المملكة العربية السعودية
جـامعة حـائــل
كلية التربية
قسم الحاسب آلي

"أمن شبكة الحاسب وشبكة الانترنت "

إعداد الطالب:
حمدان لافي حمدان الويبار الشمري
الرقم الأكاديمي/٢٠٠٧٢٠٩٣٠

تحت إشراف الدكتور /علي العبد

المادة / شبكات (٢)

رمز المقرر ٣٤٣

المحـــــتويات

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

مقدمة:

الشبكات NETWORKS

الشبكات بشكل عام هي وصل الحواسيب الموضوعة على مساحة محددة من أجل الاستخدام المشترك للمعلومات .الشبكات تقدم إمكانيات مذهلة في مجال تبادل المعطيات ومجال التعامل مع الملفات لعدد من المستثمرين بآن واحد معاً ، بالإضافة إلى بساطة المشاركة في الملفات FILES يمكن لمستثمري الشبكة أن يتشاركوا في الطابعات PRINTERS وسواقات الأقراص الليزرية CD-ROM والمودم MODEM وحتى جهاز الفاكس FAX .وعموماً يقصد بالشبكة التفاعل المتداخل بين أجهزة الكمبيوتر أي كيف تعمل الأجهزة فيما بينها ضمن شبكة اتصال لتحسين قدراتك في إنجاز الأمور . وشبكات الاتصال وضعت عموماً للمشاركة في أمور مثل معالجة النصوص وبرامج أوراق العمل وفي الطابعات وفي الربط على أجهزة كمبيوتر وشبكات واسعة وأنظمة البريد هي وظيفة شبكة الاتصال .

أنواع الشبكات :

هنالك ثلاثة أنواع رئيسية من الشبكات :

(أ) الشبكات الواسعة WIDE AREA NET WORKS(WAN)

(ب) الشبكات المحلية LOCAL AREA NET WORKS (LAN)

(ت) الشبكات العنكبوتية MEDIUM AREA NET WORKS(MAN)

شبكة الحاسبات:

مجموعة من الحاسبات التي تتوزع على مواقع مختلفة و تربط بينها وسائل الاتصالات المختلفة و تقوم بجمع و تبادل البيانات الرقمية و الاشتراك في المصادر المرتبطة بها.

و من هنا يتضح لنا أن شبكة الحاسب تقوم بارسال البيانات الرقمية من اجهزة الحاسبات إلى وحداتها الطرفية و بين اجهزة الحاسبات بعضها البعض باستخدام وسائل الاتصال المختلفة كالاقمار الصناعية و الكيابل المحورية و الاسلاك الهاتفية.

أمن المعلومات والإنترنت:

الإنترنت سلاح ذو حدين، فهو مدخل للكثير من الأشياء النافعة، ولكن مع الأسف، فهو يفتح المجال أمام الكثير من الأشياء المؤذية للدخول إلى جهازك. وثمة العديد من المسائل الأمنية الواجب الاعتناء بها للإبقاء على سلاسة تشغيل أجهزة الكمبيوتر والشبكات. وسنناقش في هذا المقال أهم القضايا الأمنية وبعض الحلول لها.

ما هو أمن المعلومات؟

يعني أمن المعلومات إبقاء معلوماتك تحت سيطرتك المباشرة والكاملة، أي بمعنى عدم إمكانية الوصول لها من قبل أي شخص آخر دون إذن منك، وان تكون على علم بالمخاطر المترتبة عن السماح لشخص ما بالوصول إلى معلوماتك الخاصة.
أنت بالتأكيد لا ترغب أن يكون للآخرين مدخلاً لمعلوماتك الخاصة. ومن الواضح أن معظم الأشخاص يرغبون في الحفاظ على خصوصية معلوماتهم الحساسة مثل كلمات المرور ومعلومات البطاقة الائتمانية وعدم تمكن الآخرين من الوصول إليها، والكثير من الأشخاص لا يدركون بأن بعض المعلومات التي قد تبدو تافهة أو لا معنى لها بالنسبة لهم فإنها قد تعني الكثير لأناس آخرين وخصوصاً إذا ما تم تجميعها مع أجزاء أخرى من المعلومات. فعلى سبيل المثال، يمكن للشركة الراغبة في الحصول على معلومات شخصية عنك للأغراض التسويقية أن تشتري هذه المعلومات من شخص يقوم بتجميعها من خلال الوصول إلى جهاز كمبيوترك بشكل غير شرعي.
ومن المهم كذلك أن تفهم أنك حتى ولو لم تقم بإعطاء معلوماتك لأي شخص عبر الإنترنت، فقد يتمكن بعض الأشخاص من الوصول إلى نظام الكمبيوتر لديك للحصول على المعلومات التي يحتاجونها دون علم أو إذن منك.

المخاطر الشبكة المختلفة وسبل الحماية منهاً :

تحدث المشكلة الأمنية عندما يتم اختراق النظام لديك من خلال أحد المهاجمين أو المتسللين (الهاكر) أو الفيروسات أو نوع آخر من أنواع البرامج الخبيثة.
وأكثر الناس المستهدفين في الاختراقات الأمنية هم الأشخاص الذي يقومون بتصفح الإنترنت، حيث يتسبب الاختراق في مشاكل مزعجة مثل تبطئ حركة التصفح وانقطاعه على فترات منتظمة. ويمكن أن يتعذر الدخول إلى البيانات وفي أسوأ الأحوال يمكن اختراق المعلومات الشخصية للمستخدم.
وفي حالة وجود أخطاء برمجة أو إعدادات خاطئة في خادم الويب، فمن الجائز أن تسمح بدخول المستخدمين عن بعد غير المصرح لهم إلى الوثائق السرية المحتوية على معلومات شخصية أو الحصول على معلومات حول الجهاز المضيف للخادم مما يسمح بحدوث اختراق للنظام. كما يمكن لهؤلاء الأشخاص تنفيذ أوامر على جهاز الخادم المضيف مما يمكنهم تعديل النظام وإطلاق هجمات إغراقية مما يؤدي إلى تعطل الجهاز مؤقتاً، كما أن الهجمات الإغراقية (DoS) تستهدف إبطا او شل حركة مرور البيانات عبر الشبكة. كما أنه من خلال الهجمات الإغراقية الموزعة(DDoS) ، فإن المعتدي يقوم باستخدام عدد من الكمبيوترات التي سيطر عليها للهجوم على كمبيوتر أو كمبيوترات أخرى. ويتم تركيب البرنامج الرئيسي للهجمات الإغراقية الموزعة (DDoS) في أحد أجهزة الكمبيوتر مستخدماً حساباً مسروقاً.
إن التجسس على بيانات الشبكة واعتراض المعلومات التي تنتقل بين الخادم والمستعرض يمكن أن يصبح أمراً ممكناً إذا تركت الشبكة أو الخوادم مفتوحة ونقاط ضعفها مكشوفة.

فيروسات الكمبيوتر:

فيروسات الكمبيوتر هي الأكثر شيوعاً من بين مشاكل أمن المعلومات التي يتعرض لها الأشخاص والشركات.
وفيروس الكمبيوتر هو برنامج غير مرغوب فيه ويدخل إلى الجهاز دون إذن ويقوم بإدخال نسخ من نفسه في برامج الكمبيوتر، والفيروس هو أحد البرامج الخبيثة أو المتطفلة. والبرامج المتطفلة الأخرى تسمى الديدان أو أحصنة طروادة أو برامج الدعاية أو برامج التجسس.
يمكن للبرامج الخبيثة أن تكون فقط للإزعاج من خلال التأثير على استخدامات الكمبيوتر وتبطئيه وتتسبب في حدوث انقطاعات وأعطال في أوقات منتظمة وتؤثر على البرامج والوثائق المختلفة التي قد يرغب المستخدم في الدخول إليها. أما البرامج الخبيثة الأكثر خطورة فيمكن أن تصبح مشكلة أمنية من خلال الحصول على معلوماتك الشخصية من رسائلك الإلكترونية والبيانات الأخرى المخزنة في جهازك.
أما بالنسبة لبرامج الدعاية وبرامج التجسس فهي مزعجة في الغالب وتؤدي إلى ظهور نوافذ دعائية منبثقة على الشاشة. كما أن برامج التجسس تجمع معلوماتك الشخصية وتقدمها إلى جهات أخرى تطلب الحصول عليها لأغراض تجارية.
يمكنك حماية كمبيوترك وحماية نفسك باستخدام برامج مناسبة لمكافحة البرامج الخبيثة غير المرغوب فيها والتي قد تكون نتائجها مدمرة.
أولاً) فيروسات تقليدية Classic Virus و هي برامج هدفها تخريب النظام و إحداث أعطال و أخطاء فيه بشكل رئيسي
و هناك نوع جديد من الفيروسات يستخدم أسلوب الإلحقان بالملفات حيث يضيف جزء من كوده البرمجي إلى الملف فيصيبه و يصبح جزء منه و بشكل عام تضع الفيروسات قيودا و تعديلات في الريجستري فمثلاً تمنع المستخدم من استخدام إدارة المهام و إظهار الملفات المخفية و ملفات النظام بطئ بسبب استهلاكها لموارد النظام و غيرها الكثير و تقسم الفيروسات إلى :
١) File Viruses و تتبع واحدا على الأقل من هذه الأساليب لإصابة النظام :
أ) فيروسات منحقنه تصيب الملفات التنفيذية و في هذه الحالة عندما يكتشفه مضاد فيروسات يعطيك خيار التصحيح(Disinfect , Cure , Repair ,...etc) حيث يختلف حسب نوع مضاد الفيروسات الذي تستخدمه و من أشهر هذه الفيروسات فيروس سالتي الشهير Sality و فيروس Mabezat و للأسف أكثر الفيروسات من هذا النوع.
ب) فيرروسات تكرر الملفات الموجودة على الجهاز Duplicate Files حيث تمتلئ ذاكرة الجهاز بسبب تكرار الملفات (تخيل لديك ملفات و بيانات شركة و تملئ ٧٥% من ذاكرة الجهاز فإذا بدء الفيروس بنسخ كل ملف مرة واحدة تكون النتيجة الجهاز لا يملك ذاكرة كافية) و لهذا تسمى هذه الفيروسات بفيروسات الشركات مثل فيروس Temp.exe.

ت) و هذه الفيروسات تعمل نسخ عن نفسها في مسارات مشهورة بالجهاز، % , %Temp% ,%SystemRoot%
%systemdrive% %userprofile%,...etc،

ث) فيروسات تستعمل ميزات ملفات النظام :
١) viruses Boot sector و هي فيروسات تصيب الملفات المسؤولة عن إقلاع الجهاز و النظام . فتضيف نفسها إلى ملفات الإقلاع و قد تغير مسار تلك الملفات . و لا تصيب إلا الأقراص المرنة .
هذه الفيروسات إنتشرت في التسعينيات من القرن الماضي و لكن مع تقدم معالجات ٣٢ بت و تناقص استخدام الأقراص المرنة تضاءل عددها مع أنه من الناحية التقنية يمكن إنشاء هكذا فيروسات تعتمد على ال Cd و على الفلاشات .
٢) viruses Macro و هذه الفيروسات تصيب ملفات محررات النصوص مثل -MS Exel- MS Worde Point Power
و هذا النوع من الفيروسات غير منتشر و نادر .
حيث بمجرد فتح مثل هذه الفيروسات تصاب الملفات الأخرى بهذا الجهاز .
مثال عليها أحد الفيروسات ما أن تفتحه بالجهاز حتى تمحى كل ملفات الأوفس التي تعمل بالجهاز حتى و لو كانت مخزنة .
٣) Script Viruses و هي فيروسات تستخدم الأكواد للغات رمزية (جافا سكريبت ، فيجوال بيسك سكريبت ، Php، ملفات باتش ،...الخ)
و هي تصيب النظام و تؤدي إلى تحويل الأكواد إلى عمليات تخل بالنظام .
ثانياً) أحصنة طروادة Trojan تقسم إلى :
١) Backdoors و هي الأخطر لأنها تأخذ صلاحيات مدير نظام و تعمل بسرية تامة و من دون علم المستخدم . و تستخدم شبكة محلية أو الإنترنت للتحكم بجهاز الضحية و تتبع سلوك أدوات مدير النظام RAT = Remote Administrator Toolو الفرق الوحيد بين التروجانات و برامج الإدارة هي أن التروجانات تنزل و تعمل بدون علم المستخدم بينما أدوات الإدارة تكون واضحة و تعطيك رسالة أنها تراقب النظام و هذا النوع يستخدم للتحكم بروتوكول TCP\IP و هو نفس البروتوكول المستخدم بالمسنجر و إدارة مقاهي الإنترنت و بعض البرامج و هذا النوع يتكون من جزأين الأول بجهاز الضحية يعمل بشكل خفي بحيث يتلقى الأوامر من المخترق و الثاني عند المخترق الذي بعث التروجان
خطورتها تكمن في :
إرسال و إستقبال الملفات من و إلى جهاز الضحية
الدخول للملفات الخاصة و إمكانية حذفها و تعديلها
توجيه المستخدم إلى موقع إنترنت بدون إرادته و تغيير الصفحة الرئيسية أيضاً .
سرقة المعلومات الخاصة و كلمات السر
تشغيل البرامج و الأجهزة المرتبطة بالجهاز (طابعة أو كمرة ....الخ)
إعادة تشغيل الجهاز و إطفاءه
General Trojans و هذا النوع يخرب الجهاز و يسرق البيانات من جهاز الضحية و أغلب مبرمجين البرامج الخبيثة يضيفون خصائص كثيرة لهذا النوع
PSW Trojans و هو سارق كلمات السر حيث يقوم بفحص المواقع التي تحفظ بها كلمات السر و يأخذها ثم يرسلها للشخص الذي كونه . و بالعادة يسرق
معلومات عن النظام و الرقم التسلسلي لنظام التشغيل (بالدول الغربية نظام التشغيل غالي فسرقة الرقم التسلسلي مهم جداً)
بيانات الدخول للإنترنت (رقم البطاقة و كلمة المرور للإنترنت)
كلمات السر للألعاب على الشبكات (بعض الألعاب على الشبكة تكون بمقابل مادي)
كلمات السر للإيميل و المواقع
Clickers Trojan و هذا النوع يقوم بتوجيه الضحية لموقع معين بدون إرادته و الهدف منه هو إما زيادة العدد للزائرين لموقع معين أو إستنفاذ حجم التبادل الشهري لموقع أو الهجوم على موقع أو مخدم معين بواسطة DOS Attack أو أخذ الضحية لموقع معين حيث يكون هذا الموقع مصاباً فيتم تنزيل فيروس أو برنامج أخر بجهاز الضحية .
قد تقوم هذه البرامج أيضا من منع المستخدم من الدخول إلى مواقع معينة كمواقع شركات الحماية و التحديث فلا

يستطيع المستخدم تحديث مضاد فيروساته .
Trojan Downloaders و هي برامج تتميز بصغر حجمها و وظيفتها تنزيل برامج أخرى (تروجانات أو فيروسات) إلى جهاز الضحية .
فمثلا دمج أحدهم برنامج مكرك مع تروجان كامل (١٠٠ كيلوبايت) سيلفت الانتباه فيلجأ إلى دمجه مع برنامج صغير لا يتعدى ٥ كيلوبايت وظيفته عند الإتصال بالإنترنت تحميل الملف الكبير من الإنترنت و فتحه بجهاز الضحية
Droppers Trojan و هي برامج هدفها إخفاء البرامج الخبيثة عن أعين المستخدم أو عن مضاد الفيروسات كل ملف بالجهاز له توقيع رقمي يختلف عن غيره و مضاد الفيروسات يحوي بداخله تواقيع الفيروسات و البرامج الخبيثة (التحديث هو عملية إضافة تواقيع البرامج الحديثة المكتشفة إلى أرشيف البرنامج) فيقوم هذا النوع من البرامج بتشفير الكود البرمجي للبرنامج الخبيث و تغير توقيعه الرقمي فيصبح ملفا غير مكتشف بالنسبة لمضاد الفيروسات و يمر من قبضته .
و تحوي هذه البرامج على خيارات لإيهام الضحية أن البرنامج الذي تم إخفاؤه ملف سليم عن طريق تشغيل تطبيق أخر أو إظهار رسالة خطأ توهم المستخدم أن الملف سليم
مثال : دمج فيروس مع صورة فعند الضغط على البرنامج المشفر يظهر للضحية صورة أو دمج فيروس مع برنامج مسروق فيضغط الضحية على ملف التنصيب و ينصب البرنامج بشكل طبيعي و لا يدري أنه ينصب و بشكل خفي في جهازه فيروساً
Trojan Proxies و هي برامج تستخدم لتحويل جهاز الضحية لبروكسي يمكن الذي ارسل التروجان إلى إستخدامه للدخول للإنترنت بشكل متخفي .
و هذا النوع منتشر بكثرة بين الذين يستخدمون الرسائل المزعجة لكي يتمكنوا من الدخول لأعداد كبيرة من الأجهزة و بشكل متخفي لإرسال رسائل من أجهزة غيرهم .
Trojan Spies و هذا النوع يستخدم للتجسس على نشاطات الضحية (ليس فقط كلمات السر كما في PSW Trojans بل على نشاطات أخرى) مثل تصوير سطح المكتب أو صور من الكمرة أو أية نشاطات يقوم بها المستخدم
Trojan Notifiers و هي فقط لإعلام المخترق الذي أرسل التروجان بنجاح إصابة الجهاز بالبرنامج الخبيث حيث ترسل للمخترق معلومات عن الجهاز و IP و المنافذ المفتوحة .
كثير من Backdoors و PSW Trojans ترسل مثل هذه التنبيهات أيضاً .
Rootkits و هي برامج تقوم بإخفاء نشاطات التروجانات عن البرامج و لكن بطريقة لا تثير الريبة أبداً حيث تبقى مثلا إدارة المهام فعالة و لكن لا تظهر فيها أية نشاطات للتروجانات و لا تظهر بلوحة العمليات و تقوم بإخفاء نفسها بمفاتيح بالريجستري و قد تقوم أيضا بسرقة المعلومات الخاصة كسارق كلمات السر و تتميز هذه البرامج أنها تضيف نفسها كملفات نظام و تأخذ حقوق المدير .
ArcBombs و هي ملفات مؤرشفة صممت لتخريب الملفات المضغوطة حيث تتضاعف أحجامها تلقائيا ألوف المرات فتتخرب و يمتلئ الجهاز بملفات فارغة تسمى قنابل الهواء
خطورتها تكمن في إصابة خوادم الإنترنت و مخدمات البريد الإلكتروني .
هناك ثلاث أنواع لها الأول :
النوع الأول يملئ الملفات المضغوطة بمعلومات و بيانات مكررة
النوع الثاني يخرب الملفات المضغوطة
النوع الثالث يضغط الملفات بشكل صغير جدا فمثلا حجم ٥ جيجا يصبح ٢٠٠ كيلو بايت

الهاكر:

الهاكر هو الشخص الذي يقوم بإنشاء وتعديل البرمجيات والعتاد الحاسوبي. وقد أصبح هذا المصطلح ذا مغزى سلبي حيث صار يطلق على الشخص الذي يقوم باستغلال النظام من خلال الحصول على دخول غير مصرح به للأنظمة والقيام بعمليات غير مرغوب فيها وغير مشروعة. غير أن هذا المصطلح (هاكر) يمكن أن يطلق على الشخص الذي يستخدم مهاراته لتطوير برمجيات الكمبيوتر وإدارة أنظمة الكمبيوتر وما يتعلق بأمن الكمبيوتر.

اللصوصية(Phishing) :

يستخدم مصطلح (Phishing) للتعبير عن سرقة الهوية، وهو عمل إجرامي، حيث يقوم شخص أو شركة بالتحايل والغش من خلال إرسال رسالة بريد إلكتروني مدعياً أنه من شركة نظامية ويطلب الحصول من مستلم الرسالة على المعلومات الشخصية مثل تفاصيل الحسابات البنكية وكلمات المرور وتفاصيل البطاقة الائتمانية. وتستخدم المعلومات للدخول إلى الحسابات البنكية عبر الإنترنت والدخول إلى مواقع الشركات التي تطلب البيانات الشخصية للدخول الى الموقع.
هناك برامج لمكافحة اللصوصية Phishing والكشف عن هوية المرسل الحقيقي، وأفضل وسيلة لحماية الشخص من نشر معلوماته الشخصية لمن يطلبها هو أن يكون الشخص متيقظاً وحذراً ولديه الوعي الكافي، فلا يوجد هناك أي بنك معروف أو مؤسسة فعلية يطلبون من عملائهم إرسال معلوماتهم الشخصية عبر البريد الإلكتروني.

البريد الإلكتروني:

يجدر بنا أن نتذكر دائماً إلى أن البريد الإلكتروني لا يضمن الخصوصية، فخصوصيته تشابه خصوصية البطاقة البريدية. ويتنقل البريد الإلكتروني في طريقه إلى المستلم عبر العديد من الخوادم حيث يمكن الوصول إليه من قبل الأشخاص الذين يديرون النظام ومن الأشخاص الذين يتسللون إليه بشكل غير نظامي. والطريقة الوحيدة للتأكد إلى حد ما من خصوصية بريدك الإلكتروني هو تشفيره.

سبل الحماية منهاً:

عليك بالحذر والحرص الدائمين لحماية نظامك كي لا يكون عرضة للهجمات بسبب نقاط الضعف فيه، ويمكنك تركيب برامج فعالة لجعل استخدام الإنترنت أكثر أماناً لك.

الحصول على جدار حماية ناري(Firewall) :

جدار الحماية الناري من الإنترنت هو برنامج أو جهاز يقوم بفرز وتصفية الفيروسات والديدان والمتسللين والمعتدين الذين يحاولون الوصول إلى جهازك عبر الإنترنت .ويعتبر تركيب جدار حماية ناري أكثر الطرق فاعلية، وأهم خطوة أولية يمكنك اتخاذها لحماية جهاز الكمبيوتر لديك هو القيام بتركيب جدار حماية ناري قبل الدخول إلى الإنترنت للمرة الأولى والإبقاء عليه عاملاً في كافة الأوقات.
يمكنك الحصول على جدار حماية ناري لجهازك من محلات الكمبيوتر أو من خلال الإنترنت. علما أن بعض أنظمة التشغيل مثل ويندوز إكس بي مع الحزمة الخدمية/الإصدار-٢ (Service Pack2) ونظام التشغيل ماكنتوش (MacOS X)يوجد من ضمنها جدار حماية ناري.

الحصول على برنامج مكافحة فيروسات :

إضافة لبرنامج الحماية الناري(Firewall) ، فإن عليك الحصول على برنامج مكافحة فيروسات قبل الدخول إلى الإنترنت للمرة الأولى. حيث يقوم برنامج مكافحة الفيروسات بفحص جهازك لمعرفة الفيروسات الجديدة التي أصيب بها ومن ثم تنظيف هذه الفيروسات بما يكفل عدم إلحاق المزيد من الأذى بجهازك.
وكما هو الحال في جدار الحماية الناري، فإن عليك الإبقاء على برنامج مكافحة الفيروسات عاملاً في جميع الأوقات بحيث أنه بمجرد تشغيل جهازك يبدأ البرنامج بالعمل للكشف عن الفيروسات مما يضمن التعامل معها بأسرع ما يمكن.
كما يقوم برنامج مكافحة الفيروسات بالكشف عن الفيروسات في الأقراص المدخلة في جهازك والبريد الإلكتروني الذي تستلمه والبرامج التي تقوم بتحميلها في جهازك من الإنترنت.
في حالة دخول فيروس إلى جهازك، فإن برنامج مكافحة الفيروسات سينبهك بذلك ومن ثم سيقوم بمحاولة إصلاح الملف المصاب، كما يقوم هذا البرنامج بعزل الفيروسات التي لا يستطيع إصلاحها مع محاولة إنقاذ وإصلاح أية ملفات مصابة يستطيع إصلاحها. هذا علماً بأن بعض برامج مكافحة الفيروسات تطلب منك إرسال الفيروس إلى شركة مكافحة الفيروسات، كي يتسنى لها إدخاله ضمن قاعدة بياناتها إذا كان من الفيروسات الجديدة.
يمكنك شراء برامج مكافحة الفيروسات عبر الإنترنت أو من محلات بيع البرمجيات، كما يستحسن التأكد فيما إذا كان مزود خدمات الإنترنت الذي تتعامل معه يزود مثل هذه البرمجيات. ومما تجدر ملاحظته، أنه في حالة كون جهازك مصاباً بالفيروسات، فمن الخطر شراء برنامج الحماية عبر الإنترنت لأنه يمكن لبرنامج التجسس التلصص على

معلومات بطاقتك الائتمانية وسرقتها حتى ولو أدخلتها في صفحة ويب آمنة.
يجب أن يكون برنامج مكافحة الفيروسات مناسباً لجهاز الكمبيوتر لديك والبرامج التي لديك. وهناك العديد من أنواع البرامج المتوفرة التي تناسب مستخدمي أنظمة التشغيل ويندوز ولينكس وماكنتوش .(MacOS) علماً بأن أكثر برامج مكافحة الفيروسات استخداماً هي البرامج المزودة من ماكافي(McAfee) ، ونورتن (Norton Antivirus) من سيمانتك(Symantic) ، وأنظمة سيسكو (Cisco System) وميكروسوفت.(Microsoft)

حافظ على تحديث برامج وجهازك:

نظراً لأن الفيروسات تتغير باستمرار، فمن الأهمية بمكان قيامك بالتحديث المستمر لنظام التشغيل الموجود في جهازك وبرنامج جدار الحماية الناري وبرنامج مكافحة الفيروسات المركب في جهازك، بحيث يتم إدخال آخر تحديثات صدرت عن هذه البرامج .وسيقوم برنامج مكافحة الفيروسات بسؤالك تلقائياً بتحديث البرنامج وعليك التأكد من قيامك بالتحديث.
علماً بأن الكثير من برامج مسح الفيروسات يمكن الحصول عليها مرة كل سنة، وننصحك بترقية البرنامج بعد ذلك حفاظاً على تضمين جهازك آخر التحديثات.

لا تفتح رسائل البريد الإلكتروني المشكوك فيها:

تصل معظم الفيروسات إلى أجهزة الكمبيوتر عبر البريد الإلكتروني، لذا لا تفتح أي مرفقات بريد إلكتروني لا تعرف مصدره أو غير متأكد من محتوياته حتى ولو كنت تستخدم برنامج مكافحة فيروسات. مع ملاحظة أنه يمكن أن تصلك رسائل بريد إلكتروني مصابة بالفيروسات حتى من أصدقائك وزملائك والمسجلين لديك في قائمة البريد الإلكتروني.
ولا يكون الفيروس خطيراً إلا إذا فتحت المرفقات المصابة. وتأكد من أن محتويات الرسالة تبدو منطقية قبل فتح المرفقات. كما يجدر بك ألا تقوم بتمرير أو إحالة أي مرفقات قبل أن تتأكد من أنها آمنة. وقم بحذف أية رسالة تعتقد أنها مصابة وقم كذلك بتفريغ الرسائل المحذوفة من المجلد الذي يحتوي عليها بشكل منتظم.

الحذر عند إقفال النوافذ المنبثقة:

النوافذ المنبثقة هي النوافذ التي تقفز على شاشة الكمبيوتر لديك عند ذهابك إلى مواقع إلكترونية محددة. وبعض المواقع الإلكترونية تحاول خداعك لتنزيل برامج تجسس أو برامج دعاية في جهازك من خلال الضغط على موافق (OK) أو اقبل (Accept) الموجودة في النافذة المنبثقة. وعليك إتباع وسيلة آمنة لإقفال هذه النوافذ آلا وهي الإقفال من مربع العنوان (X) الموجود في أعلى النافذة.

فكر ملياً قبل تنزيل ملفات من الإنترنت:

يمكن كذلك أن تُصاب بفيروسات وبرامج دعاية وبرامج تجسس من خلال تنزيل برامج وملفات أخرى من الإنترنت.
فإذا كان البرنامج مجانياً ومزود من قبل مطور برمجيات مجهول، فهو من المرجح أن يحتوي على برمجيات إضافية وغير مرغوب فيها أكثر مما لو كانت قد تمت بتنزيل أو شراء برنامج من مطور برمجيات مشهور ومرموق.
ولحسن الحظ، فإن نظام الترشيح المعمول به في المملكة العربية السعودية، يحمي مستخدمي الإنترنت من الدخول مصادفة إلى معظم المواقع الإلكترونية الخطيرة، ولكن من الحكمة والتعقل توخي الحذر عند تنزيل ملفات من الإنترنت أو إقفال النوافذ المنبثقة غير المرغوب فيها.

برامج مراقبة بيانات الشبكةPacket Sniffers :

طريقة فعالة لمراقبة الحركة المرورية عبر الشبكة باستخدام أحد برامج مراقبة بيانات الشبكة، حيث يتم من خلاله تجميع البيانات الداخلة والخارجة، وهي طريقة ممكن أن تكون مفيدة في الكشف عن محاولات التسلل عبر الشبكة، وكذلك يمكن استخدامها لتحليل مشاكل الشبكة وتصفية وحجب المحتوى المشكوك فيه من الدخول إلى الشبكة.

عمل نسخ احتياطية من ملفاتك:

لتفادي فقد ملفات العمل لديك في حالة تعرض كمبيوترك للإصابة بالفيروسات، عليك التأكد من عمل نسخ احتياطية لملفاتك المهمة. وإذا كنت تقوم بشكل منتظم بعمل نسخ احتياطية للمعلومات الموجودة في جهازك على أقراص صلبة خارجية أو أقراص ضوئية قابلة للكتابة أو أقراص مرنة، فلا تضع أقراص النسخ الاحتياطية المساندة في جهاز الكمبيوتر لديك إذا كنت تعتقد أن لديك فيروساً، لأنه يمكن للفيروس الانتشار إلى تلك الأقراص.

التحديثات:

حافظ على تحديث جميع برامجك بما في ذلك أحدث نسخة من برنامج التشغيل الذي تستخدمه. وإذا كنت تستخدم التحديث التلقائي الذي يقوم بالبحث يومياً عن التحديثات عند بدء تشغيل الجهاز، فعليك إعادة تشغيل جهازك يومياً.

التشفير:

التشفير هو ترميز البيانات كي يتعذر قراءتها من أي شخص ليس لديه كلمة مرور لفك شفرة تلك البيانات. ويقوم التشفير بمعالجة البيانات باستخدام عمليات رياضية غير قابلة للعكس. ويجعل التشفير المعلومات في جهازك غير قابلة للقراءة من قبل أي شخص يستطيع أن يتسلل خلسة إلى جهازك دون إذن. ومن أشهر برامج التشفير.

كيف يمكنني الحصول على برامج مكافحة الفيروسات أو جدار الحماية الناري؟

كيف تعرف فيما إذا كان لديك جدار حماية ناري أو برنامج مكافحة فيروسات مركبة في جهازك؟
جدار الحماية الناري :إذا كنت تستخدم نظام تشغيل بخلاف ويندوز اكس بي مع الحزمة الخدمية/ الإصدار الثاني (service pack2)أو ماكنتوش(MacOSX) ، إذن عليك المبادرة بالبحث عن برنامج حماية يحتوي اسمه على (Firewall).
برنامج مكافحة الفيروسات :ابحث عن برنامج يوجد ضمن اسمه كلمة (antivirus) وهناك كلمات توجد في أسماء البرامج تدل على أنها برامج مكافحة فيروسات أو جدار حماية ناري مثل "Guard" أو"Defender" ، حيث تتغير الأسماء والماركات من وقت لآخر، فأفضل شئ أن تسأل الشخص الذي اشتريت جهاز كمبيوترك منه فيما إذا ركب فيه برنامج مكافحة فيروسات أو جدار حماية ناري.

كيف تجد أفضل البرامج لجدار الحماية الناري أو مكافحة الفيروسات؟

لعل أسهل الطرق لإيجاد برامج جيدة لجدار الحماية الناري أو مكافحة الفيروسات هو الذهاب للمحل الذي اشتريت منه جهازك وطلب مشورتهم في هذا الأمر.

أما إذا أردت قائمة أفضل برامج جدار الحماية الناري أو مكافحة الفيروسات من الإنترنت، فابحث في الإنترنت عن أفضل البرامج باستخدام الكلمات التالية (Top Firewalls) أو (Top Antivieus) ثم اكتب السنة الحالية، وهناك الكثير من المواقع الإلكترونية تحتوي على قوائم بأفضل البرامج. وعلى سبيل المثال فإن المواقع الإلكترونية الخاصة بمجلات الكمبيوتر تعتبر مصدراً موثوقاً لهذه المعلومات، واحرص على قراءة آخر القوائم لديهم.
عند العثور على برنامجين يناسبانك واحد لجدار الحماية الناري والآخر لمكافحة الفيروسات، اذهب للمواقع الإلكترونية لهذه البرامج حيث أن جميع الشركات المطورة لبرامج الموثوقة تقدم الكثير من المعلومات عن برامجهم ضمن مواقعهم الإلكترونية. ابحث عن نبذة (Snapshot) من هذه البرامج ثم اختر قسم المساعدة للحصول على المعلومات حول تنزيل هذه البرامج وتثبيتها في الجهاز واستخدامها

نظم التشفير

عُرف علم التشفير أو التعمية منذ القدم، حيث استخدم في المجال الحربي والعسكري. فقد ذكر أن أول من قام بعملية التشفير للتراسل بين قطاعات الجيش هم الفراعنة. وكذلك ذكر أن العرب لهم محاولات قديمة في مجال التشفير. و استخدم الصينيون طرق عديدة في علم التشفير والتعمية لنقل الرسائل أثناء الحروب. فقد كان قصدهم من استخدام التشفير هو إخفاء الشكل الحقيقي للرسائل حتى لو سقطت في يد العدو فإنه تصعب عليه فهمها. وأفضل طريقة استخدمت في القدم هي طريقة القصير جوليوس وهو أحد قياصرة الروم. أما في عصرنا الحالي فقد باتت الحاجة ملحة لاستخدام هذا العلم "التشفير" وذلك لإرتبط العالم ببعضه عبر شبكات مفتوحة. وحيث يتم استخدام هذه الشبكات في نقل المعلومات إلكترونياً سواءً بين الأشخاص العاديين أو بين المنظمات الخاصة والعامة، عسكرية كانت أم مدنية. فلابد من طرق تحفظ سرية المعلومات. فقد بذلت الجهود الكبيرة من جميع أنحاء العالم لإيجاد الطرق المثلى التي يمكن من خلالها تبادل البيانات مع عدم إمكانية كشف هذه البيانات.

ومازال العمل والبحث في مجال علم التشفير مستمراً وذلك بسبب التطور السريع للكمبيوتر والنمو الكبير للشبكات وبخاصة الشبكة العالمية الإنترنت.

يتم حماية الشبكة اللاسلكية باستخدام بروتوكول تشفير الشبكات اللاسلكية .(WEP) ويعمل هذا البروتوكول بتضمين مفتاح مشترك ٦٤ أو ١٢٨ بت بين العملاء ونقطة الدخول، ومن ثم يتم استخدام هذا المفتاح لتشفير وفك تشفير البيانات بينهم، وهذا يوفر قدر كاف من الأمن للشبكات المنزلية. عليك الرجوع إلى الوثائق الخاصة بالأجهزة اللاسلكية لديك لتعرف كيفية تمكين وإعداد بروتوكول التشفير اللاسلكي (WEP) على شبكتك. أما بالنسبة لبيئات الشركات، فيجب اعتبار هذا البروتوكول (WEP) فقط كنقطة بداية للترتيبات الأمنية، وعلى الشركات البحث جدياً في ترقية شبكاتهم اللاسلكية إلى مستوى (WPA) أكثر أماناً.

ما هو التشفير أو التعمية (Cryptography) :

التشفير هو العلم الذي يستخدم الرياضيات للتشفير وفك تشفير البيانات. التشفير يُمكِّنُك 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.

التشفير هو ترميز البيانات كي يتعذر قراءتها من أي شخص ليس لديه كلمة مرور لفك شفرة تلك البيانات. ويقوم التشفير بمعالجة البيانات باستخدام عمليات رياضية غير قابلة للعكس. ويجعل التشفير المعلومات في جهازك غير قابلة للقراءة من قبل أي شخص يستطيع أن يتسلل خلسة إلى جهازك دون إذن. ومن أشهر برامج التشفير(PGP)

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**).

الشهادة الرقمية

تعريف الشهادة الرقمية :

"هي وثيقة رقمية تحتوي على مجموعة من المعلومات التي تقود إلى التحقق من هوية الشخص أو المنظمة أو الموقع الإلكتروني و تشفر المعلومات التي يحويها جهاز الخادم (server) عبر ما يسمى بتقنية (Secure 1] (Sockets Layer SSL].

مفاهيم أساسية:

المفتاح الخاص:

مفتاح سري يستخدمه صاحبه لفك تشفير الرسائل المرسلة له. وكذلك يستخدمه للتوقيع الالكتروني. ومن مسؤولية صاحبه المحافظة على سريته.

المفتاح العام:

مفتاح ليس سري يستخدم لتشفير الرسائل المرسلة لصاحب هذا المفتاح. وكذلك للتحقق من توقيعه.

هيئة التوثيق (Certification Authority):

هي الجهة التي تقوم بإصدار الشهادة الرقمية والتوقيع عليها. قبل أن تقوم الهيئة بالتوقيع على الشهادة تتأكد من هوية الشخص (صاحب الشهادة) وتتم عملية التأكد من الهوية على حسب استخدامات الشهادة الرقمية فإذا كانت ستستخدم لحماية البريد الإلكتروني فيتم التأكد من هويته بعنوان البريد الإلكتروني فقط أما إذا كانت لاستخدامات حساسة مثل: إرسال مبالغ كبيرة من المال عن طريق الانترنت فهذه تتطلب حضور الشخص (صاحب الشهادة) إلى هيئة التوثيق للتأكد من هويته وتوقيع الشهادة. وكذلك من خلال هيئة التوثيق يستطيع الشخص أن يجدد شهادته المنتهية. ومن الهيئات comodo و verysign و thwat وهي مواقع موجودة على الانترنت [٣] .

هيئة التسجيل (Authority Registration):

هي هيئات تساعد هيئة التوثيق وتخفف الضغط عنها في عمل بعض الوظائف مثل التحقق من الهوية وإصدار التوقيع الإلكتروني [٣].

مخزن الشهادات الرقمية (Certificate Repository):

هو دليل عام متاح للكل تخزن فيه الشهادات الملغاة والفعالة بحيث يستفيد الأشخاص من هذا الدليل للبحث عن المفتاح العام للشخص المراد التعامل معه سواء لتشفير الرسائل المرسلة له بمفتاحه العام لضمان السرية أو لفك التوقيع للتأكد من هوية المرسل [٣].

أهم المعلومات الموجودة في الشهادة الرقمية:

- الرقم التسلسلي: وهو الذي يميز الشهادة عن غيرها من الشهادات.
- خوارزمية التوقيع: الخوارزمية المستخدمة لإنشاء التوقيع الالكتروني.
- صالحة – من: تاريخ بداية صلاحية الشهادة.
- صالحة – إلى: تاريخ نهاية صلاحية الشهادة.
- المفتاح العام: المفتاح العام المستخدم لتشفير الرسائل المرسلة إلى صاحب الشهادة.
- مصدر الشهادة: الجهة التي أصدرت الشهادة.
- أسم مالك الشهادة: سواء كان شخص أو منظمة أو موقع الكتروني [٢]

أنواع الشهادات الرقمية:

- **شهادات هيئة التوثيق:**

هذا النوع من الشهادات يصدر من هيئة التوثيق مباشرة وعادة ما يكون لحماية البريد الإلكتروني.

- **شهادات الخادم:**

هذا النوع من الشهادات يصدر من خادم الشبكة (web server) أو خادم البريد (server mail) للتأكد من أمان إرسال واستقبال البيانات.

- **شهادات ناشر البرامج:**

تستخدم للتأكد من أن البرامج الخاصة بناشر معين برامج آمنه [٣].

معيار الشهادة الرقمية (X.509):

هو معيار عالمي أصدره اتحاد الاتصالات الدولي (ITU) لتوحيد شكل وبنية (format) الشهادة الرقمية. أكثر الشهادات الرقمية حاليا تتبع هذا المعيار .[٣]

الفرق بين التوقيع الرقمي والشهادة الرقمية:

في التوقيع الرقمي لا يوجد ضمان أن المفتاح العام هو لهذا الشخص بالفعل مثلا يستطيع خالد أن ينشئ له مفتاحين عام وخاص ثم ينشر مفتاحه العام على أساس أنه أحمد فلو أراد شخص أن يرسل رسالة سريه لأحمد سوف يشفرها باستخدام المفتاح العام الذي نشره خالد وبالتالي سوف يستطيع خالد فك تشفير الرسالة والاطلاع عليها . أي أنه في التوقيع الرقمي لا يوجد ربط بين الشخص بالفعل ومفتاحه العام لذلك ظهرت الشهادة الرقمية والتي تربط بين الشخص ومفتاحه العام حيث تحتوي الشهادة على صاحب الشهادة ومفتاحه العام وموقعه من طرف موثوق فيه يثبت ذلك[٣] .

الشهادة الرقمية للتحقق من الهوية Authentication)):

لنفرض أن أحمد يريد أن يرسل رسالة لخالد لكي يثبت أحمد لخالد بأن المرسل هو بالفعل أحمد فانه سوف يوقع المختصر الحسابي (hash) بالمفتاح الخاص فيه ويرسل الرسالة الأصلية والمختصر الحسابي المشفر لخالد في الطرف الآخر يقوم خالد بفك تشفير المختصر الحسابي باستخدام المفتاح العام لأحمد الموجود في شهادته الرقمية والمتاحة كما ذكرت مسبقا على دليل عام (مخزن الشهادات الرقمية) ثم يقوم بإجراء نفس المختصر الحسابي الذي أجراه احمد على الرسالة بعد ذلك يقارن المختصرين الحسابيين إذا تطابقا فهذا يعني انه بالفعل المرسل هو أحمد. وبهذا ضمنت الشهادة الرقمية التحقق من الهوية. وتسمى العملية السابقة بالتوقيع الإلكتروني.

الشهادة الرقمية لضمان السرية: (Confidentiality)

لنفرض أن أحمد يريد أن يرسل لخالد رسالة سريه فلكي يضمن سريتها سوف يقوم بتشفير الرسالة بالمفتاح العام لأحمد ولن يفك التشفير إلا بالمفتاح الخاص لأحمد (حيث أن المفتاح العام والخاص مربوطة يبعضها أي انه إذا شفرت رسالة بالمفتاح العام لشخص فانه لا يفك تشفير هذه الرسالة إلا بالمفتاح الخاص لنفس الشخص) وبهذا ضمنت السرية.

إدارة الشهادات الرقمية:

يستطيع الشخص أن يختار هيئة التوثيق (CA) التي يريد إصدار شهادته منها وبعد إصدار الشهادة يمكنه تنزيل و تخزين الشهادة والمفتاح العام (public key)على كمبيوتره. بالنسبة لهيئات التوثيق يوجد بعضها تأتي مع متصفح الانترنت في وقت تنزيله ويكون موثوق فيها

سياسة الشهادة الرقمية (Certificate Policy):

هي مجموعة من القواعد والسياسات الإدارية والتي تطبق عند إدارة الشهادة الرقمية في جميع مراحل حياتها[٣].

دورة حياة الشهادات الرقمية:

هناك بعض الأحداث التي تؤثر على فعالية الشهادة الرقمية مثل إضافة جهاز (hardware) جديد على الكمبيوتر أو تحديث برنامج وغيره لذلك أصبح للشهادة الرقمية حالات تمر فيها منذ إصدارها.

- **الإصدار**:

وهي أول مرحلة وتشمل التأكد من هوية الشخص قبل الإصدار. ويعتمد التأكد على نوع الشهادة المصدرة ففي الشهادات الرقمية التي تصدر للبريد الالكتروني يتم التأكد من هوية الشخص بطلب إرسال رسالة من بريده الالكتروني فقط أما الشهادات الرقمية المستخدمة للعمليات المالية فتتطلب إجرآت اخرى للتأكد من الهوية . بعد التأكد من الهوية يتم إرسال الطلب لهيئة التوثيق وتوافق على إصدار الشهادة.

- **الإلغاء**:

يستطيع الشخص أن يلغي شهادته قبل تاريخ انتهائها عندما يفقد المفتاح الخاص بالشهادة أو ينتشر لأنه بعد انتشار المفتاح الخاص تبطل فعالية الشهادة وهي الثقة بالطرف الآخر.(Authentication) ويتم إضافة الشهادة الملغاة إلى قائمة الشهادات الملغاة.

- **الانتهاء**:

لكل شهادة تاريخ انتهاء بعد هذا التاريخ تصبح الشهادة غير صالحه للاستخدام ولابد من إصدار شهادة جديدة ويمكن أن تكون الشهادة الجديدة لها نفس المفتاح العام والخاص للشهادة المنتهية.

- **التعطيل المؤقت:**

يمكن للشخص أن يوقف أو يعطل استخدام الشهادة لفترة زمنية لا يحتاج فيها لاستخدام الشهادة حتى لا تستغل من قبل أشخاص آخرين [٣].

كيفية الحصول على الشهادة الرقمية المستخدمة لغرض حماية البريد المثالي:

١. اذهب إلى احد المواقع الإلكترونية التي تمنح الشهادات على سبيل المثال .comodo
٢. قم بتعبئة البيانات المطلوبة (الاسم الأول، الاسم الأخير، عنوان البريد الإلكتروني، البلد، الرقم السري

الخلاصة:

إذا تعتبر الشهادة الرقمية من الوسائل الأمنية التي ساعدت على استخدام الانترنت سواء في التعاملات التجارية أو استخدام البريد الإلكتروني وغيرها بكل أمن وثقة وسرية.

التواقيع الالكترونية

يعتبر التوقيع ' Signature' شرطا أساسيا في توثيق أغلب المستندات سواء إن كانت في المراسلات العادية اليدوية أو المراسلات الإلكترونية الرقمية بجميع أنواعها وحتى إن كانت محلية أو دولية، ومع ظهور التحديات الجديدة التي يواجهها الاقتصاد الرقمي والأمني خصوصا وأهمها الحكومات الإلكترونية وعدم توافر الضمانات الكافية التي تحمي المجتمع الذي يتعامل بالخصوص مع هذا النظام الإلكتروني والتعامل معه بكل ثقة وأمان أصبحت الحاجة إلى ظهور طريقة آمنة وسريعة وفعالة في عمليات تصديق الوثائق التي يتم تبادلها إلكترونيا على جميع المستويات بكل مراحلها و إضفاء الصفة القانونية عليها ومن ثم أرشفتها إلكترونيا هو ظهور ما يسمى بالتوقيع الإلكتروني.
فما هو التوقيع الإلكتروني ودوره الفعال في الوثائق الحكومية الإلكترونية بأنواعها وطرق استخداماتها عند التطبيق في إثبات هوية صاحب التوقيع الإلكتروني؟

ما هو التوقيع الإلكتروني Digital Signature ؟

هو عبارة عن ملف رقمي صغير مكون من بعض الحروف والأرقام والرموز الإلكترونية تصدر عن إحدى الجهات المتخصصة والمعترف بها حكوميا ودوليا ويطلق عليها الشهادة الرقمية Digital Certificate وتخزن فيها جميع معلومات الشخص وتاريخ ورقم الشهادة ومصدرها، وعادة يسلم مع هذه الشهادة مفتاحان أحدهما عام والآخر خاص، أما المفتاح العام فهو الذي ينشر في الدليل لكل الناس والمفتاح الخاص هو توقيعك الإلكتروني، ومن أشهر الهيئات التي تقوم بإصدار تلك الشهادات الرقمية والتي تكون بمقابل رسوم معينة هي :
وباختصار شديد يمكننا أن نعرف التوقيع الإلكتروني على أنه طريقة اتصال مشفرة رقميا تعمل على توثيق المعاملات بشتى أنواعها والتي تتم عبر صفحات الإنترنت.

أنواع التوقيعات الإلكترونية:

هناك نوعان من التوقيعات الإلكترونية الشائعة:
1-التوقيع المحمي : ' Key Based Signature ' وهنا يتم تزويد الوثيقة الإلكترونية بتوقيع رقمي مشفر يقوم بتشخيص المستخدم 'الموقع' الذي قام بالتوقيع ووقت التوقيع ومعلومات عنه الشخص نفسه وهو عادة مميز لأصحاب التوقيع.
2-التوقيع البيومتري : ' Signature Biometric' يقوم الموقع هنا باستخدام قلم إلكتروني يتم توصيله بجهاز الكمبيوتر ويبدأ الشخص بالتوقيع باستخدام القلم مما يسجل نمط حركات يد الشخص الموقع وأصابعه، ولكل منا له نمط مختلف عن الآخر حيث يتم تحديد هذه السمة، وهنا تقودنا أيضا البصمة الإلكترونية التي تعمل بنفس تقنية النمط نفسها .

الهدف من التوقيع الإلكتروني

ليس الهدف من إنشاء التوقيع الإلكتروني هو الفانتازيا الرقمية، ولكن الهدف يندرج تحت مضمون الأمن والسلامة الرقميين، وعند ثبوت صحتها فإنها بالطبع تحقق جميع الجوانب العملية والأهداف المرجوة منها ولعدة أهداف قانونية بحتة تبعد المتطفلين عن التلصص وسرقة البيانات وأهمها:

توثيق التوقيع الإلكتروني للموقع

كما شرحنا سابقا عند إنشاء الشهادة فإنه يتم إنشاء مفتاحين (عام وخاص)، وفي حالة إن كان المفتاحان مرتبطين بصاحب التوقيع الإلكتروني فإن كل وظيفة يقوم بها من إرسال الوثائق من عنده فإنها تكون خاصة به، وهنا لا يمكن القيام بعملية التزوير إلا في حالة واحدة وهي إن فقد صاحب التوقيع الإلكتروني المفتاح الخاص به أو تم تسريبه.

ضمان توثيق الرسالة 'Hash Function'

عندما يقوم المستخدم بإنشاء رسالة مصاحبة لتوقيعه الإلكتروني فإنها عادة تكون مدمجة معها بعض الشفرات

كوظيفة أساسية تسمى 'وظيفة الهاش' وتستخدم في بداية إنشاء التوقيع الإلكتروني والتأكد من صحته، أما الطريقة التي تعمل بها فإنها تقوم على أساس إنشاء تمثيل رقمي معين على شكل قيمة رقمية 'هاش 'أو 'نتيجة الهاش' عادة تكون هذه القيمة أصغر من الرسالة وتوضع إما في بدايتها أو نهايتها وتكون مدمجة بها، وفي هذه الحالة إن تم التلاعب بتلك الرسالة فإنه على الفور تختلف قيمة 'الهاش' التي تم احتسابها منذ البداية عند إنشاء الرسالة، وحتى إن تم التعرف على قيمة 'الهاش' الثانية فإنه من الصعوبة تقفي أثر قيمة 'الهاش ' الأولية.

الضمان

عند البدء في إنشاء التوقيع الإلكتروني بوساطة الهيئات المعتمدة فإنها بالطبع تتطلب ضمانا عاليا حسب المستويات والتراخيص الدولية والتي تتم عادة بموافقة الموقع الإلكتروني، وهنا فإنها ومن دون شك تولد أعلى درجات السلامة الأمنية.

توسيع التجارة الإلكترونية

إن انتشار التوقيع الإلكتروني له من المميزات الكبيرة التي من شأنها القيام بالتوسع في التجارة الإلكترونية وتأمين جميع معاملاتها على الصعيدين الدولي والمحلي، وحقيقة تذكر أن بعض الدول العربية باتت بالعمل في سن قوانين كثيرة تخص التوقيع الإلكتروني ومنهجيته ومدى الاستفادة منه في تأمين سرية المعلومات المرسلة مع عدم قدرة أحد على الاطلاع عليها أو تعديل جزء منها، والتي من شأنها أن تقضي على 'الواسطة' في بعض البلدان.

التوقيع الإلكتروني وتأثيره على الخدمات العامة

أهمية التوقيع الإلكتروني في مدى السرية والضمان اللذين يتمتعان به وعليه تجدر الإشارة إلى أي مدى يمكن الاستفادة منه والمنفعة الكبرى من استخداماته في شتى المجالات:

1-تحويل المعلومات الشخصية بصورة سرية ومضمونة لكل مواطن.

2-يمكن الاعتماد اعتمادا كليا على التوقيع الرقمي ضمن الإجراءات القانونية والقضائية في المنازعات بين الأشخاص والشركات الخاصة أو المؤسسات والهيئات الحكومية.

3-توفير الهوية الرقمية لكل مواطن.

4-التوقيع باستخدام التوقيع الرقمي الإلكتروني على جميع المستندات ونماذج الطلبات والعقود وغيرها من الطلبات.

5-التوفير في جميع إجراءات إرسال البيانات إلى المواطن والحصول على المعلومات منه (التوفير في الورق، الطلبات، الطباعة، الأحبار، إلخ.(..

6-توفير عامل الوقت الثمين للمواطن والموظف وفي هذه الحالة لن يضطر المواطن إلى أن يذهب بسيارته أو باستخدام وسائل النقل إلى الدوائر الحكومية والانتظار مطولا كما هو الحال في بلداننا العربية وعلى النقيض تماما في البلدان الغربية، حيث إنه بالكاد أن ترى أشخاصا يكملون معاملاتهم إلى بأضيق الحالات، وهي ظهوره الشخصي إن لزم.

7- خلق وعي رقمي وفكري للمواطن، وتطوير التعامل في الإنترنت وأثره على التجارة الإلكترونية، فنرى الكثيرين من الأشخاص الأذكياء الذين يملكون شركات ضخمة حققت الكثير من الأرباح من دون أن يكون لها مقر بحجم الشركات الكبيرة، وهنا يقوم باستخدام الضمان الرقمي ومدى أهميته واستخدامه بعمليات البيع والشراء والوسطاء أكثر المستخدمين لهذه التقنية.

تم بحمد الله جمع هذا البحث المتواضع

حمدان لافي الشمري

HAMDAN.97@hotmail.com