# الوحدة الثانية

# أمن المعلومات والبيانات والإنترنت



## موضوعات الوحدة:

- أمن وحماية المعلومات.
- علوم وأنظمة التشفير.
- حماية تطبيقات الإنترنت.
- إرشادات أمنية لحماية معلوماتك.

## بعد دراستك لهذه الوحدة سوف تحقق الأهداف الآتية:

- تصيغ مفهومًا لأمن المعلومات.
- تحدد عناصر أمن المعلومات.
- تعدد أبرز تهديدات أمن المعلومات.
- تذكر بعض حوادث انتهاك أمن المعلومات.
- تتعرف على أنظمة المملكة العربية السعودية في مكافحة جرائم المعلومات.
- تحدد مفهومًا لعلم تشفير المعلومات.
- تميز بين أنواع أنظمة التشفير.
- تصنف أنظمة تشفير الشبكات اللاسلكية.
- تذكر أهم وسائل حماية تطبيقات الإنترنت.



## الأهمية:

مع تزايد الخدمات الإلكترونية المقدمة للأفراد والشركات والمؤسسات عبر أجهزة الحاسب والأجهزة الذكية إلا أنه لا قيمة لهذه الخدمات إذا لم يتوفر الأمن الكافي لمستخدميها، والذي يحميهم على سبيل المثال من الخسارة المادية نتيجة فقد معلومات الحسابات البنكية كرقم بطاقة الإئتمان، أو فقد معلومات حساسة وسرية كالمعلومات العسكرية أو التجارية، ونقصد بالأمن هنا هو الأمن المعلوماتي، ونعني به الحفاظ على سرية بيانات المستخدمين ومعلوماتهم أثناء الاستخدام وعدم تعرضها للسرقة والضياع، بالإضافة إلى أن تكون هذه البيانات صحيحة ومتوفرة يمكن الوصول إليها بشكل دائم.

## ١-٢ المقدمة

أدى ظهور الحاسب وتطوره السريع إلى نقلة كبيرة في حياة الناس، وذلك لما يقدمه من خدمات سهلت تعاملاتهم اليومية، فأصبح الاعتماد على الحاسب بشكل كبير في القيام بكثير من المهام والواجبات، فنجد أنه أصبح بالإمكان التعامل مع الدوائر الحكومية المختلفة عن طريق شبكة الإنترنت، وكذلك الحال مع البنوك في تحويل الأموال وتسديد الفواتير، بالإضافة إلى كثير من المهام كالدراسة والتسوق والتواصل الاجتماعي وغيرها من التطبيقات الشائعة في عالم اليوم.

**إثارة التفكير**

بماذا تختلف المخاطر الناجمة عن أمن المعلومات في عصر الحاسب عنها في العصور السابقة؟ دعّم إجابتك بأمثلة توضح الضرر الناتج عنهما

وتعتمد هذه الخدمات على كم كبير من البيانات والمعلومات والتي يجب أن تحاط بسرية تامة وتحفظ بشكل يمنع الوصول إليها من قبل أيدي العابثين، ولأهمية هذه المعلومات وضرورة المحافظة عليها فقد توسع البحث في مصطلح أمن البيانات والمعلومات (Data Security) وارتبط بالحاسب، ويمكننا تعريفه بما يأتي:

هو العلم الذي يبحث في نظريات وأساليب حماية البيانات والمعلومات، ويضع الأدوات والإجراءات اللازمة لضمان حمايتها، ويسهم في وضع التشريعات التي تمنع الاعتداء على المعلومات ومعاقبة المعتدين عليها.

## ٢-٢ أمن المعلومات

### ١-٢-٢ عناصر أمن المعلومات:

للمحافظة على أمن البيانات والمعلومات في البرنامج أو النظام الذي نتعامل معه يجب أن تتوفر فيه ثلاثة عناصر، كما في الشكل (٢-١) هي: السرية، السلامة، والتوافر والإتاحة، وفيما يأتي توضيح لها:

شكل (٢-١) عناصر أمن المعلومات

١ **السرية (Confidentiality):**

تعني منع الوصول إلى المعلومات إلا من الأشخاص المصرح لهم فقط سواء عند تخزينها أو عند نقلها عبر وسائل الاتصال، وكذلك تحديد صلاحية التعديل والحذف والإضافة.

٢ **السلامة (Safety):**

المقصود بها أن تكون المعلومة صحيحة عند إدخالها، وكذلك أثناء تنقلها بين الأجهزة في الشبكة وذلك باستخدام مجموعة من الأساليب والأنظمة.

### ٣ التوافر والإتاحة (Availability):

تعني بقاء المعلومة متوفرة للمستخدم وإمكانية الوصول إليها، وعدم تعطل ذلك نتيجة لخلل في أنظمة إدارة قواعد المعلومات والبيانات أو وسائل الاتصال.

## ٢-٢-٢ تهديدات أمن المعلومات:

تتعرض المعلومات أثناء استخدامنا لأجهزة الحاسب والأجهزة الذكية لكثير من المخاطر، وتتنوع هذه المخاطر فمنها مخاطر طبيعية تتمثل في الحرائق والغرق والزلازل والبراكين وغيرها، ومنها مخاطر عامة كانقطاع التيار الكهربائي والإنترنت، ومنها مخاطر إلكترونية تتمثل في انتحال الشخصية، التنصت، الفيروسات، الاختراق، والتجسس والتي تتنوع وتتطور بشكل مستمر نتيجة لتطور وتقدم التقنية، ومن أبرز التهديدات الإلكترونية ما يأتي:

### ١ انتحال الشخصية (Spoofing):

في مثل هذه الحالة يتم استخدام هوية مستخدم ما (اسم المستخدم وكلمة المرور) للحصول على معلومات سرية أو أمنية أو مبالغ نقدية، ويتم ذلك بعدة طرق منها:

- تخمين اسم المستخدم وكلمة المرور. ومما يسهل الأمر إذا كان اسم المستخدم وكلمة المرور سهلة أو ذات دلالة بصاحب الحساب (كاسمه وتاريخ ميلاده).
- إرسال رسائل للمستهدفين يطلب منهم تحديث بياناتهم البنكية أو غيرها عبر روابط تحوي صفحات مشابهة تماماً للموقع الأصلي، في حين أن البيانات تذهب لمعد هذه الصفحة.
- استخدام أجهزة أو برامج تقوم بتسجيل كل ما يتم النقر عليه في لوحة المفاتيح وإرساله إلى بريد إلكتروني معين.
- الاتصال مباشرة على المستهدفين والإدعاء بأنه موظف في شركة أو بنك ويطلب المعلومات السرية بحجة تحديث النظام أو ما شابه ذلك.

### ٢ التنصت (Eavesdropping):

يتم الحصول على المعلومات بهذه الطريقة عن طريق التنصت على حزم البيانات أثناء تنقلها عبر شبكات الحاسب كما في الشكل (٢-٢)، ومما يسهل ذلك أن تكون حزم هذه البيانات غير مشفرة.

شكل (٢-٢) التنصت على حزم البيانات

**إثراء علمي**

مركز التميز لأمن المعلومات التابع لجامعة الملك سعود، يجمع أفضل الباحثين والمتميزين في مجال أمن المعلومات، ويساعدك للاطلاع على معلومات إضافية وآخر مستجدات أمن المعلومات على مستوى العالم، وذلك على الرابط الإلكتروني (http://coeia.Ksu.edu.sa)

مركز التميز لأمن المعلومات
Center of Excellence in Information Assurance

**فائدة**

العمل العسكري عمل محفوف بالمخاطر ولا يَقدم عليه إلا رجال شجعان مؤمنين بأهمية الأمن للمجتمع والفرد.

٣ **الفيروسات (Viruses):**

عبارة عن برامج قام بتطويرها وكتابتها مبرمجين محترفين؛ بهدف تنفيذ أوامر معينة في جهاز الضحية كإلحاق الضرر بالحاسب وما يحتويه من بيانات، أو فتح منافذ في الحاسب يمكن عن طريقها اختراقه ومراقبته. وهناك أنواع للفيروسات يمكن تقسيمها كما يأتي:

- **الفيروس:** برنامج تنفيذي يهدف إلى تحقيق أهداف محددة أو إحداث خلل في نظام الحاسب.
- **الدودة (worm):** سميت بذلك لأنها قادرة على نسخ نفسها والانتشار سريعًا عبر وسائل الاتصال كالبريد الإلكتروني، بهدف تحقيق أهداف محددة.
- **حصان طروادة (Trojan Horse):** سمي هذا الفيروس بحصان طروادة لأنه يذكر بالقصة الشهيرة لحصان طروادة، حيث اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طروادة والتغلب على جيشها، وبالتالي فإن هذا الفيروس يكون مرفقًا مع برنامج دون علم المستخدم، ويهدف إلى سرقة البيانات وكشف كلمات المرور والحسابات المصرفية.
- **الاختراق (Penetration):** محاولة الوصول إلى أجهزة وأنظمة الأفراد أو المنظمات والشركات باستخدام برامج خاصة عن طريق ثغرات في نظام الحماية بهدف الحصول على معلومات أو تخريب تلك الأنظمة وإلحاق الضرر بها.
- **برامج التجسس (Spyware):** نوع من الاختراق يقتصر على معرفة محتويات النظام المستهدف بشكل مستمر دون إلحاق الضرر به.

**إثراء علمي**

CERT.sa
المركز الوطني الإرشادي لأمن المعلومات
COMPUTER EMERGENCY RESPONSE TEAM

عند تعرضك لعملية انتهاك أمن معلوماتي يمكنك التوجه لأقرب مركز شرطة وتقديم ما يثبت للمطالبة بحقوقك، أما إذا أردت الحصول على دعم تقني لكيفية التعامل مع هذه الحادثة فيمكنك الابلاغ لدى المركز الوطني الإرشادي لأمن المعلومات على الموقع الإلكتروني (http://www.cert.gov.sa)

## ٣-٢-٢ أمثلة من حوادث انتهاك أمن المعلومات:



حدثت عمليات انتهاك أمن معلومات متعددة سواء داخل المملكة أو حول العالم. وفيما يأتي بعض من أمثلة هذه الانتهاكات:

١ تمكنت الجهات الأمنية من القبض على أحد الهكر نتيجة قيامه بسرقة بريد إلكتروني أحد المواطنين والعبث بمحتوياته، وذلك بعد أن قدم الضحية بلاغًا في الشرطة وضح فيه تفاصيل الحادثة.

٢ تمكنت الجهات الأمنية من القبض على خمسة أحداث قاموا بسرقة مبالغ مالية كبيرة من أحد البنوك، وذلك باستخدام بطاقات ممغنطة للسحب من أجهزة الصراف الآلي.

٣ أطاحت الجهات الأمنية بمواطن استطاع اختراق جهاز الحاسب الشخصي لمواطن آخر والحصول على ملفات متنوعة من جهازه.

**نشاط**

اذكر بعض الحوادث التي تعرفها حول انتهاك أمن المعلومات.

.....
.....
.....
.....
.....
.....

٤ قامت إحدى جماعات قرصنة الحاسب بمهاجمة موقع وزارتي الداخلية والعدل بإحدى الدول والحصول على معلومات مهمة.

٥ في عام 2000م انتشر فيروس سمي (فيروس الحب) في كل دول العالم عبر البريد الإلكتروني، وكان يقوم بحذف جميع ملفات الوسائط وتعطيل نظام التشغيل في جميع الأجهزة التي يصيبها.

## ٤-٢-٢ أنظمة المملكة العربية السعودية في مكافحة جرائم أمن المعلومات:

نظرًا لأهمية الأمن المعلوماتي فقد صدر نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية وذلك بقرار من مجلس الوزراء برقم ٧٩ وتاريخ ١٤٢٨/٣/٧هـ، وتمت المصادقة عليه بموجب المرسوم الملكي الكريم رقم م/١٧ وتاريخ ١٤٢٨/٣/٨هـ. ويهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، مما يسهم فيما يأتي:

١ المساعدة على تحقيق الأمن المعلوماتي.

٢ حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.

٣ حماية المصلحة العامة، والأخلاق، والآداب العامة.

٤ حماية الاقتصاد الوطني.

### نشاط

استعرض نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية في القرص المرفق مع كتاب التدريبات لتحديد عقاب جرائم المعلومات الآتية:

١ التنصت.

السجن لمدة لاتزيد عن سنة وغرامة لاتزيد عن خمسمائة الف ريال او بإحدى هاتين العقوبتين

٢ الاستيلاء على الأموال عن طريق انتحال الشخصية.

غرامة لا تزيد عن مليوني ريال سعودي و السجن مدة لا تزيد عن ثلاث سنوات او بإحدى هاتين العقوبتين

٣ إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها، أوتدمير، أو مسح البرامج، أو البيانات الموجودة.

السجن لمدة لاتزيد عن اربع سنوات وغرامة لاتزيد عن ثلاثة ملايين ريال او بإحدى هاتين العقوبتين

٤ إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة.

السجن لمدة لاتزيد عن خمس سنوات وغرامة لاتزيد عن ثلاثة ملايين ريال او بإحدى هاتين العقوبتين

٥ الدخول غير المشروع إلى موقع إلكتروني، للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة.

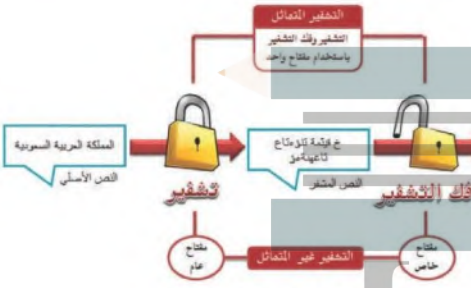
السجن لمدة لاتزيد عن عشر سنوات وغرامة لاتزيد عن خمسة ملايين ريال

## ٢-٣ علوم وأنظمة تشفير المعلومات

هناك من بين ملفاتك المخزنة على حاسبك الشخصي ما هو مهم وسري لا تريد لأحد أن يطلع عليه، وكذلك الحال بالنسبة للمنظمات والشركات فهناك ملفات تحوي بيانات مهمة وسرية لا ينبغي الاطلاع عليها إلا من قبل الأشخاص المصرح لهم. وفي هذه الحالة يجب علينا حفظ هذه الملفات والبيانات بطريقة يصعب التعرف على محتوياتها حتى لو تعرضت للسرقة أو الاختراق، وهو ما يسمى بعملية التشفير. وقد استخدم التشفير في الحروب قديمًا، وذلك بتشفير الرسائل عند نقلها وتغيير شكلها الحقيقي وبالتالي يصعب كشفها حتى لو سقطت في أيدي العدو.

### ٢-٣-١ تعريف تشفير المعلومات

هو وسيلة لحفظ البيانات بصورة تختلف عن محتواها الأصلي باستخدام معادلات وخوارزم رياضية معقدة، ويتم إعادتها إلى شكلها الأصلي بطرق خاصة يعرفها المرسل والمستقبل فقط شكل (٢-٣).




شكل (٢-٣) آلية عمل التشفير

### ٢-٣-٢ أنواع أنظمة التشفير

هناك نوعان للتشفير وهي كما يأتي:

أ **التشفير المتماثل (Symmetric Cryptography):**

يستخدم هذا النوع مفتاح واحد للتشفير وفك التشفير. ويجب المحافظة على سرية مفتاح التشفير لأن من يحصل على هذا المفتاح يستطيع فك عملية التشفير.

ولتوضيح هذا النوع من التشفير سنقوم بتشفير الأحرف الهجائية وذلك بإبدال كل حرف بالحرف الخامس الذي يليه وفق ترتيب الحروف الهجائية كما يوضح الشكل (٢-٤)، وبالتالي فإن مفتاح التشفير هو (٥). وستصبح كلمة (محمد) بعد تشفيرها (أزأش).

| الحرف الأصلي | أ | ب | ت | ث | ج | ح | خ | د | ذ | ر | ز | س | ش | ص |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| الحرف بعد التشفير | ح | خ | د | ذ | ر | ز | س | ش | ص | ض | ط | ظ | ع | غ |
| الحرف الأصلي | ض | ط | ظ | ع | غ | ف | ق | ك | ل | م | ن | هـ | و | ي |
| الحرف بعد التشفير | ف | ق | ك | ل | م | ن | هـ | و | ي | أ | ب | ت | ث | ج |

شكل (٢-٤) الحرف الهجائي وما يقابله بعد التشفير

**ب تشفير غير المتماثل (Asymmetric Cryptography):**

يعتمد هذا النوع من التشفير على مفتاحين أحدهما للتشفير ويسمى المفتاح العام (Public key)، والآخر يستخدم لفك التشفير ويسمى المفتاح الخاص (Private key)، وبالتالي من يشفر بهذه الطريقة يستخدم المفتاح العام والذي يكون معروف لدى الجميع ومن ثم يتم إرسال الرسالة فقط دون مفتاحها، ويقوم مستقبل الرسالة بفكها من خلال مفتاحه الخاص والذي يكون معروف لديه فقط دون غيره.

**نشاط**

أنشئ جدول للتشفير مماثل للشكل (٢-٤) ولكن مع مفتاح التشفير (٣)، ثم استخدمه لتشفير كلمة (عبد الرحمن) ودوّن الإجابة هنا:

.....

.....

.....

## ٢-٣-٢ تشفير الشبكات اللاسلكية

لا شك أن الاتصال بالشبكة لاسلكيًا أسهل ومرغوب بشكل أكثر من استخدام كيابل الشبكة لأسباب تتعلق بتقييد التنقل وحرية العمل، ولكن استخدام الشبكات اللاسلكية دون تشفير يعرضها للخطر، إذ يمكن لأي مستخدم الاتصال بالشبكة متى ما توفرت لديه، وبالتالي يعرض جميع الأجهزة المتصلة بالشبكة لخطر أمن المعلومات.

ولحل ذلك يجب علينا تشفير اتصال الشبكة اللاسلكية وذلك باستخدام أنظمة التشفير المتوفرة مع وسائل الاتصال اللاسلكية سواء في أجهزة الحاسب أو أجهزة الاتصال بالإنترنت أو أجهزة الجوال وغيرها. وهناك عدة أنواع لتشفير الشبكات اللاسلكية ومنها:

**أ نظام التشفير (WEP):**

وهو اختصار للجملة (Wired Equivalent Privacy) وينقسم لنوعين هما:

- **نظام التشفير (64 Bit WEP):** ويسمى بمفتاح التشفير المشترك. وفيه يتكون مفتاح التشفير من (10) خانات، ويستخدم لكتابته الأرقام من (0) إلى (9) والحروف الإنجليزية (A) إلى (F) فقط، وهي تشكل ما يسمى بالأرقام الست عشرية.

**مثال:** مفتاح التشفير (A12345678H) غير صحيح لأن حرف (H) ليس من سلسلة الأعداد الست عشرية.

- **نظام التشفير (128 Bit WEP):** وفيه يتم كتابة مفتاح التشفير بنفس الطريقة السابقة، ولكن يجب أن يكون طولها عبارة عن (26) خانة تنتمي جميعها إلى الأرقام الست عشرية.

**ب نظام التشفير (WPA):**

وهو اختصار للجملة (WI-FI Protected Access)، ويتكون مفتاح التشفير من (8) خانات يستخدم فيها جميع الأرقام والأحرف الإنجليزية.

**ج نظام التشفير (WPA2):**

وهو مشابه تمامًا للنظام(WPA)، لكنه يستخدم خوارزميات حديثة وأقوى للتشفير، ويعد أفضل أنواع التشفير للشبكات اللاسلكية.

**نشاط**

أنشئ كلمات مرور صالحة لكل من أنواع تشفير الشبكات اللاسلكية الآتية:

نظام التشفير (64 Bit WEP)

.....

.....

.....

نظام التشفير (128 Bit WEP)

.....

.....

.....

نظام التشفير (WPA)

.....

.....

.....

## ٢-٤ حماية تطبيقات الإنترنت

لم تعد مواقع الإنترنت جامدة تقتصر على عرض المعلومات، بل أصبحت أكثر تفاعلية، حيث يمكن للمستخدم الاضافة والحذف والتعديل والتفاعل مع الموقع بشكل كبير جدًّا، وهو ما يطلق عليه الآن بتطبيقات الإنترنت. وهذا التفاعل بين تطبيق الإنترنت والمستخدم يلزم توفير مستوى عالي من الأمن المعلوماتي، وذلك لحماية البيانات التي يرسلها المستخدم والتي قد تكون سرية ومهمة كاسم المستخدم وكلمة المرور ورقم بطاقة الإئتمان وغيرها. وفيما يأتي عرض لأهم وسائل حماية تطبيقات الإنترنت:

### أولًا جدار الحماية (Firewall):

جدار الحماية عبارة عن برنامج أو جهاز يتحكم في عملية الاتصال بين الحاسب والإنترنت أو شبكة حاسب، أو بين شبكة حاسب وأخرى، حيث يقوم بمنع البرامج الضارة والمتسللين من الوصول إلى جهاز الحاسب، وذلك بمراجعة المعلومات التي يتم تبادلها مع الإنترنت أو الشبكة، ثم السماح لها بالوصول أو حظرها. ويوضح الشكل (٢-٥) آلية هذه العملية. ويجدر أن ننوه بأن استخدام برامج جدران الحماية لا يغني عن استخدام برامج مكافحة الفيروسات.


شكل (٢-٥) جدار الحماية

### ثانيًا مداولة (https):

لعلك تلاحظ أن أي موقع إلكتروني تقوم بفتحه عبر متصفح الإنترنت له عنوان خاص به، ويبدأ بـ (http) وهو اختصار للجملة (Hypertext Transfer Protocol) ويسمى هذا بمداولة أو بروتوكول نقل النص التشعبي، والمداولة هي "الطريقة التي يتخاطب بها جهاز المرسل والمستقبل" وهي مسؤولة عن نقل وعرض صفحات مواقع الإنترنت. ويُعاب على مداولة (http) أن البيانات التي يتم إرسالها من قبل المستخدم غير مشفرة، وبالتالي يمكن اعتراضها وسرقتها وهذه معضلة كبيرة في أمن المعلومات لا سيما إذا كانت هذه البيانات مهمة كاسم المستخدم وكلمة المرور ورقم بطاقة الإئتمان... وغيرها.

ولحل هذه المعضلة فقد تم تطوير هذه المداولة إلى مداولة الأمن حيث تُدعى (https) وهي نفس المداولة السابقة مدعومة بمداولة (SSL/TLS)، والتي تقوم بتشفير البيانات المدخلة في المتصفح أثناء تنقلها بين جهاز المرسل والمستقبل. ونلاحظ أن جميع المواقع التي تتطلب بيانات خاصة وسرية تستخدم هذه المداولة كموقع نظام نور للإدارة التربوية التابع لوزارة التعليم.

## ثالثًا التوقيع الرقمي (Digital Signature):

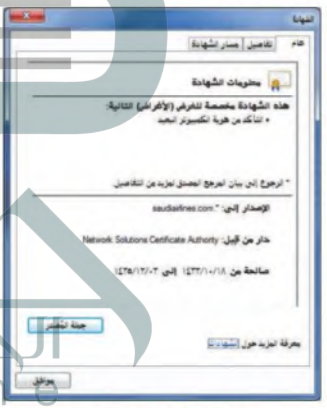
عندما يأتيك خطاب ورقي موقع من مدير المدرسة فإن هذا دليل على صحة الخطاب، ولكن على الإنترنت لا يمكن تطبيق ذلك بنفس الصورة. بل ابتكر ما يسمى بالتوقيع الرقمي وهو عبارة عن "علامة أو برهان إلكتروني يتم إضافته للملفات يتيح للمستخدم مستقبل الملف التأكد من أن الملف على صورته وشكله الأساسي ولم يتعرض للتعديل أو التزييف".

ويحتوي التوقيع الرقمي على قيمة خوارزمية فريدة تمثل بصمة خاصة للملف، ويتم حساب هذه القيمة بالاعتماد على محتويات الملف، ومن ثم يتم إضافة هذه القيمة إلى الملف عند إرساله، وعند فتح الملف من قبل المستقبل يتم حساب القيمة مرة أخرى وفقًا لمحتويات الملف فإذا اختلفت هذه القيمة يعني هذا أن محتويات الملف قد تغيرت ويصبح الملف مزور. ويطلق على هذه القيمة اسم قيمة هاش (Hash Value) أو نتيجة هاش (Hash result).

## رابعًا الشهادات الرقمية (Digital Certificates):

عندما تريد أن تتأكد من معرض تجاري أو مصرف فإنك تطلب من المسؤولين تصاريحهم الرسمية كالسجل التجاري مثلًا. ولكن على شبكة الإنترنت يختلف الوضع إذ لا يمكن الاعتماد على ذلك، ولذلك وجدت حلول أخرى ومنها ما يسمى بالشهادة الرقمية.

الشهادة الرقمية: هي عبارة عن "وثيقة إلكترونية تمنح من قبل هيئات عالمية تسمى هيئة إصدار الشهادات (Certification Authority)". تقوم هذه الشهادة بتوثيق جهة ما كالبنوك أو المواقع التجارية المختلفة. وتحتوي الشهادة على اسم الشركة أو الجهة، تاريخ صلاحية الشهادة، رقم تسلسلي، مفتاح التشفير العام، والتوقيع الإلكتروني للجهة المانحة كما في الشكل (٢-٦).




شكل (٢-٦) شهادة رقمية

### نشاط

للاطلاع على الشهادة الرقمية لأي موقع اتبع ما يأتي:

١. افتح موقع نور (https://noor.moe.sa) في متصفح الإنترنت (Internet Explorer).
٢. ستجد بجانب اسم الموقع علامة "القفل المغلق" والتي تشير إلى أن الموقع آمن، انقر على هذه العلامة.
٣. سيظهر لك قائمة، انقر منها على عرض الشهادات.
٤. ستظهر لك الشهادة الرقمية الخاصة بالموقع.
٥. دوّن معلومات الشهادة هنا.

.....

.....

## ٢-٥ إرشادات أمنية لحماية معلوماتك

هناك مجموعة من الإجراءات والاحتياطات تسهم في المحافظة على أمن المعلومات أثناء استخدام جهاز الحاسب أو الأجهزة الذكية المتصلة بشبكة الإنترنت، وفيما يأتي بعضًا منها:

١. استخدم أحد برامج مكافحة الفيروسات الجيدة، واحرص على تحديثه باستمرار.
٢. استخدم أحد برامج الجدران النارية، علمًا بأن نظام التشغيل ويندوز يحوي أحدها فتأكد من تفعيله فقط.
٣. ضع كلمة مرور على الشبكة اللاسلكية للإنترنت المنزلية أو أي شبكة تعمل عليها.
٤. استخدم في كلمات المرور حروف وأرقام ورموز حتى يصعب اختراقها، واحرص ألا تكون ذات دلالة.
٥. لا تقم بتحميل ملفات لا تعرف مصدرها.
٦. تأكد من وجود (https) في شريط العنوان الخاص بالصفحة التي تطلب بياناتك الخاصة مثل اسم المستخدم وكلمة المرور ورقم بطاقة الإئتمان.
٧. تجنب الدخول للمواقع الحساسة كالبنوك عن طريق روابط من مواقع أخرى.
٨. قبل التخلص من جهازك القديم احذف بياناتك بشكل آمن باستخدام برامج متخصصة.
٩. لا تحمل البرامج المقرصنة وغير الأصلية.
١٠. احذر من الذين يتصلون بك لطلب معلوماتك الشخصية دون سابق معرفة.
١١. لا تعلن عن مكانك عبر شبكات التواصل الاجتماعي، كقولك أنا الآن في مطعم. فقد تستغل للقيام بعمليات سرقة نتيجة غيابك عن المنزل.
١٢. لا تكتب معلوماتك الشخصية في مواقع التواصل الاجتماعي كاسمك وتاريخ ومكان الميلاد ورقم الهاتف ومكان السكن، فقد تستغل لانتحال شخصيتك.

## مشروع الوحدة

### المشروع الأول:

قم بإعداد نشرة من أربع صفحات على شكل مطوية حول نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية، مدعمًا ذلك بأمثلة لكل مادة من مواد النظام. ثم قم بطباعتها وتوزيعها في مدرستك لتعرفهم بهذا النظام.

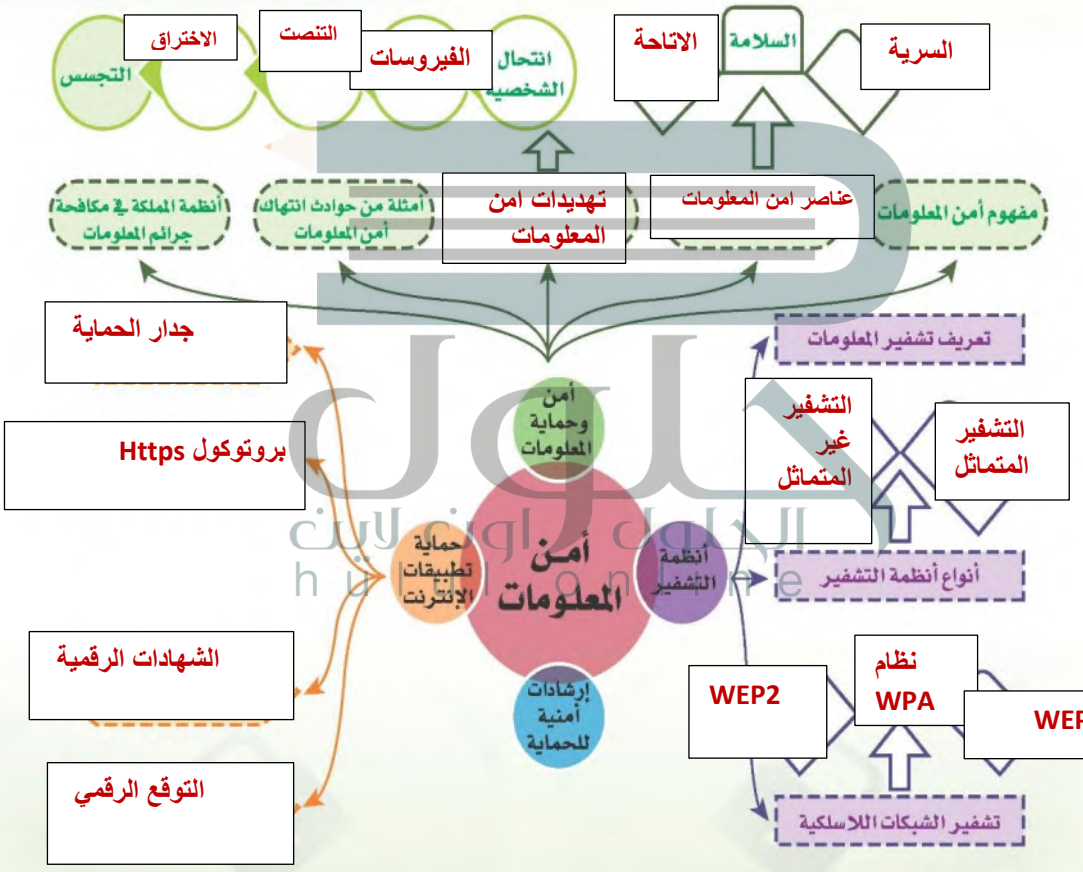
يمكن الاستعانة بنظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية والموجود ضمن مجلد (أمن المعلومات) في القرص المرفق مع الكتاب أو عن طريق موقع هيئة الاتصالات وتقنية المعلومات، ضمن محتويات أنظمة الهيئة (www.citc.gov.sa).

### المشروع الثاني:

انشئ عرض تقديمي تتحدث فيه عن أهمية أمن المعلومات، والتهديدات الممكنة، ووسائل المحافظة على أمن المعلومات. وأسماء خمسة برامج مجانية في مجال مضادات الفيروسات، والجدار الناري، ومكافحة التجسس، مدعماً ذلك بالصور ومقاطع الفيديو.

# خارطة الوحدة

أكمل الخارطة باستخدام المصطلحات والمعلومات التي اكتسبتها في الوحدة:



# دليل الدراسة

| مفردات الوحدة | المفاهيم الرئيسة |
| --- | --- |
| ■ أمن المعلومات. | ■ تعريف أمن المعلومات.<br>■ عناصر أمن المعلومات: السرية، السلامة، التوفر، والإتاحة.<br>■ تهديدات أمن المعلومات: انتحال الشخصية، التنصت، الفيروسات، الاختراق، التجسس.<br>■ أمثلة من حوادث انتهاك أمن المعلومات.<br>■ أنظمة المملكة العربية السعودية في مكافحة جرائم أمن المعلومات. |
| ■ علوم وأنظمة التشفير. | ■ تعريف تشفير المعلومات.<br>■ أنواع أنظمة التشفير: التشفير المتماثل، التشفير غير المتماثل.<br>■ تشفير الشبكات اللاسلكية: نظام التشفير (WEP)، نظام التشفير (WPA)، نظام التشفير (WPA2). |
| ■ حماية تطبيقات الإنترنت. | ■ جدار الحماية (Firewall).<br>■ مداولة (https).<br>■ التوقيع الرقمي (Digital Signature).<br>■ الشهادات الرقمية (Digital Certificates). |
| ■ إرشادات أمنية لحماية معلوماتك. | ■ مجموعة من الإجراءات والاحتياطات التي تسهم في المحافظة على أمن المعلومات أثناء استخدام جهاز الحاسب أو الأجهزة الذكية المتصلة بشبكة الإنترنت. |

## تمرينات

**س١** ضع علامة (✓) أمام العبارة الصحيحة وعلامة (✗) أمام العبارة غير الصحيحة فيما يأتي:

أ) توضع التشريعات التي تمنع الاعتداء على المعلومات بدون مشاركة المتخصصين بأمن المعلومات. ( X )

ب) تقتصر تهديدات أمن المعلومات على المخاطر الإلكترونية. ( X )

ج) التجسس هو نوع من الاختراق. ( ✓ )

د) لم تسجل أي حادثة انتهاك أمن معلومات داخل المملكة. ( X )

هـ) في نظام تشفير الشبكات اللاسلكية (WPA2) يتكون مفتاح التشفير من (10) خانات. ( X )

و) جميع مواقع الإنترنت الآن تستخدم مداولة (https). ( ✓ )

**س٢** أكمل الفراغات في العبارات الآتية:

أ) عناصر أمن البيانات هي: السلامة – السرية – التوافر

ب) أنواع أنظمة التشفير هي: نظام التشفير المتماثل ونظام التشفير غير المتماثل

ج) من أنواع فيروسات الحاسب: الفيروس – حصان طروادة – الدودة و .....

د) من أنظمة تشفير الشبكات اللاسلكية: نظام التشفير WEP -نظام التشفير WPA -نظام التشفير WPA2

هـ) التوقع الرقمي: عبارة عن علامة أو برهان إلكتروني يتم إضافته للملفات، يستطيع المستخدم مستقبل الملف التأكد من عدم تعرضه للتعديل والتزييف.

**س٣** اختر للعمود الأول ما يناسبه من العمود الثاني:

| | العمود الأول | | العمود الثاني |
|---|---|---|---|
| 3 | مداولة (https) | ١ | برنامج أو جهاز يتحكم في عملية الاتصال بين الحاسب والإنترنت أو شبكة حاسب. |
| 5 | الشهادة الرقمية | ٢ | تشفير الشبكات اللاسلكية. |
| 2 | نظام (WPA) | ٣ | يقوم بتشفير البيانات المدخلة في المتصفح أثناء تنقلها بين جهاز المرسل والمستقبل. |
| | جدار الحماية | ٤ | المفتاح الذي يقوم بفك التشفير. |
| 1 | | ٥ | عبارة عن وثيقة إلكترونية تمنح من قبل هيئات عالمية. |

## اختبار

اختر رمز الإجابة الصحيحة فيما يأتي:

١ عنصر أمن المعلومات المسؤول عن كون المعلومة صحيحة عند إدخالها، وكذلك أثناء تنقلها بين الأجهزة في الشبكة هو:

أ - السرية. ب- السلامة.

ج- التوفر. د- الإتاحة.

٢ يطلق على الوثيقة الإلكترونية التي تمنح من قبل هيئات عالمية:

أ - الشهادة الرقمية. ب- جدار الحماية.

ج- التوقيع الرقمي. د- نظام التشفير.

٣ تسمى الطريقة التي يتم بها استخدام هوية مستخدم للحصول على معلومات سرية أو أمنية أو مبالغ نقدية:

أ - انتحال الشخصية. ب- التنصت.

ج- التجسس. د- الاختراق.

٤ تسمى فيروسات الحاسب التي تقوم بنسخ نفسها والانتشار سريعًا عبر وسائل الاتصال كالبريد الإلكتروني:

أ - فيروس مدمر. ب- الدودة.

ج- حصان طروادة. د- التجسس.

٥ يسمى نظام التشفير الذي يستخدم مفتاح واحد للتشفير وفك التشفير:

أ - التشفير المتماثل. ب- التشفير العام.

ج- التشفير غير المتماثل. د- التشفير الخاص.

٦ عدد الخانات التي يستخدمها نظام تشفير الشبكات اللاسلكية (128 Bit WEP) هو:

أ - (10) خانات. ب- (20) خانة.

ج- (16) خانة. د- (26) خانة.

٧ يسمى المفتاح المستخدم لفك التشفير في نظام التشفير غير المتماثل:

أ - المفتاح العام. ب- المفتاح الخاص.

ج- المفتاح السري. د- المفتاح المتماثل.

٨ أقوى أنظمة تشفير الشبكات اللاسلكية هو:

أ - نظام التشفير (64 Bit WEP).
ب- نظام التشفير (WPA).
ج- نظام التشفير (128 Bit WEP).
د- نظام التشفير (WPA2).

٩ من الوسائل التي قد تساعد على تعرض أمنك المعلوماتي للخطر:

أ - استخدام بروتوكول (https).
ب- استخدام برنامج جدار ناري.
ج- نشر المعلومات الشخصية في مواقع التواصل.
د- تحميل ملفات من جهات موثقة.