة الاتصالات و تقنية المعلومات بتقديم خدمات البيانات ة، بما في ذلك البوابات الرئيسية التي يتم المرور عبرها إلى شبكة الإنترنت العالمية.

قد تكون شركة أو مؤسسة تملكها الدولة أو تمنح رخص تزويد خدمة الإنترنت لشركات أما محلية أو إقليمية أو دولية والتي تفرض تعرفه أو رسوم اشتراكات محددة على المستخدمين سواءً أفراد أو مؤسسات أو شركات.

وخدمة الإنترنت قد تكون عن طريق خط الهاتف العادي والتي تستخدم المودم بمنفذ RG-11 والتي تسمى (Dial up) وتكون السرعة محددة ومحصورة بـ (56 KBPS) أو تكون عن طريق خدمة الخط الرقمي أو ما يسمى (ADSL) وتوصل عن طريق كرت الشبكة (NIC) بمنفذ RG-45 وتكون سرعتها عالية تصل حتى (100 MBPS).

أسماء النطاق (Domain Name):

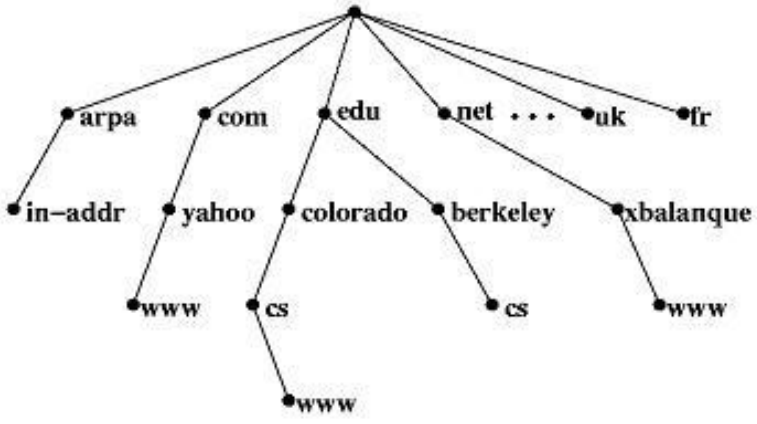
تكلمنا عن أسماء النطاق بشكل سريع فيما سبق وسوف نتكلم عنها هنا ببعض الإسهاب والتوسع.

مقدمة :

من المعروف أن جميع الأجهزة علي شبكة الإنترنت لها عنوان وحيد وهذا العنوان يطلق علية IP Address وهو مكون من أربع مقاطع وتتراوح قيمة كل مقطع من ٠ حتي ٢٥٥ مثال 192.168.0.100 ، ويمكن الوصول إلي أي جهاز عن طريق هذا الرقم ، ومن الصعوبة بمكان استخدام IP في التعاملات لذلك فانه يتم إعطاء اسم وحيد لكل عنوان حيث يتم التعامل مع هذا الاسم عوضاً عن IP مثل موقع www.google.com فإن عنوانه علي شبكة الإنترنت 216.239.59.99 ولكن كيف تتم عملية تحويل الأسماء إلي العناوين المقابلة لها لان الأصل في التعامل هو العنوان وليس الاسم ومن هنا بدأت فكرة تكوين ما يسمي "نظام أسماء النطاقات" DNS (Domain Name System) حيث يتم من خلال هذا النظام تحويل الأسماء إلي العناوين وتسمي هذه العملية Address Resolution وبالعكس يمكن الحصول علي اسم النطاق بمعلومية العنوان ، ويمكن توضيح هذا الأمر بشكل بسيط كالآتي:

١. يتم كتابة اسم الموقع www.google.com في المتصفح .
٢. يتم البحث في الجدول الخاص بأسماء النطاقات عن www.google.com .
٣. في حالة العثور علي الاسم يتم ارجاع العنوان الخاص بالموقع .

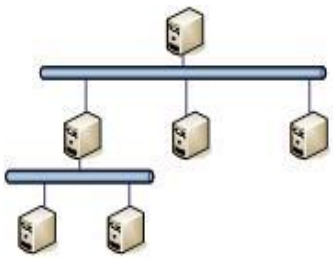
الاسم	العنوان
www.example.com	211.215.20.1
www.google.com	216.239.59.99

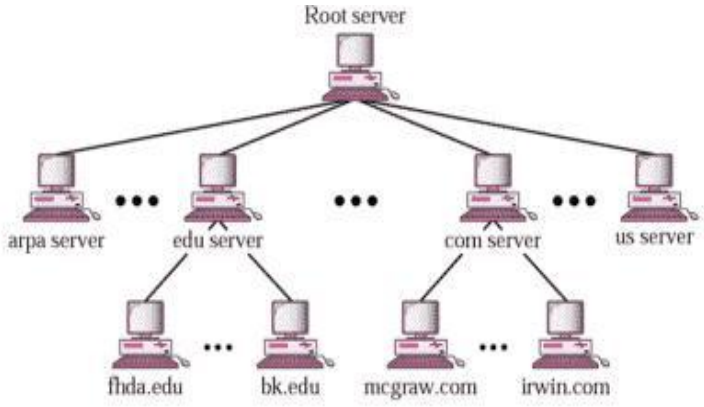


تخزن أسماء النطاقات داخل النظام بشكل شجري

ومن الممكن أيضا إجراء العملية السابقة بشكل عكسي أي أنه يمكن معرفة اسم النطاق باستخدام العنوان ويمكن الاستفادة من هذا النظام لتقديم خدمة الاستعلام عن النطاقات والمعلومات الخاصة بها والتأكد من عدم استخدام هذا النطاق من قبل جهة أخري.

ونظرا لضخامة بيانات أسماء النطاقات فإنه يتم تخزين هذه البيانات بعدة ملقمات Servers ملقم رئيسي وفرعي وهكذا .





ملقمات DNS

وبهذا الشكل يمكننا الحصول علي عنوان موقع www.google.com كالآتي:

١. يتم كتابة اسم الموقع www.google.com في المتصفح .
٢. يتم البحث داخل الملقم الرئيسي عن أسم النطاق www.google.com .
٣. في حالة العثور علي الاسم يتم أحد الأمرين:
   a. الحصول مباشرتا علي العنوان الخاص بالاسم.
   b. الإحالة إلي ملقم أخر يحتوي علي الاسم .
٤. وهكذا تتكرر العملية أ ' ب في الخطوة السابقة حتي يتم الوصول إلي عنوان الموقع.

ومن الواضح أن أي خلل في هذا النظام قد يسبب إرباك للمستخدمين فمثلا إذا تم اختراق هذا النظام بشكل أو بأخر وتم تغير عنوان موقع ما فإن المستخدم الذي سيقوم باستخدام الاسم لتصفح الموقع سوف يتصفح موقع أخر ومن هنا تأتي أهمية حماية هذا النظام والذي يعرف بحماية نظام أسماء النطاقات DNS Security .

آلية عمل "نظام أسماء النطاقات"DNS ":

كان السؤل عن متابعة وتحديث معلومات أسماء النطاقات حول العالم هو معهد

Stanford Research Institute's Network Information Center (SRI-NIC)

وكانت الطريقة المتبعة من قبل SRI-INC هي إنشاء ملف ضخم يسمي hosts.txt حيث يحتوي علي جميع أسماء النطاقات والعناوين ويقوم SRI-NIC بتحديثه ورعايته بشكل دوري .

ومع اتساع شبكة الإنترنت ونمو عدد المواقع فقد أصبح من الصعب متابعة وصيانة نظام أسماء النطاقات DNS بهذه الطريقة ولذلك فقد تم اعتماد آلية أخري وهي توزيع أسماء النطاقات علي ملقمات في صورة قواعد بيانات يمكن صيانتها وتحديثها بشكل أسهل وأسرع وقد ساعد هذا البناء علي تحسين أداء نظام أسماء النطاقات DNS بشكل كبير وهذا هو المتبع الآن وبهذه الطريقة أصبح نظام DNS غير مركزي بمعني أن معلومات أسماء النطاقات موزعة علي مجموعة من الملقمات .

تطبيقات "نظام أسماء النطاقات" DNS Implementation :

من أشهر التطبيقات علي شبكة الإنترنت لنظام أسماء النطاقات DNS هو Berkeley Internet Name Daemon (BIND) وهذا التطبيق يحتوي علي برامج خاصة بالملقمات Servers والأجهزة الطرفية Clients وكذلك مجموعة من الأدوات المساعدة للصيانة والدعم ، وقد أصبح هذا التطبيق في يومنا هذا الأشهر في العالم .

تهديدات "نظام أسماء النطاقات" Threats to the Domain Name System :

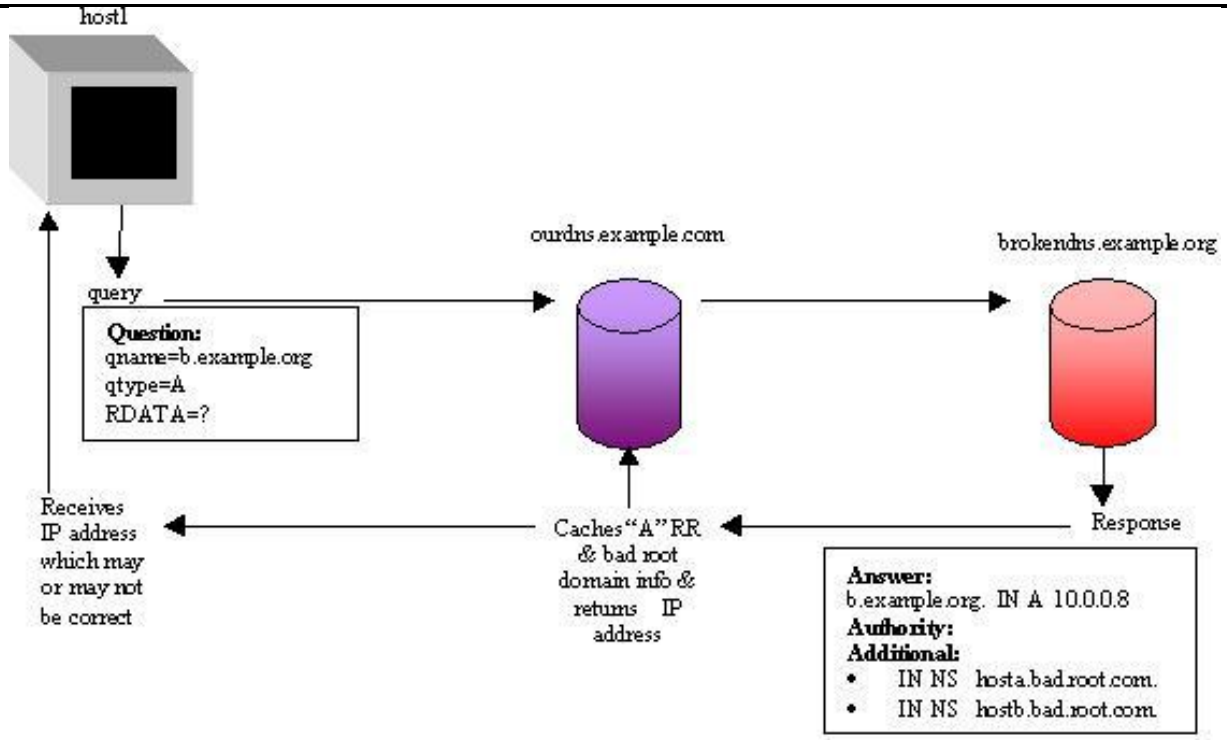
إن نظام أسماء النطاقات DNS تم بناءه في الأصل لهدف تحويل أسماء النطاقات إلي العناوين والعكس ولكن هذا النظام لم يعني في البداية ببناء نظام أمني للتأكد من صحة الإجابات التي يصدرها النظام ولذلك فقد ظهر في بعض الأوقات خلل بهذا النظام مما أدي إلي إحداث فوضي علي الإنترنت ويمكن عرض الثغرات أو الخروقات التي يتعرض لها نظام أسماء النطاقات DNS إلي عدة مستويات:

١. تلوث الذاكرة المؤقتة Cache Poisoning:

كما ذكرنا سبقا فإن طريقة عمل نظام أسماء النطاقات DNS يعتمد علي وجود ملقم رئيسي وملقمات وفرعية وسوف نستعرض الآن دور ما يسمي بالذاكرة المؤقتة في النظام ، فمثلا إذا تم الاستفسار عن عنوان موقع www.example.com فأنه:

- يتم الاستعلام عن عنوان الموقع في الملقم الرئيسي Root Server وفي حالة الإحالة إلي ملقم فرعي فأنه يتم انتظار رد الملقم حيث يقوم الملقم الفرعي بالبحث داخل قاعدة البيانات وفي حالة الحصول علي العنوان يتم إرسال النتيجة إلي الملقم الرئيسي وفي حالة الإحالة إلي ملقم فرعي أخر يتم انتظار الرد وهكذا حتي يتم الحصول علي العنوان ويتم إرسال العنوان إلي الملقم الرئيسي.
- ماذا لو تم الاستفسار مرة أخري عن عنوان الموقع www.example.com هل سيقوم الملقم الرئيسي بنفس الخطوات السابقة مرة أخري ، هنا يظهر دور ما يسمي "بالذاكرة المؤقتة " Cache ويتلخص دور الذاكرة المؤقتة في الاحتفاظ بنتائج البحث السابقة وفي حالة الاستفسار مرة أخري عن نفس العنوان فإنه يتم التأكد أولا من قاعدة البيانات الموجودة بالملقم وفي حالة عدم الحصول علي العنوان فإنه يتم التأكد من الذاكرة المؤقتة وفي حالة العثور علي الإجابة يتم الرد بناء علي البيات الموجودة بالذاكرة المؤقتة.

ويتضح من المثال السابق أن دور الذاكرة المؤقتة هو تحسين أداء النظام ، وتمكن الخطورة في هذه العملية في حالة اختراق نظام الذاكرة المؤقتة وتم تغير البيانات بداخلها ففي هذه الحالة سيقوم الملقم الرئيسي باستخدام هذه البيانات الخاطئة وبالتالي سنحصل علي نتيجة غير صحيحة للاستفسار بمعني أخر أنه في حالة الاستعلام عن عنوان الموقع www.example.com قد نحصل علي عنوان موقع أخر أو عنوان غير موجود .وتسمي هذه العملية "بتلوث الذاكرة المؤقتة" Cache Poisoning .



٢. إغمار الجهاز العميل Client Flooding:

تحدث عملية إغمار جهاز العميل Client Flooding في حالة القيام بتوجيه استفسار إلي الملقم ويتم استقبال آلاف الردود من النظام DNS ولكن هذه الردود مرسلة من قبل مهاجمين والمشكلة أنه لا توجد آلية للتأكد من مصداقية هذه الردود أي لا يمكن التأكد ما إذا كانت هذه الردود واردة بالفعل من الملقم أو من أحد المهاجمين وفي هذا السبب يكمن نجاح المهاجم في اختراق النظام .

٣. الحلّ الوسط لبيانات الخادم موضع الثّقة authoritative data Compromise of DNS server's :

من التهديدات التي تواجه نظام أسماء النطاقات DNS هو حصول المهاجم علي صلاحيات عالية داخل نظام التشغيل (مثل صلاحية root داخل نظام UNIX) مما يمكنه من تعديل معلومات المجال zone area الخاصة بالملقم .

ويمكن التغلب علي هذا التهديد بتقليص الخدمات الموجودة علي الملقم الواحد وإعطاء الصلاحية للمديرين فقط وهذا هو المتبع بتطبيق BIND .

٤. حماية "نظام أسماء النطاقات" DNSSEC :

قام مهندسي الإنترنت The Internet Engineering Task Force (IETF) بتشكّل لجنة عمل لتزويد نظام أسماء النطاقات DNS بالامتدادات الأمنيّة اللازمة لحماية النظام وعادة ما يطلق عليها امتدادات حماية نظام أسماء النطاقات DNSSEC extensions .هذه التّحسينات الأمنيّة إلى البروتوكول صممت لتكون قابلة لمعالجة الثغرات الغير مدركة داخل نظام أسماء النطاقات DNS .

ولزيادة الحماية فقد تم استخدام نظام توثيق البيانات باستخدام ما يسمي بالمفتاح العام والخاص Public and Private Key حيث يتم تشفير البيانات باستخدام المفتاح الخاص بالملقم ويقوم الجهاز الطرفي بالتأكد من صحة مصدر البيانات عن طريق المفتاح العام للملقم وبذلك يكون قد تم إنجاز خطوة هامة في حماية ودرجة وثوقية البيانات .

الـ IDN:

الـ IDN هي اختصار لـ Internationalized Domain Namesو هي عبارة عن نطاقات تكتب باللغات المحلية و يتم تحويلها إلى الإنجليزية لتعريفها على الانترنت و أطلقتها شركة VeriSign لمساعدة أصحاب العلامات التجارية للحفاظ على أسماء شركاتهم بلغاتهم المحلية في نوفمبر من عام ٢٠٠٠ بشكل تجريبي و هي مقتصرة على بعض الامتدادات ، كما أنها ليست مدعومة من كل لغات العالم ، و لكنها تدعم الشائع منها:

http://www.يبرع.com

http://www.网域com

http://www.ドメイン123.net

يصل عدد اللغات المدعومة إلى ٣٥ لغة من ضمنها اللغة العربية و كذلك البنغالية و التايلندية و غيرها ،، و لكن المشكلة تتمثل في عدم دعم المتصفح (Microsoft Internet Explorer) هذا النوع من النطاقات و هذا أدى إلى الحد من انتشار هذه النطاقات بشكل كبير . والمتصفحات التي تدعم هذا النوع من النطاقات حسب موقع VeriSign هي : Camino، Epiphany، Firefox، Galeon، Konqueror، Mozilla ، Netscape Navigator، Opera و Safari.لاستعمال هذه النطاقات باستخدام الإنترنت إكسبلورر لابد من إضافة تسمى i-Nav مقدمة من شركة VeriSign.

أسماء النطاقات البديلة:

من المعلوم والمعروف لدى الجميع أنه ومنذ أن ظهرت الانترنت تدوين أسماء النطاقات باللغة اللاتينية بصيغة www.name.com أو name@domain.com.أي عدم إمكانية استخدام اللغات الأخرى لكتابة اسم نطاق ما.فأصبح تحقيق ذلك حلما للكثير من مستخدمي الانترنت.

لتحقيق هذا الحلم قامت شركة(Native Names– الأسماء البديلة الأمريكية) بتطوير حلول لنظام عناوين انترنت تدعم لغات مختلفة من جميع أنحاء العالم.، فمن المعلوم أن نشأة الإنترنت كانت في الولايات المتحدة الأمريكية ، ومنذ ذلك الحين تم اعتماد نظام الترميز ASCII المبني على سبع خانات (8bits) والذي لا يدعم سوى الحروف و الرموز الإنجليزية ، وقد أدى ذلك إلى اعتماد هذه الطريقة في نظام أسماء النطاقات ، و الذي بدوره أصبح لا يدعم سوى الحروف و الأرقام و الرموز الإنجليزية . لكن في الوقت الراهن أصبح هناك توجه قوي نحو اعتماد نظام أسماء نطاقات متعدد اللغات يسمح بإعطاء أسماء النطاقات بلغات غير الإنجليزية ، وهذا التوجه نابع من الرغبة في جعل الإنترنت أكثر انتشارا و حل مشكلة التزاحم على أسماء النطاقات الإنجليزية .وقد قدمت العديد من الحلول و الاقتراحات كضوابط لأسماء النطاقات العربية، و يرعى هذه الجهود عدد من الجهات و المنظمات الإقليمية و العالمية الغير ربحية والتي تسعى لإيجاد معايير لتعدد اللغات على الإنترنت ، ومن هذه الجهات:

:MINC

هي منظمة دولية غير حكومية وغير ربحية ، هدفها الزيادة في تعددية اللغات على الإنترنت ، ويشمل ذلك تعددية اللغات في : أسماء النطاقات ، المصطلحات الرئيسية والأنظمة و المعايير القائمة ، علما أن هذه المنظمة تلعب دورا مهما في التنسيق مع الجهات الأخرى المهتمة بهذا الموضوع

:INC

أنشئت في أبريل عام ٢٠٠١ خلال اجتماع عمان–الأردن . وهدف هذه المنظمة هو تنسيق الجهود بين الناطقين بالعربية من أجل زيادة المحتوى العربي على الإنترنت ، و محاولة تسخير تقنيات المعلومات من أجل خدمة اللغة العربية و تراثها ، وقد تبنت هذه المنظمة عملية تعريب أسماء النطاقات كواحد من أهم التحديات التي تواجه الناطقين بالعربية على الإنترنت .

تعتبر هذه التقنية في نظام أسماء النطاقات حلا متينا يعمل بتفوق ويندمج بشفافية مع البنية التحتية الحاضرة لنظام التسميات التقليدي والذي لا يسمح إلا بالحروف اللاتينية. وتمكنك هذه التقنية بدون تصادم مع النظام القديم من أن تستعمل أسماء نطاقات بكل اللغات الحية الرئيسية المكتوبة بالحروف اللاتينية وغير اللاتينية مع كل البروتوكولات الشائعة الاستعمال كالبريد الإلكتروني و http و ftp و telnet و gopher وغيرها. وتعتمد تقنية الأسماء البديلة هذه على تشفير دولي يدعى UTF-8 يتوافق مع تشفير ASCII الذي يستعمل في كتابة العناوين بالحروف اللاتينية. ولهذا فهي قابلة للتطور ولا تتصادم مع أي من المعايير الموجودة حاليا.

يتواصل نظام التسميات بكل شفافية و تناسب مع أنظمة BIND 9.x الحالية. ويؤمن هذا التناسب والتجانس مع باقي الانترنت انعدام التصادمات كما يؤمن فعالية DNS حتى إن أي مزود DNS في العالم يمكنه أن يحل أي سؤال عن أي اسم نطاق في العالم بكل فعالية. وتكمن إحدى الايجابيات في تقنية

الأسماء البديلة في أنها لم تغير شيئا من بنية الـ DNS الموجودة و تقدم بالرغم عن ذلك دعما لمختلف اللغات على مستوى الشبكة و على مستوى برامج الحاسوب التي تستعمل الشبكة. وعلاوة على هذا فإنها لا تعرض أمن الـ DNS لأي خطر، ذلك أنها متناسبة تماما مع مواصفات أمن الـ DNS الحالية (DNS).

كيف يجيب النظام الحالي على طلبات أسماء النطاق بالإنجليزية:

عندما يتلقى مزود الدي إن إس السؤال من طرف البرنامج الزبون الذي هو غالبا متصفح المستعمل يبحث في ذاكرته ليجد العنوان المطابق للاسم الذي سئل عنه، فإن وجد الجواب رد العنوان الرقمي للزبون. وإلا بعث بالمسؤولية إلى مزود الـ DNS جذري، فينظر هذا الأخير إلى الاسم المسئول عنه ليحدد إلى إي نطاق أعلى أو إلى أي نطاق قطري تنتمي ويقرر بناء على ذلك إلى أي مزود DNS ثانوي يبعث بالسؤال ، وبعد أن يوجد حل للسؤال يُبعث بالجواب إلى متصفح المستعمل على هيئة عنوان رقمي مطابق لمواصفات بروتوكول الإنترنت، وحينها يستعمل المتصفح هذا العنوان الرقمي ليتصل بالمزود الذي يبحث عنه.

عمل نظام الـ DNS على التقنية الجديدة على أسماء النطاق المتعددة اللغات:

على البرنامج الزبون أن يبعث بسؤاله بتشفير UTF-8 إلى مزود DNS متوافق مع تقنية الأسماء البديلة، والشرط الوحيد للتوافق مع نظام الأسماء البديلة هو ترقية برنامج BIND 9.x فما فوق، وهذا أمر في منتهى البساطة بالنسبة لمقدمي خدمات الإنترنت ولغيرهم من الذين يديرون مزودات DNS. ويترجم نظام DNS في تقنية الأسماء البديلة الاسم المشفر بتشفيرUTF-8 إلى عنوان إنترنت رقمي دون أن يمس ذلك ببنية الـ DNS المنتشرة حاليا أو يتطلب حصول أي تغيير عليها وبهذا يفتح نظام الأسماء البديلة آفاقا جديدة أمام مستعملي إنترنت إكسبلورر إصدار ٥.٠ فما فوق وذلك بتمكينهم من استعمال أسماء النطاقات المتعددة اللغات.

ومن مزايا تقنية الأسماء البديلة البساطة فهي تمكن من استعمال الحروف غير اللاتينية في أسماء النطاقات وترجمة هذه الأسماء إلى عناوين رقمية دون أن تتطلب أي تغيير قل أو كثر لبروتوكول DNS الأصلي.

إضافة إلى ذلك التوافق فنظام الأسماء البديلة لا يقوم على أي تغيير لبروتوكول DNS ولا لبرنامج بايند وهو البرنامج المستعمل في الغالبية العظمى من مزودات DNS. ولهذا فإن هذا النظام متوافق تمام التوافق مع الـ DNS الشائع حاليا فيما يخص التعامل مع السجلات و استقبال الإرساليات وبعثها وما إلى ذلك من الأمور.

التعامل مع الأنظمة الأخرى،سمة يتميز بها نظام الأسماء البديلة بالتوافق القبلي، أي أنه يعمل بفعالية مع كل ما كان قبله في عالم الـ DNS ، بما في ذلك هيكلية الـ DNS وهرميته، كل هذا مع دعم للغات ذات الكتابة غير اللاتينية لم يسبق له مثيل.
كما يدعم نظام الأسماء البديلة كل اللغات التي يدعمها تشفير اليونيكود/ إيسو(Unicode/ISO) (المنظمة الدولية للمعايير)، ولهذا فإنه يسمح مستقبلا بإضافة الحروف والرموز التي قد تفرض الأيام الحاجة إلى إضافتها،وهذا ما يميزها بقابلية التوسيع.
المرونة،يستعمل نظام الأسماء البديلة تشفير UTF-8 الذي يرمز إلى الحروف اللاتينية بنفس القيم الرقمية التي يرمز بها إليها نظام تشفير الآسكي المستعمل في نظام الـ DNS التقليدي. وبضمان التوافق التام مع تشفير الآسكي فإن نظام الأسماء البديلة يمكنه استعمال أي تشفير متوافق مع الآسكي إذا اختير هذا التشفير كمعيار دولي في المستقبل.

الـ ICANN:

الـ هي اختصار لـ ICANN:(Internet Corporation for Assigned Names and Numbers

(الآيكان ICANN) هي منظمة تم تأسيسها دوليا لتتولى:

١. مسؤولية توزيع مجالات العناوين في بروتوكول الإنترنت .
٢. تخصيص معرّفات البروتوكول وإدارة نظام سجلات المواقع العامة عالية المستوى (gTLD) وسجلات المواقع عالية المستوى لرمز الدولة (ccTLD) .
٣. لها مسؤولية تجاه وظائف إدارة نظام الخوادم المركزية.
٤. بتنفيذ السياسة الموحدة لحل نزاعات أسماء المواقع (UDRP)

وقد كانت هذه الخدمات تقدم أصلاً، بموجب عقد حكومي أمريكي، من قبل سلطة تخصيص أسماء الإنترنت (IANA) وغيرها من الهيئات، أما الآن فتقوم الآيكان بالمهام التي كانت تؤديها السلطة.

ونظراً لكونها شراكة بين القطاعين العام والخاص، تلتزم ICANN بالمحافظة على الاستقرار التشغيلي لشبكة الإنترنت وتحقيق تمثيل واسع النطاق لمجتمعات الإنترنت العالمية، إضافة إلى سعيها لصياغة سياسات تلائم رسالتها من خلال عمليات تعتمد على استطلاع الآراء من القاعدة إلى القمة مروراً بجميع المستويات.

تتولى الآيكان مسؤولية تنسيق إدارة العناصر الفنية في نظام أسماء المواقع وذلك لضمان تيسير الاتصال على نطاق العالم،بحيث يتسنى لجميع مستخدمي الإنترنت إيجاد العناوين الصحيحة . وتقوم الآيكان بهذا عن طريق مراقبة توزيع المعرّفات الفنية المستخدمة في عمليات الإنترنت، وتخصيص أسماء المواقع العليا (ومثال ذلك .com، .info، وغيرها).

أما المواضيع الأخرى التي يُعنى بها مستخدمو الإنترنت مثل قواعد المعاملات المالية والرقابة على محتوى الإنترنت والبريد الإلكتروني غير المرغوب (Spam) وحماية البيانات فهي خارج نطاق مهمة الآيكان في مجال التنسيق الفني.

كما اعتمدت الآيكان إرشادات خاصة بنشر أسماء المواقع الدولية (IDN)، مما أتاح الفرصة لتسجيل مواقع بمئات اللغات حول العالم.

وفي عام ٢٠٠٠ استحدثت سبعة أسماء مواقع عامة عالية المستوى وهي:

.coop, .info, .museum, .name, .pro ،.aero, .biz

﴿القوانين الدستورية (Constitutional Law)﴾

الحرية في استخدام الإنترنت:

يقصد بالحرية في استخدم الإنترنت إلى أي مدى يحق للشخص بتصفح موقع أو الكتابة في موقع أو استخدام مواقع الإنترنت بأي طريقة قبل أن يتعرض للمنع من استخدام ذلك الموقع أو قد يتعرض للعقوبة الجنائية والتي تحددها القوانين المختلفة لكل بلد .

فهناك قوانين تنظم عملية استخدام الإنترنت بحيث لا تسمح للشخص بتجاوز صلاحياته في استخدام الإنترنت وكذلك تحمي المستخدم من أي إجراء تعسفي قد يقع ضد حريته في استخدام الإنترنت من أي جهة كانت.

بحث ومراقبة القرص الصلب والإنترنت (مثل البريد الإلكتروني):

إن عملية المراقبة سواء كانت للقرص الصلب أو للإنترنت وهو الغالب وعلى رأسها مراقبة البريد الإلكتروني هو انتهاك لخصوصيات وحريات الأشخاص والتي هي مكفولة بجميع الشرائع السماوية والقوانين الدستورية فلا يحق لأي جهة كانت أن تقوم بمراقبة بريد إلكتروني لأي شخص عبثاً وإنما يتوجب أن تكون هناك أسباب تحتم على الجهة المخولة بذلك مراقبة البريد الإلكتروني كأن يكون الشخص محل شبه مثلاً وحتى وأن كان الشخص كذلك فلا يجب أن تكون المراقبة والمتابعة عبثية وإنما يجب أن تنظمها القوانين وتشرف عليها الجهات ذات العلاقة.

من يملك بريدنا الإلكتروني بعد موتنا ؟ أو هل يورث البريد الإلكتروني؟

قلّة هم أولئك الذين سألوا أنفسهم هذا السؤال أو الذين خطر على بالهم أساسًا ، لكن قي هذا العصر عصر المعلومة والذي أصبح لك شخص تقريباً بريد إلكتروني .

للإجابة على هذا السؤال في ما يلي هناك صورة من كتاب أبحاث في القانون وتقنية المعلومات للمحامي عدنان غسان برانبو والذي تحدث فيه عن هذا الموضوع كما ورد في الكتاب:

قائمة المراجع:

١) البرمجيات وبراءة الاختراع د. نزار الحافظ .

٢) David Brainbridge, "Introduction to computer law", forth edition, Longman, 2000.

٣) د. نزار الحافظ، م. جلال فارس الحداد، "تطبيق حماية الملكية الفكرية على برامج الحاسوب"، مكتبة الأسد، كانون الثاني ٢٠٠٠.

٤) التجارة الإلكترونية – إبراهيم بختي.

٥) الإدارة الدولية والتسويق الدولي – بحث لنيل درجة الدكتوراه . الأكاديمية الأمريكية للعلوم والتكنولوجيا – زياد قبلان.

٦) العقود الإلكترونية دراسة فقهية مقارنة – د. عبدالله بن إبراهيم الناصر.

٧) العقود الإلكترونية – منتدى طلبة جامعة البحرين _ كلية الحقوق.

٨) الملكية الفكرية في مجتمع المعلومات – محمد حجازي.

٩) حقوق الملكية الفكرية – محمد السيد عرفة – مجلة البحوث الأمنية العدد (٢٤).

١٠) القانون والإنترنت -- تنظيم الفضاء الإلكتروني – إدوارد ليليان.

١١) Trademarks on the Internet – Ronald B. Standler .

١٢) Computer Law - Ronald B. Standler .

١٣) كيف نفرق بين التشهير وكشف المفاسد؟ – د. محمد سالم.

١٤) التشهير عبر الإنترنت.. سابقة قضائية – بدر البدر.

١٥) الرقابة المنزلية على الإنترنت – هلا بطرس.

١٦) أبحاث في القانون وتقنية المعلومات – المحامي عدنان غسان برانبو – دار شعاع للنشر – ٢٠٠٧م.

١٧) http://www.rsc-northwest.ac.uk/technical/dns/The%20DNS.asp

١٨) /http://www.sanog.org-sanog1-dnstrain.pdf

١٩) http://www.fistconference.org/data/presentaciones/dnssecurity.pdf

٢٠) http://www.ep.net/training/tld-rio-day2.pdf

٢١) http://security.polito.it/doc/pub/dnssec.pdf