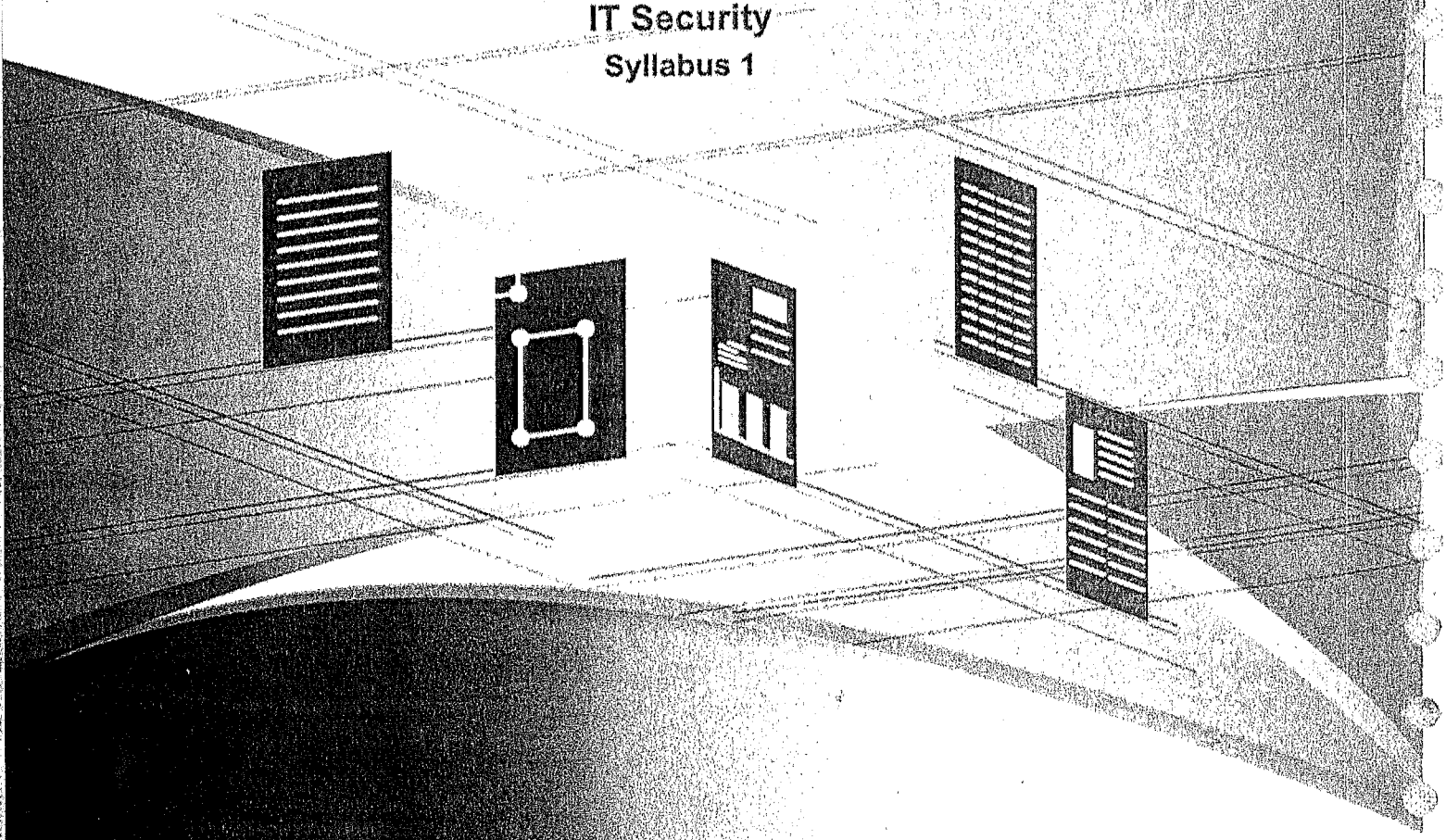
ICDL Syria | APPROVED COURSEWARE

# أمن تكنولوجيا المعلومات

## المنهاج الاول

## IT Security

## Syllabus 1



الرخصة الدولية لقيادة الحاسوب - الإصدار السادس

باستخدام ويندوز 7 واوفيس 2010

ICDL V6 - Using Windows 7 and Office 2010

7

measuring ICT skills

# أمن تكنولوجيا المعلومات

# IT Security

جدول المحتويات

**1 مفاهيم الأمن SECURITY CONCEPTS ..... 1**

**1.1 تهديدات البيانات DATA THREATS ..... 1**

1.1.1 تمييز البيانات من المعلومات Distinguishing between data and information ..... 1

2.1.1 الجريمة الإلكترونية Cybercrime ..... 1

3.1.1 فهم الفرق بين كل من القرصنة، وكسر الحماية والاختراق الأخلاقي The difference between hacking, cracking and ethical hacking ..... 2

4.1.1 تهديدات البيانات بسبب ظروف قاهرة Threats to data from force majeure ..... 2

5.1.1 تهديدات البيانات من الأشخاص Threats to data from persons ..... 3

تمرين (1-1) ..... 3

**2.1 أهمية وقيمة المعلومات VALUE OF INFORMATION ..... 4**

1.2.1 الأسباب التي تدعو إلى حماية المعلومات الشخصية The reasons for protecting personal information ..... 4

2.2.1 الأسباب التي تدعو إلى حماية المعلومات التجارية الحساسة The reasons for protecting commercially sensitive information ..... 4

3.2.1 التدابير التي تمنع الوصول غير المسموح به إلى البيانات Measures for preventing unauthorised access to data ..... 4

4.2.1 الميزات الأساسية لأمن المعلومات Basic characteristics of information security ..... 5

5.2.1 حماية الخصوصية/البيانات، والاحتفاظ بها، ومتطلبات التحكم بها The main data/privacy protection, retention and control requirements ..... 5

6.2.1 أهمية إنشاء الإرشادات والسياسات العامة المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات، والالتزام بها The importance of creating and adhering to guidelines and policies for ICT use ..... 5

تمرين (1-2) ..... 6

**3.1 الأمن الشخصي PERSONAL SECURITY ..... 7**

1.3.1 الهندسة الاجتماعية Social Engineering ..... 7

1.1.3.1 مفهوم الهندسة الاجتماعية The term: Social engineering ..... 7

2.1.3.1 الآثار المترتبة على الهندسة الاجتماعية Implications of social engineering ..... 7

2.3.1 أساليب الهندسة الاجتماعية Methods of social engineering ..... 7

3.3.1 سرقة الشخصية/الهوية Identity theft ..... 8

4.3.1 طرق سرقة الشخصية/الهوية Methods of identity theft ..... 8

تمرين (1-3) ..... 9

**4.1 أمن الملفات FILE SECURITY ..... 10**

1.4.1 تأثير تمكين/عدم تمكين إعدادات أمان الماكرو The effect of enabling/ disabling macro security settings ..... 10

2.4.1 تعيين كلمة مرور للملفات Setting a password for files ..... 11

1.2.4.1 تعيين كلمة مرور للمستندات Setting a password for documents ..... 11

2.2.4.1 تعيين كلمة مرور للملفات المضغوطة Setting a password for compressed files ..... 12
3.2.4.1 تعيين كلمة مرور للجداول الإلكترونية Setting a password for spreadsheets ..... 15
3.4.1 إيجابيات وقيود التشفير The advantages and limitations of encryption ..... 16
1.3.4.1 إيجابيات التشفير The advantages of encryption ..... 16
2.3.4.1 قيود التشفير The limitations of encryption ..... 16
تمرين (1-4) ..... 16
**2 البرمجيات الخبيثة/الضارة MALWARE ..... 17**
**1.2 التعريف والوظيفة DEFINITION AND FUNCTION ..... 17**
1.1.2 مفهوم البرمجيات الخبيثة/الضارة The term: Malware ..... 17
2.1.2 الطرق التي تختبئ وتختفي بها البرمجيات الخبيثة/الضارة Ways that malware can be concealed 17
تمرين (2-1) ..... 17
**2.2 الأنواع TYPES ..... 18**
1.2.2 أنواع البرمجيات الخبيثة المعدية، وآلية عملها Types of infectious malware and how they work 18.
2.2.2 أنواع البرمجيات الخبيثة لسرقة البيانات، وتوليد الأرباح/الابتزاز، وآلية عملها Types of data theft, profit generating/extortion malware and how they work ..... 18
تمرين (2-2) ..... 19
**3.2 الحماية PROTECTION ..... 20**
1.3.2 آلية عمل برامج مكافحة الفيروسات، ومحدداتها How anti-virus software works and its limitations 20
2.3.2 استخدام برنامج مكافحة الفيروسات Using anti-virus software ..... 20
1.2.3.2 فحص محركات أقراص محددة من الفيروسات Scanning specific drives ..... 20
2.2.3.2 فحص مجلدات محددة من الفيروسات Scanning specific folders ..... 21
3.2.3.2 فحص ملفات محددة من الفيروسات Scanning specific files ..... 22
4.2.3.2 جدولة الفحص Schedule scans ..... 23
3.3.2 الحجر، وأثره على الملفات المصابة أو المشكوك بها The quarantine and its effect on infected/suspicious files ..... 24
4.3.2 أهمية تحميل وتثبيت تحديثات البرامج، وملفات تعريف مكافحة الفيروسات The importance of downloading and installing software updates, anti-virus definition files ..... 24
تمرين (2-3) ..... 25
**3 أمن الشبكات NETWORK SECURITY ..... 26**
**1.3 الشبكات NETWORKS ..... 26**
1.1.3 مفهوم الشبكة، وأهم أنواعها The term: Network and common network types ..... 26
2.1.3 دور مسؤول الشبكة The role of the network administrator ..... 27
3.1.3 الجدار الناري The firewall ..... 28
1.3.1.3 وظيفة الجدار الناري The function of a firewall ..... 28
2.3.1.3 قيود ومحددات الجدار الناري The limitations of a firewall ..... 28
تمرين (3-1) ..... 28
**2.3 اتصالات الشبكة NETWORK CONNECTIONS ..... 29**
1.2.3 خيارات الاتصال بالشبكة The options for connecting to a network ..... 29

2.2.3 الآثار الأمنية المترتبة على الاتصال بالشبكة How connecting to a network has implications for security ..... 30
تمرين (3-2) ..... 30
**3.3 أمن الشبكات اللاسلكية Wireless Security ..... 30**
1.3.3 أهمية حماية الشبكة اللاسلكية بكلمة مرور The importance of requiring a password for protecting wireless network access ..... 30
2.3.3 أنواع أمان الشبكات اللاسلكية Types of wireless security ..... 30
1.2.3.3 الوصول المحمي بالدقة اللاسلكية Wi-Fi Protected Access (WPA) ..... 30
2.2.3.3 خوارزميات السرية المتكافئة Wired Equivalent Privacy (WEP) ..... 31
3.2.3.3 التحكم بالوصول إلى الوسائط Media Access Control (MAC) ..... 31
3.3.3 آثار استخدام شبكة لاسلكية غير محمية Implications of using an unprotected wireless network ..... 32
4.3.3 الاتصال بشبكة لاسلكية Connecting to a wireless network ..... 32
تمرين (3-3) ..... 34
**4.3 التحكم بالوصول Access Control ..... 34**
1.4.3 الهدف من حساب الشبكة The purpose of a network account ..... 34
2.4.3 سياسات كلمة المرور الجيدة Good password policies ..... 35
3.4.3 التقنيات الأمنية الحيوية/البيومترية الشائعة المستخدمة في التحكم بالوصول Common biometric security techniques used in access control ..... 35
تمرين (3-4) ..... 37
**4 الاستخدام الآمن للويب SECURE WEB USE ..... 38**
**1.4 تصفح الويب Web Browsing ..... 38**
1.1.4 أنشطة معينة على الإنترنت يجب عدم القيام بها إلا ضمن صفحات ويب آمنة Certain online activity should only be undertaken on secure web pages ..... 38
2.1.4 كيفية تحديد مواقع الويب الآمنة How to Identify secure websites ..... 38
3.1.4 تزوير/قرصنة العناوين Pharming ..... 39
4.1.4 الشهادة الرقمية Digital certificate ..... 40
1.4.1.4 مفهوم الشهادة الرقمية The term: Digital certificate ..... 40
2.4.1.4 أنواع الشهادات الرقمية Types of digital certificate ..... 41
3.4.1.4 التحقق من صحة الشهادة الرقمية Validating a digital certificate ..... 41
5.1.4 كلمة السر المستخدمة لمرة واحدة The term one-time password (OTP) ..... 42
6.1.4 الإكمال التلقائي، والحفظ التلقائي Autocomplete, Autosave ..... 42
1.6.1.4 اختيار الإعدادات المناسبة لتمكين أو تعطيل الإكمال التلقائي Selecting appropriate settings for enabling/disabling autocomplete when completing a form ..... 42
2.6.1.4 اختيار الإعدادات المناسبة لتمكين أو تعطيل الحفظ التلقائي Selecting appropriate settings for enabling/disabling autosave when completing a form ..... 44
7.1.4 ملف تعريف الارتباط (الكوكي) The term: Cookie ..... 44
8.1.4 اختيار الإعدادات المناسبة للسماح بـ أو لمنع ملفات تعريف الارتباط (الكوكيز) Selecting appropriate settings for allowing, blocking cookies ..... 44

9.1.4 حذف البيانات الخاصة من متصفح الويب Deleting private data from a browser ..... 46
10.1.4 برمجيات التحكم بالمحتوى Content-control software ..... 47
تمرين (4-1) ..... 48
**2.4 الشبكات الاجتماعية SOCIAL NETWORKING ..... 50**
1.2.4 فهم أهمية عدم الكشف عن معلومات سرية على مواقع الشبكات الاجتماعية The importance of not disclosing confidential information on social networking sites ..... 50
2.2.4 الحاجة إلى تطبيق الإعدادات الخصوصية المناسبة على حساب الشبكات الاجتماعية The need to apply appropriate social networking account privacy settings ..... 50
3.2.4 الأخطار المحتملة عند استخدام الشبكات الاجتماعية Potential dangers when using social networking sites ..... 50
تمرين (4-2) ..... 51
**5 الاتصالات COMMUNICATIONS ..... 52**
**1.5 البريد الإلكتروني E-MAIL ..... 52**
1.1.5 الهدف من تشفير/فك تشفير رسائل البريد الإلكتروني The purpose of encrypting, decrypting an e-mail ..... 52
2.1.5 التوقيع الرقمي The term: Digital signature ..... 52
3.1.5 إنشاء توقيع رقمي وإضافته Creating and adding a digital signature ..... 53
4.1.5 الحذر من استقبال رسائل احتيالية، أو رسائل غير مرغوب فيها Be aware of the possibility of receiving fraudulent and unsolicited e-mail ..... 56
5.1.5 الخداع/التصيد Phishing ..... 56
6.1.5 خطر إصابة الحاسوب بالبرامج الخبيثة/الضارة The danger of infecting the computer with malware ..... 57
تمرين (5-1) ..... 57
**2.5 المراسلة اللحظية/الفورية INSTANT MESSAGING (IM) ..... 58**
1.2.5 مفهوم المراسلة اللحظية/الفورية، واستخداماتها The term: Instant Messaging (IM) and its uses ..... 58
2.2.5 الثغرات الأمنية في المراسلة اللحظية The security vulnerabilities of IM ..... 59
3.2.5 أساليب ضمان السرية أثناء استخدام المراسلة اللحظية Methods of ensuring confidentiality while using IM ..... 59
تمرين (5-2) ..... 60
**6 الإدارة الآمنة للبيانات SECURE DATA MANAGEMENT ..... 61**
**1.6 النسخ الاحتياطي وتأمين البيانات SECURING AND BACKING UP DATA ..... 61**
1.1.6 طرق ضمان الأمن المادي للأجهزة Ways of ensuring physical security of devices ..... 61
2.1.6 أهمية النسخ الاحتياطي The importance of having a back-up procedure ..... 61
3.1.6 ميزات النسخ الاحتياطي The features of a back-up procedure ..... 62
4.1.6 إجراء النسخ الاحتياطي للبيانات Back up data ..... 62
5.1.6 استعادة وتقييم البيانات التي تم نسخها نسخا احتياطيا Restoring and validating backed up data ..... 64
تمرين (6-1) ..... 65

**2.6 التدمير الآمن SECURE DESTRUCTION ..... 66**

1.2.6 أسباب حذف البيانات من محركات الأقراص أو من الأجهزة بشكل دائم The reason for permanently deleting data from drives or devices ..... 66

2.2.6 الفرق بين حذف البيانات وتدميرها بشكل دائم Distinguish between deleting and permanently destroying data ..... 66

3.2.6 وسائل تدمير البيانات بشكل دائم Common methods of permanently destroying data ..... 66

تمرين (6-2) ..... 67

**ملحق إجابات الأسئلة، والمراجع ..... 68**

## تبرئة وتنويه (Disclaimer)

تعد كل من الرخصة الأوروبية لقيادة الحاسوب ECDL، والرخصة الدولية لقيادة الحاسوب ICDL، وجميع الشعارات الخاصة بها علامات تجارية مسجلة تابعة لمؤسسة الرخصة الأوروبية لقيادة الحاسوب. وإن شركة سبيكتو ليميتد مستقلة عن المشغل الوطني للرخصة الدولية لقيادة الحاسوب، وليس لها أيّ نوع من الشراكة مع مؤسسة الرخصة الأوروبية لقيادة الحاسوب في أي أمر من الأمور. ويمكن لهذه المادة أن تستخدم في مساعدة الطلبة على التقدم إلى اختبار الرخصة الدولية لقيادة الحاسوب (ICDL). وليس هناك أية ضمانات يقدمها المشغل الوطني أو سبيكتو ليميتد على أن استخدام هذه المادة سيضمن اجتياز الاختبار المتعلق بها. إن المشغل الوطني قد راجع واعتمد هذا الكتاب بشكل مستقل وتأكد من تغطيته لأهداف التعلم لمنهاج الرخصة الدولية لقيادة الحاسوب.

تم إخضاع هذا الكتاب لعملية مراجعة تقنية، ولكنها لا تضمن أن يجتاز الطالب اختبارات الرخصة الدولية لقيادة الحاسوب. وفيما يتعلق بأي من الاختبارات التقييمية أو جميعها أو تدريبات تقييم الأداء المحتواة في هذا المنتج، فهي تقتصر فقط على هذا المنتج ولا تحتوي بشكل صريح أو ضمني ترخيصا من مؤسسة الرخصة الأوروبية لقيادة الحاسوب لاختبارات (ICDL) أو أية اختبارات أخرى. وبغض النظر عن كيفية استخدام هذه المادة التدريبية، فلا يجوز أن توحي للطالب أن هذه المادة تؤدي إلى شهادة إلا إذا جلس الطالب للاختبارات الرسمية المعتمدة من مؤسسة الرخصة الأوروبية لقيادة الحاسوب. وللحصول على معلومات للتقدم لاختبارات الرخصة الدولية لقيادة الحاسوب، الرجاء الاتصال بالمشغل الوطني للرخصة الدولية لقيادة الحاسوب في دولتك، أو قم بزيارة موقع مؤسسة الرخصة الأوروبية لقيادة الحاسوب www.ecdl.org.

إذا رغبت في الحصول على شهادة الرخصة الدولية لقيادة الحاسوب فيجب عليك أولا التسجيل لدى المزود الوطني في بلدك وذلك بالتسجيل في أحد مراكز اختبار ICDL المعتمدة. وبدون هذا التسجيل لا يمكن الجلوس لأي امتحان، كما لا يمكن الحصول على أي شهادة أو وثيقة رسمية.

## كيف تقرأ هذا الكتاب

1) تعتمد المادة التدريبية على التعلم الذاتي من خلال تطبيق المهارات عمليا على ملفات معدة مسبقا، ويجب عليك الحصول على هذه الملفات من القرص المدمج إن وجد، أو يمكنك تنزيلها من الموقع www.specto.co/Data. قم بفك الضغط عن الملفات إلى المجلد C:/ICDL V6.

2) اتبع الخطوات المفصولة بأرقام على الترتيب.

3) ستقوم بحفظ الملفات أو تفتحها - بشكل افتراضي - من المجلد C:/ICDL V6، ما لم يطلب إليك غير ذلك.

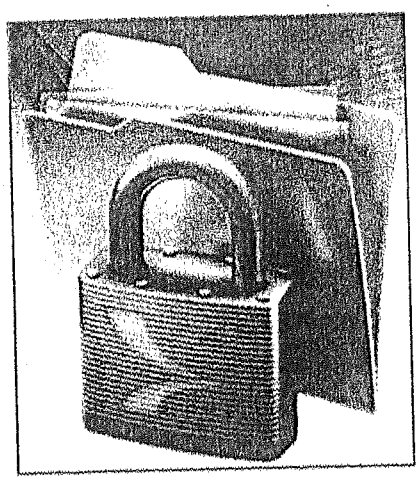
4) يفضل أن تكون النوافذ المفتوحة في وضع التكبير، كي تتوافق مع الرسومات والصور الموجودة في هذا الكتاب.

إذا عثرت على أية أخطاء في هذه المادة التدريبية، يمكنك الاتصال بالمؤلف على العنوان التالي info@Specto.co. وعلى الرغم من الجهد الذي بذل من أجل معالجة أية أخطاء مطبعية أو تقنية فنحن نلتمس العذر حيال الأخطاء التي قد تعثر عليها. ويعتزم المؤلف تحديث هذه المادة بصفة دورية، لذا فإن أية ملحوظة تأتي من جانبكم سيكون لها دورها الفعال في مساعدتنا على تحقيق أعلى المواصفات.

## تحذير

- لا يجوز نشر أي جزء من هذا الكتاب أو نقله على أي نحو أو بأية طريقة، سواء أكانت إلكترونية أو بالتصوير أو بخلاف ذلك، أو استخدامها في إنتاج أية مادة مماثلة إلا بموافقة خطية من المؤلف، ومن يخالف ذلك يعرض نفسه للمساءلة القانونية، مع حفظ كافة الحقوق المدنية والجنائية.
- إن أسماء العلامات التجارية وأسماء المنتجات التي تم استخدامها في إعداد هذه المادة التدريبية جميعها هي أسماء تجارية أو علامات تجارية مسجلة خاصة بمالكيها فحسب، ودار النشر لا علاقة لها بأي من المنتجات أو الشركات التي ورد ذكرها في هذه المادة.

## 1 مفاهيم الأمن Security Concepts



مع تطور العلم والتكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة، أو ما يسمى نقل البيانات عبر الشبكة من موقع لآخر، أصبح النظر إلى أمن تلك البيانات والمعلومات أمرا مهما للغاية.

يمكن تعريف أمن المعلومات بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها بالسرقة أو التعديل، وذلك من خلال توفير الأدوات والوسائل اللازمة لحماية المعلومات من المخاطر الداخلية أو الخارجية، واتباع المعايير وإجراءات الاتصالات المناسبة؛ لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين، ولضمان أصالة وصحة تلك الاتصالات.

### 1.1 تهديدات البيانات Data Threats

#### 1.1.1 تمييز البيانات من المعلومات Distinguishing between data and information

- (البيانات/ *Data*): يمكن أن تكون البيانات حروفا أو كلمات أو أرقاما أو رموزا أو صورا أو أصواتا لم تتم معالجتها، وإنما يتم جمعها لغايات معالجتها. وبالتالي يمكنك القول بأن البيانات هي معلومات لم تتم معالجتها.
- (المعلومات/ *Information*) هي البيانات بعد معالجتها، بحيث تصبح ذات معنى عند الشخص الذي يستقبلها.

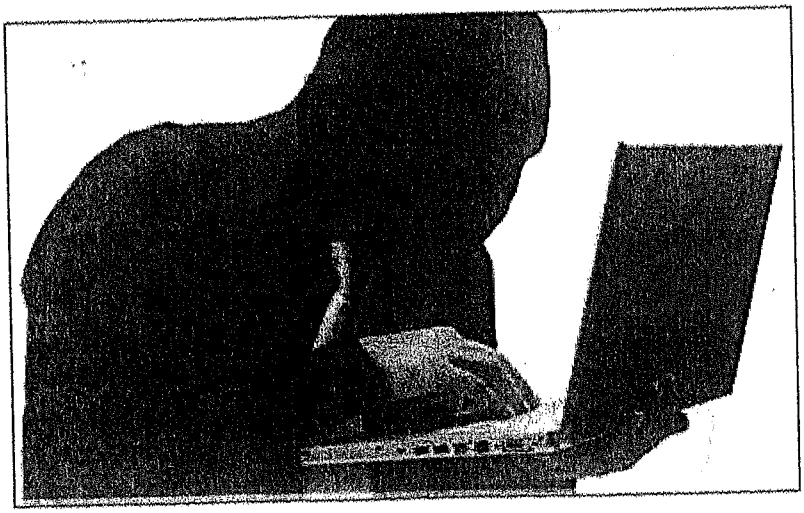
وكي تدرك الفرق بين البيانات والمعلومات؛ فإن الكلمات (علي، 920، 92) تشير إلى بيانات، ولكن عند تفسيرها بأنها بيانات لطالب اسمه علي، ومجموع علاماته 920، ومعدله 92، تصبح هذه البيانات معلومات.

وهنا تجدر الإشارة إلى أنه عند تفسير البيانات بشكل مختلف، فإنه قد ينتج من البيانات نفسها معلومات مختلفة.

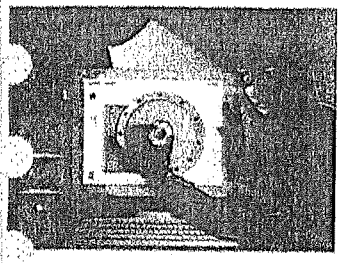
#### 2.1.1 الجريمة الإلكترونية Cybercrime

هي أي نشاط غير قانوني يتم باستخدام الإنترنت أو الحاسوب. ومن الأمثلة عليها: سرقة الهوية الشخصية، والهندسة الاجتماعية، والاختراق الأمني، وكسر حماية البرامج، وسرقة تفاصيل بطاقة الائتمان عبر الإنترنت.

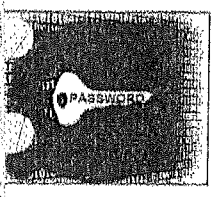
وبذلك فإن الجريمة الإلكترونية تشمل أية مخالفة ترتكب ضد أفراد أو جماعات بدافع جرمي، أو بنية الإساءة لسمعة الضحية أو لجسدها أو عقليتها، كل ذلك باستخدام وسائل الاتصالات الحديثة مثل الإنترنت، وغرف الدردشة أو البريد الإلكتروني أو المجموعات ... إلخ.



### 3.1.1 فهم الفرق بين كل من القرصنة، وكسر الحماية والاختراق الأخلاقي The difference between hacking, cracking and ethical hacking



- تقوم (القرصنة أو الاختراق/ *Hacking*) على استخدام الإبداع والخبرة الحاسوبية في الوصول إلى نظام الحاسوب دون تخويل بذلك؛ من أجل العبث بالبيانات والبرامج الموجودة على الحاسوب أو استغلالها لأغراض التجسس أو سرقة الأموال، أو قد يقوم القرصان بهذا العمل لاستخدام موارد الحاسوب، أو يكتفي بإثبات أنه يستطيع الوصول إلى حاسوبك.
- يقوم (الاختراق الأخلاقي/ *Ethical hacking*) أو ما يسمى بالقرصنة الأخلاقية على اختراق النظام الأمني للحاسوب، بتصريح من المالك نفسه؛ لكن ليس لتعطيل الخدمة أو نحو ذلك، بل لحماية نظام الحاسوب من خلال إيـ نقاط الضعف والثغرات في شبكة المنظمة، التي يمكن للقرصان الماكر استغلالها، فيقوم المخترق الأخلاقي بمحاول تفادي جميع معوقات أنظمة الحماية التي يواجهها في سبيل الوصول إلى معلومة ليس من المفترض أن يصل إ وأحيانا يطلب من المخترق أن يحاول الإطاحة بنظام قائم بهدف منع المستخدمين من الوصول إلى هذا النظام أو الخدمة، وتنتهي هذه العملية بتقديم تقرير مفصل عن مستوى الحماية الذي توفره المنظمة، وما يمكن أن تقوم به تحسينات لتفادي الأضرار التي قد تمس بالمنظمة جراء محاولات قادمة للقراصنة غير الأخلاقيين.




- يقوم (كسر حماية كلمة المرور/ *Password Cracking*) على استرداد ومعرفة كلمات السر إما من البيانات التي تم تخزينها أو التي تم نقلها عبر نظام الحاسوب. ويتم هذا الأمر إما يدويا بتخمين كلمة المرور، أو باستخدام برامج خاصة.
- يقوم (كسر حماية البرامج/ *Software Cracking*) على عدم تمكين أو على إزالة ميزات معينة غير مرغوب من البرنامج، ومن الأمثلة على تلك الميزات حقوق النشر، والأرقام السرية، ومفاتيح المعدات والأجهزة، وتاريـ الفحص.

### 4.1.1 تهديدات البيانات بسبب ظروف قاهرة Threats to data from force majeure

الظروف القاهرة هي القوى الفائقة أو الحدث غير المتوقع الذي لا يمكن للشركة أن تتنبأ به، لكنه يمكن أن يهدد البيانات، النار، والفيضانات، والحروب، والزلازل، وهذه كلها قد تؤدي إلى تدمير بيانات الأفراد والشركات.

### 5.1.1 تهديدات البيانات من الأشخاص Threats to data from persons

إن خطر الأشخاص لا يقل عن خطر القوى القاهرة، فإن احتمالية سرقة البيانات والتلاعب بها واستخدامها لمصالح شخصية أو مالية احتمال كبير نسبيا ما لم تتخذ إجراءات الحماية المناسبة، وفيما يأتي أهم الأشخاص الذين يمكنهم الوصول إلى البيانات:

- (الموظفون/ *Employees*): يمكن للموظفين أن يسرقوا بيانات الشركة، مثل المعلومات عن المنتج الجديد الذي ستنتجه الشركة، إما لحسابهم الشخصي، أو لحساب جهة خارجية.
- (مزودو الخدمة/ *Service providers*): يمكن لموظفي مزود الخدمة أن يطلعوا على البيانات بقصد أو دون قصد، كما يمكنهم أن يدمروا أو يسرقوا بيانات قيمة للشركة؛ لأنهم كما هو معلوم هم الذين يقومون بمعالجة بيانات الشركات على أجهزة الخادم.
- (الأفراد من الخارج/ *External individuals*): كالقراصنة، فإنهم يمكنهم الوصول إلى نظام الحاسوب، وسرقة أو حذف البيانات.

**تمرين (1-1)**

اختر الإجابة الصحيحة من بين البدائل الأربعة المذكورة لكل سؤال مما يلي: *(انظر الإجابات في ملحق الإجابات ص 68).*

1. ماذا يطلق على النشاط غير المشروع باستخدام الانترنت؟
أ- الجريمة الإلكترونية. ب- الجريمة المادية. ج- الجريمة العنكبوتية. د- الجريمة الافتراضية.

2. أي من الآتية يعد مثالا على جرائم الإنترنت؟
أ- القرصنة الأخلاقية. ب- التمزيق. ج- الخداع. د- الجدار الناري.

3. يمكن تعريف القرصنة الأخلاقية بأنها:
أ- التنصت على شبكة اتصال لاسلكية. ب- الاختراق المصرح به للنظام.
ج- الاختراق غير المصرح به إلى النظام. د- التنصت على شبكة اتصال سلكية.

4. أي من الآتية لا يعد من القوى القاهرة التي تهدد البيانات؟
أ- مزودو الخدمة. ب- الحريق. ج- الفيضانات. د- الزلزال.

5. ما المقصود بكسر حماية كلمة المرور؟
أ- إدخال كلمة مرور غير صحيحة عدة مرات. ب- معرفة نص كلمة المرور.
ج- سرقة تفاصيل شخصية لشخص ما عبر الإنترنت. د- تغيير كلمة المرور بشكل دوري.

6. أي مما يلي لا يمكن أن يكون تهديدا محتملا للبيانات؟
أ- القراصنة. ب- مزودو الخدمة. ج- الشهادات الرقمية. د- الموظفون.

7. ما المقصود بالمعلومات؟
أ- البيانات التي تمت معالجتها. ب- الأرقام التي لم تتم معالجتها.
ج- الأصوات والنصوص. د- البيانات التي لم تتم معالجتها.

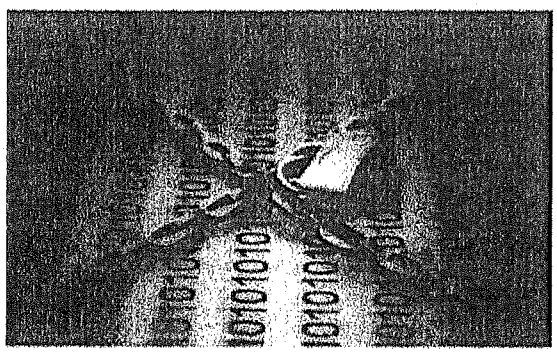
8. ماذا يطلق على اختراق النظام الأمني للحاسوب، بتصريح من المالك نفسه؟
أ- القرصنة. ب- كسر حماية البرامج. ج- انتحال الشخصية. د- الاختراق الأخلاقي.

## 2.1 أهمية وقيمة المعلومات Value of Information

### 1.2.1 الأسباب التي تدعو إلى حماية المعلومات الشخصية The reasons for protecting personal information

عليك أن تحرص أشد الحرص على حماية معلوماتك الشخصية، لأنك بذلك تمنع أمورا خطيرة من أهمها:

- سرقة/انتحال الشخصية من قبل أشخاص يدعون أنهم أنت من أجل الحصول على خدمات باسمك.
- الاحتيال من قبل أشخاص قد يستخدمون معلوماتك الشخصية في الاحتيال على الآخرين الذين يثقون بك.



### 2.2.1 الأسباب التي تدعو إلى حماية المعلومات التجارية الحساسة The reasons for protecting commercially sensitive information

عليك أن تحرص أشد الحرص على حماية المعلومات التجارية، لأنك بذلك تمنع أمورا خطيرة تتعلق بسرقة البيانات، من أهمها:

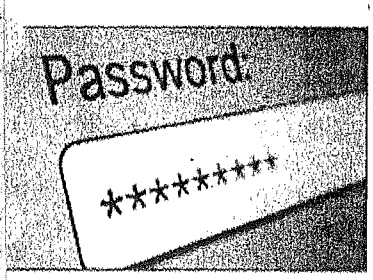
- سرقة أو إساءة استخدام تفاصيل العملاء من قبل الشركات المنافسة.
- سرقة أو إساءة استخدام المعلومات المالية الخاصة بالشركة.

### 3.2.1 التدابير التي تمنع الوصول غير المسموح به إلى البيانات Measures for preventing unauthorised access to data

تستخدم شبكة الإنترنت بشكل واسع لنقل المعلومات حول العالم، وتتميز بعض هذه المعلومات - مثل الحركات المالية والمعلومات الشخصية للأفراد - بحاجتها إلى السرية العالية. وللحفاظ على سرية البيانات التي يتم تبادلها من خلال الإنترنت يتم اتخاذ العديد من الإجراءات، وفيما يأتي أهم هذه التدابير والإجراءات:

- (التشفير/ *Encryption*): هو عملية ترميز البيانات والمعلومات، وتحويلها إلى صيغة غير مفهومة، باستخدام المفاتيح العامة والخاصة في تشفير الرسالة، وتستند هذه المفاتيح إلى صيغ رياضية معقدة؛ لمنع الأشخاص غير المخولين بالاطلاع على المعلومات من الاطلاع عليها.

  أما عملية (فك التشفير/ *Decryption*) فهي عملية إعادة تحويل البيانات إلى صيغتها الأصلية، وذلك باستخدام المفتاح المناسب لفك الشيفرة.




- (كلمات المرور/ *Passwords*): هي سلسلة من الرموز (حروف وأرقام وبعض الرموز الخاصة) تستخدم للتأكد من الهوية وللتعريف بالشخص المخول، وتمكنه من فتح ملف، أو تشغيل حاسوب، أو تشغيل برنامج، أو الدخول إلى شبكة حواسيب، والحصول على إذن الوصول إلى موارد الحاسوب. وعند إنشاء كلمات المرور يجب أن تكون قوية، يصعب تخمينها أو كسر حمايتها.

### 4.2.1 المميزات الأساسية لأمن المعلومات Basic characteristics of information security

أمن المعلومات يعني حمايتها من أي دخول غير مصرح به، ولا يتحقق هذا الأمن إلا إذا توفرت الأمور الآتية:

- (الخصوصية والسرية/ *Confidentiality*): تشير إلى حماية المعلومات من الوصول غير المصرح به، أو من إفشائها.
- (الكمال/ *Integrity*): يشير إلى الثقة بمصادر المعلومات، وأنها معلومات صحيحة وكاملة ولم يتم تعديلها.
- (التوفر/ *Availability*): يشير إلى توفر مصادر المعلومات، وأنه يمكن الوصول والحصول على المعلومات والبيانات عندما يتم طلبها من الأشخاص المخولين. ويشمل هذا الأمر ضمان عدم تعطل أنظمة المعلومات بسبب الصيانة أو تحديثها، أو بسبب وجود برامج خبيثة.

### 5.2.1 حماية الخصوصية/البيانات، والاحتفاظ بها، ومتطلبات التحكم بها The main data/privacy protection, retention and control requirements

يتصل عادة مفهوم (حماية البيانات/ *Data Protection*) بـ (خصوصية المعلومات/ *Information Privacy*)، والتي تتضمن القواعد التي تحكم جمع وإدارة البيانات الخاصة، كمعلومات بطاقات الهوية والمعلومات المالية والسجلات الطبية والسجلات الحكومية وغيرها. وبناء على هذا فإن قانون حماية البيانات هو القانون الذي يحمي الخصوصية الشخصية وحقوق الأفراد، ويقوم هذا القانون على ضمان أن تكون المعلومات متاحة فقط لأولئك الذين يؤذن لهم بالاطلاع عليها.

في دول الاتحاد الأوروبي يتم تطبيق تشريع حماية البيانات الأوروبي لعام 1995م، لكن يجب أن يتوفر في كل بلد قانون أو تشريع لحماية هذه البيانات من الاستخدام الخاطئ مراعيا الأهداف الرئيسية الآتية لقانون حماية البيانات:

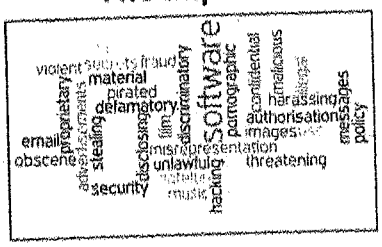
- وضع معايير لاستخدام البيانات الشخصية بشكل يحفظ للأفراد خصوصيتهم ويحمي حقوقهم.
- تحديد مسؤوليات مراقب البيانات، للتعامل مع البيانات بشكل أخلاقي وقانوني والمحافظة على سرية تلك المعلومات.

ويتضمن هذا القانون في أية دولة عددا من المبادئ التي يجب اتباعها للتعامل مع البيانات الشخصية، والتي تكون مسؤولية مراقب البيانات، منها:

- أن تتم معالجة البيانات الشخصية بصورة عادلة وقانونية.
- أن يتم الحصول عليها لأغراض محددة.
- أن تكون كافية وذات صلة وليس مفرطة.
- أن تكون دقيقة وحديثة.
- أن لا تحفظ وقتا أطول من اللازم.
- أن تتم معالجتها وفقا لحقوق صاحب البيانات.
- أن لا يتم نقل البيانات خارج البلد ما لم يكن هناك مستوى كاف من الحماية لهذه البيانات.

### 6.2.1 أهمية إنشاء الإرشادات والسياسات العامة المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات، والالتزام بها

### The importance of creating and adhering to guidelines and policies for ICT use




ينبغي على الشركات أن تقوم بتزويد جميع موظفيها بمعايير معينة كي يتبعوها، وليضمنوا وجود موقف واضح حول كيفية استخدام تكنولوجيا المعلومات والاتصالات بشكل يحمي بيانات المنظمة.

ولعله من الضروري لك كمستخدم لتكنولوجيا المعلومات والاتصالات أن تدرك مسؤوليتك تجاه الوصول الى لائحة كبيرة من الخدمات والمواقع والأنظمة والأشخاص على الشبكة. وتذكر دائما حقيقة أن قدرتك على القيام بعمل معين لا تعني بالضرورة وجوب قيامك بذلك العمل. فاستخدام الشبكة يعتبر ميزة وليس حقا، وقد تعرض هذه الميزة للإساءة الأخلاقية والقانونية أحيانا إذا ما تصرفت بشكل غير لائق.

ومن أهم هذه الإرشادات العامة:

- التأكد من أن إعدادات برامج الحماية على الإنترنت صحيحة ومناسبة لاستخداماتك.
- مراجعة سياسة الخصوصية الخاصة بالمواقع الإلكترونية التي تنوي التسجيل بها أو تزويدها ببياناتك الشخصية.
- إذا كنت تعمل لدى أية هيئة أو مؤسسة سواء أكانت حكومية أم خاصة، يجب التأكد من وجود الاتفاقية السرية التي تتضمن عدم الكشف عن المعلومات، قبل تبادل أية معلومات مع طرف ثالث خارج مؤسستك.
- استخدام جهاز تمزيق الأوراق للتخلص من أية أوراق تحتوي على معلوماتك الشخصية.
- عدم الاستجابة لرسائل البريد الإلكتروني التي تطلب منك بيانات شخصية، أو تلك الواردة من الأشخاص غير المعروفين لديك.
- تثبيت برنامج مكافحة الفيروسات وتحديثه بشكل مستمر.
- تشغيل برنامج الجدار الناري، وتعيين الإعدادات المناسبة له.
- عدم استخدام نفس اسم المستخدم وكلمة المرور على مواقع إلكترونية مختلفة، والتأكد من سرية كلمات المرور.
- عدم إدخال بيانات بطاقات الائتمان أو الحسابات البنكية في أي موقع دون التأكد من مدى الأمان لذلك الموقع.
- يستحسن الحد من المعلومات التي يتم نشرها في ملف التعريف الشخصي الخاص ببرامج المراسلة الفورية.
- التأكد من أن عمليات التحديث التلقائية مبرمجة بشكل صحيح.

**تمرين (1-2)**

اختر الإجابة الصحيحة من بين البدائل الأربعة المذكورة لكل سؤال مما يلي: *(انظر الإجابات في ملحق الإجابات ص 68).*

1. أي مما يأتي لا يعد سببا لحماية معلوماتك الشخصية أو التجارية؟
   أ- منع سرقة/انتحال الشخصية. ب- منع سرقة أو إساءة استخدام تفاصيل العملاء.
   ج- منع الاحتيال. د- منع القرصنة الأخلاقية.
2. أي مما يأتي من التدابير التي تساعد على منع الوصول غير المصرح به للبيانات؟
   أ- الخداع. ب- استخلاص كلمات المرور.
   ج- استراق النظر للحصول على المعلومات. د- التشفير.
3. ما المقصود بالكمال كخاصية من خصائص أمن المعلومات؟
   أ- توفر مصادر المعلومات. ب- الثقة بمصادر المعلومات، وأنها صحيحة وكاملة.
   ج- حماية المعلومات من الوصول غير المصرح به. د- ازدياد إمكانية قرصنة العناوين.
4. أي من الآتية هو أحد أسباب منع الاحتيال؟
   أ- حماية المعلومات الشخصية من الوصول غير المعتمد. ب- حماية نفسك من القرصنة الأخلاقية.
   ج- الحد من ميزة الإكمال التلقائي في المتصفح. د- الحد من ميزة الحفظ التلقائي في المتصفح.

5. أي العبارات التالية صحيح فيما يتعلق بالإرشادات والسياسات العامة المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات؟
أ- هذه الإرشادات متعلقة فقط بالمؤسسات المالية.
ب- ينبغي قراءة هذه الإرشادات ولكن لا يشترط تنفيذها.
ج- هذه الإرشادات مهمة لأنها توفر معيارا للمستخدمين كي يتبعوه.
د- هذه الإرشادات تطبق فقط على الموظفين العاديين في الشركة.

6. أي من الآتية يعد من سمات أمن المعلومات التي تضمن عدم تعديل البيانات دون إذن أو تصريح؟
أ- الكمال. ب- إمكانية الوصول. ج- التوفر. د- السرية.

7. أي مما يلي ليس سببا شائعا لحماية المعلومات التجارية الحساسة المخزنة على الشبكة؟
أ- لحماية العملاء من الاحتيال. ب- لتشجيع الوصول الخارجي إلى الشبكة.
ج- للتأكد من بقاء تفاصيل العميل سرية. د- للتحكم في الوصول إلى المعلومات.

8. في دول الاتحاد الأوروبي يتم تطبيق تشريع حماية البيانات الأوروبي لعام:
أ- 1995. ب- 1996. ج- 1997. د- 1998.

9. أي من الآتية هو أحد سمات أمن المعلومات التي تضمن حماية تلك المعلومات من الوصول غير المصرح به أو الكشف عنها؟
أ- الموثوقية. ب- الكمال. ج- التوفر. د- السرية.

## 3.1 الأمن الشخصي Personal Security

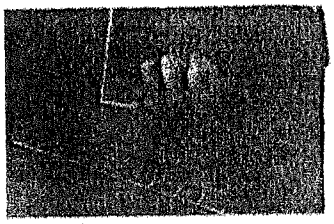
### 1.3.1 الهندسة الاجتماعية Social Engineering

#### 1.1.3.1 مفهوم الهندسة الاجتماعية The term: Social engineering

هي مجموعة من التقنيات التي تستخدم للتلاعب بالأشخاص، واستغلالهم من أجل القيام بعمل ما أو إفشاء معلومات سرية، ولهذا تعرف الهندسة الاجتماعية أحيانا بفن اختراق العقول، بدلا من القرصنة أو اختراق النظام للحصول على تلك المعلومات.

#### 2.1.3.1 الآثار المترتبة على الهندسة الاجتماعية Implications of social engineering

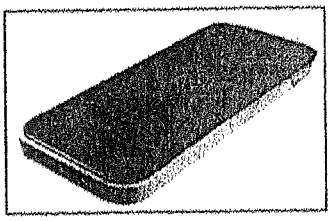
يترتب على الهندسة الاجتماعية العديد من الآثار السيئة، منها:



- (جمع المعلومات/ *Information gathering*): التي يمكن أن تكون سرية أو قيمة.
- (الاحتيال/ *Fraud*): استخدام المعلومات التي تم جمعها في الاحتيال على الآخرين.
- (الوصول إلى نظام الحاسوب/ *Computer system access*): يؤدي الوصول إلى البيانات المخزنة على نظام الحاسوب إلى تسهيل واحتمالية الكشف عن معلومات سرية.

### 2.3.1 أساليب الهندسة الاجتماعية Methods of social engineering

للهندسة الاجتماعية أساليب ووسائل عديدة، منها:



- (المكالمات الهاتفية/ *Phone calls*): استخدام الاتصال الهاتفي في تضليل شخص ما حول هويتك؛ للحصول على معلومات قيمة. حيث يتصل المهاجم مدعيا أنه شخص ذو منصب، وله صلاحيات، ثم يقوم تدريجيا بسحب المعلومات من الضحية.
- (استراق النظر/ *Shoulder surfing*): استخدام الملاحظة المباشرة للحصول على المعلومات، وذلك بمراقبة الأشخاص عند كتابة أرقامهم السرية ومعلوماتهم الشخصية. فإذا كنت ممن يستخدمون الحاسوب المحمول في الأماكن

العامة كثيرا، فينصح بوضع شاشة الخصوصية وهي شاشة إضافية تركب على الحاسوب، وتمنع التلصص أو النظر من الزوايا والجوانب لضمان عدم قدرة الآخرين على رؤية ما تقوم به، وبخاصة عندما تدخل اسم المستخدم وكلمة المرور.

- (الخداع والتصيد/ *Phishing*): تضليل شخص ما حول هويتك باستخدام الإنترنت؛ للحصول على معلومات قيمة. حيث يحصل المهاجم على المعلومات التي يريدها من خلال التحدث مع الضحية وحثها على الإدلاء بمعلومات حساسة أو ذات علاقة بهدف المهاجم، وذلك من خلال إثارة انطباع جيد لدى الضحية والتملق وغيرها من الأساليب.

### 3.3.1 سرقة الشخصية/الهوية Identity theft

هي انتحال هوية شخص آخر من أجل الحصول على مكاسب شخصية. حيث يتم اقناع الشخص المراد أخذ المعلومات منه أن سارق الشخصية صديق أو ما شابه، أو أنه أحد الأفراد الذين يحق لهم الحصول على المعلومات، لدفعه إلى كشف المعلومات التي لديه والتي يحتاجها سارق الشخصية.

وسرقة الشخصية/الهوية تؤدي إلى الاستخدام الخاطئ للمعلومات الشخصية أو القانونية أو المالية أو تلك المتعلقة بالعمل، فقد يتظاهر شخص ما على كونه شخصا آخر، عادة ما يكون الهدف بقصد الوصول إلى موارد معينة أو الحصول على فوائد تحت اسم الشخص الآخر. قد يعاني ضحية سرقة الهوية عواقب خطيرة إن تحمل عواقب تصرفات الشخص الذي قام بسرقة هويته. كما أن الأشخاص أو المؤسسات التي تتعرض للتلاعب نتيجة سرقة الهوية قد تتعرض لخسائر ومتاعب كبيرة.

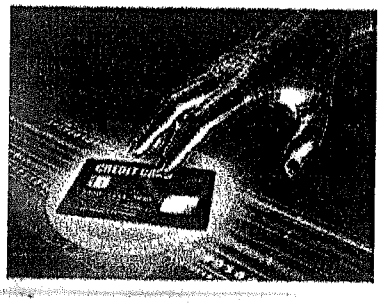
ويمكن تصنيف سرقة الشخصية/الهوية إلى خمسة أصناف:

- سرقة هوية عمل أو تجارية: استخدام الاسم التجاري لشخص آخر من أجل الحصول على أموال.
- سرقة هوية جرمية: التظاهر كهوية شخص آخر عند ارتكاب جريمة ما.
- سرقة هوية مالية: استخدام هوية شخص ما عند الحصول على أموال أو بضائع أو خدمات.
- استنساخ الهوية: استخدام معلومات شخصية لشخص آخر على أنها معلوماته في الحياة اليومية.
- سرقة هوية طبية: استخدام هوية شخص آخر من أجل الحصول على رعاية طبية أو أدوية.

### 4.3.1 طرق سرقة الشخصية/الهوية Methods of identity theft

هناك العديد من الطرق للحصول على معلومات شخص، وانتحال شخصيته، منها:

- (استعادة المعلومات/ *Information diving*): ممارسة استعادة المعلومات من المواد المهملة، سواء في سلات الفضلات والقمامة، أو في وسائط التخزين المهملة والتي لم يتم حذف البيانات نهائيا منها.
- (الاستخلاص/ *Skimming*): استخدام الماسح الضوئي للشريط المغناطيسي الذي يحتوي المعلومات، لاستخلاص تلك المعلومات، وغالبا ما تكون من بطاقة الائتمان. وأحيانا يكون ذلك بنسخ وصولات البطاقات الائتمانية وما تحتويه من معلومات.
- (التستر/ *Pretexting*): الحصول على معلوماتك باستخدام المكر والخداع والادعاءات الزائفة.



تمرين (1-3)

اختر الإجابة الصحيحة من بين البدائل الأربعة المذكورة لكل سؤال مما يلي: *(انظر الإجابات في ملحق الإجابات ص 68).*

1. ما المقصود بالهندسة الاجتماعية؟

أ- التلاعب بالأشخاص واستغلالهم. ب- قرصنة النظام للحصول على تلك المعلومات.

ج- الوصول المصرح به إلى الشبكة. د- تعطيل الجدار الناري.

2. أي مما يلي ليس نتيجة مباشرة للهندسة الاجتماعية؟

أ- سرقة الهوية. ب- الاحتيال.

ج- الوصول غير المصرح به إلى الشبكة. د- تعطيل الجدار الناري.

3. أي مما يلي هو وسيلة لسرقة الهوية؟

أ- استخدام اسم غير صحيح على موقع شبكات اجتماعية. ب- استخدام تقنية استعادة المعلومات من مواد مهملة.

ج- إزالة مغناطيسية وسائط التخزين القابلة للإزالة. د- استخدام مفتاح غير صحيح لفك تشفير مستند.

4. ماذا يطلق على التظاهر بأنك شخص آخر من أجل تحقيق مكاسب شخصية أو مالية؟

أ- سرقة الهوية. ب- القرصنة الأخلاقية. ج- الخداع/التصيد. د- التحقق من الهوية.

5. أي مما يأتي ليست من وسائل الهندسة الاجتماعية؟

أ- القيام بمكالمات هاتفية للحصول على معلومات عن طريق الخداع.

ب- القيام بمكالمات صوتية ومرئية مع الأصدقاء باستخدام شبكة الانترنت.

ج- وجود حسابات متعددة، وأسماء مستعارة على موقع الشبكات الاجتماعية.

د- إرسال بريد إلكتروني مع رابط إلى صفحة ويب احتيالية.

6. أي مما يلي يبين المقصود بسرقة الهوية؟

أ- استخدام برامج مراقبة المحتوى عندما تكون متصلا بشبكة الإنترنت.

ب- انتحال الشخصية لتحقيق مكاسب ذاتية.

ج- استخدام اسم مستخدم عندما تكون متصلا بشبكة الانترنت.

د- التزويد بعنوان عملك لغايات التسليم عند الشراء عبر الإنترنت.

7. أي مما يلي يعد مثالا على تقنية استعادة المعلومات من مواد مهملة؟

أ- استراق النظر من فوق كتف الشخص للحصول على معلومات.

ب- استرجاع المعلومات من قرص صلب تم التخلص منه.

ج- إجراء مكالمة هاتفية احتيالية.

د- استخدام شبكة الانترنت للبحث عن معلومات.

## 4.1 أمن الملفات File Security

### 1.4.1 تأثير تمكين/عدم تمكين إعدادات أمان الماكرو The effect of enabling/ disabling macro security settings

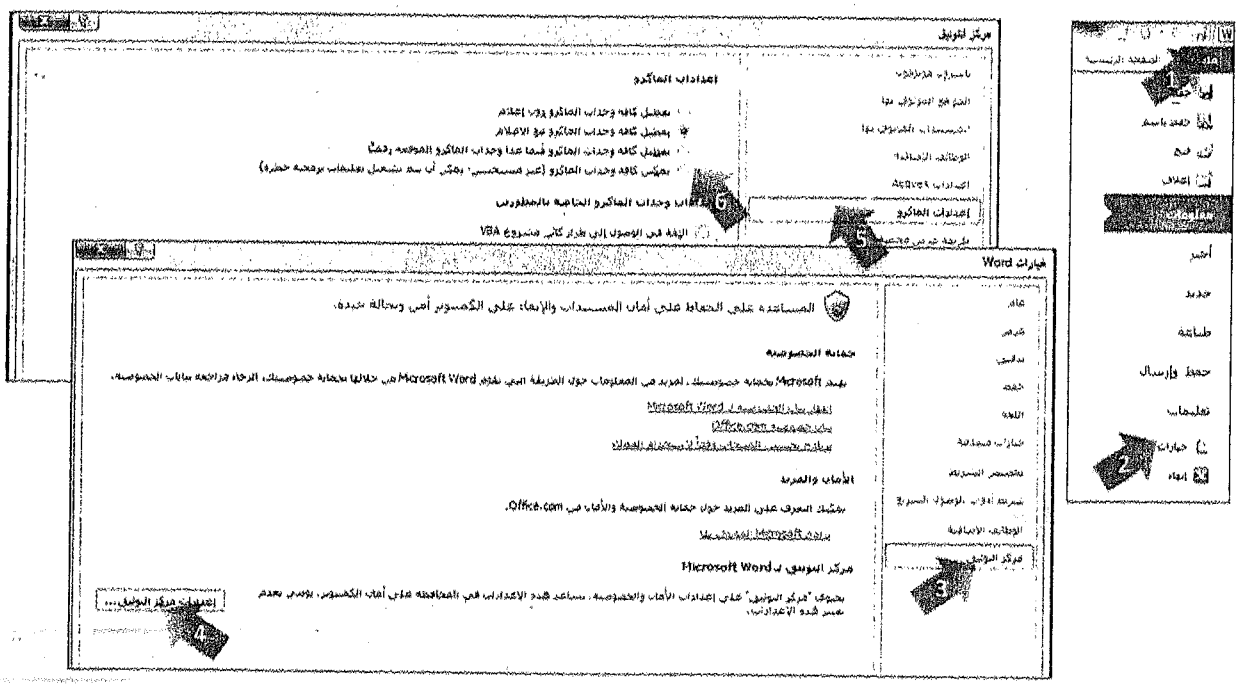
تنفذ وحدات الماكرو المهام التي يتكرر استخدامها بشكل تلقائي، وذلك لتوفير الوقت المستغرق في الضغط على لوحة المفاتيح، أو تحريك الفأرة. فالماكرو يسجل كل ما تقوم به باستخدام لوحة المفاتيح، أو ما تختاره من الشريط، ثم يقوم بإعادته تماما كما تم تسجيله، ولهذا من الضروري جدا الانتباه خلال عملية التسجيل؛ لأن معظم الأعمال التي تقوم به سوف يتضمنها الماكرو. وعندما يتم إنشاء ماكرو، يمكنك استخدامه في أي وقت، وعلى أي ملف يستخدم القالب نفسه الذي تم إنشاء الماكرو فيه.

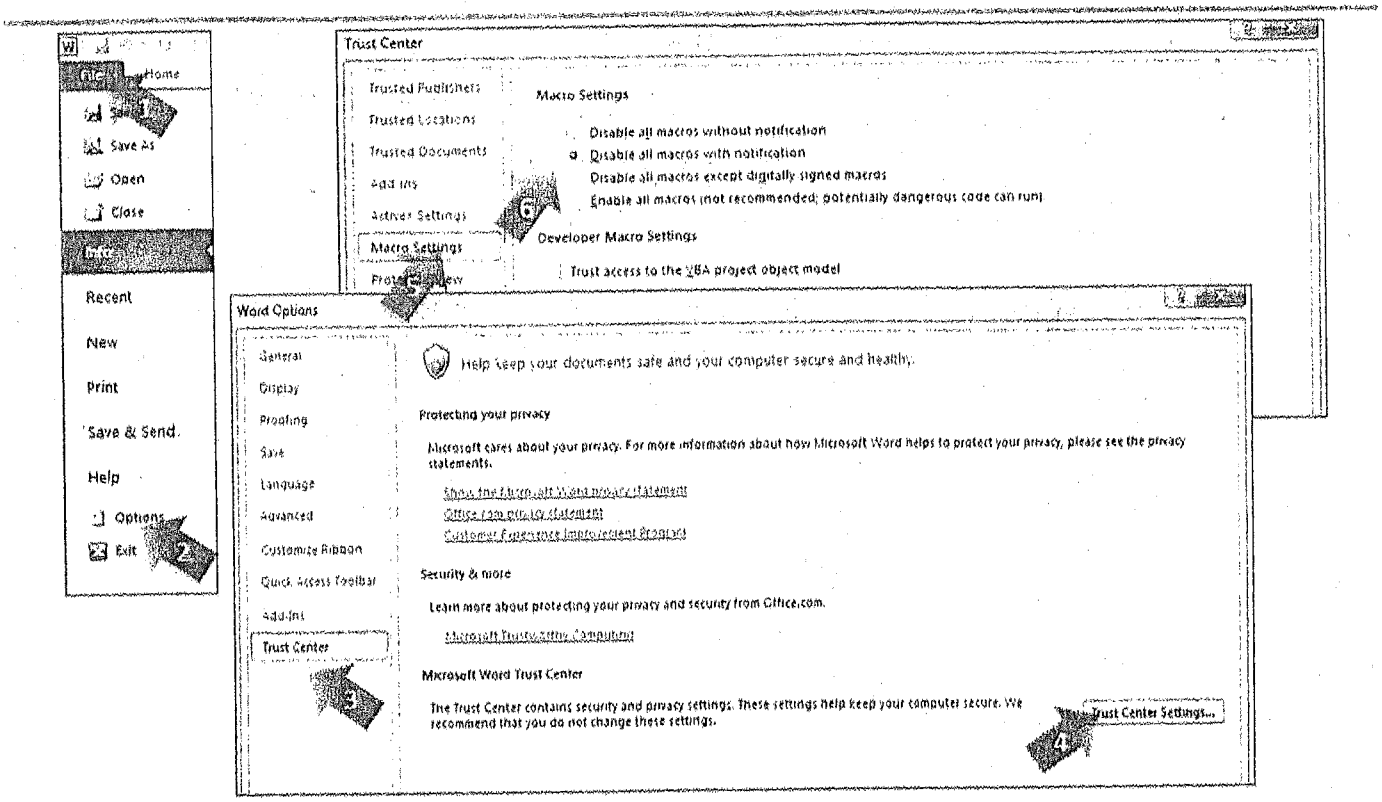
على الرغم من هذه الفائدة الكبيرة لوحدات الماكرو، فإن الفيروسات قد تختبئ في وحدات الماكرو، ولهذا السبب فإن بعض البرامج التطبيقية تمكنك من تمكين أو عدم تمكين وحدات الماكرو في الملفات الشخصية التي تنشئها باستخدام تلك البرامج:

- يؤدي تمكين وحدات الماكرو إلى تشغيل الماكرو، مع احتمالية إلحاق الضرر بالحاسوب، إذا كان مصدر الملف الذي يحتوي وحدات الماكرو جهة غير معروفة.
- أما تعطيل وحدات الماكرو فإنه وإن كان يؤدي إلى عدم تشغيل الماكرو، وما يمكن أن يحتويه من فيروسات، إلا أنه سيمنعك من استخدام كافة ميزات ذلك الملف.

وللتحكم بتمكين أو عدم تمكين وحدات الماكرو في مستندات Word 2010 مثلا، اتبع الخطوات الآتية:

1. افتح برنامج Word 2010.
2. ضمن علامة التبويب (ملف/ *File*)، انقر على زر (خيارات/ *Options*)، فيظهر مربع الحوار (خيارات Word/ *Word Options*).
3. انقر على فئة (مركز التوثيق/ *Trust Center*)، ومن الجهة المقابلة، انقر على زر (إعدادات مركز التوثيق/ *Trust Center Settings*)، فيظهر مربع الحوار (مركز التوثيق/ *Trust Center*).
4. انقر على فئة (إعدادات الماكرو/ *Macro Settings*)، إذا لزم الأمر. ومن الجهة المقابلة انقر على ما تراه مناسبا من إعدادات الماكرو.
5. انقر على زر (موافق/ *OK*) في كافة مربعات الحوار المفتوحة.
6. أغلق برنامج Word 2010.





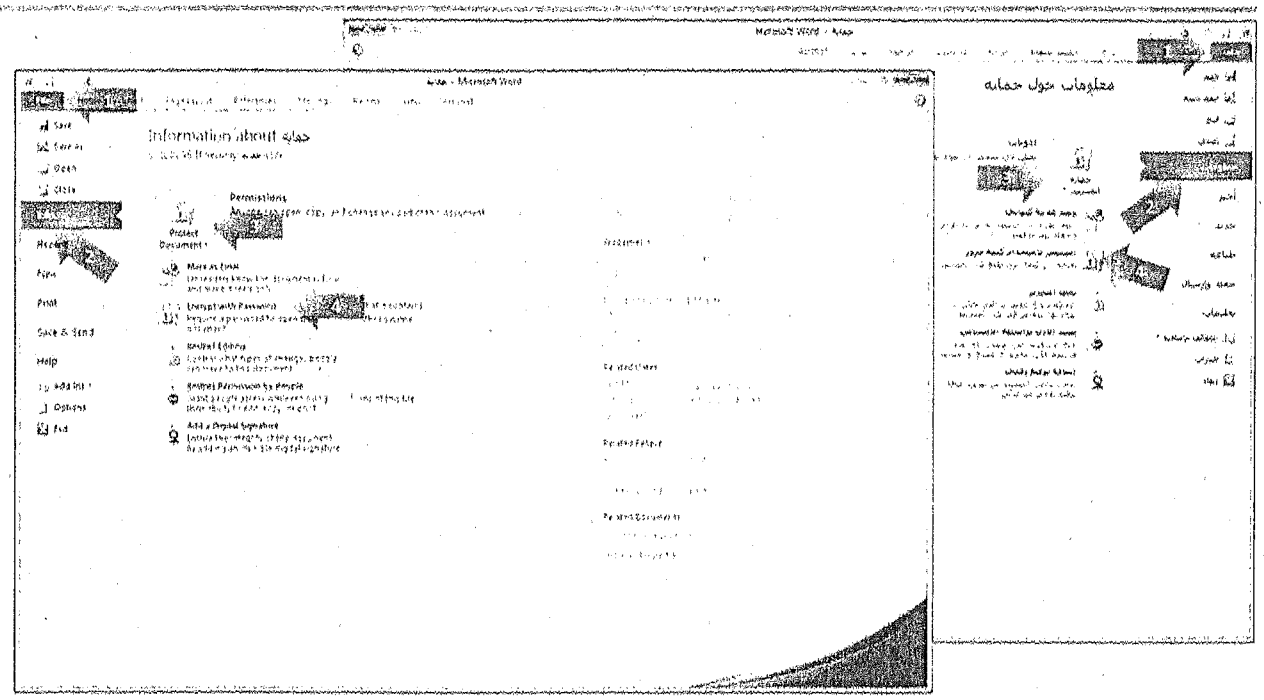

### 2.4.1 تعيين كلمة مرور للملفات Setting a password for files

إن تعيين كلمة مرور للملفات المختلفة وبخاصة تلك التي تتشاركها مع الأخرين يمنع أي وصول غير مصرح به للمعلومات الموجودة في تلك الملفات، ولكن من المهم أن تعي أن فقدانك أو نسيانك لكلمة المرور قد يتسبب في عدم قدرتك على فتح تلك الملفات، وفيما يأتي ستتعلم كيفية تعيين كلمة مرور لبعض أنواع الملفات الشائعة:

#### 1.2.4.1 تعيين كلمة مرور للمستندات Setting a password for documents

لتعيين كلمة المرور: P@12 لفتح المستند حماية.docx، اتبع الخطوات الآتية:

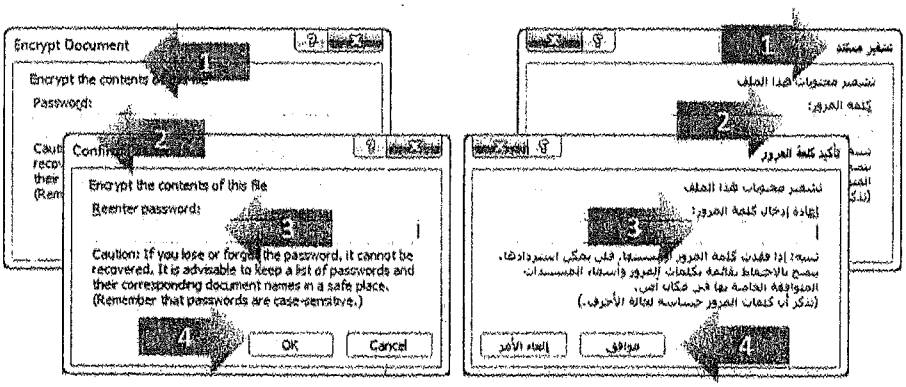
1. افتح المستند حماية.docx من مجلد ملفات العمل الخاص بك.
2. انقر على علامة التبويب (ملف/ *File*)، فيظهر المستند في طريقة العرض Backstage.
3. انقر على تبويب الفئة (معلومات/ *Info*).
4. انقر على زر (حماية المستند/ *Protect Document*)، فتظهر لائحة.




5. من اللائحة السابقة، انقر على (التشفير باستخدام كلمة مرور/ *Encrypt with Password*)، فيظهر مربع الحوار (تشفير مستند/ *Encrypt Document*).

6. في مربع (كلمة المرور/ *Password*)، اكتب P@12، دون إغفال حالة الأحرف؛ لأن كلمات المرور حساسة تجاه حالة الأحرف، ثم انقر على زر (موافق/ *OK*)، فيظهر مربع الحوار (تأكيد كلمة المرور/ *Confirm Password*).

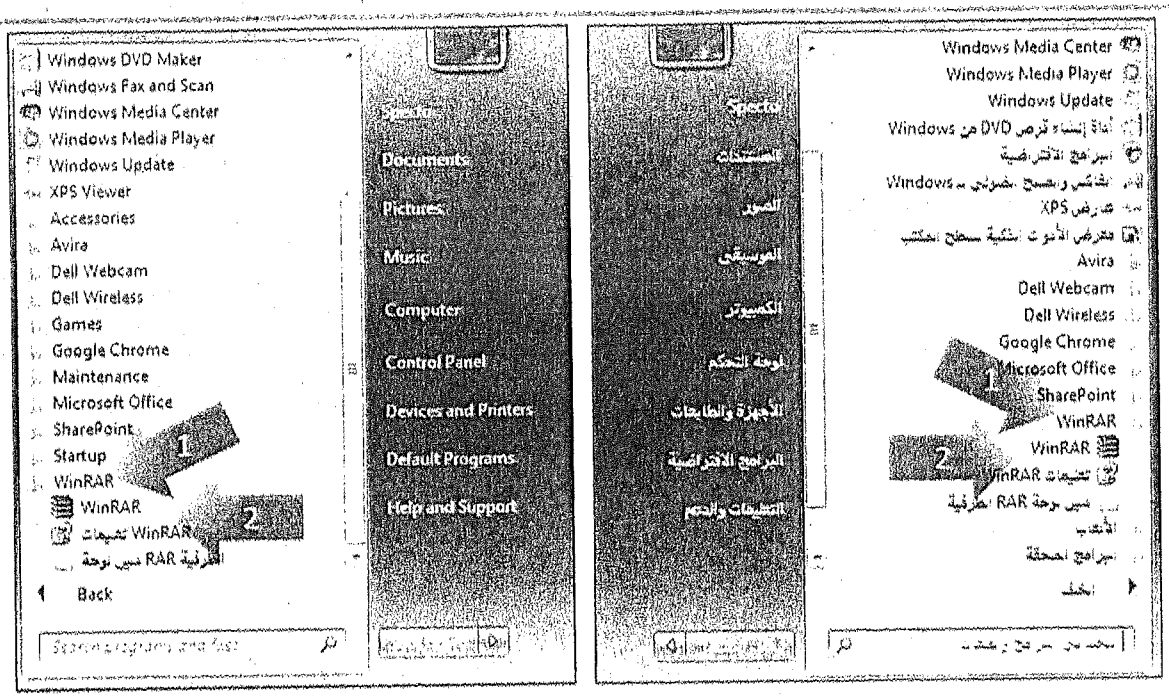
7. في مربع (إعادة إدخال كلمة المرور/ *Reenter password*)، أعد كتابة كلمة المرور P@12، ثم انقر على زر (موافق/ *OK*).

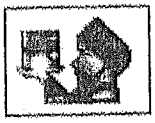



### 2.2.4.1 تعيين كلمة مرور للملفات المضغوطة Setting a password for compressed files

لتعيين كلمة المرور: #25*2% عند ضغط المستند (نصائح للحماية.docx)، اتبع الخطوات الآتية:

1. انقر على زر (ابدأ/ *Start*).
2. من اللائحة التي ستظهر، انقر على (كافة البرامج/ *All Programs*)، فتظهر لائحة بالبرامج المثبتة على الحاسوب.
3. انقر على مجلد Winrar، ثم انقر على برنامج التطبيق Winrar، فتفتح نافذة البرنامج.



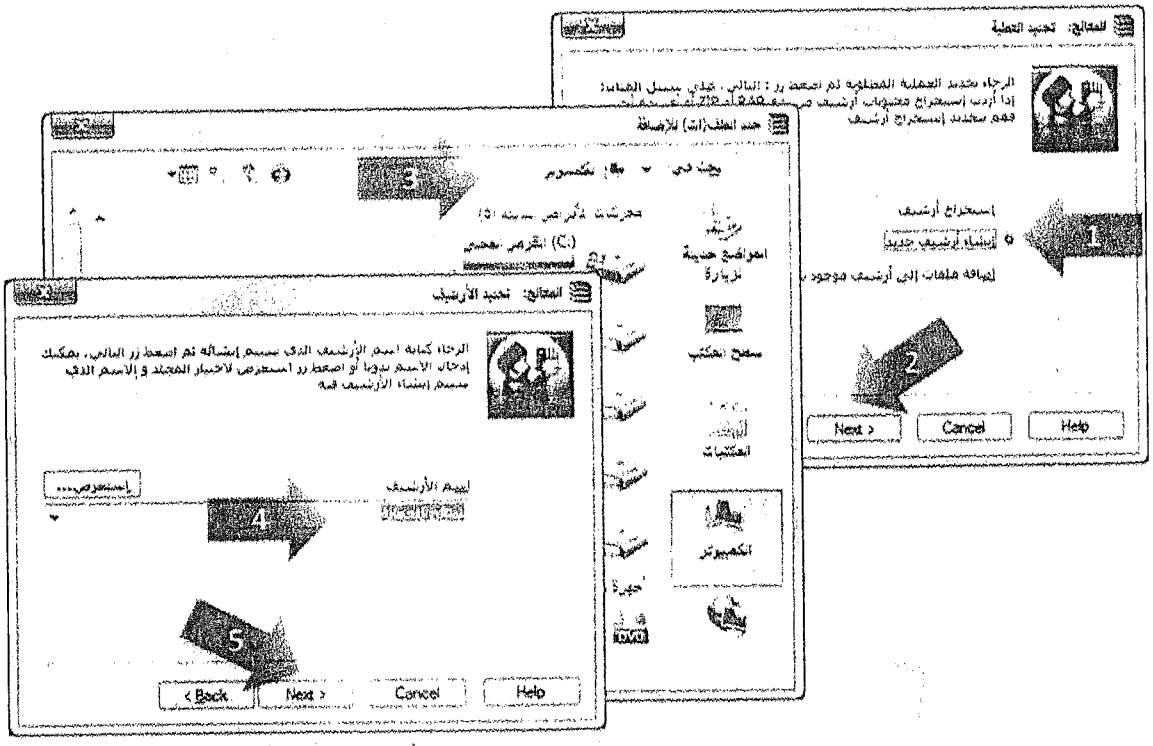



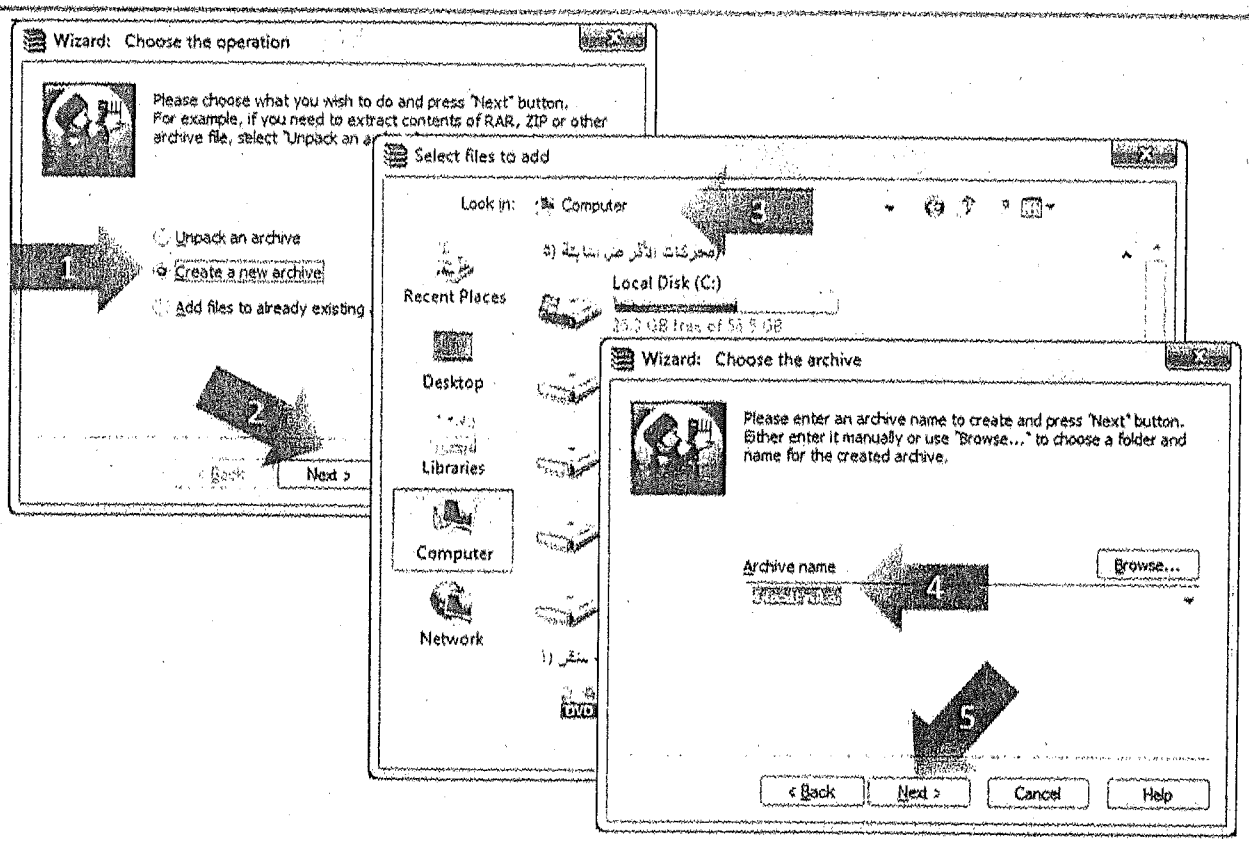
4. من شريط الأدوات، انقر على أيقونة (المعالج/ *Wizard*)، فتظهر نافذة (المعالج: تحديد العملية/ *Wizard: Choose the operation*).

5. انقر على زر (إنشاء أرشيف جديد/ *Create a new archive*)، ثم انقر على زر (التالي/ *Next*)، فتظهر نافذة (حدد الملف (ات) للإضافة/ *Select files to add*).

6. انتقل إلى مجلد ملفات العمل الخاص بك، ثم حدد المستند (نصائح للحماية.docx)، ثم انقر على زر (حسنا/ *OK*).

7. في مربع (اسم الأرشيف/ *Archive name*)، أبق الاسم الافتراضي كما هو، ثم انقر على زر (التالي/ *Next*).

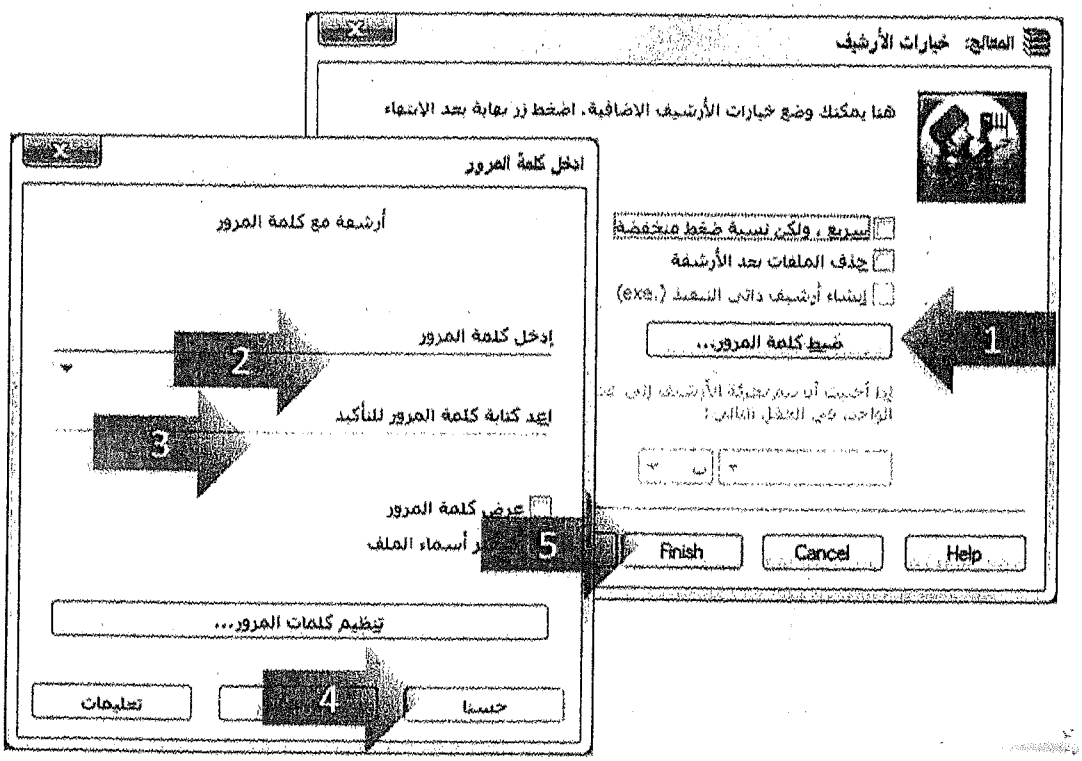


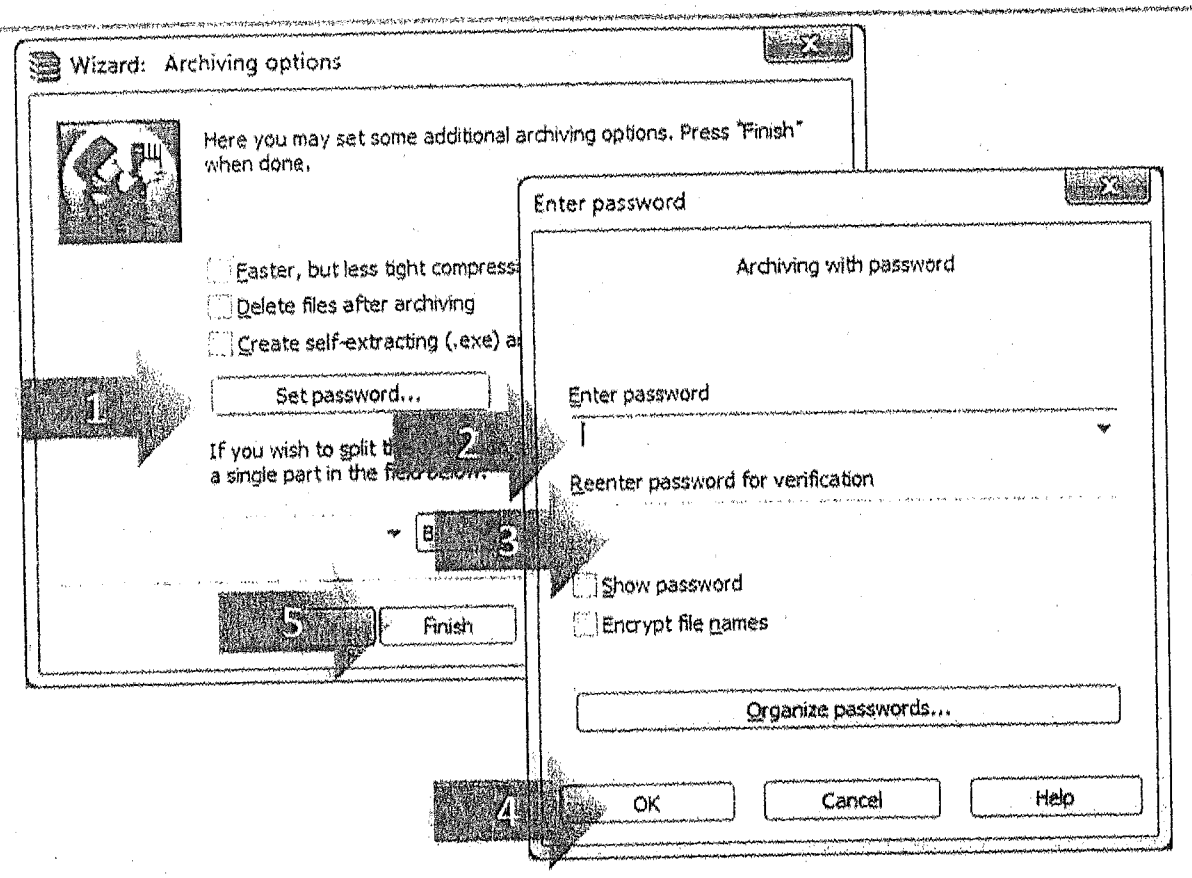



8. انقر على زر (ضبط كلمة المرور/ *Set password*)، فيظهر مربع الحوار (إدخال كلمة المرور/ *Enter password*).

9. في مربع (أدخل كلمة المرور/ *Enter password*)، اكتب #25*2%، ثم أعد كتابتها في مربع (أعد كتابة كلمة المرور للتأكيد/ *Reenter password for verification*)، ثم انقر على زر (حسنا/ *OK*).

10. انقر على زر (إنهاء/ *Finish*)، ثم أغلق نافذة البرنامج..





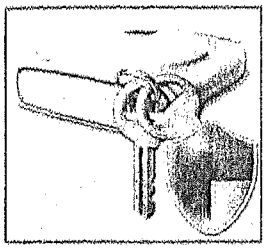

### 3.2.4.1 تعيين كلمة مرور للجداول الإلكترونية Setting a password for spreadsheets

لا يختلف تشفير المصنفات باستخدام كلمة مرور كثيرا عن تشفير المستندات، ولتعيين كلمة المرور: $علم7! لفتح المصنف أمان.xlsx، اتبع الخطوات الآتية:

1. افتح المصنف أمان.xlsx من مجلد ملفات العمل الخاص بك.
2. ضمن علامة التبويب (ملف/ *File*)، ومن الفئة (معلومات/ *Info*)، انقر على زر (حماية المصنف/ *Protect Workbook*)، فتظهر لائحة.
3. من اللائحة السابقة، انقر على (التشفير باستخدام كلمة مرور/ *Encrypt with Password*)، فيظهر مربع الحوار (تشفير مستند/ *Encrypt Document*).
4. في مربع (كلمة المرور/ *Password*)، اكتب $علم7!، ثم انقر على زر (موافق/ *OK*)، فيظهر مربع الحوار (تأكيد كلمة المرور/ *Confirm Password*).
5. في مربع (إعادة إدخال كلمة المرور/ *Reenter password*)، أعد كتابة كلمة المرور $علم7!، ثم انقر على زر (موافق/ *OK*).

## 3.4.1 إيجابيات وقيود التشفير The advantages and limitations of encryption

### 1.3.4.1 إيجابيات التشفير The advantages of encryption



ذكرنا أن التشفير يقوم على ترميز البيانات والمعلومات، وتحويلها إلى صيغة غير مفهومة، باستخدام مفاتيح عامة وخاصة، تستند إلى صيغ رياضية معقدة، وبالتالي فإن للتشفير إيجابيات عديدة، منها:

- لا يمكن قراءة البيانات التي تم تشفيرها دون مفتاح فك التشفير.
- المستقبل المصرح له هو وحده الذي يستطيع قراءة البيانات المشفرة.

### 2.3.4.1 قيود التشفير The limitations of encryption

يجب أن تكون على دراية بأن البيانات لا تزال عرضة للتهديدات ممن يملكون مفتاح فك التشفير، وإذا ضاع مفتاح التشفير، فإن البيانات لا يمكن قراءتها ولا استخدامها، لذا ينبغي تأمين مفتاح فك التشفير والمحافظة عليه.

**تمرين (1-4)**

اختر الإجابة الصحيحة من بين البدائل الأربعة المذكورة لكل سؤال مما يلي: *(انظر الإجابات في ملحق الإجابات ص 68).*

1. أي مما يلي يبين تأثير تعطيل وحدات الماكرو على ملف يتضمن وحدات ماكرو؟

أ- سيتم حذف الماكرو من الملف. ب- سيمنعك من استخدام كافة ميزات ذلك الملف.

ج- لا يمكن إرسال الماكرو بالبريد الإلكتروني. د- سيسمح لك باستخدام كافة ميزات ذلك الملف.

2. أي مما يلي يعد من القيود المؤثرة على التشفير؟

أ- يجب توفر الجدار الناري لتشفير ملف.

ب- البيانات لا تزال عرضة للتهديدات ممن يملكون مفتاح فك التشفير.

ج- لن يمكن نسخ البيانات احتياطيا.

د- لا يمكن إرسال بيانات مشفرة بالبريد الإلكتروني.

3. افتح مصنف المنتجات.xlsx الموجود في مجلد ملفات العمل، مستخدما كلمة المرور ICDL@s1 لفتح الملف.

4. قم بتعيين كلمة المرور H@n@N، لفتح المستند إرشادات.docx الموجود في مجلد ملفات العمل.

## 2 البرمجيات الخبيثة/الضارة Malware

### 1.2 التعريف والوظيفة Definition and Function

#### 1.1.2 مفهوم البرمجيات الخبيثة/الضارة The term: Malware

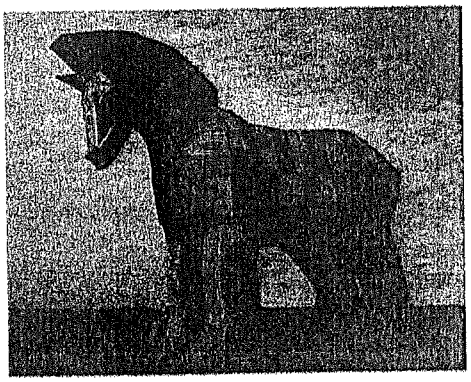
أخذت كلمة Malware من كلمة malicious، وتعني خبيث أو ماكر، ومن كلمة software، وتعني برمجيات، ولهذا يطلق عليها بالبرمجيات الخبيثة، وهي برامج ضارة يتم تصميمها لتثبيت نفسها في الحاسوب دون موافقة أو رضا مالك الحاسوب.

وما أن يتم تثبيت البرمجيات الخبيثة فإنه من الصعب إزالتها، ومن الممكن أن يتراوح أذاها من إزعاج بسيط كبعض النوافذ الإعلانية غير المرغوب بها إلى أذى غير قابل للإصلاح قد يتطلب إعادة تهيئة القرص الصلب.

#### 2.1.2 الطرق التي تختبئ وتختفي بها البرمجيات الخبيثة/الضارة Ways that malware can be concealed

تختفي البرمجيات الخبيثة قبل مهاجمة النظام بعدة طرق، وفيما يأتي أهم هذه الطرق:

- (أحصنة طروادة/ *Trojans*): برنامج تدميري يتنكر كبرنامج تطبيقي، فعندما يظن المستخدم أن هذا البرنامج مرغوب به، فيعمل على تنصيبه، دون أن يعلم ما الذي يقوم بعمله هذا البرنامج. وهذه هي التقنية التي يستخدمها حصان طروادة.



- (الأدوات الجذرية/ *Rootkits*): تستخدم لتمكين استمرار الوصول إلى الحاسوب بينما يخفي نشاطها وجودها، فبعد أن يتم تنصيب البرمجية الخبيثة على النظام يكون من الأفضل في العديد من الأحيان لكاتب البرمجية أن تبقى مخفية، والأمر ذاته صحيح عندما يخترق شخص ما حاسوبا بشكل مباشر. وهذه الأدوات الجذرية تؤمن هذا الإخفاء، وذلك عن طريق تعديل ملفات النظام المضيف بحيث يكون البرنامج الخبيث مخفيا عن المستخدم.

  علاوة على ذلك قد تقوم الأدوات الجذرية بمنع ظهور العملية الخاصة بالبرمجية الخبيثة في قائمة البرامج التي تعمل، أو منع ملفاتها من القراءة.

- (المداخل الخلفية/ *Back doors*): تستخدم لاختراق أمن النظام، فقد يقوم مبرمج أو مدير على وشك أن يطرد من عمله بترك مداخل خلفية للنظام تسمح له بالدخول إلى نظام صاحب العمل السابق وتخريب عمله.

**تمرين (2-1)**

اختر الإجابة الصحيحة من بين البدائل الأربعة المذكورة لكل سؤال مما يلي: *(انظر الإجابات في ملحق الإجابات ص 68).*

1. أي من أنواع البرامج الآتية يتم إنشاؤه وتوزيعه لأغراض ماكرة؟

أ- برامج مكافحة الفيروسات. ب- البرمجيات الخبيثة.

ج- الجدران النارية. د- برمجيات التشفير.

2. أي مما يلي يقوم بتثبيت نفسه على جهاز الحاسوب دون موافقة المالك مباشرة؟
أ- برامج مراقبة الوالدين. ب- برامج مكافحة الفيروسات.
ج- البرامج الخبيثة. د- برامج تصفية المحتوى.

3. ماذا يطلق على البرنامج التدميري الذي يتنكر كبرنامج تطبيقي مفيد؟
أ- الادعاءات الزائفة. ب- حصان طروادة. ج- المداخل الخلفية. د- البرمجيات الجذرية.

4. أي مما يأتي يمكن استخدامه لإخفاء البرامج الماكرة على جهاز الحاسوب؟
أ- تشغيل الجدار الناري. ب- قرصنة البطاقات الائتمانية.
ج- المقاييس البيومترية. د- البرمجيات الجذرية.

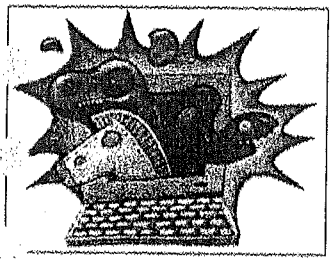
5. أي مما يلي يمكن أن يؤدي إلى وصول البرامج الخبيثة إلى جهاز الحاسوب؟
أ- تشغيل الجدار الناري. ب- تعطيل وحدات الماكرو في ملف.
ج- المداخل الخلفية. د- مسح محفوظات الاستعراض.

## 2.2 الأنواع Types

### 1.2.2 أنواع البرمجيات الخبيثة المعدية، وآلية عملها Types of infectious malware and how they work

البرمجيات الخبيثة المعدية أنواع، منها ما يأتي:

- (الفيروسات/ *viruses*): برامج حاسوبية يمكن أن تكرر نفسها، وتسبب أضرارا متفاوتة للحاسوب.
- (الديدان/ *worms*): برامج ماكرة ذاتية التكرار، تستخدم شبكة الحاسوب لإرسال نسخ من نفسها إلى الحواسيب الأخرى على الشبكة.



وقد عرفت هذه البرامج (الديدان والفيروسات) بهذه التسمية لا بسبب العمل المحدد الذي تقوم به، بل للطريقة التي تنتشر بها، فالفيروس يرتبط انتشاره بتنشيط برامج أخرى، بينما الدودة تقوم بنشر نفسها على الشبكة لتصيب الحواسيب الأخرى.

ويحدد البعض الفرق بين الفيروسات والديدان بأن الفيروس يتطلب تدخل المستخدم كي ينتشر، بينما الدودة تنتشر بشكل تلقائي. وهذا يعني أن العدوى المنتشرة بواسطة البريد الإلكتروني والتي تعتمد على فتح مستلم الرسالة الملف المرفق كي تقوم بإصابة النظام تصنف على أنها فيروسات.

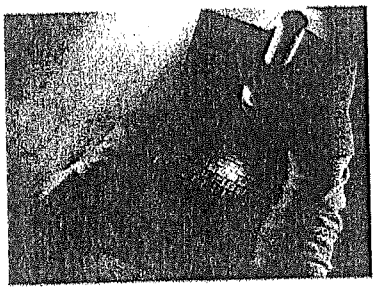
### 2.2.2 أنواع البرمجيات الخبيثة لسرقة البيانات، وتوليد الأرباح/الابتزاز، وآلية عملها Types of data theft, profit generating/extortion malware and how they work

خلال فترة الثمانينيات والتسعينيات كانت الفكرة عن البرامج الخبيثة أنها برمجيات تم إنشاؤها بهدف التخريب أو المزاح. وفي الآونة الأخيرة فإن معظم البرمجيات الخبيثة قد تمت كتابتها بدافع ربحي. يقصد منها كاتبو هذه البرامج السيطرة على الأنظمة المصابة، وتحويل هذه السيطرة لتعود عليهم بعائد مادي. ويتوافر العديد من هذه البرمجيات الخبيثة، وفيما يأتي أهم هذه الأنواع.

1. (برامج الدعاية/ *Adware*): حزمة برامج تقوم تلقائيا بأداء وعرض إعلانات غير مرغوب بها بهدف حصول د هذه الإعلانات (والذي هو منشئ البرنامج) على عائد إعلاني من جراء تكرار وصول المستخدمين الكبير إليها.

2. (برامج التجسس/ *Spyware*): برامج ماكرة تقوم بجمع معلومات عن عادات متصفح المستخدمين دون موافقتهم، وتعديل أداء متصفح الإنترنت ليفيد صانع البرمجية ماديا. وبعض برامج التجسس تعدل على شيفرة داعمي الإعلانات بحيث يصبح الدخل العائد لهم موجها إلى منشئ البرنامج الماكر.

3. (شبكات الروبوت/ *Botnets*): يمكن أن تصيب الحواسيب وتتحكم بها دون أخذ موافقة على ذلك، حيث تقوم هذه البرمجيات بتحويل جهازك إلى روبوت أو آلة يسهل التحكم بها عن بعد؛ لأنه في هذه الأنظمة تقوم البرمجية الخبيثة بالدخول إلى قناة (*Internet Relay Chat*) أو نظام دردشة آخر، ويستطيع المهاجم إعطاء تعليمات إلى جميع الأنظمة المصابة بنفس الوقت. ومن الممكن استخدام شبكات الروبوت لتحميل نسخة محدثة من البرمجية الخبيثة إلى النظام المصاب لتبقيهم عاصين على برنامج مكافحة الفيروسات أو أية مقاييس أمنية أخرى.



4. (تسجيل حركات لوحة المفاتيح/ *Keystroke logging*): تقوم على التقاط المعلومات التي يتم طباعتها باستخدام لوحة المفاتيح. حيث تقوم هذه البرمجيات بنسخ ضربات المستخدم على لوحة مفاتيح الحاسوب عند إدخاله كلمة سر أو رقم بطاقة ائتمانية أو أية معلومة مفيدة أخرى، ومن ثم يتم إرسالها إلى منشئ البرنامج تلقائيا، مما يمكنه من سرقة البطاقة الائتمانية وأي شكل آخر من السرقة. وبالطريقة نفسها يمكن للبرمجية نسخ مفتاح القرص الليزري أو كلمة سر للعبة على الإنترنت فتسمح له بسرقة حسابات أو أمور أخرى افتراضية.

5. (برامج الاتصال بالإنترنت/ *Diallers*): برامج ماكرة تثبت نفسها في الحاسوب، وتحاول الاتصال بخطوط هاتف مميزة في مواقع أخرى. حيث تقوم هذه البرمجيات بالتحكم بالمودم والقيام باتصالات مرتفعة الثمن، ومن ثم ترك الخط مفتوحا؛ مما يكلف المستخدم فواتير هاتف بمبالغ مالية كبيرة.

**تمرين (2-2)**

اختر الإجابة الصحيحة من بين البدائل الأربعة المذكورة لكل سؤال مما يلي: *(انظر الإجابات في ملحق الإجابات ص 68)*.

1. أي مما يلي هو نوع من البرمجيات الضارة التي تقوم بجمع معلومات عن عادات مستخدمي المتصفح دون موافقتهم؟
أ- برامج التجسس. ب- برامج الاتصال بالإنترنت. ج- أحصنة طروادة. د- برامج الدعاية.

2. أي مما يلي يمكن استخدامه لسرقة البيانات؟
أ- التقطيع/التكسير. ب- شبكات الروبوت. ج- إزالة المغناطيسية. د- المقاييس البيومترية.

3. أي مما يلي هو أفضل وصف لكيفية عمل الفيروس؟
أ- لا يتطلب الأمر عملا بشريا لتكرار الفيروس نفسه.
ب- يتطلب الأمر عملا بشريا لتكرار الفيروس نفسه.
ج- تنشئ مداخل خلفية في الحاسوب، بحيث تسمح للآخرين للوصول إلى الشبكة.
د- تنتشر الفيروسات عن طريق إرسال نسخة من نفسها إلى كافة جهات الاتصال الخاصة بك.

4. أي مما يلي هو أفضل وصف لبرامج التجسس؟
أ- هي برامج الاتصال بالإنترنت.
ب- هي البرمجيات التي تراقب أي نشاط مشبوه على جهاز الحاسوب وتنبه المستخدم.
ج- هي البرمجيات التي تراقب محاولات الدخول غير المصرح به.
د- هي نوع من البرمجيات الخبيثة التي تقوم بجمع معلومات عن عادات مستخدمي المتصفح دون موافقتهم.

5. أي مما يلي هو أفضل وصف لكيفية عمل برامج الدودة؟
أ- يتطلب الأمر عملا بشريا لتكرار الدودة نفسها.
ب- لا تتكاثر عن طريق إصابة الملفات الأخرى أو تكرار الذات.
ج- ذاتية التكرار.
د- تبدو وكأنها برامج مفيدة ولكن بمجرد تثبيتها فإنها تلحق الضرر بالحاسوب.

## 3.2 الحماية Protection

### 1.3.2 آلية عمل برامج مكافحة الفيروسات، ومحدداتها How anti-virus software works and its limitations

برنامج مكافحة الفيروسات هو برنامج يستخدم لمنع واكتشاف وإزالة البرمجيات الخبيثة على اختلاف أنواعها، ويقوم برنامج مكافحة الفيروسات بعملية الفحص للكشف عن الفيروسات ومنعها من الانتشار قبل أن تصيب النظام.

لكن هذه البرامج يجب أن تبقى محدثة باستمرار مع ملفات التعريف لأنها إذا لم تكن محدثة فلن تستطيع اكتشاف البرمجيات الخبيثة الجديدة. ومن القيود أيضا على برامج مكافحة الفيروسات أنها لا يمكنها إيقاف الهجوم على الخلل والثغرات الأمنية في النظام سواء في نظام التشغيل أم في البرامج التطبيقية المختلفة.

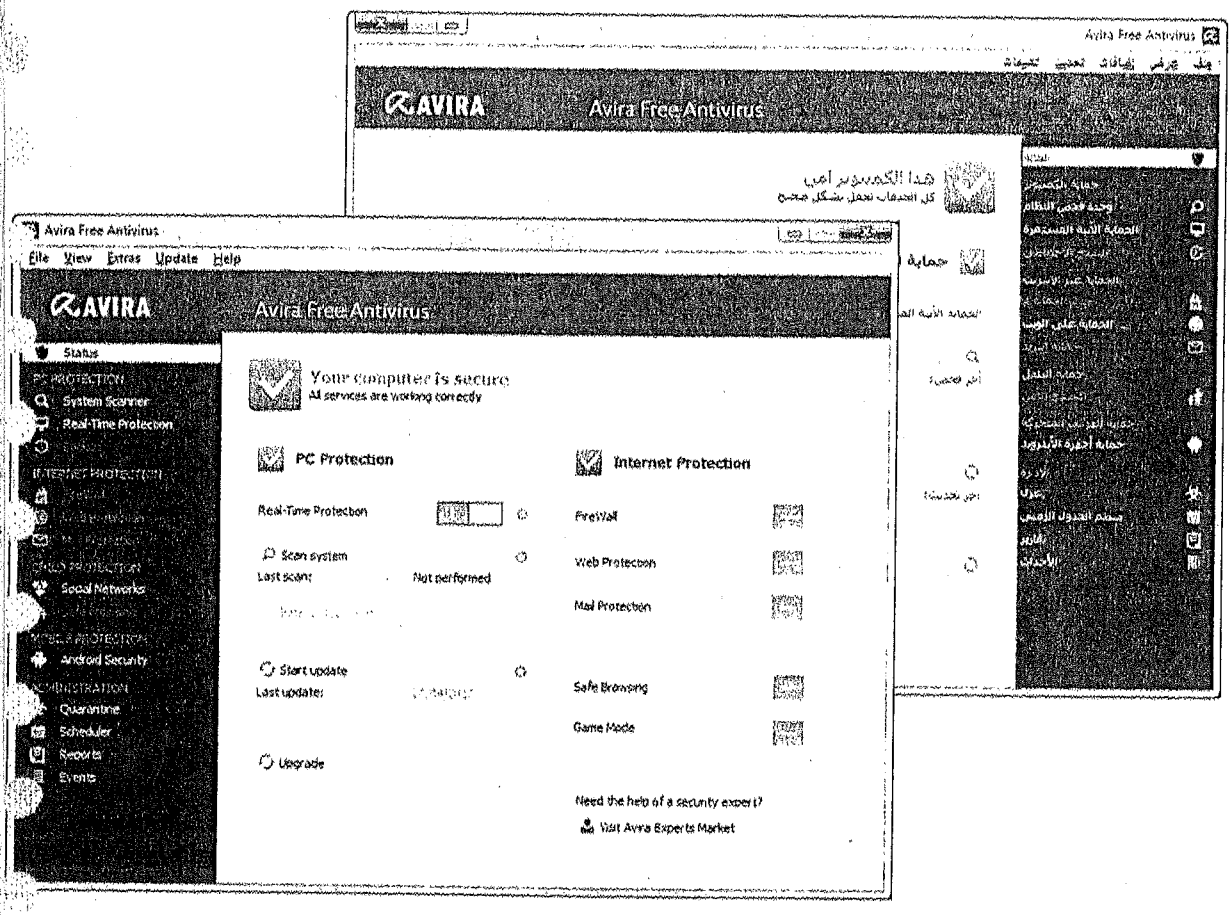
### 2.3.2 استخدام برنامج مكافحة الفيروسات Using anti-virus software

### 1.2.3.2 فحص محركات أقراص محددة من الفيروسات Scanning specific drives

هناك العديد من برامج مكافحة الفيروسات التي يمكنك استخدامها، لكننا في هذا الشرح سنستخدم برنامج Avira، لكنها كلها متشابهة في طريقة العمل.

ولفحص محتويات القرص الصلب من الفيروسات، اتبع الخطوات الآتية:

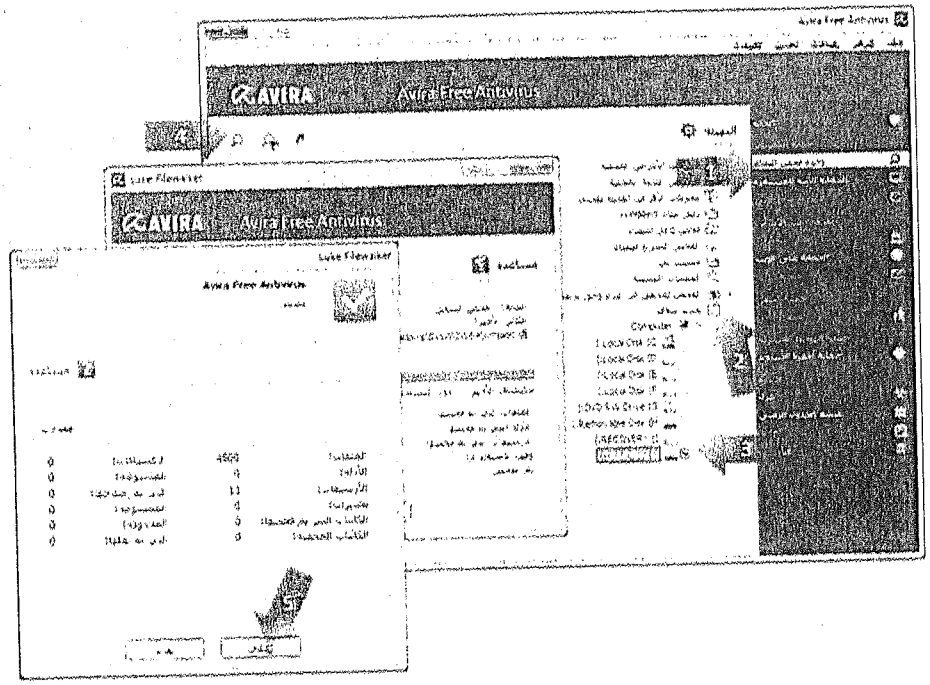
1. انقر نقرا مزدوجا على أيقونة برنامج *Avira* الموجودة في (منطقة الإعلام/ *Notification Area*)، فتفتح نافذة البرنامج.

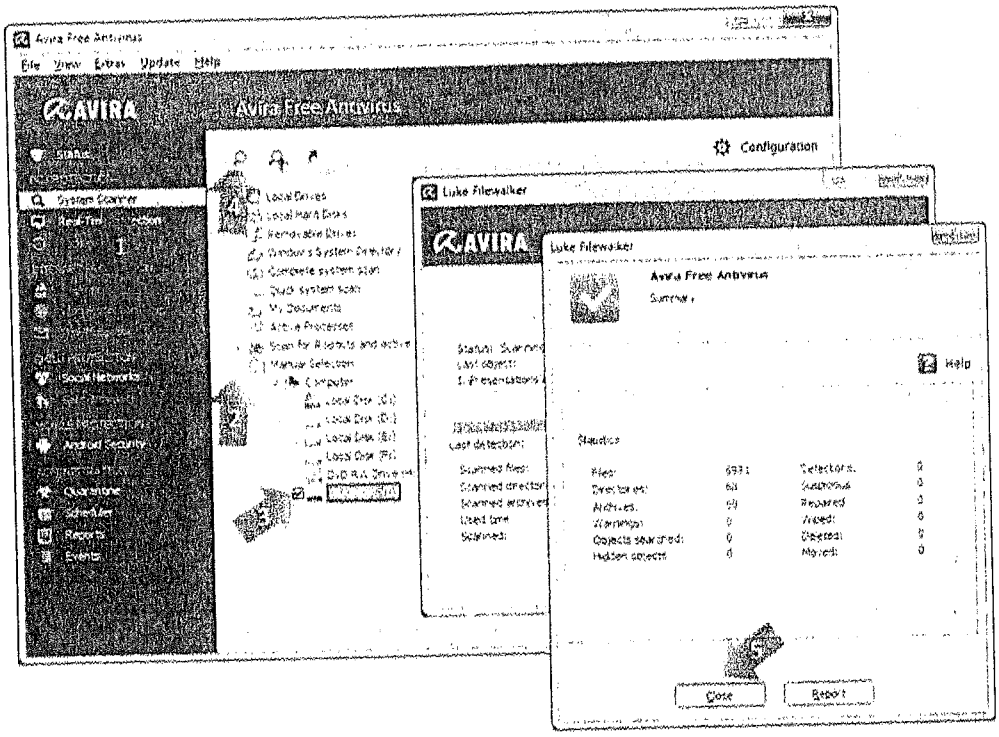



2. انقر على تبويب (وحدة فحص النظام/ *System Scanner*)، ثم انقر على (تحديد يدوي/ *Manual Selection*).
3. فعل مربع القرص الصلب المراد فحصه (*C:*، *D:*،...)، ثم انقر على زر (بدء الفحص / *Start scan*).

4. بعد الانتهاء من الفحص يظهر تقرير على النافذة الرئيسية للبرنامج يبين نتيجة الفحص والإجراء الذي تم اتخاذه

5. انقر على زر (إنهاء/ *End*). ثم انقر على زر (إغلاق/ *Close*).



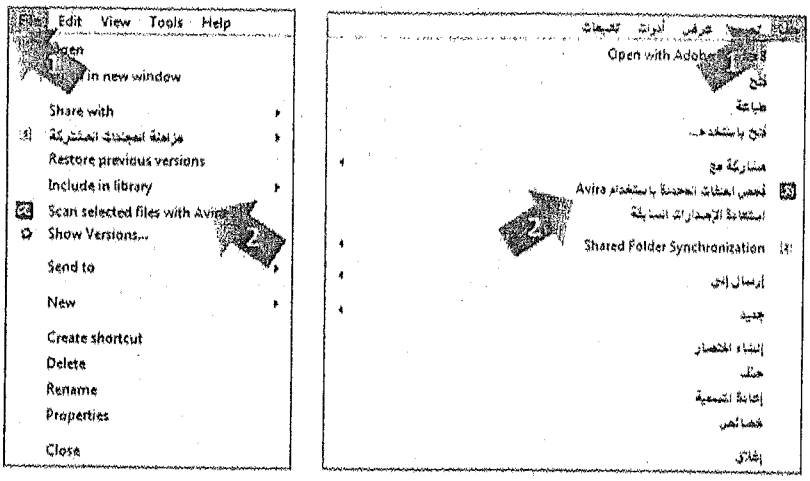

### 2.2.3.2 فحص مجلدات محددة من الفيروسات Scanning specific folders

لفحص محتويات مجلد ملفات العمل، اتبع الخطوات الآتية:

1. انتقل إلى القرص الذي يحتوي مجلد ملفات العمل، ثم حدد المجلد.

2. انقر على لائحة (ملف/ *File*)، واختر منها الأمر (فحص الملفات المحددة باستخدام Avira/ *Scan selected files with Avira*).

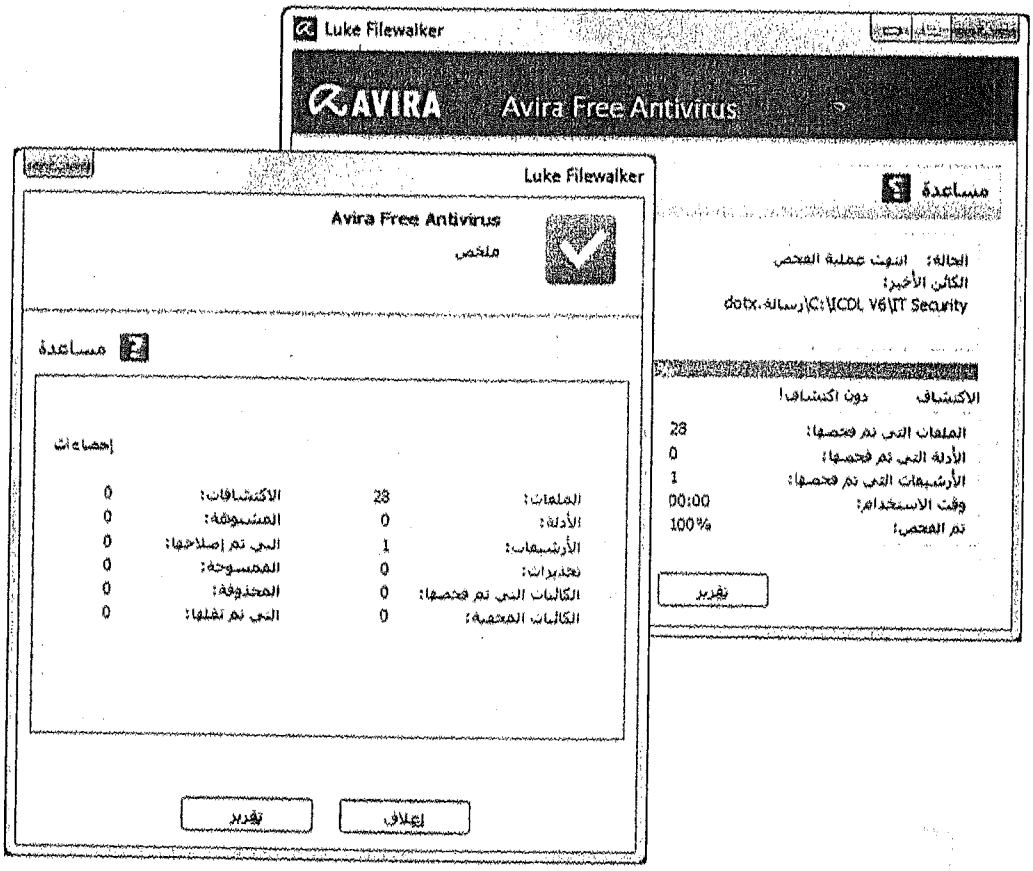
3. بعد الانتهاء من الفحص، انقر على زر (إنهاء/ *End*)، ثم انقر على زر (إغلاق/ *Close*).

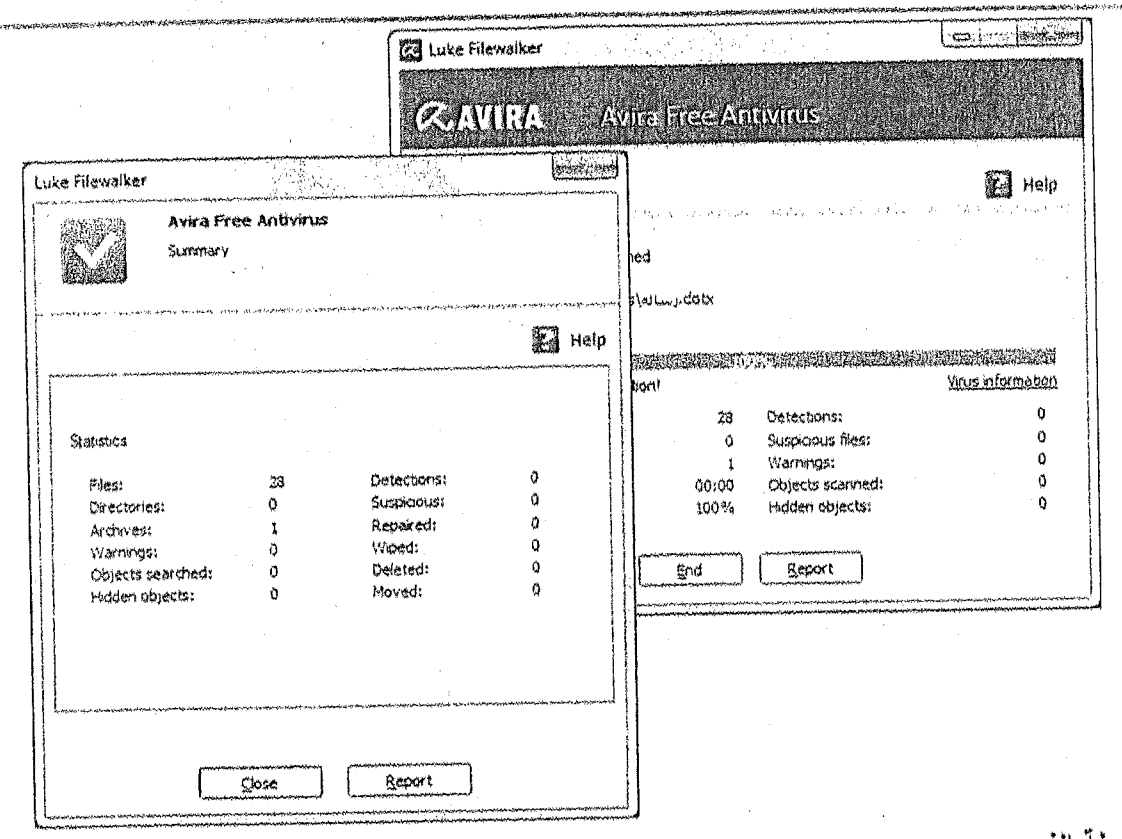



### 3.2.3.2 فحص ملفات محددة من الفيروسات Scanning specific files

لفحص الملف (رسالة.dotx) الموجود في مجلد ملفات العمل، اتبع الخطوات الآتية:

1. ضمن مجلد ملفات العمل، انقر بزر الفأرة الأيمن على الملف (رسالة.dotx)، فتظهر لائحة السياق.
2. من لائحة السياق، اختر (فحص الملفات المحددة باستخدام Avira/ *Scan selected files with Avira*).
3. بعد الانتهاء من الفحص، انقر على زر (إنهاء/ *End*)، ثم انقر على زر (إغلاق/ *Close*).

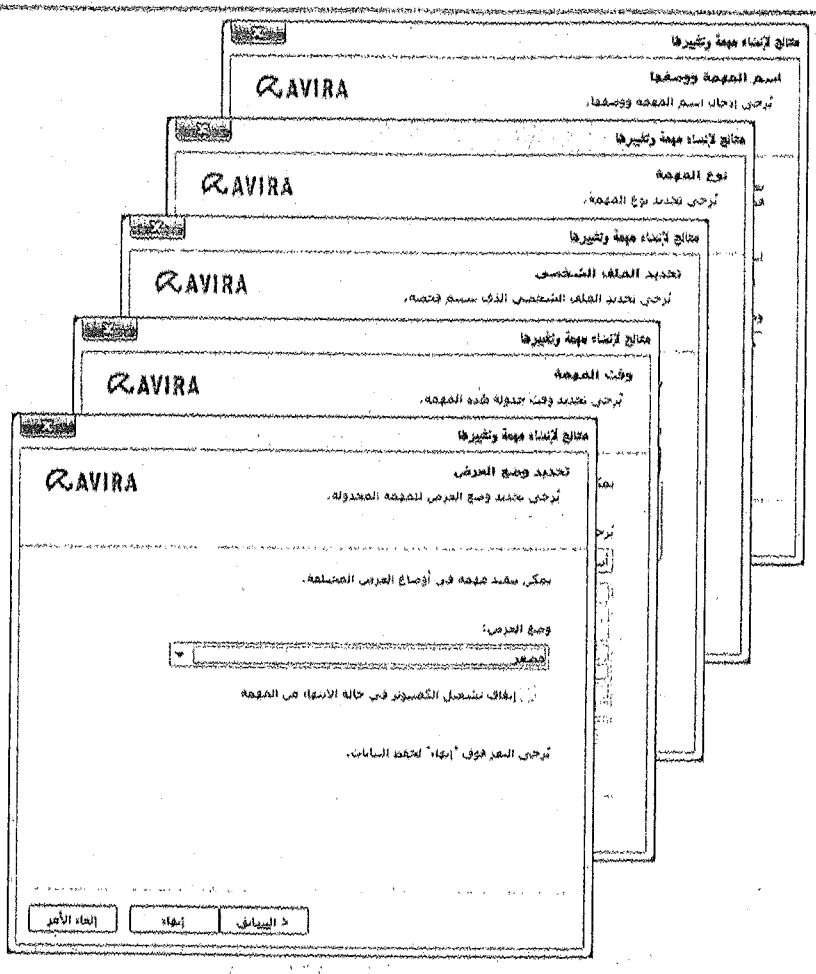





### 4.2.3.2 جدولة الفحص Schedule scans

لتحديد جدول زمني لعملية الفحص ضد الفيروسات، اتبع الخطوات الآتية:

1. انقر نقرا مزدوجا على أيقونة برنامج Avira الموجودة في (منطقة الإعلام/ *Notification Area*)، فتفتح نافذة البرنامج.
2. انقر على تبويب (منظم الجدول الزمني/ *Scheduler*)، ومن الجهة المقابلة انقر على زر (إضافة مهمة جديدة/ *Add new task*) +، فيظهر معالج لإنشاء المهمة وتغييرها.
3. في الخطوة الأولى، اكتب اسم المهمة ووصفها، ثم انقر على زر (التالي/ *Next*).
4. في الخطوة الثانية، حدد نوع المهمة، ثم انقر على زر (التالي/ *Next*).
5. في الخطوة الثالثة، حدد الملف الشخصي الذي سيتم فحصه، ثم انقر على زر (التالي/ *Next*).
6. في الخطوة الرابعة، حدد الجدول الزمني للمهمة، ثم انقر على زر (التالي/ *Next*).
7. في الخطوة الخامسة، حدد وضع العرض هل هو مصغر أم مكبر، ثم انقر على زر (إنهاء/ *Finish*).
8. أغلق برنامج Avira.




### 3.3.2 الحجر، وأثره على الملفات المصابة أو المشكوك بها The quarantine and its effect on infected/suspicious files

إذا تعرف برنامج الفحص على فيروس ما فإنه سيقوم عادة بتزويدك بإرشادات للتعامل مع الفيروس. إن اكثر الخيارات شيوعا هي: مسح، أو حذف، أو الحجر على الملفات المصابة بالفيروس. يمكنك إعداد أو تغيير برنامج الفحص وخيارات التخلص من الفيروسات المضبوطة في أي وقت.

لكن الذي يهمنا هنا معرفة أن حجر ملف يعني نقله إلى موقع آمن على محرك الأقراص، تتم إدارته من قبل برنامج مكافحة الفيروسات، ويكون فيها غير قادر على فعل أي شيء، ثم يمكنك حذف ذلك الملف، مع الحفاظ على إمكانية استعادة الملف من الحجر الأمني، إذا لزم الأمر.

وهنا ينبغي التأكيد على أنه في حال نقل ملف من ملفات النظام أو ملف برنامج معين إلى موقع الحجر الأمني، فإنه قد لا يعمل البرنامج المرتبط بذلك الملف بشكل مناسب.

### 4.3.2 أهمية تحميل وتثبيت تحديثات البرامج، وملفات تعريف مكافحة الفيروسات The importance of downloading and installing software updates, anti-virus definition files

إن تثبيت تحديثات برنامج مكافحة الفيروسات، وملفات التعريف الخاصة به، يمكن أن يصلح العيوب أو المخاطر الأمنية في التطبيق، بالإضافة إلى أن التحديث يقي من المخاطر الأمنية الجديدة.

لأنك إذا لم تقم بتحديث قاعدة بيانات برنامج مكافحة الفيروسات بعد تنصيبه فكأنك لم تقم بتنصيب مضاد الفيروسات أساسا, لأنه لن يستطيع حماية حاسوبك من الفيروسات المحتمل الإصابة بها أبدا؛ لذلك يجب عليك الاتصال عبر الإنترنت وتحميل التحديثات الضرورية والتي تحوي معلومات جديدة عن آخر الأخطار الأمنية الجديدة, وآخر الفيروسات والبرامج الخبيثة الجديدة

أيضا وطرق التعامل معها, وربما تحتوي أيضا على تحديث لتطبيق مكافحة الفيروسات نفسه لإصلاح خطأ ما أو لإضافة خدمة جديدة عليه.

**تمرين (2-3)**

اختر الإجابة الصحيحة من بين البدائل الأربعة المذكورة لكل سؤال مما يلي: *(انظر الإجابات في ملحق الإجابات ص 68).*

1. أي مما يلي ليست من ميزات برنامج مكافحة الفيروسات؟
   أ- يعزل الملفات المشبوهة ويحجر عليها. ب- يسمح بجدولة عمليات الفحص.
   ج- قد يمنع ميزات أمنية لتطبيقات أخرى. د- يفحص النظام من البرامج الخبيثة.

2. ماذا تسمى عملية عزل الملفات المصابة بالفيروسات كي لا تضر النظام؟
   أ- الاستعادة. ب- الحجر. ج- الحذف. التدمير.

3. أي مما يلي يعد سببا لتثبيت تحديثات البرامج؟
   أ- لحذف ملفات تعريف ارتباط الإنترنت. ب- لإصلاح الأخطاء أو المخاطر الأمنية في التطبيق.
   ج- لتمكين ميزة الحفظ التلقائي. د- لحذف محفوظات الاستعراض.

4. أي مما يلي يعد من إيجابيات برامج مكافحة الفيروسات؟
   أ- تحمي أنظمة الحاسوب من البرامج الخبيثة. ب- تقلل من الوقت الذي يقضيه الشخص على الانترنت.
   ج- تحمي النظام من القرصنة الأخلاقية. د- تكشف عن عيوب تسجيل البرامج.

5. أي من التالية تعتبر واحدة من القيود على برامج مكافحة الفيروسات؟
   أ- تحمي النظام من القرصنة الأخلاقية. ب- تتطلب تحديثات منتظمة.
   ج- لا تكشف عن عيوب تسجيل البرامج. د- تزيد من الوقت الذي يقضيه الشخص على الانترنت.

6. أي مما يلي يعد صحيحا فيما يتعلق بالملفات الموجودة في موقع الحجر الأمني الخاص ببرامج مكافحة الفيروسات؟
   أ- هي ملفات تحديث برنامج مكافحة الفيروسات. ب- يمكن استعادتها من الحجر إذا لزم الأمر.
   ج- هي ملفات تحديث البرامج التطبيقية. د- لا يمكن استعادتها من الحجر.

7. أي مما يلي يقلل من مخاطر البرمجيات الخبيثة؟
   أ- تمكين ميزة الحفظ التلقائي. ب- فتح ملف مرفق من مصدر غير معروف.
   ج- تحديث برنامج مكافحة الفيروسات. د- تمكين وحدات الماكرو في التطبيق.

8. قم بفحص مجلد ملفات العمل الخاص بك من الفيروسات.

## 3 أمن الشبكات Network Security

### 1.3 الشبكات Networks

### 1.1.3 مفهوم الشبكة، وأهم أنواعها The term: Network and common network types

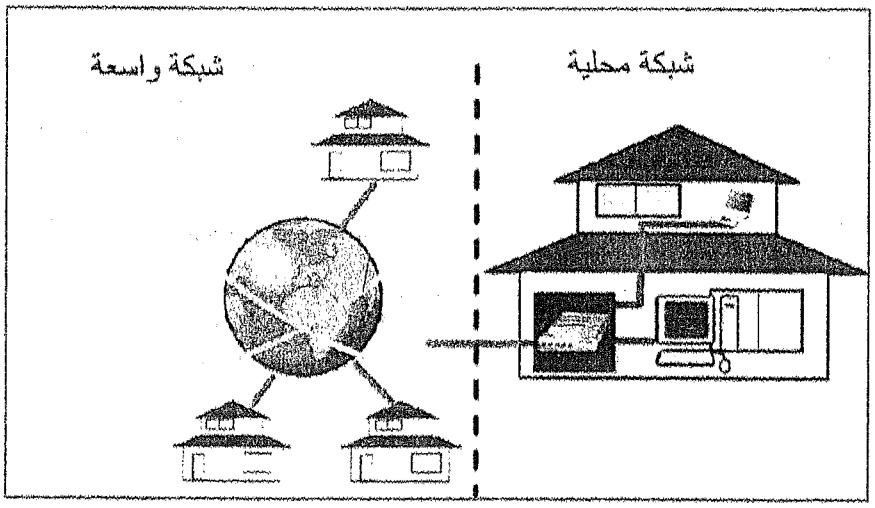
الشبكة هي مجموعة من أنظمة حاسوبين فأكثر، يتم ربطها معا بقنوات اتصال معينة؛ للسماح بمشاركة المصادر والمعلومات. وتقوم شبكات الحاسوب بنقل البيانات بين الأجهزة المرتبطة بالشبكة بغض النظر عن اختلاف أنواعها وأنظمة تشغيلها، وذلك من خلال أسلوب تخاطب موحد يدعى بروتوكول. وفيما يأتي أهم أنواع هذه الشبكات:

- (الشبكة المحلية/ *Local area network (LAN)*): الشبكة التي يتم فيها ربط الحواسيب المتجاورة، وعادة ما تكون في البناية نفسها كالمنزل والمكتب، وبذلك تعمل هذه الشبكة على تسهيل تبادل الملفات بين الأجهزة، وتوفر في الوقت المستغرق لنقل الملفات والمعلومات، كما أنها تتضمن عامل توفير اقتصادي في الشبكات حيث يمكن مشاركة الطابعة ونحوها.

ومن الأمثلة على هذا النوع من الشبكات شبكة الند للند التي تتميز كل الأجهزة المرتبطة بها بأنها متساوية ومتكافئة وبإمكان أي جهاز في الشبكة أن يكون خادما أو عميلا، وشبكة الخادم والعميل التي يكون فيها أحد الأجهزة خادما وباقي الأجهزة تكون عميلا يستفيد من الخدمات التي يتيحها جهاز الخادم.

- (الشبكة الواسعة/ *Wide area network (WAN)*): الشبكة التي يتم فيها ربط الحواسيب الموجودة في مسافات متباعدة، باستخدام خطوط الهاتف والأقمار الصناعية. وأفضل مثال عن الشبكات الواسعة هو شبكة الإنترنت وشبكة الصراف الآلي، وتستخدم الشبكات الواسعة لوصل الشبكات المحلية مع بعضها.

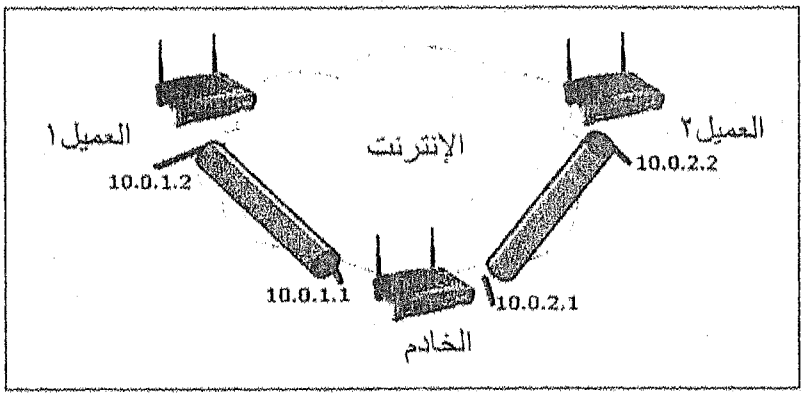
وتكمن فائدة الشبكات الواسعة في أنها تتيح نقلا آمنا وسريعا للمعلومات بين الأجهزة المختلفة، ناهيك عما يمتاز به نقل المعلومات عبر الشبكة الواسعة من موثوقية عالية، وانخفاض الكلفة. ولعل المنظمات والشركات الكبيرة - التي تنتشر فروعها في أرجاء العالم المختلفة - هي من يحقق الاستفادة الكبرى من الشبكات الواسعة؛ لأن هذه الشبكات تتيح لها الاتصال مع موظفيها وزبائنها وشركائها عبر العالم. وللشبكات الواسعة دور كبير في تشجيع وحفز الأعمال الإلكترونية (*e-business*) التي انتشرت في عصر الإنترنت.




- (الشبكة الافتراضية الخاصة/ *Virtual private network (VPN)*): الشبكة المحلية أو الواسعة التي تسمح للمستخدمين بتبادل المعلومات سرا بين مواقع متباعدة، أو بين مكان بعيد والشبكة المنزلية للأعمال التجارية. لا تستخدم هذه الشبكة الخاصة الافتراضية لربط المستخدمين المصرح لهم بشكل آمن مع شبكة عمل، للتواصل فيما بينهم، ولمشاركة البيانات.

وهي شبكة افتراضية لا وجود لها في الواقع والذي يحمل هذه الافتراضية إلى أرض الواقع هو الشبكة العنكبوتية والإنترنت التي تم توظيف خصائصها لتلائم سرية نقل البيانات والحفاظ على امن المعلومات.

وفي الشبكة الخاصة الافتراضية يتم توصيل حاسوبين أو شبكتين معا عن طريق شبكة الإنترنت، عبر مسار آمن (*Tunnel*) حيث يتم إنشاء هذا المسار بين جهازي الحاسوب مباشرة؛ ليتم نقل المعلومات وتبادلها بين الجهازين بشكل مشفر، ثم يقومان بفك التشفير عند استلام المعلومات من الطرف الأخر من النفق الافتراضي، بعد أن يبعد الجدار الناري أي اتصال غير مسموح به من الاتصالات التي يعينها مسبقا مدير النظام أو المسؤول عن الشبكة في الشركة أو فرعها.



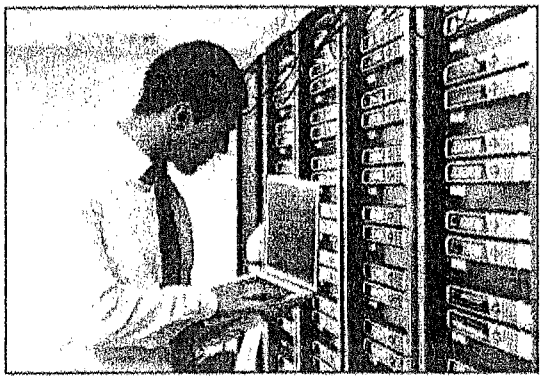

وقد ساهمت هذه الشبكة في تخفيض تكاليف نقل المعلومات الخاصة بالشركات والمؤسسات بين فروعها البعيدة عن المقر الرئيسي لها وبين المستخدم المنزلي الذي يريد الوصول إلى معلوماته المتوفرة في جهاز الحاسوب المنزلي.

وخلاصة القول إن الشبكة الخاصة الافتراضية مفيدة للمستخدمين الذين يتطلب عملهم السفر بشكل كبير، أو أولئك الذين يعملون في مكاتب نائية أو بعيدة. وتستخدم الشبكة الخاصة الافتراضية بنية تحتية عامة للاتصالات السلكية – عادة ما تكون الإنترنت – وذلك لتمكين المستخدمين المصرح لهم من الاتصال الآمن والفعال مع شبكة شركتهم، وهذا ما يعرف باسم " الاتصال الافتراضي"، ويتم تشفير البيانات المرسلة والمستقبلة في هذه الشبكة، فلا يمكن قراءتها من أي شخص يحاول التعرض لها.

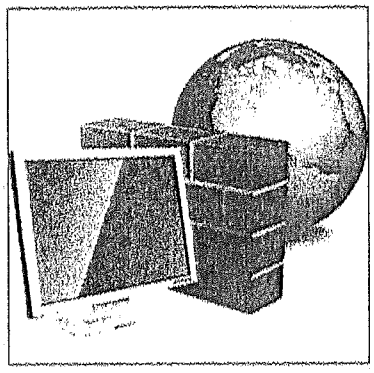
### 2.1.3 دور مسؤول الشبكة The role of the network administrator

يختلف الدور الحقيقي لمسؤول الشبكة من شركة إلى أخرى، لكنه في كل الأحوال سوف يشمل على أنشطة مختلفة، منها ما يأتي:

- إدارة كل من المصادقة والتوثيق، والإذن والتفويض، والمحاسبة، والتخطيط ضمن الشبكة.
- المهام المتعلقة بالمحافظة على وصول الموظفين إلى البيانات المطلوبة على الشبكة، فهو المسؤول عن تعيين عناوين بروتوكول الإنترنت للأجهزة المتصلة بالشبكات، وكذلك تأمين الشبكة لمنع اختراق النظام وغيرها.
- التأكد من تماشي استخدام الشبكة مع سياسة (تكنولوجيا المعلومات والاتصالات/ *ICT*)، وما يتطلبه ذلك من حضور المؤتمرات ذات الصلة.



### 3.1.3 الجدار الناري The firewall



الجدار الناري هو نظام أمان مصمم لحماية الشبكة من الأخطار الخارجية، وهو أحد البرامج أو الأجهزة التي تتولى فحص المعلومات الواردة من الإنترنت أو من إحدى الشبكات، ثم يقوم إما باستبعادها، أو يسمح لها بالمرور إلى الحاسوب، وذلك استنادا إلى إعدادات جدار الحماية. ويمكن لجدار الحماية أن يساعد في منع المتطفلين أو البرامج الضارة مثل الفيروسات المتنقلة من الوصول إلى الحاسوب من خلال إحدى الشبكات أو الإنترنت، كما أنه يساعد في إيقاف الحاسوب عن إرسال برامج ضارة إلى أجهزة الحاسوب الأخرى.

#### 1.3.1.3 وظيفة الجدار الناري The function of a firewall

تعمل الجدران النارية على تصفية وفلترة وفحص كل محاولات الدخول إلى الشبكة بحيث لا تسمح بالمرور إلا للاتصالات المسموح بها، وتمنع كل ما عدا ذلك، وبذلك فإن دور هذه الجدران النارية يشمل الآتي:

- حماية الشبكة من الاعتداء عليها من مصادر خارجية، وذلك بمنع عمليات الدخول غير المصرح بها إلى الشبكة.
- المحافظة على سلامة الحواسيب بتسجيل المعلومات التي تصل إليه من حواسيب أخرى.
- إعطاء المستخدم مزيدا من السيطرة على البيانات المخزنة في الحواسيب.

#### 2.3.1.3 قيود ومحددات الجدار الناري The limitations of a firewall

على الرغم من الدور الكبير الذي تقوم به الجدران النارية، إلا أن لها بعض القيود والمحددات الآتية التي ينبغي الانتباه إليها:

- لا يزودك دائما بإعلامات وتنبيهات تلقائية إذا تعرضت شبكتك للقرصنة.
- لا يحمي الشبكة من الهجوم عليها إذا صدر هذا الهجوم من داخل الشبكة نفسها.
- قد يمنع مرور اتصالات مشروعة وصحيحة.

**تمرين (3-1)**

اختر الإجابة الصحيحة من بين البدائل الأربعة المذكورة لكل سؤال مما يلي: *(انظر الإجابات في ملحق الإجابات ص 69).*

1. أي مما يلي يبين المقصود بالشبكة الخاصة الافتراضية (VPN)؟
   أ- لا تتطلب كلمة مرور للاتصال بالشبكة. ب- تسمح لأي شخص بالوصول إلى الشبكة.
   ج- شبكة حاسوب تغطي مساحة مادية صغيرة. د- توفر وصولا خاصا آمنا إلى الشبكة.

2. ماذا يطلق على شبكة الاتصال التي تستخدم في المنزل؟
   أ- شبكة المدينة MAN. ب- الشبكة المحلية LAN.
   ج- الشبكة الواسعة WAN. د- الشبكة الافتراضية الخاصة VPN.

3. الشبكة التي يتم فيها ربط الحواسيب الموجودة في مسافات متباعدة، باستخدام خطوط الهاتف والأقمار الصناعية تسمى:
   أ- شبكة المدينة MAN. ب- الشبكة المحلية LAN.
   ج- الشبكة الواسعة WAN. د- الشبكة الافتراضية الخاصة VPN.

4. أي مما يأتي هو أحد أنواع شبكة الاتصال التي تستخدم الانترنت لتوفير وصول آمن إلى شبكة مؤسسة ما؟
أ- شبكة المدينة MAN.
ب- الشبكة المحلية LAN.
ج- الشبكة الممتدة WAN.
د- الشبكة الافتراضية الخاصة VPN.

5. أي مما يلي ليس من المهام المنوطة بمسؤول الشبكة؟
أ- السماح للعامة أن يصلوا وأن يعدلوا جميع البيانات على الشبكة.
ب- ضمان أن جميع البيانات يمكن الوصول إليها من قبل الجهات المخولة بذلك.
ج- السماح لموظفين محددين بتعديل البيانات.
د- ضمان أن المستخدمين لديهم أذونات للوصول إلى المجلدات المطلوبة.

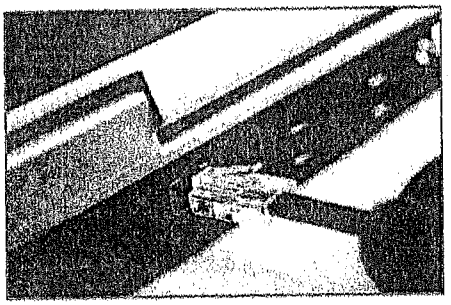
6. أي مما يلي هو أفضل وصف للشبكة المحلية؟
أ- شبكة من أجهزة حاسوب متصلة ببعض وتغطي منطقة جغرافية واسعة.
ب- شبكة من أجهزة حاسوب متصلة ببعض حول العالم.
ج- شبكة عامة تسمح بالاتصال الآمن بين الحواسيب.
د- عدد من أجهزة الحاسوب المرتبطة معا في الغرفة نفسها.

7. أي مما يلي يمنع الاتصالات غير المصرح بها من خارج الشبكة فيحميها من الاختراق؟
أ- برامج الاتصال بالإنترنت.
ب- الجدار الناري.
ج- ملفات تعريف ارتباط الإنترنت.
د- الشهادة الرقمية.

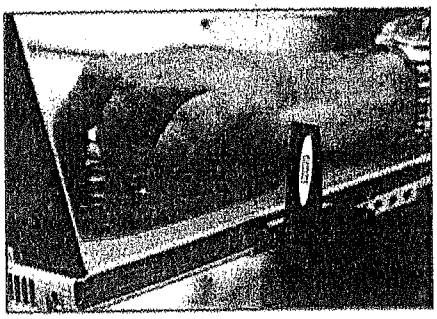
## 2.3 اتصالات الشبكة Network Connections

### 1.2.3 خيارات الاتصال بالشبكة The options for connecting to a network

يمكن تصنيف الشبكات حسب طرق الربط فيها إلى نوعين رئيسين:



- الربط (السلكي/ *Cable*): يقوم على الربط بالشبكة باستخدام أسلاك معدنية، وقد تكون هذه الأسلاك مجدولة/ملتوية، ويتكون من 8 أسلاك داخلية، وكل سلكين من الثمانية يكونان ملفوفين على بعضهما، وقد تكون الأسلاك محورية وهو الأقدم وتكون سرعته أقل من السلك المجدول، وقد يكون الربط السلكي من خلال خطوط الألياف البصرية، وهي ألياف مصنوعة من الزجاج النقي، تكون طويلة ورفيعة ولا يتعدى سمكها سمك الشعرة. يجمع العديد من هذه الألياف في حزم داخل الكيبلات البصرية، وتستخدم في نقل الإشارات الضوئية لمسافات بعيدة وبسرعات عالية.



- الربط (اللاسلكي/ *Wireless*): الربط الذي يسمح لك بالاتصال بالشبكة لاسلكيا دون الحاجة إلى أسلاك معدنية، وذلك باستخدام الأقمار الصناعية وإشارات الراديو والأشعة تحت الحمراء في الأجهزة.

### 2.2.3 الآثار الأمنية المترتبة على الاتصال بالشبكة How connecting to a network has implications for security

يترتب على الاتصال بالشبكة بعض المخاطر الأمنية، التي ينبغي الحذر منها والعمل على تفاديها، ومن هذه المخاطر ما يلي:

- يمكن للحواسيب المتصلة بالشبكة أن تكون مصابة بـ (البرامج الخبيثة الضارة/ *Malware*).
- الاتصال بالشبكة يمكن أن يفتح النظام إلى احتمالية (الوصول غير المصرح به للبيانات/ *Unauthorised data access*)
- الاتصال بالشبكة يمكن أن يزيد من التحدي المتعلق بـ (الحفاظ على الخصوصية/ *Maintaining privacy*).

**تمرين (3-2)**

اختر الإجابة الصحيحة من بين البدائل الأربعة المذكورة لكل سؤال مما يلي: *(انظر الإجابات في ملحق الإجابات ص 69)*.

1. لماذا تستخدم خطوط الألياف البصرية؟
أ- لربط الحاسوب بشبكة لاسلكية. ب- لربط الحاسوب بشبكة سلكية.
ج- لحماية العين من الإجهاد. د- لتحديد كمية الضوء الداخلة إلى العين.

2. أي مما يلي ليس سمة من سمات الشبكة اللاسلكية؟
أ- تستخدم الموجات الكهرومغناطيسية أو ترددات الراديو.
ب- يمكن استخدامها لمسافات طويلة.
ج- يمكن استخدامها لمسافات قصيرة.
د- هي أقل عرضة للتهديدات الأمنية من الشبكة السلكية.

3. أي مما يأتي ليس أحد الآثار الأمنية المحتملة المترتبة على الاتصال بالشبكة؟
أ- زيادة التحدي المتعلق بالحفاظ على الخصوصية.
ب- الوصول غير المصرح به إلى البيانات.
ج- أجهزة الحاسوب المتصلة بالشبكة قد تكون مصابة بالبرمجيات الضارة.
د- سوف تكون هناك حاجة إلى مداخل خلفية للوصول إلى الملفات على الشبكة.

## 3.3 أمن الشبكات اللاسلكية Wireless Security

### 1.3.3 أهمية حماية الشبكة اللاسلكية بكلمة مرور The importance of requiring a password for protecting wireless network access

إن طلب كلمة مرور في الشبكة يضمن لك أن المستخدمين المعتمدين والمصرح لهم فقط يمكنهم الوصول إلى الشبكة وإلى البيانات.

### 2.3.3 أنواع أمان الشبكات اللاسلكية Types of wireless security

يمكن للأشخاص الذين يستقبلون إشارة الشبكة عرض المعلومات الشخصية والملفات الموجودة على الشبكة اللاسلكية. يمكن أن يؤدي هذا إلى سرقة الهوية أو أفعال ضارة. يمكن أن يساعد مفتاح أمان الشبكة أو كلمة المرور في حماية الشبكة اللاسلكية الشخصية من هذا النوع من الوصول غير المصرح به. ويوجد أساليب عديدة لتشفير الشبكات اللاسلكية حاليا، منها ما يأتي:

#### 1.2.3.3 الوصول المحمي بالدقة اللاسلكية Wi-Fi Protected Access (WPA)

يتطلب WPA وWPA2 من المستخدمين توفير مفتاح أمان الشبكة حتى يتم الاتصال. بمجرد التحقق من صحة المفتاح، يتم إرسال كافة البيانات بين الحاسوب أو الجهاز وبين نقطة الوصول التي تم تشفيرها.

هناك نوعان من أنواع مصادقة WPA: WPA وWPA2. استخدم WPA2 إن أمكن، لأنه الأكثر أمانا. تدعم أغلب محولات الشبكة اللاسلكية الجديدة كلا من النوعين WPA وWPA2، لكن لا تدعمها المحولات القديمة. يعطى كل مستخدم نفس عبارة الوصول في كل من WPA-Personal وWPA2-Personal. لذا يعد هذا الوضع المستحسن للشبكات المنزلية. تم تصميم WPA-Enterprise وWPA2-Enterprise لاستخدامها مع خادم المصادقة x802.1، الذي يقوم بتوزيع المفاتيح المختلفة لكل مستخدم. لذا يستخدم هذا الوضع في الأساس في شبكات العمل.

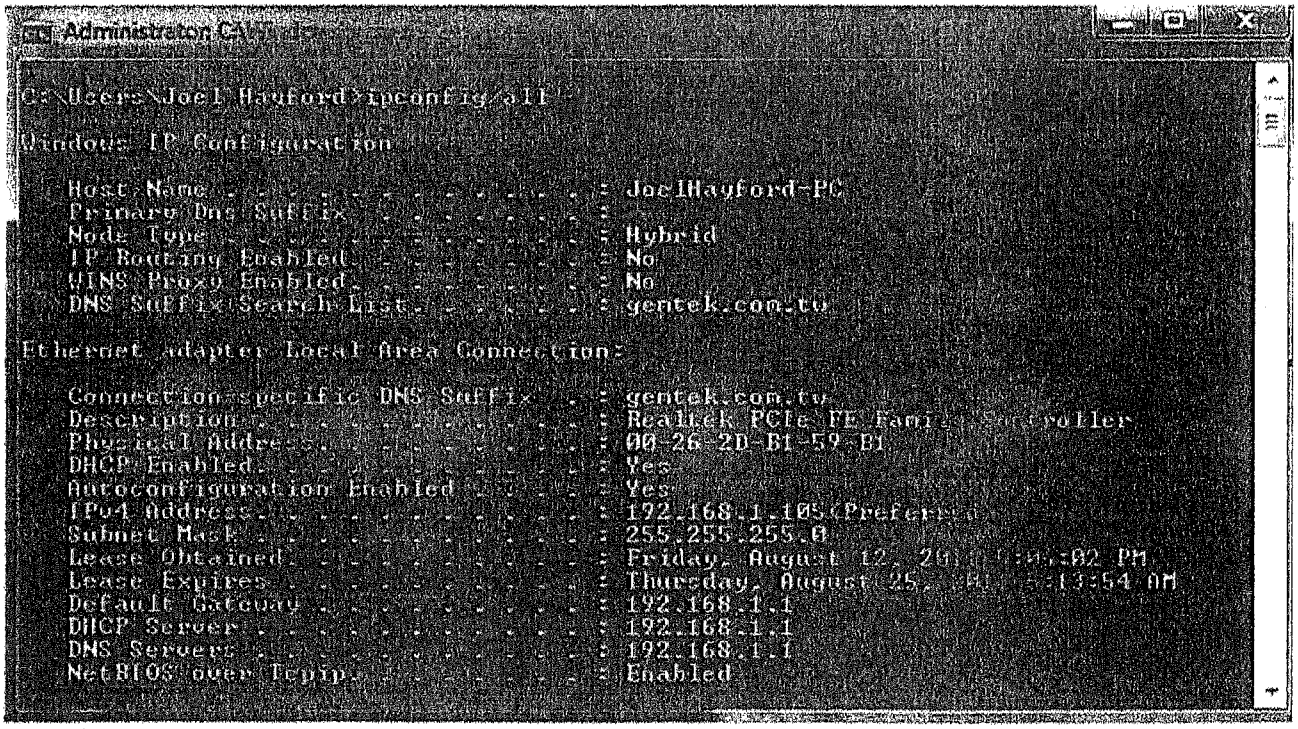
### 2.2.3.3 خوارزميات السرية المتكافئة Wired Equivalent Privacy (WEP)

هو نظام للحماية والتشفير للشبكات اللاسلكية من نوع IEEE 802.11، وهو أسلوب قديم لأمان الشبكة، ولا يزال هذا الأسلوب متوفرا لدعم الأجهزة القديمة، إلا أنه لم يعد مستحسنا. فعند تمكين WEP، ستقوم بإعداد مفتاح أمان الشبكة، ويعمل هذا المفتاح على تشفير المعلومات التي يقوم أحد أجهزة الحاسوب بإرسالها إلي حاسوب آخر عبر الشبكة. ومع ذلك، من السهل بشكل نسبي اختراق أمان WEP؛ حيث ان هذا النظام يستخدم مفتاح تشفير للبيانات التي تنتقل عبر موجات الراديو، والتي هي عرضة أصلا للتنصت والحصول على المعلومات.

### 3.2.3.3 التحكم بالوصول إلى الوسائط Media Access Control (MAC)

يفضل البعض أن يحدد الأجهزة التي تستطيع أن ترتبط بالشبكة اللاسلكية عن طريق تحديد عنوان للجهاز، يسمى هذا العنوان بعنوان ماك، وهو قيمة فريدة تربط ببطاقة شبكة من قبل المصنع للتمييز بين بطاقات الشبكة الموجودة على شبكة محلية. والمفروض أن يكون هذا العنوان مميزا وعالميا فلا توجد أي بطاقة شبكة أخرى في العالم تأخذ نفس عنوان الماك.

هناك فضاءات لصياغة عنوان الماك تدار من قبل الجمعية Institute of Electrical and Electronics Engineers (IEEE)، وبما أنه يحدد من قبل الشركة الصانعة فغالبا ما يتضمن رقم الشهادة المسجلة الخاص بهذه الشركة. وبما أنه يعمل في طبقة فيزيائية لذا يسمى أحيانا physical address.




لكل بطاقة شبكة عنوان ماك خاص بها يميزها عن غيرها، وبالتالي يمكنك اختيار مجموعة من عناوين الماك، بحيث لن يتمكن غيرها من الدخول إلى الشبكة، فمثلا إذا كنت تملك 3 حواسيب في البيت يمكنك إدخال عناوين الماك الخاصة بها ضمن قائمة الشبكات .

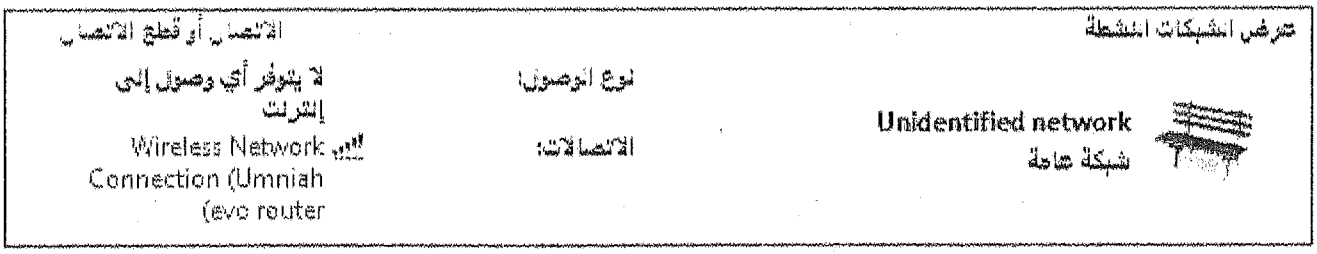
### 3.3.3 آثار استخدام شبكة لاسلكية غير محمية Implications of using an unprotected wireless network

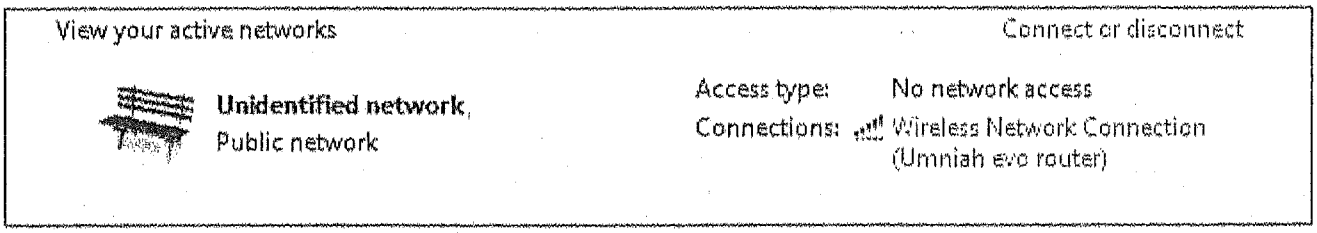
إن استخدام شبكة لاسلكية غير محمية يمكن أن يسمح للمتنصتين وغيرهم من المستخدمين غير المخولين من الوصول إلى بياناتك، وبالتالي استغلالها والإضرار بك.

### 4.3.3 الاتصال بشبكة لاسلكية Connecting to a wireless network

الشبكات اللاسلكية قد تكون شبكات محمية أو آمنة وذلك لمنع الوصول غير المصرح به إلى الشبكة، وقد تكون شبكات مفتوحة متاحة للجميع. ويوفر (مركز الشبكة والمشاركة/ *Network and Sharing Center*) معلومات عن حالة الشبكة، حيث يمكنك مشاهدة هل حاسوبك متصل بالشبكة المحلية أم بالإنترنت، وكذلك معرفة نوع الاتصال هل هو اتصال محمي آمن أم اتصال مفتوح، بالإضافة إلى مستوى الوصول المسموح لك مع الحواسيب أو الأجهزة الأخرى على الشبكة.

هذه المعلومات مفيدة جدا عندما تقوم بإعداد الشبكة الخاصة بك، أو عندما تواجهك مشاكل في التوصيل، وبإمكانك مشاهدة معلومات مفصلة بشكل أكبر حول شبكتك إذا نقرت على (عرض المخطط بالكامل/ *See full map*).




وهنا تجدر الإشارة إلى أنك قبل الاتصال بشبكة لاسلكية عامة كتلك الموجودة في المقاهي أو المطارات، قم بقراءة بيان الخصوصية بعناية وتأكد من أنك تعرف الملفات التي يتم حفظها على الحاسوب، ونوع المعلومات التي يجمعها مزود الشبكة من الحاسوب. لأنك إذا اتصلت بشبكة غير آمنة، فلتعلم أنه بإمكان شخص آخر يمتلك الأدوات المناسبة رؤية كل ما تفعله بما في ذلك مواقع ويب التي تزورها والمستندات التي تعمل فيها وأسماء المستخدمين وكلمات المرور التي تستخدمها. تأكد من أنك لا تستخدم أية معلومات حساسة خاصة بالشركة أو زيارة مناطق محمية بكلمة مرور على شبكة العمل أثناء الاتصال بهذه الشبكة.

وتظهر الشبكات اللاسلكية المتوفرة في قائمة الشبكات إذا كان الحاسوب يحتوي على محول شبكة لاسلكية، وبرنامج تشغيل تم تثبيته بشكل صحيح. وللاتصال بشبكة لاسلكية، اتبع الخطوات الآتية:

1. من شريط الإعلام، انقر على رمز الشبكة ، فتظهر قائمة بالشبكات المتوفرة.
2. انقر فوق إحدى الشبكات، فتظهر لائحة.
3. انقر على (اتصال/ *Connect*)، وإذا كانت الشبكة محمية فقد تتطلب مفتاح أمان للشبكة أو كلمة المرور، لذا اطلب من مسؤول الشبكة أو مزود الخدمة الحصول على مفتاح الأمان أو كلمة المرور.

وهنا تجدر الإشارة إلى أنه قد يتم إيقاف تشغيل بث الشبكة، وقد تحتاج إلى إضافة الشبكة يدويا. وللقيام بذلك اتبع الخطوات الآتية:

1. انقر على زر (ابدأ/ *Start*)، فتظهر لائحة، انقر منها على (لوحة التحكم/ *Control Panel*)، فتفتح نافذتها.

2. انقر على رابط (الشبكة وإنترنت/ *Network and Internet*)، ثم انقر على رابط (مركز الشبكة والمشاركة/ *Network and Sharing Center*)، فتفتح نافذته.

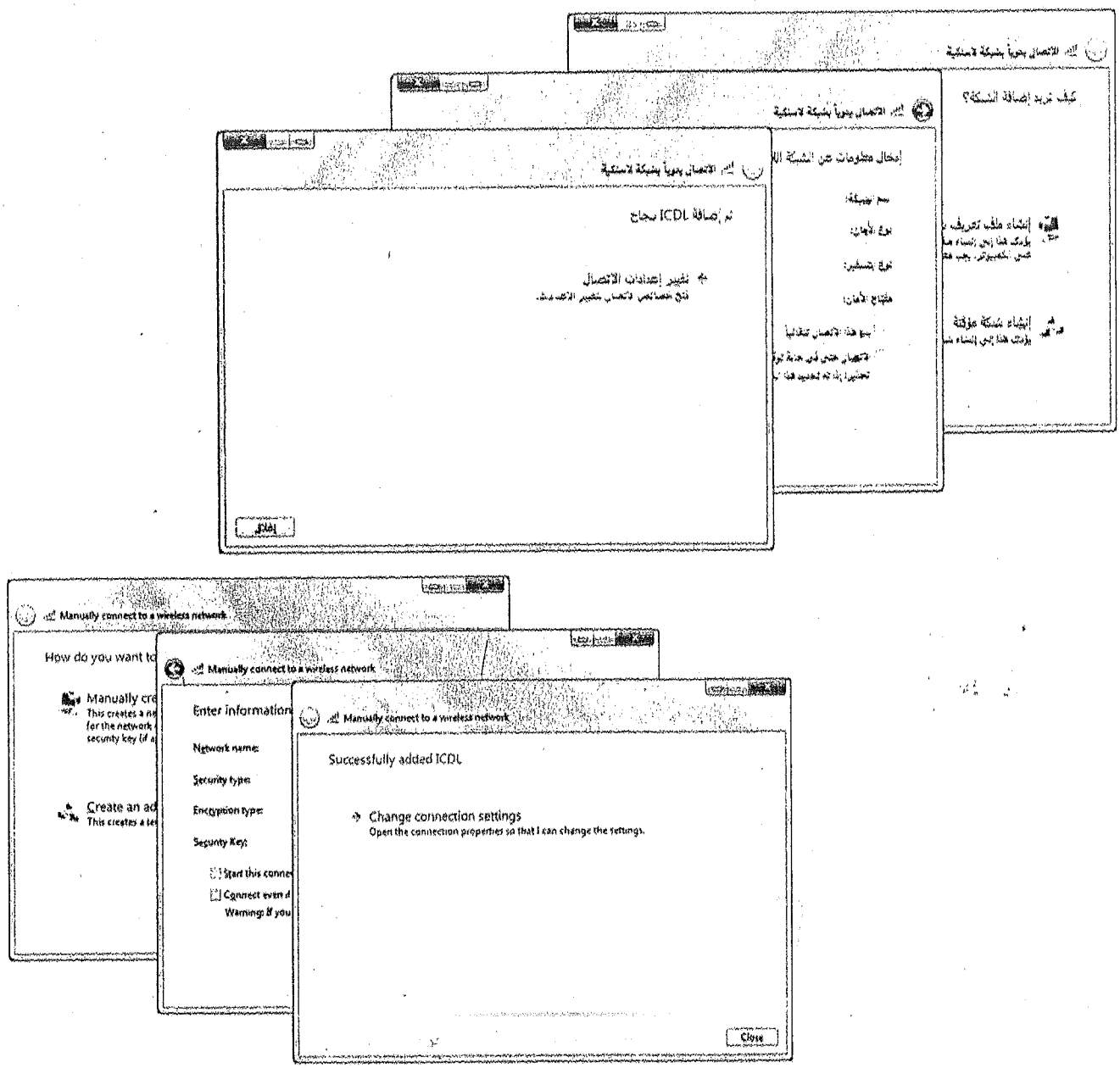
3. انقر على تبويب (إدارة الشبكات اللاسلكية/ *Manage wireless networks*).

4. من شريط الأدوات، انقر على زر (إضافة/ *Add*)، فيظهر معالج الاتصال يدويا بالشبكة اللاسلكية.

5. انقر على (إنشاء ملف تعريف شبكة يدويا/ *Manually create a network profile*)، ثم اكتب معلومات الشبكة.

6. إذا كنت ترغب في تعيين Windows للاتصال تلقائيا بهذه الشبكة عندما تكون داخل النطاق، فقم بتفعيل الاختيار (بدء هذا الاتصال تلقائيا/ *Start this connection automatically*). وإذا قمت بتفعيل الاختيار (الاتصال حتى في حالة توقف الشبكة عن البث/ *Connect even if the network is not broadcasting*) فقد تتعرض خصوصية حاسوبك إلى الخطر.

7. انقر على زر (التالي/ *Next*)، ثم انقر على زر (إغلاق/ *Close*)، فيتم إضافة الشبكة لقائمة الشبكات، وستكون متوفرة للاتصال بها عند وجود الحاسوب داخل نطاق الشبكة.



**تمرين (3-3)**

اختر الإجابة الصحيحة من بين البدائل الأربعة المذكورة لكل سؤال مما يلي: *(انظر الإجابات في ملحق الإجابات ص 69).*

1. أي مما يأتي يقيد الوصول إلى الشبكة اللاسلكية فلا يسمح إلا للمستخدمين المصرح لهم فقط؟
أ- استخدام سجل تسجيل. ب- استخدام كلمات مرور.
ج- تمكين الحفظ التلقائي لنماذج الويب. د- تثبيت برامج مكافحة الفيروسات.

2. أي مما يلي هو أحد أنواع الأمن اللاسلكي؟
أ- الشبكة الممتدة WAN. ب- الشبكة المحلية LAN.
ج- الوصول المتخفي باستخدام المداخل الخلفية. د- الوصول المحمي بالدقة اللاسلكية WPA.

3. أي مما يلي يمكن أن يسمح بالوصول غير المصرح به للبيانات؟
أ- تشفير البيانات. ب- نظام مراقبة الوصول باستخدام المقاييس البيومترية.
ج- الشهادات الرقمية. د- التنصت اللاسلكي من الأطراف غير المصرح لهم.

4. أي مما يلي صحيح عند الاتصال بشبكة لاسلكية محمية؟
أ- سوف تحتاج إلى كلمة المرور للوصول إلى الشبكة. ب- انعدام التعرض إلى البرامج الضارة.
ج- يتم تشفير البيانات بشكل تلقائي. د- يتم تنشيط برنامج تصفية الإنترنت تلقائيا.

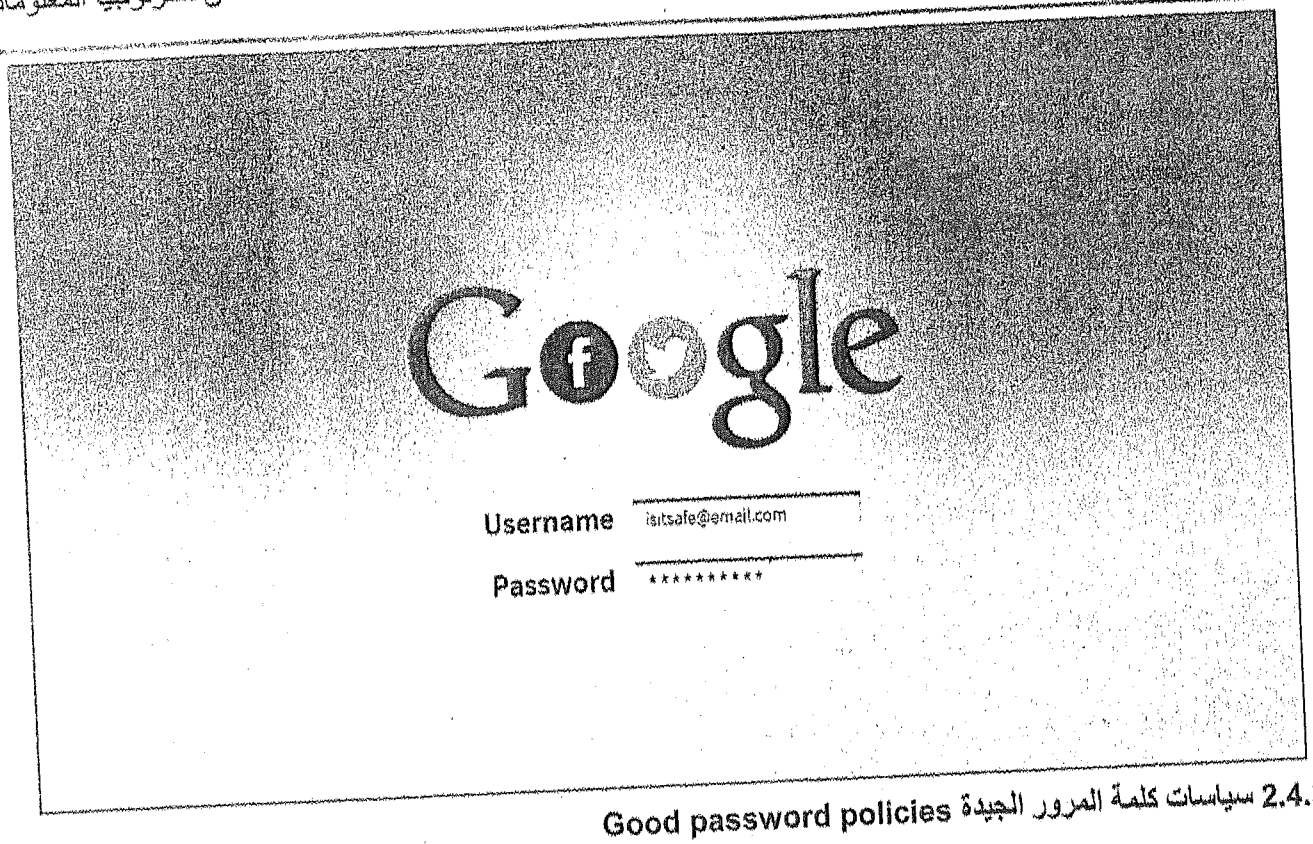
5. أي مما يلي يعد صحيحا عند الاتصال بشبكة لاسلكية غير محمية؟
أ- سيتمكن المستخدمون غير المصرح لهم من الوصول إلى ملفات تعريف ارتباط الإنترنت المخزنة في المتصفح.
ب- سيطلب من المستخدمين غير المصرح لهم إدخال كلمة مرور تستخدم لمرة واحدة كي يتمكنوا من الوصول إلى الشبكة.
ج- جميع المعاملات المالية التي تتم عبر الشبكة سوف تكون آمنة.
د- يجب فك تشفير كل الملفات قبل نشرها على الشبكة.

6. أي مما يلي يساعد على حماية الشبكة اللاسلكية؟
أ- تعيين كلمة مرور. ب- الشهادة الرقمية. ج- ملفات تعريف الارتباط. د- وحدات الماكرو.

## 4.3 التحكم بالوصول Access Control

### 1.4.3 الهدف من حساب الشبكة The purpose of a network account

لأسباب أمنية ينبغي إنشاء حساب على الشبكة، بحيث يتطلب الدخول إلى هذا الحساب (اسم مستخدم/ *User Name*) و(كلمة المرور/ *Password*)، وذلك لحماية الشبكة من الوصول غير المعتمد ولا المصرح به.




### 2.4.3 سياسات كلمة المرور الجيدة Good password policies

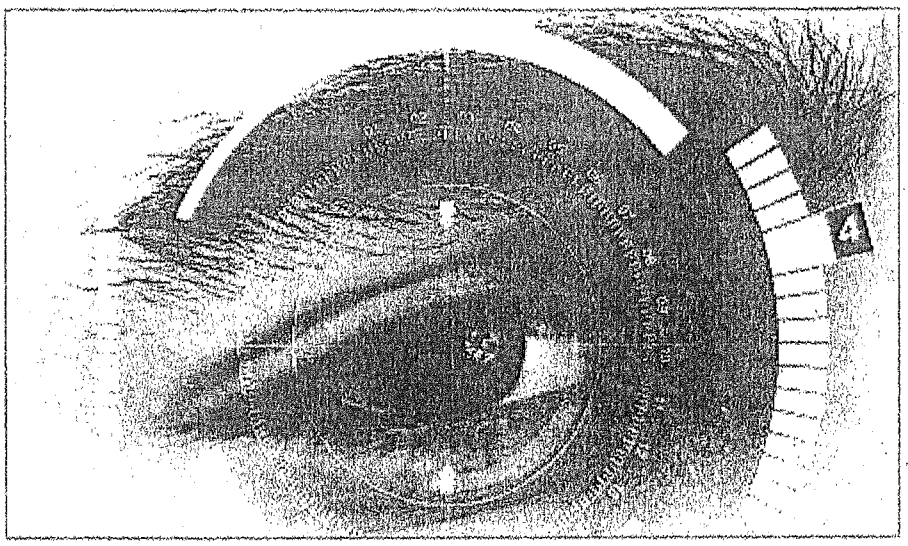
كلمة المرور هي سلسلة من الرموز (حروف وأرقام وبعض الأحرف الخاصة) تستخدم للتعريف بالشخص المخول، وتمكنه من الدخول إلى شبكة الحاسوب.

وعند إنشاء كلمات المرور يجب أن تكون قوية، يصعب تخمينها أو كسر حمايتها، لذا ينصح بمراعاة ما يلي:

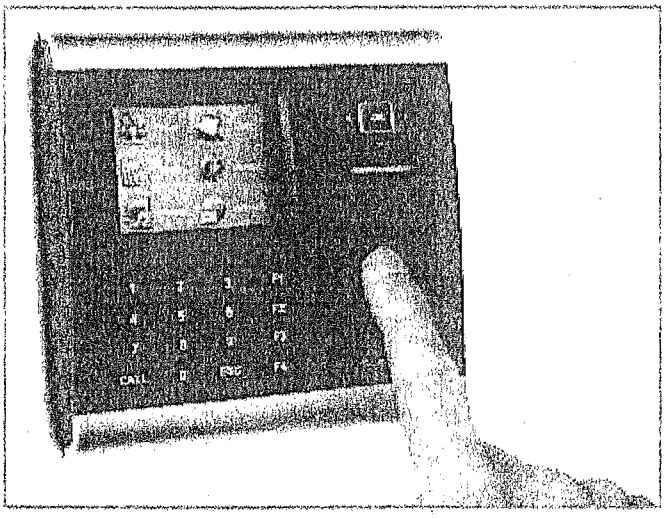
- المحافظة على سرية كلمات المرور، وعدم مشاركتها مع الآخرين، أو كتابتها في أماكن متوقعة، وعدم حفظها على جهاز الحاسوب أو قريبا منه.
- العمل على تغييرها بانتظام خلال فترات زمنية قصيرة.
- أن يكون طول كلمات المرور مناسبا، فلا تقل عن ثمانية عناصر.
- تجنب كلمات المرور ذات الدلالات الشخصية، كالاسم، أو تاريخ الميلاد، أو رقم الهاتف وغيرها، وأن لا تكون كلمة متكاملة يمكن إيجادها في القاموس، بل خليطا من الحروف والأرقام والأحرف الخاصة ( ~ ! @ # $ % & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? / )، وأن تشتمل على حروف كبيرة وصغيرة إذا كانت باللغة الإنجليزية، مثل: *MYpassw@rd234*.

### 3.4.3 التقنيات الأمنية الحيوية/البيومترية الشائعة المستخدمة في التحكم بالوصول Common biometric security techniques used in access control

التقنية البيومترية عبارة عن علم يدرس كيفية استخدام معادلات رياضية وإحصائية لقياس العلاقات الرقمية والنسب المختلفة التي تظهر في الكائنات الحية وأعضائها المختلفة. لذا تعتمد التقنية البيومترية على الميزات والصفات الخاصة في الجسم، ويتم التعرف على تلك الصفات عبر جهاز الحاسوب الذي يتعرف على بصمات الإصبع عبر المجسات المختلفة مثل قارئ الخطوط الالكتروني أو الماسح الضوئي لبصمات الأصابع أو ماسح العين والوجه، وعبر معادلات رياضية دقيقة ومعقدة، يقارن جهاز الحاسوب تلك المعلومات بالمعلومات المخزنة ليرى إذا كانت تتطابق معها.



وأنواع التقنيات البيومترية كثيرة ومتنوعة، فمن تقنية التعرف على الوجه أو العينين، أو شكل الأذنين، إلى التوقيع اليدوي، أو طريقة الكتابة على لوحة المفاتيح، مرورا ببصمات الأصابع والشكل الهندسي المميز لليد، والحامض النووي، والتعرف على بصمة الصوت، والرائحة المميزة لكل جسد، وغيرها من الوسائل المتعددة والمميزة لكل فرد، إلا أن الكثير من تلك التقنيات بعد باهظ الثمن بشكل كبير، فلا يستطيع الكثيرون الاعتماد عليه، كما أن البعض الآخر لا يمكن الاعتماد عليه بالشكل الكافي، مثل التعرف على الصوت، أو طريقة السير أو الكتابة، إذ إنه يسهل تقليدها كما أن هناك تشابهات طبيعية لدى الكثير من البشر في هذه المجالات، لذلك فقد أصبحت تقنية التعرف على (بصمة الأصبع/ *Fingerprint*)، أو (المسح الضوئي للعين/ *Eye scanning*) الأكثر انتشارا لأنها الأقل تكلفة.



وبالنسبة للشركات فيمكن تخزين معلومات تخص مئات الأشخاص، وفي كل الأحوال لا تفتح الأبواب إلا إذا تطابقت البصمة أو الأعين الممسوحة مع تلك المعلومات المخزنة. وبالطبع لا يمكن ضمان الحماية الكاملة في هذه الأنظمة، فهناك نسبة من الخطأ، لكن التزوير في تلك المعلومات أو نقلها يعد صعبا إذ إنها صفات خاصة تميز كل شخص، ولكن درجة الخطأ وندرته تتوقفان في تلك الحالة بشكل أكبر على الدقة في المعادلات المستخدمة للتعرف على تلك الصفات المميزة. لذلك فقد سعى العلماء لاكتشاف وسائل تجعل الكشف عن البصمات أو الأعين أكثر أمانا.

ولكن بالتأكيد فإن استخدام أكثر من ميزة بيومترية والجمع بينها هو ما يمكن أن يعطي أكبر قدر من الأمان لفتح الأبواب أو التعامل مع المعلومات.

**تمرين (3-4)**

اختر الإجابة الصحيحة من بين البدائل الأربعة المذكورة لكل سؤال مما يلي: *(انظر الإجابات في ملحق الإجابات ص 69).*

1. أي الإجراءات الآتية مطلوبة لحماية الشبكة من الوصول غير المعتمد ولا المصرح به؟
   أ- تمكين ميزة الإكمال التلقائي. ب- تعطيل إعدادات الجدار الناري.
   ج- استخدام التوقيع الرقمي. د- إنشاء حساب يتطلب اسم مستخدم وكلمة مرور.

2. ماذا تفعل لتعريف المستخدمين أنفسهم عند تسجيل الدخول إلى حساب الشبكة؛ لحماية المعلومات الخاصة والحفاظ على أمن البيانات؟
   أ- اسم مستخدم، وكلمة مرور. ب- تنصيب جدار ناري.
   ج- تشفير البيانات بكلمة سر. د- استخدام التواقيع الرقمية.

3. أي العبارات التالية هي صحيحة عن كلمة السر؟
   أ- يجب تغييرها فقط إذا تم المساس بها أو تخمينها. ب- لا يمكن أن تحتوي على رموز وحروف خاصة.
   ج- يجب تغييرها بانتظام. د- ينبغي أن لا تكون طويلة.

4. أي مما يلي هو السبب الذي يجعل المستخدمين يقومون بتسجيل الدخول باستخدام اسم المستخدم وكلمة المرور؟
   أ- لمعرفة الأشخاص المتواجدين في المبنى. ب- للتأكد من حفظ وقت الدخول للمستخدمين.
   ج- لحماية الحواسيب من الاستخدام غير المسموح به. د- لإلقاء التحية الشخصية لكل مستخدم.

5. أي كلمات المرور الآتية هي الأنسب؟
   أ- password; ب- PASSword. ج- PASS.Word. د- Pass@Word456.

6. أي مما يلي هي تقنية مقاييس حيوية/بيومترية تستخدم لحماية البيانات؟
   أ- التقطيع. ب- المسح الضوئي للعين.
   ج- النسخ الاحتياطي للبيانات. د- قرصنة البطاقات الائتمانية.

## 4 الاستخدام الآمن للويب Secure Web Use

### 1.4 تصفح الويب Web Browsing

#### 1.1.4 أنشطة معينة على الإنترنت يجب عدم القيام بها إلا ضمن صفحات ويب آمنة Certain online activity should only be undertaken on secure web pages

هناك بعض الأنشطة على الإنترنت يجب أن لا تقوم بها إلا ضمن صفحات ويب آمنة، ومن الأمثلة على هذه الأنشطة ما يأتي:

- (الشراء/ *Purchasing*): ومن الأمثلة على ذلك التسوق عبر الإنترنت.
- (المعاملات المالية/ *Financial transactions*): ومن الأمثلة على ذلك المعاملات المصرفية، وتحويل الأم عبر الإنترنت.

#### 2.1.4 كيفية تحديد مواقع الويب الآمنة How to Identify secure websites

تعتمد معرفة متى تثق في موقع ويب في جزء منها على هوية ناشر موقع الويب، والمعلومات التي تطلب منك، وماذا تحتا به من الموقع. ولمعرفة أمن موقع الويب الذي تريد تصفحه ابحث عن رمز التأمين في شريط عناوين متصفح الإنترنت، فإن المواقع التي تحافظ على سرية بيانات مستخدميها تتميز بظهور صورة قفل على شريط العنوان في متصفح الإنترنت وإضافة Hyper Text Transfer Protocol Secure (https) بدلا من (http) في بداية عنوان الموقع.

https://www.icdladmin.com/Login.aspx

وبصفة عامة قد لا يكون موقع الويب آمنا ومحل ثقة في الحالات الآتية:

- الإشارة إلى موقع الويب عن طريق رسالة بريد إلكتروني قادمة من شخص لا تعرفه.
- عرض الموقع لمحتوى غير مقبول، مثل المواد الإباحية أو غير المشروعة.
- إتاحة الموقع لعروض مغرية لا يمكن تصديقها، مما يعني إمكانية التعرض لعمليات خداع أو بيع منتجات غير شرعية أو مسروقة، من خلال مخطط (التضليل)، حيث يكون المنتج أو الخدمة بخلاف ما تتوقع.
- طلب بطاقة الائتمان للتحقق من الهوية، أو دون وجود دليل على أن المعاملة آمنة.
- طلب معلومات شخصية تبدو غير ضرورية.

وإذا لم يظهر رمزا الأمان السابقان فلا يعني هذا أن موقع الويب ليس آمنا، لكن عليك التأكد من أمان الموقع من خلال الإ ة عن الأسئلة التالية:

- هل موقع الويب معتمد من قبل إحدى منظمات منح الثقة عبر الإنترنت؟

منظمة منح الثقة عبر الإنترنت هي شركة تتحقق من امتلاك أحد مواقع الويب على بيان خصوصية (إعلام منشور ن كيفية استخدام معلوماتك الشخصية)، ومن أن موقع الويب قد أتاح لك خيار كيفية استخدام معلوماتك. يمكن لمواقع الويب المعتمدة من قبل منظمات منح الثقة عبر الإنترنت عرض أختام ترخيص الخصوصية، غالبا في عدة أماكن على الصفحة الرئيسية أو على نماذج الطلب، ومع ذلك فلا تضمن لك هذه الأختام الوثوق بموقع الويب؛ إنما تعني فقط أن موقع الويب يتطابق مع الشروط المقبولة من جهة منظمة منح الثقة عبر الإنترنت.

- هل موقع الويب مملوك لشركة أو منظمة تعرفها جيدا؟

إذا اشتريت بضائع من أحد المخازن الفعلية وكنت راضيا عن تجربة الشراء تلك، فقد ترغب أيضا في محاولة الشراء من المخزن باستخدام موقع الويب الخاص بهم. ومع ذلك، وعلى الرغم من الوثوق بالشركة، فينبغي عليك دائما قراءة بيان الخصوصية أو شروط الاستخدام لموقع الويب.

في بعض الأحيان يكون موقع الويب الخاص بإحدى الشركات مستقلا بمخازنه، وربما يكون له شروط خصوصية مختلفة. ابحث عن الشروط التي لا توافق عليها، مثل طلبات الموافقة على عروض البريد الإلكتروني أو الإعلان من قبل موقع الويب، أو مشاركة معلوماتك مع شركاء الشركة، وإذا لم تكن راضيا عن الشروط أو التصرفات فلا تستخدم الموقع.

- هل يطلب منك موقع الويب معلومات شخصية؟

إذا طلب منك معلومات شخصية، مثل رقم بطاقة الائتمان أو المعلومات البنكية، تقدم بها فقط إذا كان هناك سبب مقنع لإجراء ذلك، كالشراء من موقع موثوق به، وتأكد أيضا من وجود نموذج إدخال آمن لتسجيل المعلومات. وابحث عن رسالة تفيد بأنه سيتم تشفير المعلومات.

### 3.1.4 تزوير/قرصنة العناوين Pharming

تزوير العناوين هو هجوم واختراق يقوم بإعادة توجيه مرور موقع الويب إلى موقع ويب مزيف. فإن أي موقع على شبكة الانترنت عادة ما يستخدم اسم النطاق كعنوان له مثل http://www.google.com فإن عنوانه الفعلي يتم تحديده عن طريق عنوان بروتوكول الانترنت وهو عنوان عادة ما يتكون من أربعة أرقام. عندما يكتب المستخدم اسم النطاق الذي يريده في حقل العنوان الخاص بمتصفحه ويقوم بالضغط على زر الإدخال تتم ترجمة اسم النطاق إلى عنوان بروتوكول الانترنت عبر خادم نظام أسماء النطاقات، ومن ثم يقوم المتصفح بالاتصال بالخادم عبر هذا العنوان، ثم يقوم بتحميل صفحة الويب. بعد زيارة المستخدم لموقع معين غالبا ما يتم تخزين هذا العنوان لهذا الموقع على جهاز الحاسوب الخاص بالمستخدم في ذاكرة التخزين المؤقت لنظام أسماء النطاقات. بهذه الطريقة لا يحتاج الحاسوب إلى الاتصال بخادم نظام أسماء النطاقات كلما أراد المستخدم زيارة نفس الموقع.

لكن يمكن تزوير العناوين من خلال نظام أسماء النطاقات، حيث تستخدم طرق التلاعب بذاكرة التخزين المؤقت لنظام أسماء النطاقات أو محاكاة أسماء النطاقات أو خطف النطاقات لكنها تستخدم هذه الطرق لأغراض مختلفة عن ذي قبل. بينما كانت هذه الطرق تستخدم قديما لتعطيل الخدمات والتسبب في بعض المضايقات للمستخدمين، فالأمر الآن أصبح متعلقا بالمال.

وتتم عملية التزوير وفق الخطوات الآتية:

1. يذهب المخترق إلى نظام أسماء النطاقات سواء في الذاكرة المؤقتة على حاسوب المستخدم أو على خادم الشبكة المحلية أو خادم مزود خدمة الانترنت نفسه. ويقوم المخترق باستخدام العديد من الأساليب التي تمكنه من تغيير عنوان بروتوكول الانترنت لموقع معروف – ربما يكون موقع أحد البنوك – إلى عنوان موقع آخر عادة ما يكون مشابها في الاسم.
2. يقوم المستخدم بكتابة العنوان الصحيح للموقع في حقل العنوان الخاص بمتصفحه، ثم يضغط على زر الإدخال.
3. يقوم الحاسوب الخاص بالمستخدم بالبحث في ذاكرته المؤقتة عن عنوان بروتوكول الإنترنت لهذا الموقع أو سؤال خادم نظام أسماء النطاقات عن هذا العنوان إن لم يكن موجود في الذاكرة المؤقتة.
4. إذا كان الموقع موجودا في الذاكرة المؤقتة التي تم تزييفها فإن عنوان بروتوكول الانترنت الذي يحصل عليه المتصفح يكون مزيفا، وفي حال قيام المتصفح بسؤال خادم تم التلاعب به فإنه سيحصل على عنوان مزيف أيضا.
5. يقوم المتصفح بالاتصال بهذا العنوان المزيف ظنا منه أنه صحيح، ولا يعلم المستخدم عن ذلك شيئا.

### 5.1.4 كلمة السر المستخدمة لمرة واحدة The term one-time password (OTP)

هي كلمة مرور صالحة للاستخدام لمرة واحدة فقط، عند القيام بتسجيل الدخول أو عند القيام بأي إجراء آخر، وبهذه الكلمة فإنك تتجنب الكثير من أوجه القصور التي ترتبط مع كلمات المرور التقليدية الثابتة. لأنها لن تتكرر مرة ثانية، وبالتالي فإن من يحاول اختراق النظام من خلالها – وإن اكتشفها - لن يستطيع ذلك؛ نظرا لأنها لم تعد صالحة.

لكن ينبغي أن تعي أن كلمات السر غير المتكررة يصعب على الإنسان تذكرها، ولهذا فإنها تتطلب تقنية إضافية لتعمل.

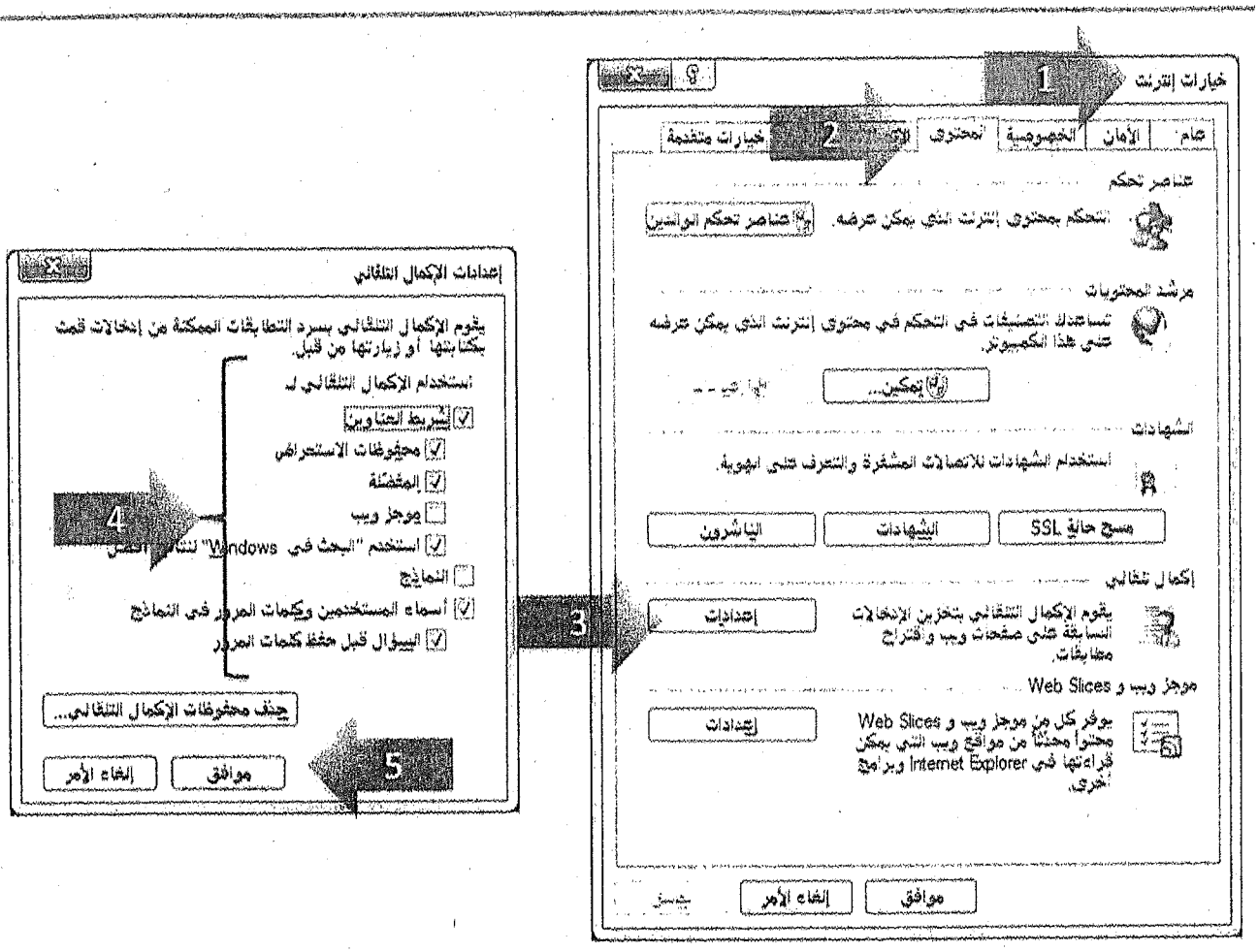
### 6.1.4 الإكمال التلقائي، والحفظ التلقائي Autocomplete, Autosave

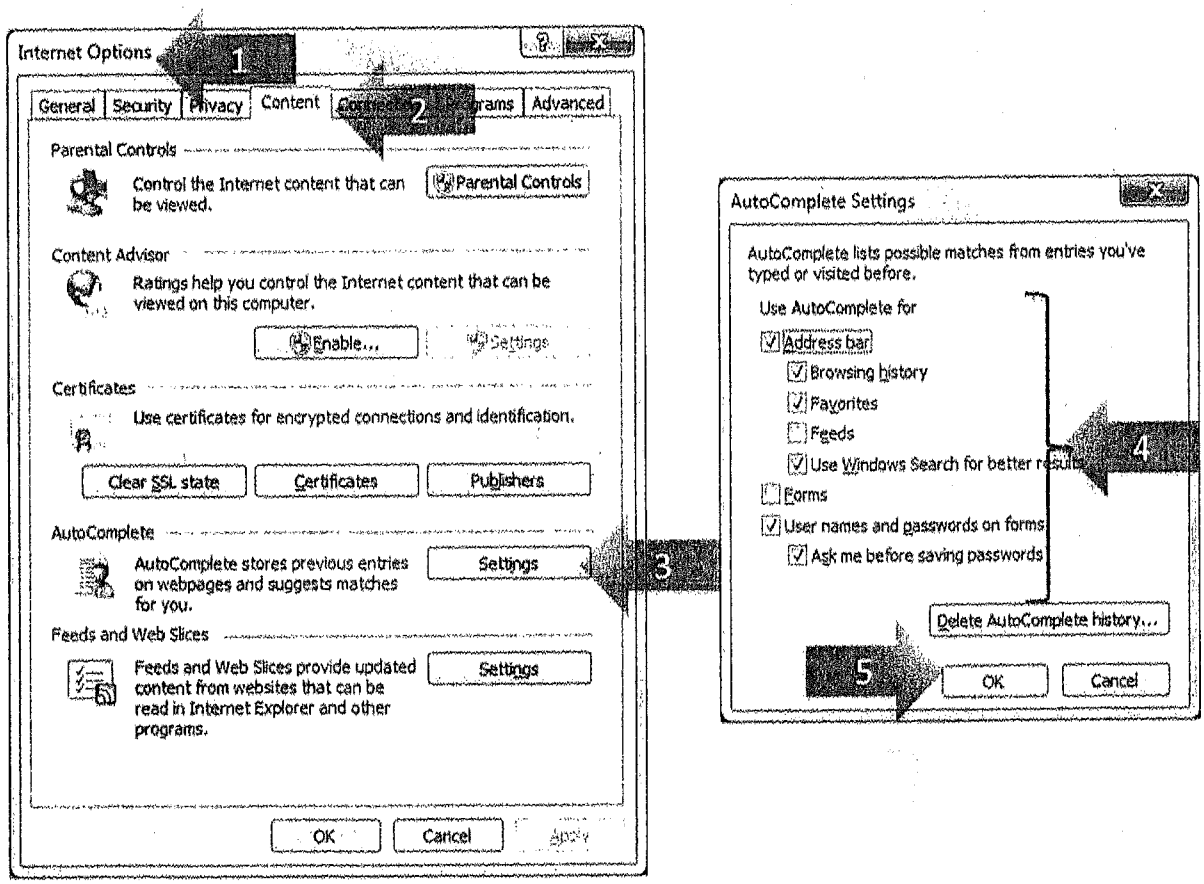
عند تعبئة نماذج الويب بالمعلومات الخاصة بها، يمكنك تمكين أو تعطيل كل من الإكمال التلقائي للبيانات، والحفظ التلقائي لنماذج الويب، وبالتالي ستنتهي من تعبئة تلك النماذج بشكل أسرع، كما ينبغي أن تقوم بإدارة بيانات الإكمال التلقائي بشكل منتظم وتحذفها من المتصفح.

#### 1.6.1.4 اختيار الإعدادات المناسبة لتمكين أو تعطيل الإكمال التلقائي Selecting appropriate settings for enabling/disabling autocomplete when completing a form

لتمكين أو تعطيل خيارات الإكمال التلقائي عند تعبئة نماذج الويب، اتبع الخطوات الآتية:

1. افتح متصفح الإنترنت.
2. من (شريط الأوامر/ *Command bar*)، انقر على زر (أدوات/ *Tools*)، فتظهر لائحة.
3. من اللائحة، انقر على (خيارات إنترنت/ *Internet Options*)، فيظهر مربع الحوار (خيارات إنترنت/ *Internet Options*).
4. انقر على تبويب (المحتوى/ *Content*).
5. من قسم (إكمال تلقائي/ *Autocomplete*)، انقر على زر (إعدادات/ *Settings*)، فيظهر مربع الحوار (إعدادات الإكمال التلقائي/ *Autocomplete Settings*).
6. انقر على الخيارات التي تريد تفعيلها/ عدم تفعيلها من خيارات الإكمال التلقائي.
7. انقر على زر (موافق/ *OK*) في كافة مربعات الحوار المفتوحة، وأبق متصفح الإنترنت مفتوحا.


خيارات إنترنت
1
2
عام
الأمان
الخصوصية
المحتوى
خيارات متقدمة
عناصر تحكم
التحكم بمحتوى إنترنت الذي يمكن عرضه.
عناصر تحكم الوالدين
مرشد المحتويات
تساعدك التصنيفات في التحكم في محتوى إنترنت الذي يمكن عرضه على هذا الكمبيوتر.
تمكين...
الشهادات
استخدم الشهادات للاتصالات المشفرة والتعرف على الهوية.
مسح حالة SSL
الشهادات
الناشرون
إكمال تلقائي
يقوم الإكمال التلقائي بتخزين الإدخالات السابقة على صفحات ويب واقتراح مطابقات.
إعدادات
موجز ويب و Web Slices
يوفر كل من موجز ويب و Web Slices محتوى محدثاً من مواقع ويب التي يمكن قراءتها في Internet Explorer وبرامج أخرى.
إعدادات
موافق
إلغاء الأمر
إعدادات الإكمال التلقائي
يقوم الإكمال التلقائي بسرد التطابقات الممكنة من إدخالات قمت بكتابتها أو زيارتها من قبل.
استخدام الإكمال التلقائي لـ
شريط العناوين
محفوظات الاستعراض
المفضلة
موجز ويب
استخدم "البحث في Windows" لنتائج أفضل
النماذج
أسماء المستخدمين وكلمات المرور في النماذج
السؤال قبل حفظ كلمات المرور
حذف محفوظات الإكمال التلقائي...
موافق
إلغاء الأمر
3
4
5


Internet Options
1
2
General
Security
Privacy
Content
Programs
Advanced
Parental Controls
Control the Internet content that can be viewed.
Parental Controls
Content Advisor
Ratings help you control the Internet content that can be viewed on this computer.
Enable...
Settings
Certificates
Use certificates for encrypted connections and identification.
Clear SSL state
Certificates
Publishers
AutoComplete
AutoComplete stores previous entries on webpages and suggests matches for you.
Settings
Feeds and Web Slices
Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.
Settings
OK
Cancel
Apply
AutoComplete Settings
AutoComplete lists possible matches from entries you've typed or visited before.
Use AutoComplete for
Address bar
Browsing history
Favorites
Feeds
Use Windows Search for better results
Forms
User names and passwords on forms
Ask me before saving passwords
Delete AutoComplete history...
OK
Cancel
3
4
5

### 2.6.1.4 اختيار الإعدادات المناسبة لتمكين أو تعطيل الحفظ التلقائي Selecting appropriate settings for enabling/disabling autosave when completing a form

لتمكين أو تعطيل خيارات الحفظ التلقائي عند تعبئة نماذج الويب، اتبع الخطوات الآتية:

1. من (شريط الأوامر/ *Command bar*)، انقر على زر (أدوات/ *Tools*)، فتظهر لائحة.
2. من اللائحة، انقر على (خيارات إنترنت/ *Internet Options*)، فيظهر مربع الحوار (خيارات إنترنت/ *Internet Options*).
3. انقر على تبويب (المحتوى/ *Content*).
4. من قسم (إكمال تلقائي/ *Autocomplete*)، انقر على زر (إعدادات/ *Settings*)، فيظهر مربع الحوار (إعدادات الإكمال التلقائي/ *Autocomplete Settings*).
5. انقر على الخيارات التي تريد تفعيلها/ عدم تفعيلها من خيارات (الحفظ التلقائي/ *Autosave*)، المتعلقة بأسماء المستخدمين وكلمات المرور.
6. انقر على زر (موافق/ *OK*) في كافة مربعات الحوار المفتوحة.
7. أبق متصفح الإنترنت مفتوحا للدرس القادم.

### 7.1.4 ملف تعريف الارتباط (الكوكي) The term: Cookie

ملفات تعريف ارتباط الإنترنت عبارة عن ملفات نصية، تقوم المواقع التي تزورها بإنشائها على حاسوبك، وتحتوي هذه الملفات معلومات تتيح للموقع الذي أنشأها أن يسترجعها عند زيارتك المقبلة للموقع، ومن أمثلة هذه المعلومات اسم المستخدم الذي تصفح الموقع ومكان سكنه وتفضيلاته المختلفة.

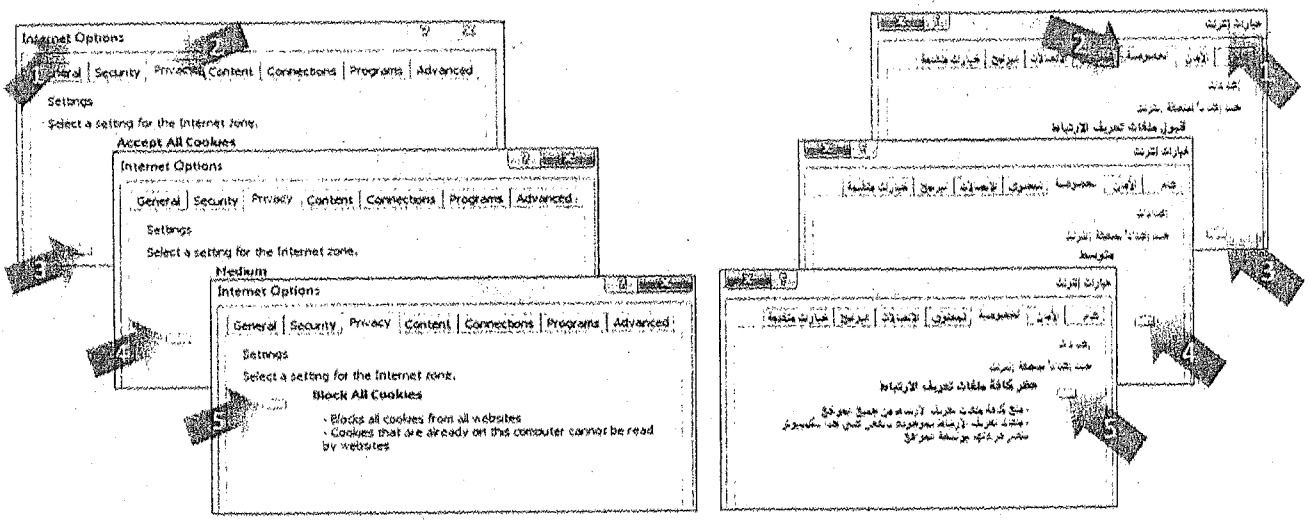
وتختلف المعلومات التي تخزن ضمن هذه الملفات من موقع لآخر، ولكن ليس بإمكان هذه المواقع استرجاع أية معلومات إضافية عنك أو عن جهازك، باستثناء تلك المعلومات المخزنة في الملف الخاص بها.

### 8.1.4 اختيار الإعدادات المناسبة للسماح بـ أو لمنع ملفات تعريف الارتباط (الكوكيز) Selecting appropriate settings for allowing, blocking cookies

يمكنك تحديد المواقع التي يسمح لها بإنشاء ملفات تعريف الارتباط بالإنترنت من خلال متصفح الإنترنت، كذلك يمكن منع بعض المواقع من إنشاء هذه الملفات، كما يمكن من خلال متصفح الإنترنت منع إنشاء ملفات تعريف الارتباط بالإنترنت بالكامل.

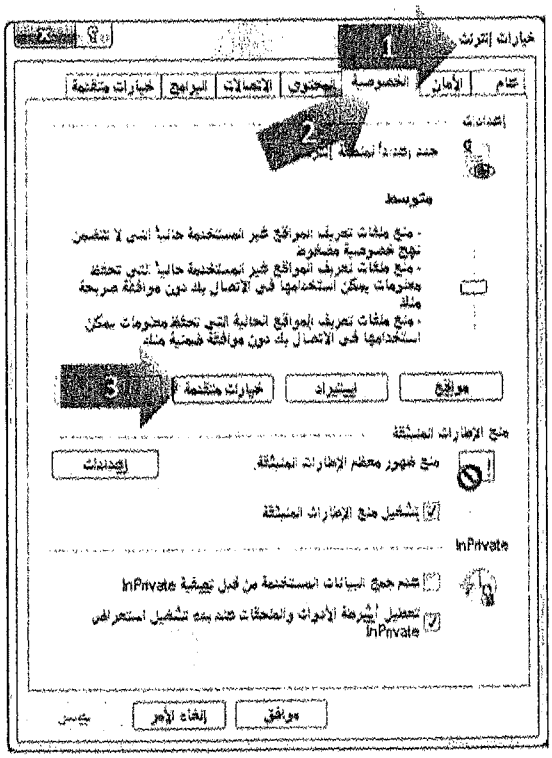
ولتحديد المواقع التي يسمح لها بإنشاء هذه الملفات أو منعها، اتبع الخطوات الآتية:

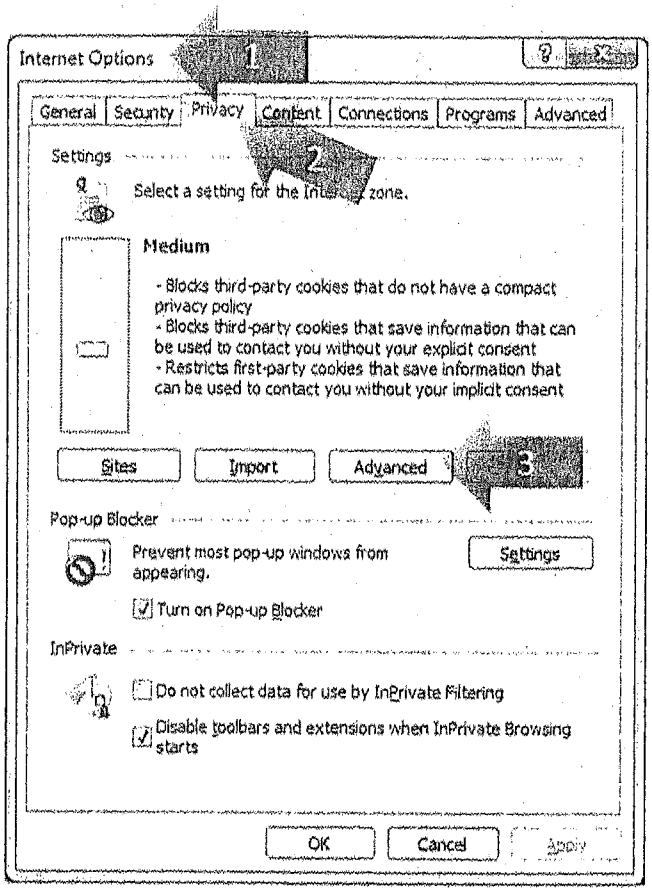
1. ضمن نافذة المتصفح المفتوحة، انقر على لائحة (أدوات/ *Tools*).
2. انقر على (خيارات إنترنت/ *Internet options*)، فيظهر مربع الحوار (خيارات إنترنت/ *Internet Options*).
3. انقر على تبويب (الخصوصية/ *Privacy*).
4. من قسم (إعدادات/ *Settings*)، حرك المنزلق إلى أعلى مستوى، عندها ستمنع جميع المواقع من إنشاء ملفات تعريف الارتباط بالإنترنت، وعند تحريك المقبض إلى أدنى مستوى سيتم السماح لجميع المواقع بإنشاء ملفات تعريف الارتباط بالإنترنت، وعند تحريك المقبض إلى الوسط سيتم السماح لبعض المواقع دون الأخرى.
5. انقر على زر (موافق/ *OK*).

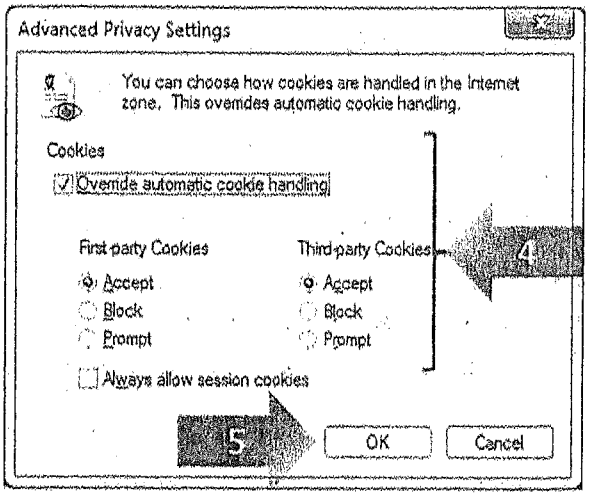



ولاختيار الإعدادات المناسبة للسماح بـ أو لمنع ملفات تعريف الارتباط (الكوكيز)، اتبع الخطوات الآتية:

1. أظهر مربع الحوار (خيارات إنترنت/ *Internet Options*)، كما تعلمت سابقا.
2. انقر على تبويب (الخصوصية/ *Privacy*).
3. انقر على زر (خيارات متقدمة/ *Advanced*)، فيظهر مربع الحوار (إعدادات خصوصية متقدمة/ *Advanced Privacy Settings*).
4. انقر على الخيارات التي تريد تفعيلها/ عدم تفعيلها من خيارات ملفات تعريف الارتباط.
5. انقر على زر (موافق/ *OK*) في كافة مربعات الحوار المفتوحة، وأبق متصفح الإنترنت مفتوحا. مع التأكيد هنا أنه يفضل منع ملفات تعريف الارتباط إذا كنت تستخدم المتصفح لاستعراض مواقع ويب غير مألوفة.





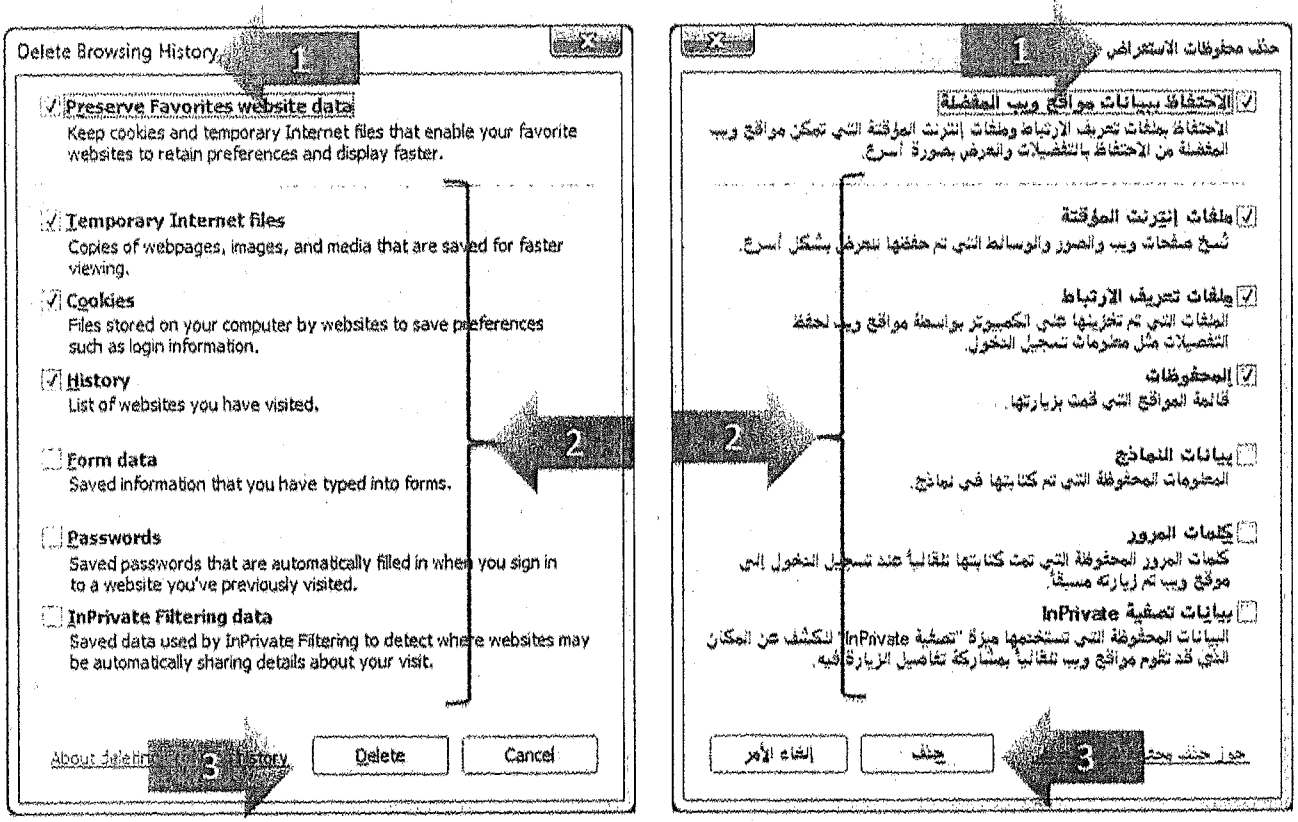




### 9.1.4 حذف البيانات الخاصة من متصفح الويب Deleting private data from a browser

تتعدد البيانات الخاصة التي يمكن أن تستخدمها أو تكتبها أثناء تصفح الإنترنت، مثل (ملفات إنترنت المؤقتة/ *Temporary Internet files*)، أو (ملفات تعريف الارتباط/ *Cookies*)، أو (المحفوظات/ *History*)، أو (محفوظات التنزيل/ *Browsing History*)، أو (بيانات النماذج/ *Form data*)، أو كلمات المرور (*Passwords*)، وغيرها، ولحذف هذه البيانات الخاصة من متصفح الإنترنت، اتبع الخطوات الآتية:

1. انقر على لائحة (أدوات/ *Tools*).
2. انقر على (حذف محفوظات الاستعراض/ *Delete browsing history*)، فيظهر مربع الحوار (حذف محفوظات الاستعراض/ *Delete Browsing History*).
3. قم بتفعيل/ عدم تفعيل الخيارات التي تراها مناسبة.
4. انقر على زر (حذف/ *Delete*)، ثم أغلق متصفح الإنترنت.

Ctrl + Shift + Del




### 10.1.4 برمجيات التحكم بالمحتوى Content-control software

من المخاطر التي ترتبط بالاتصال بشبكة الإنترنت، مخاطر محتوى المواقع، حيث تسمح الإنترنت لأي شخص بنشر أي شيء دون قيود، وتسمح لأي شخص بالدخول إليها. ويوجد على الإنترنت ملايين المواقع التي تحتوي على معلومات حول مختلف مجالات الحياة. من هذه المواقع ما يناسب كل المستخدمين، بغض النظر عن أعمارهم وثقافاتهم واختصاصاتهم. ومنها ما يتميز بمحتوى لا يناسب الكثير من المستخدمين، وخصوصا الأطفال. هذا المحتوى الذي قد يلحق ضررا بالغا في الصحة البدنية والعاطفية والنفسية، خاصة بالنسبة للشباب، لذلك ينبغي أن يتوافر لديك برنامج حاسوبي لمراقبة المحتوى، يعمل على ما يأتي:

- (الرقابة والإشراف/ *Supervision*): وهو القيام بمراقبة أنشطة الإنترنت المختلفة، من خلال تفقد المواقع التي تمت زيارتها باستمرار، للتأكد من عدم الإساءة في استخدام الإنترنت.
- (تقييد استخدام متصفح الويب/ *Web browsing restrictions*): حيث يمكنك حجب المواقع حسب المواضيع التي تحتويها. ويجب على أولياء الأمور الانتباه لمحتوى الألعاب والتأكد من مناسبتها لأطفالهم.
- (تقييد التنزيل/ *Download restrictions*): ينبغي العمل على تحديد وتقييد نوع البيانات التي يتم تنزيلها من الإنترنت، وكذلك العمل على تحديد كمية البيانات التي يتم تنزيلها.

وفيما يلي بعض هذه البرامج:

- (برمجيات تصفية الإنترنت/ *Internet filtering software*): تم تصميم هذه البرامج لتصفية ومراقبة الوصول إلى مواقع الويب، ومن الأمثلة على هذه البرمجيات برنامج (Optenet PC).
- (برمجيات رقابة الوالدين/ *Parental control software*): تستخدم للحد من طول الفترة الزمنية التي يقضيها الأطفال أمام الإنترنت، وللحد من الوصول إلى محتوى معين، ومن الأمثلة على هذه البرمجيات برنامج ( Net Nanny Parental Controls)، وبرنامج (McAfee Parental Controls).

وهناك العديد من البرامج المخصصة لحماية الأطفال والمستخدمين وتوفير المحيط الملائم لكي يتجولوا بسلامة وأمان في عالم الإنترنت. ويستطيع الأهل وأصحاب العمل بواسطة هذه البرامج التحكم بنوع المحتوى الذي يعرض على شاشة الحاسوب لمنع أو حجب ما هو غير مرغوب من صفحات ورسائل بريد إلكتروني. كما أن بعض هذه البرامج يستطيع مراقبة غرف المحادثة والدردشة، وتحليل محتوى الصفحات، الاشتباه بتبادل معلومات خصوصية (اسم، عمر، عنوان، رقم هاتف، رقم بطاقة ائتمان...)، تحديد الزمان والوقت المسموح بهما لاستعمال جهاز الحاسوب، رفع تقارير عن طريقة ووجه استخدام الإنترنت وإرسالها إلى الأهل أو مديري الشبكات، وإرسال تحذير إلى الأهل أو مديري الشبكات في حال الاشتباه بأي شيء مريب، واتخاذ بعض الإجراءات الفورية للحد من أي خطر.

وللتأكد من فعالية البرنامج وملاءمته لحاجات العائلة أو الشركة، يجب على المسؤولين التأكد من وجود الخصائص والمواصفات التالية عند البحث عن برامج تصفية محتوى الإنترنت:

- سهولة الاستعمال من أهم الخصائص التي يجب أن يتمتع بها البرنامج لتمكين أي كان خبرته في مجال استخدام الحاسوب من تركيب وإعداد البرنامج واستخدامه بكامل طاقته.
- فعالية التصفية بحيث يستطيع البرنامج الموازنة بين تصفية المحتوى غير المرغوب فيه وعدم التصفية أكثر من اللازم. ومن المزايا المهمة أيضا القدرة على إعداد مستويات ترشيح مختلفة بحسب الفئات العمرية تناسب جميع المستخدمين.
- نظام التصفية، إذ تعتمد البرامج الجيدة مزيجا من التصفية بحسب عنوان الصفحة من جهة، وعن طريق تحليل كلمات وجمل المحتوى المطلوب عرضه من جهة أخرى؛ لتوازن بين الفعالية وسرعة عرض المحتوى وتقرير ما إذا كان يجب عرض الصفحة أو حجبها.
- تقارير النشاطات بحيث يتيح البرنامج إمكانية تقديم تقارير عن نشاط أفراد العائلة أو الشركة على جهاز الحاسوب يتضمن عناوين الصفحات التي تمت زيارتها، نص الدردشات في غرف المحادثة أو على برامج المراسلة الفورية (*Instant Messaging*) وغيرها.
- التصفية بعدة لغات، إذ تعتمد فعالية برامج تحكم الوالدين على قدرتها على تحليل وترشيح محتوى بلغات عدة وذلك لتوفر المحتوى والمضمون من كافة بلاد العالم وبمختلف اللغات.
- التحكم ببرامج أو بروتوكولات الإنترنت المختلفة عند الحاجة، إذ إن هناك دائما برامج جديدة تتوفر كل يوم وتوفر طرقا جديدة للحصول على محتوى من الإنترنت سواء كان هذا المحتوى مقبولا أم غير مرغوب به. إلا أن جميع هذه البرامج تستعمل بروتوكولات معروفة لذا من المهم أن يتمكن برنامج الحماية من التحكم بمختلف بروتوكولات الإنترنت لمراقبة أو منع هذه البرامج إذا دعت الحاجة لذلك.

**تمرين (4-1)**

اختر الإجابة الصحيحة من بين البدائل الأربعة المذكورة لكل سؤال مما يلي: *(انظر الإجابات في ملحق الإجابات ص 69)*.

1. أي مما يلي ينبغي الالتزام به عند إجراء المعاملات المالية عبر الإنترنت؟
   أ- تأكد من تشغيل ميزة الإكمال التلقائي. ب- تأكد من تشغيل ميزة الحفظ التلقائي.
   ج- تأكد أن موقع الويب هو موقع ويب آمن. د- تأكد من إفراغ سلة المحذوفات بعد ذلك.
2. أي مواقع الويب الآتية تستخدم في الغالب http بدلا من https في عنوان محدد مصدر المعلومات (URL)؟
   أ- المواقع الآمنة. ب- مواقع التسوق عبر الإنترنت.
   ج- مواقع الخدمات المصرفية عبر الإنترنت. د- مواقع محركات البحث.

3. أي مما يلي يدل وجوده في محدد مصدر المعلومات (URL) على أن صفحة الويب آمنة؟
أ- edu. ب- https. ج- mil. د- http.

4. ماذا يطلق على الهجوم والاختراق الذي يقوم بإعادة توجيه مرور موقع الويب إلى موقع ويب مزيف وهمي على شبكة الانترنت؟
أ- القرصنة الأخلاقية. ب- تزوير العناوين. ج- القرصنة. د- الاختراق.

5. أي مما يلي يعمل على إعادة توجيه المستخدمين إلى موقع ويب مختلف من دون علمهم؟
أ- اختراق كلمات المرور. ب- كسر حماية البرامج. ج- تزوير العناوين. د- القرصنة الأخلاقية.

6. ماذا يطلق على الملفات التي تحتوي على المفتاح العام وغيرها من معلومات المصادقة؟
أ- فك تشفير الملفات. ب- الشهادات الرقمية. ج- وحدات الماكرو. د- استعادة البيانات.

7. أي مما يلي يستخدم في التحقق من أن مرسل الرسالة هو المرسل الحقيقي وليس شخصا آخر؟
أ- ملفات الإنترنت المؤقتة. ب- الشهادة الرقمية.
ج- ملف تعريف ارتباط الإنترنت. د- محفوظات الاستعراض.

8. متى ينبغي أن تستخدم كلمة مرور لمرة واحدة؟
أ- عند تعيين إعدادات شاشة التوقف. ج- عند تسجيل الدخول إلى جهاز الحاسوب لأول مرة.
ب- عند تعيين كلمة مرور لفتح المستندات. د- عند تسجيل الدخول إلى الشبكة الخاصة الافتراضية.

9. أي مما يلي يعد تأثيرا لتمكين الإكمال التلقائي؟
أ- ستنتهي من تعبئة النماذج عبر الإنترنت بشكل أسرع. ب- ستفقد بيانات النموذج إذا تعطل الحاسوب.
ج- سيتم حذف جميع ملفات الكوكيز. د- ستنتهي من تعبئة النماذج باستخدام مفاتيح اختصار.

10. أي مما يأتي نص صغير مخزن بواسطة متصفح الويب على جهاز الحاسوب؟
أ- حصان طروادة. ب- الكوكيز. ج- البرامج الجذرية. د- شبكات الروبوت.

11. أي مما يلي ينبغي استخدامه لحذف ملفات تعريف الارتباط بالإنترنت؟
أ- مزود الخدمة. ب- متصفح الإنترنت. ج- برامج رقابة الوالدين. د- برامج تصفية الإنترنت.

12. أي أنواع البيانات التالية ينبغي أن تقوم بإدارتها بشكل منتظم وتحذفها من المتصفح؟
أ- فك تشفير الملفات. ب- الإكمال التلقائي. ج- الجدار الناري د- تحديثات البرامج.

13. أي مما يلي تم تصميمه لمراقبة ولتقييد محتوى الإنترنت المسموح للمستخدم أن يصل إليه؟
أ- متصفح الإنترنت. ب- ملفات تعريف ارتباط الإنترنت.
ج- برامج تصفية الإنترنت. د- الوصول المتخفي.

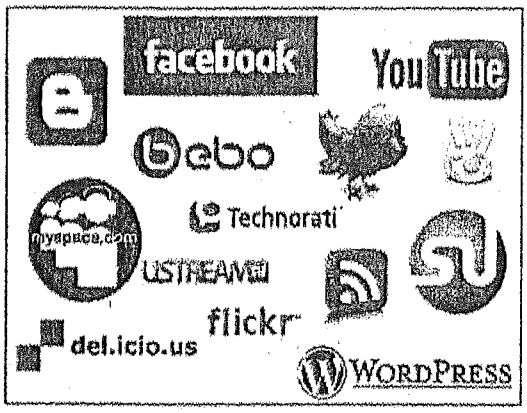
14. أي مما يلي ليست من سمات برامج تصفية الإنترنت؟
أ- تقييد الوصول إلى الميزات غير المناسبة في مواقع الشبكات الاجتماعية.
ب- السيطرة على وقت الوصول إلى الإنترنت.
ج- ضمان عدم تقييد المحتوى المشروع.
د- تقييد المحتوى الذي يمكن الوصول إليه على شبكة الانترنت.

15. أي مما يلي يمكن أن يكون سببا لمنع ملفات تعريف ارتباط الإنترنت في إعدادات المتصفح؟
أ- للسماح بتثبيت برامج مكافحة الفيروسات.
ب- للتصفح على موقع ويب غير مألوف.
ج- لتجنب تهديد الإزعاج الإلكتروني.
د- للوصول إلى الويب من خلال عمل حساب بريد إلكتروني.

## 2.4 الشبكات الاجتماعية Social Networking

### 1.2.4 فهم أهمية عدم الكشف عن معلومات سرية على مواقع الشبكات الاجتماعية The importance of not disclosing confidential information on social networking sites

ينبغي عدم الكشف عن معلومات سرية على مواقع الشبكات الاجتماعية، مثل (كلمات المرور/ *Password*)، و(الأرقام السرية/ *PIN numbers*)، والمعلومات الخاصة بالشركة، وتفاصيل العملاء، والمعلومات المالية؛ لأن الكشف عن مثل هذه المعلومات يمكن أن يؤدي إلى سرقتها أو إلى سوء استخدامها.




### 2.2.4 الحاجة إلى تطبيق الإعدادات الخصوصية المناسبة على حساب الشبكات الاجتماعية The need to apply appropriate social networking account privacy settings

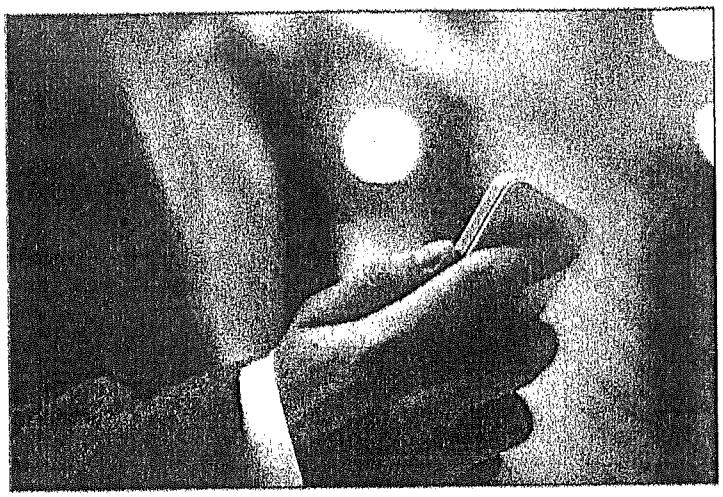
إن جعل حسابك على مواقع الشبكات الاجتماعية متاحا للعموم سيسمح لأي شخص كان أن يعرض ويعرف تفاصيلك الشخصية، لذا ينبغي ضبط إعدادات الخصوصية لحسابك في تلك المواقع الاجتماعية بما يضمن أن تفاصيلك وبياناتك الشخصية محمية ومخفية.

### 3.2.4 الأخطار المحتملة عند استخدام الشبكات الاجتماعية Potential dangers when using social networking sites

بما أنه لا يمكنك تعديل الإعدادات المتعلقة بإخفاء حقيقة أن يكون لديك حساب على موقع تواصل اجتماعي، فإن هناك مخاطر محتملة عند استخدام هذه الشبكات الاجتماعية ينبغي الحذر وأخذ الحيطة منها، منها ما يأتي:

- (المضايقة الإلكترونية/ *Cyber bullying*): قد يقوم بعض الأشخاص باستخدام الإنترنت والتقنيات المرتبطة به؛ في إيذاء الأشخاص الآخرين، من خلال سلوك عدواني متكرر ومتعمد.
- (الاستمالة/ *Grooming*): تقوم على استخدام الإنترنت والتقنيات المرتبطة به في إقامة علاقة صداقة مع شخص، لكن ليس بنية حسنة، وإنما بأسلوب سلبي يقوم على تهيئتهم كي يقبلوا بإقامة سلوك غير لائق ولا أخلاقي معهم.
- (المعلومات الخطيرة أو المضللة/ *Misleading/ dangerous information*) التي يمكن أن يرسلها مستخدمو الشبكات الاجتماعية، فليس هناك قيود على ما يكتبه أو يرسله الآخرون.

- (الهويات المزيفة/ *False identities*) التي يمكن أن يتظاهر بها مستخدمو الشبكات الاجتماعية للاتصال بمستخدمين آخرين.
- (الروابط والرسائل الاحتيالية/ *Fraudulent links or messages*) التي يمكن أن ترسل إليك لانتزاع معلومات منك.



**تمرين (4-2)**

اختر الإجابة الصحيحة من بين البدائل الأربعة المذكورة لكل سؤال مما يلي: *(انظر الإجابات في ملحق الإجابات ص 70).*

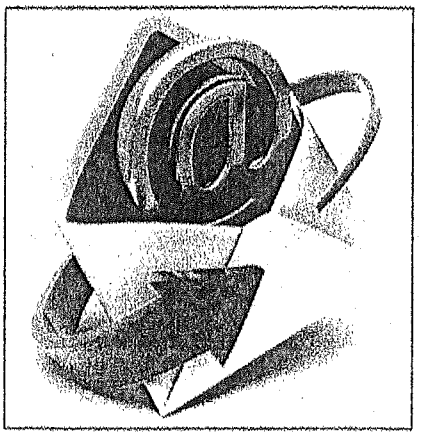
1. لماذا ينبغي عدم الكشف عن معلومات سرية على مواقع الشبكات الاجتماعية؟
   أ- خشية سرقتها أو سوء استخدامها. ب- خشية إعادة توجيهك إلى موقع ويب وهمي.
   ج- خشية تشفير البيانات. د- خشية تقييد محتوى الإنترنت المسموح لك.
2. أي مما يلي ينبغي عدم كشفه على مواقع الشبكات الاجتماعية؟
   أ- اهتماماتك الموسيقية. ب- اهتماماتك الحاسوبية. ج- مطعمك المفضل. د- رقم هاتفك الخلوي.
3. أي مما يلي ينبغي أن تحذر منه عند استخدام موقع تواصل اجتماعي؟
   أ- الهويات المزيفة. ب- بصمة الأصبع. ج- الجدار الناري. د- القرصنة الأخلاقية.
4. ما المقصود بالاستمالة عند استخدام موقع شبكة اجتماعية؟
   أ- قبول طلب صديق للانضمام إلى المنتدى.
   ب- تعيين إعدادات الجدار الناري المناسبة.
   ج- استدراج الناس لإقامة علاقات صداقة معهم للقيام بأنشطة غير أخلاقية.
   د- وضع أسماء الأصدقاء على صورهم.

## 5 الاتصالات Communications

### 1.5 البريد الإلكتروني E-Mail

#### 1.1.5 الهدف من تشفير/فك تشفير رسائل البريد الإلكتروني Understanding the purpose of encrypting, decrypting an e-mail

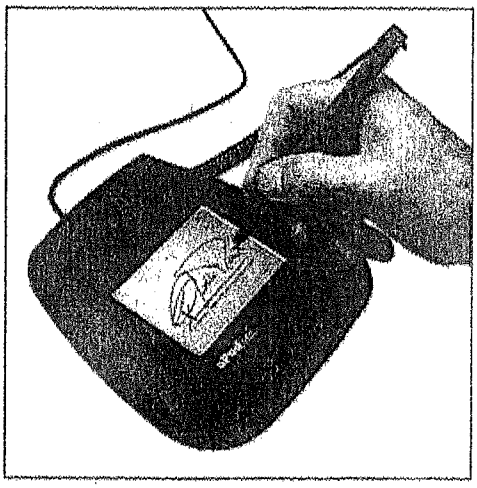
يهدف كل من تشفير رسائل البريد الإلكتروني وفك تشفيرها إلى ضمان أن الشخص المعني بالرسالة هو وحده الذي يستطيع قراءتها.



#### 2.1.5 التوقيع الرقمي The term: Digital signature

التوقيع الرقمي هو طابع أصالة إلكتروني مشفر خاص بالمعلومات الرقمية مثل رسائل البريد الإلكتروني أو وحدات الماكرو أو المستندات الإلكترونية، ويؤكد التوقيع بأن المعلومات نشأت من الموقع ولم يتم تغييرها. وبالتالي يضمن التوقيع الرقمي ما يلي:

- الأصالة: التأكد من الموقع.
- السلامة: عدم تغيير المحتوى أو العبث به منذ أن تم التوقيع عليه رقميا.
- عدم القدرة على الإنكار: إثبات مصدر المحتوى الموقع عليه لكافة الأطراف.
- التوثيق: تتوفر صلاحية التوثيق للتواقيع في ملفات Microsoft Word 2010 أو Excel 2010 أو PowerPoint 2010 التي تحمل طابعا زمنيا بواسطة خادم طابع زمني آمن، وفق حالات معينة.



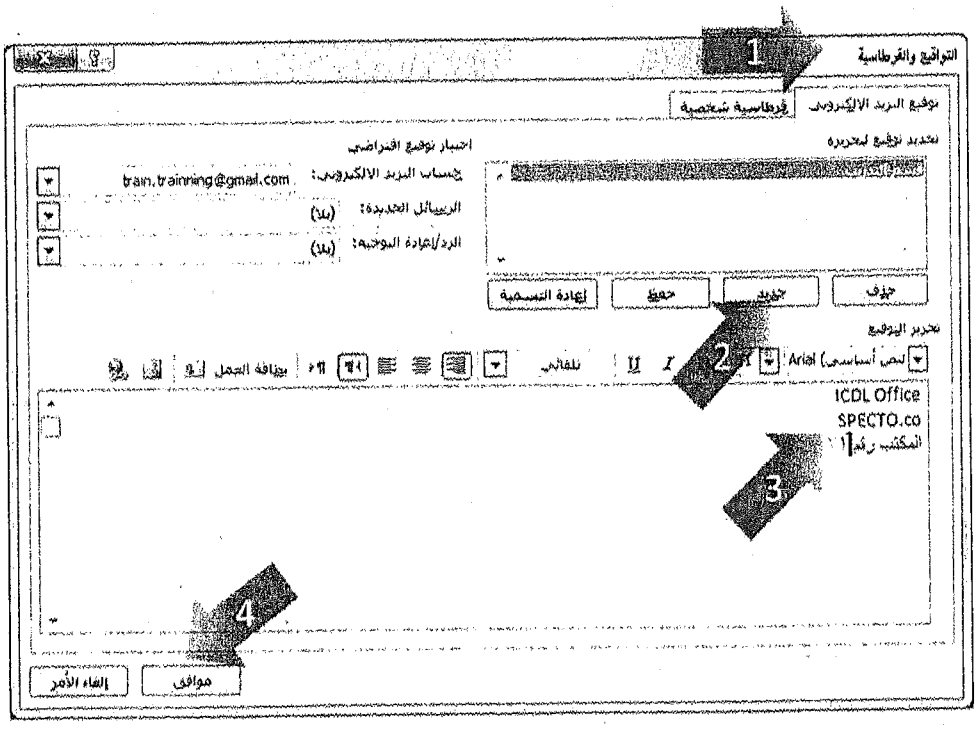
### 3.1.5 إنشاء توقيع رقمي وإضافته Creating and adding a digital signature

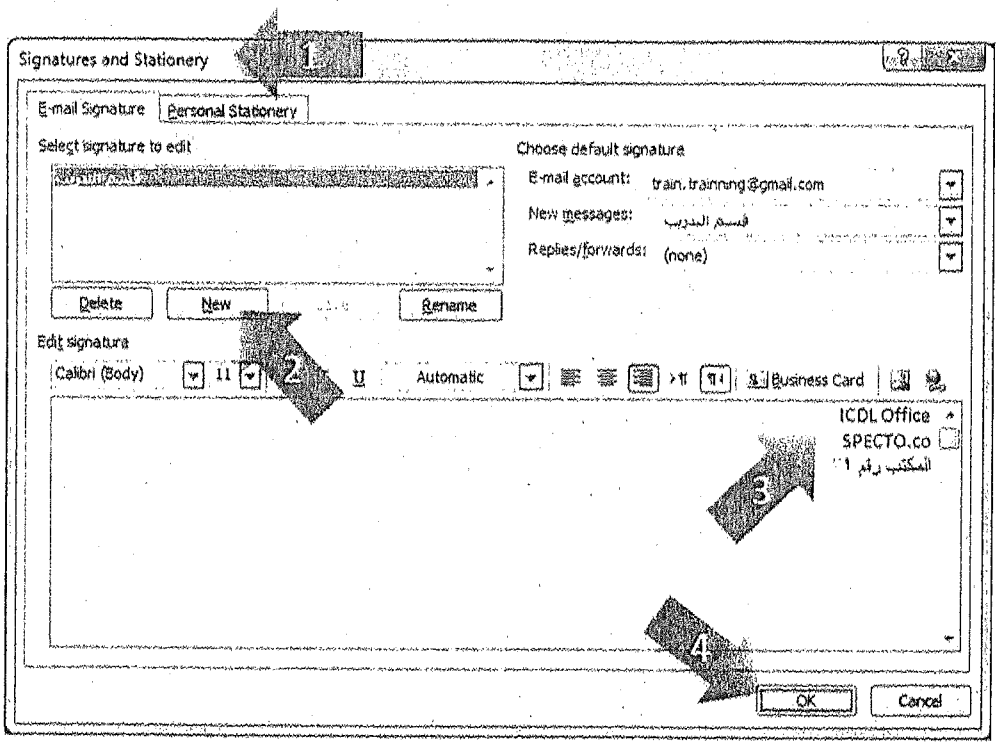
التوقيع الرقمي مع رسائل البريد الإلكتروني هو نص يرفق مع الرسالة الإلكترونية للتأكيد على هوية مرسل الرسالة، فلا يمكنه إنكار إرسالها. وهو بذلك يشبه التوقيع اليدوي من حيث الغرض منه، إلا أنه أحيانا يستخدم خوارزميات تشفير معقدة لمنع تقليده واختراقه، وبالتالي يعد علامة أمان إلكترونية يمكن إضافتها إلى الرسائل، لأنه رمز تشفير يدل على صحة الرسالة، ويتيح لك إمكانية التحقق من مرسل الرسالة، كما أنه يساعد في التحقق من أن الرسالة لم يتم تغييرها منذ تم توقيعها رقميا.

وإذا كانت الرسالة لا تحتوي توقيعا إلكترونيا صحيحا، فليس أمامك طريقة سوى التأكد من أن الرسالة قد تم إرسالها بالفعل من المصدر الذي يدعى أنها منه، أو أنها لم يتم العبث بها منذ أن أرسلت. ومن الأمان أن تجتنب فتح الرسائل ما لم تكن تعرف بالتأكيد من الذي قام بإرسالها، وإذا ما كانت المرفقات آمنة لفتحها أو لا.

ولإنشاء توقيع إلكتروني نصي مع رسائل البريد الإلكتروني باسم (قسم التدريب)، اتبع الخطوات الآتية:

1. افتح برنامج Outlook 2010، ثم أنشئ رسالة بريد إلكترونية جديدة.
2. ضمن علامة التبويب (رسالة/ *Message*)، ومن المجموعة (تضمين/ *Include*)، انقر على أيقونة (التوقيع/ *Signature*)، فتظهر لائحة أختر منها (تواقيع/ *Signatures*)، فيظهر مربع الحوار (التواقيع والقرطاسية/ *Signatures and Stationery*).
3. ضمن تبويب (توقيع البريد الإلكتروني/ *E-mail Signature*)، انقر على زر (جديد/ *New*)، فيظهر مربع الحوار (توقيع جديد/ *New Signature*).
4. في مربع (اكتب اسما لهذا التوقيع/ *Type a name for this signature*) اكتب (قسم التدريب)، ثم انقر على زر (موافق/ *OK*).
5. في مربع (تحرير التوقيع/ *Edit signature*)، اكتب النص الذي تريد تضمينه في التوقيع، كما في الشكل التالي.
6. بعد الانتهاء من إنشاء التوقيع وتحريره، انقر على زر (موافق/ *OK*).
7. أبق الرسالة مفتوحة.



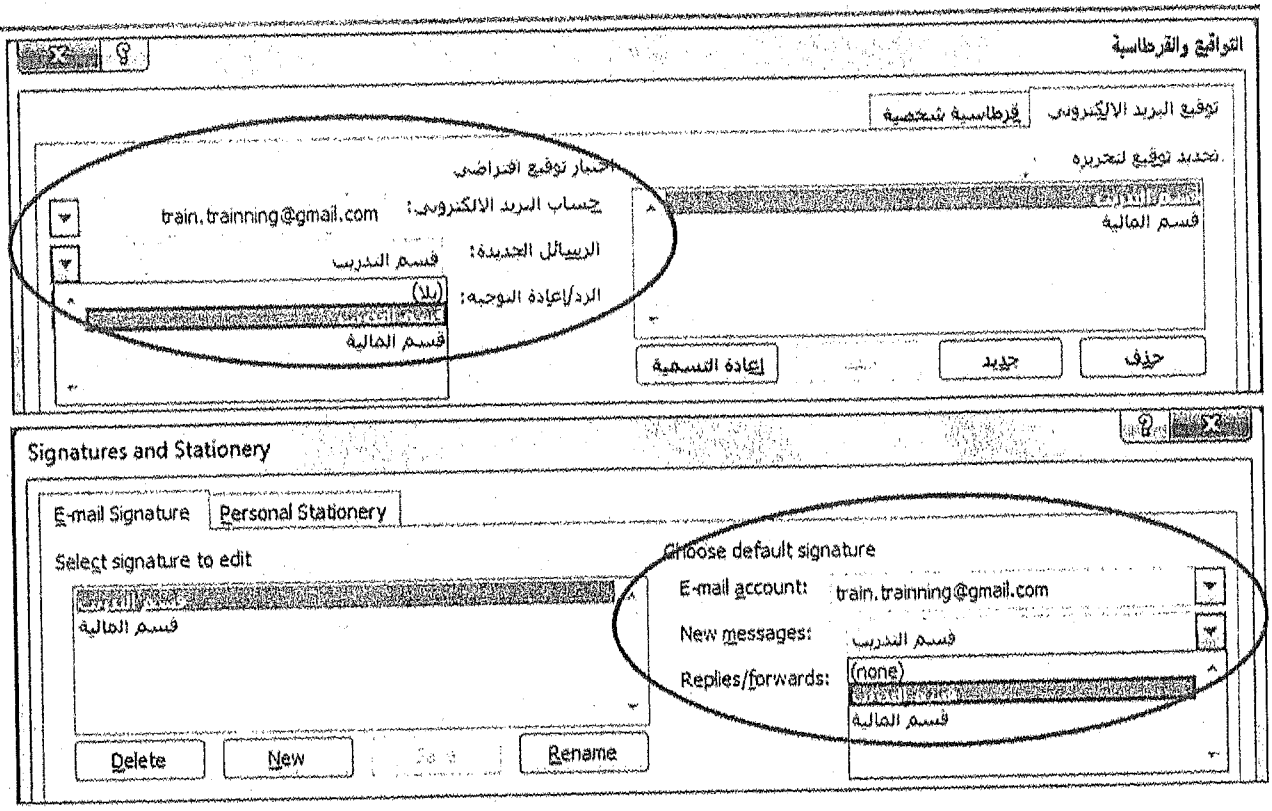



لعلك لاحظت أن التوقيع الذي أنشأته أو عدلته للتو لن يظهر في الرسالة المفتوحة حاليا؛ بل يجب إدراجه في الرسالة. ولإدراج التوقيع الذي أنشأته في الرسالة المفتوحة، اتبع الخطوات الآتية:

1. أدخل العناوين المناسبة في حقلي (إلى/ *To*)، و(الموضوع/ *Subject*).
2. اكتب نص الرسالة.
3. ضمن علامة التبويب (رسالة/ *Message*)، ومن المجموعة (تضمين/ *Include*)، انقر على أيقونة (التوقيع/ *Signature*)، فتظهر لائحة اختر منها التوقيع الذي تريده، علما أن Outlook 2010 يسمح بتوقيع واحد فقط في كل رسالة بريد إلكتروني.

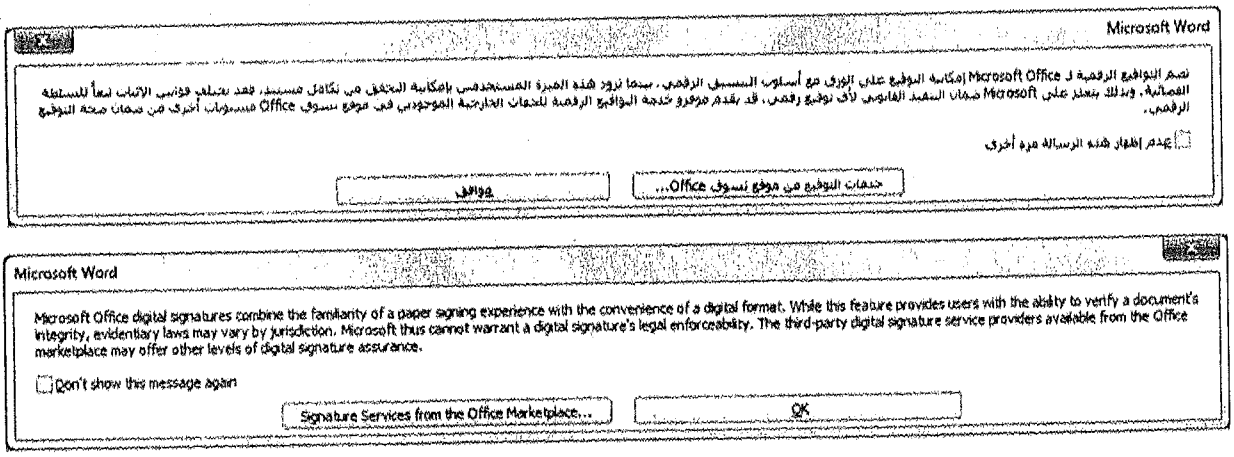
ولإضافة التواقيع بشكل تلقائي في الرسائل الصادرة، اتبع الخطوات الآتية:

4. ضمن علامة التبويب (رسالة/ *Message*)، ومن المجموعة (تضمين/ *Include*)، انقر على أيقونة (التوقيع/ *Signature*)، فتظهر لائحة أختر منها (تواقيع/ *Signatures*)، فيظهر مربع الحوار (التواقيع والقرطاسية/ *Signatures and Stationery*).
5. ضمن تبويب (توقيع البريد الإلكتروني/ *E-mail Signature*)، ومن قسم (اختيار توقيع افتراضي/ *Choose default signature*)، قم بما يأتي:
   - من مربع (حساب البريد الإلكتروني/ *E-mail account*)، انقر فوق حساب البريد الإلكتروني الذي تريد إقران التوقيع به.
   - في مربع (الرسائل الجديدة/ *New messages*)، حدد التوقيع الذي تريد تضمينه.
   - في مربع (الرد/إعادة التوجيه/ *Replies/forwards*) حدد التوقيع المطلوب، إذا أردت أن يتم تضمين التوقيع عند الرد على الرسائل أو إعادة توجيهها، وإلا، فانقر على (بلا/ *none*).
6. بعد الانتهاء من تحديد الخيارات المناسبة، انقر على زر ( موافق/ *OK*).




أما إذا أردت إضافة توقيع رقمي غير مرئي إلى ملف معين، لا إلى رسالة إلكترونية، مثل المستند (أصالة المحتوى.docx)، فاتبع الخطوات الآتية:

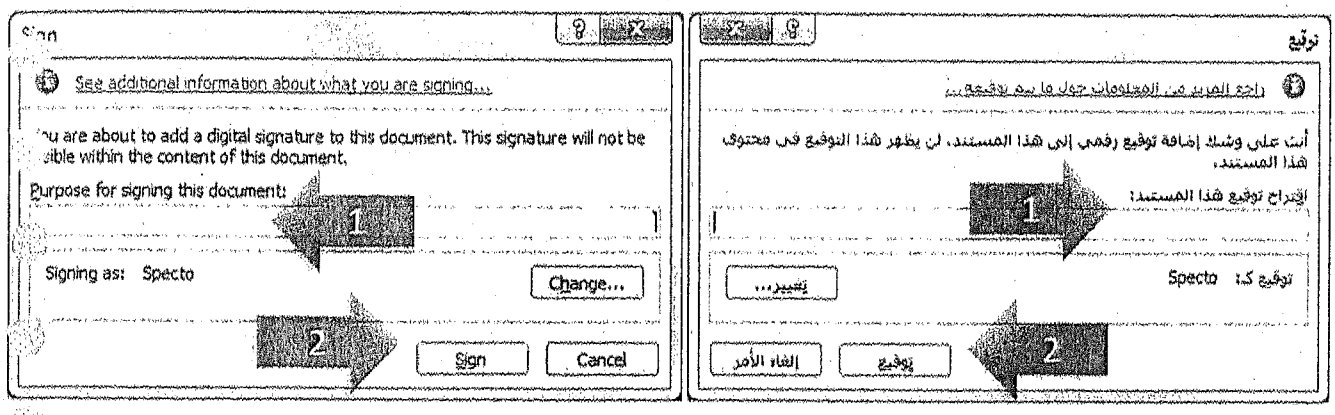
1. افتح المستند (أصالة المحتوى.docx) من مجلد ملفات العمل الخاص بك.
2. ضمن علامة التبويب (ملف/ *File*)، ومن الفئة (معلومات/ *Info*)، انقر على زر (حماية المستند/ *Protect Document*)، فتظهر لائحة.
3. من اللائحة السابقة، انقر على (إضافة توقيع رقمي/ *Add a Digital Signature*)، فتظهر رسالة تحذيرية كما في الشكل أدناه، انقر على زر (موافق/ *OK*)، فيظهر معالج الحصول على معرف رقمي.




4. انقر على زر (إنشاء المعرف الرقمي الخاص بك/ *Create your own digital ID*)، ثم انقر على زر (موافق/ *OK*)، فيظهر مربع الحوار (إنشاء معرف رقمي/ *Create a digital ID*).
5. أدخل (الاسم/ *Name*)، و(البريد الإلكتروني/ *E-Mail*)، و(المؤسسة/ *Organization*)، و(الموقع/ *Location*) في المربعات الخاصة بها، ثم انقر على زر (إنشاء/ *Create*)، فيظهر مربع الحوار (توقيع/ *Sign*).

6. في مربع (اقتراح توقيع لهذا المستند/ *Purpose for signing this document*)، اكتب التوقيع الذي تراه مناسبا، ثم انقر على زر (توقيع/ *Sign*).

7. قد تظهر رسالة تأكيد التوقيع، انقر فيها على زر (موافق/ *OK*).




وهنا تجدر الإشارة إلى أنه بعد التوقيع رقميا على الملف، يظهر الزر (عرض التواقيع/ *View Signatures*)، ويصبح الملف للقراءة فقط؛ منعا لإدخال تعديلات عليه.

### 4.1.5 الحذر من استقبال رسائل احتيالية، أو رسائل غير مرغوب فيها Be aware of the possibility of receiving fraudulent and unsolicited e-mail

ينبغي الحذر من استقبال رسائل احتيالية، أو رسائل غير مرغوب فيها؛ لأنها قد تحتوي على فيروسات، أو برامج ضارة، أو يمكن أن تكون محاولة للحصول على معلومات منك؛ لهذا كله يجب أن لا تفتح هذه الرسائل.

### 5.1.5 الخداع/التصيد Phishing

يقوم الخداع أو ما يسمى التصيد على تضليل شخص متصل بالإنترنت حول هويتك الحقيقية؛ للحصول منه على معلومات قيمة قد تكون شخصية أو مالية. ويتميز الخداع/التصيد بأنه يستخدم أسماء شركات شرعية، وأسماء حقيقية للأشخاص، لكنه يستخدم روابط ويب مزيفة.

تبدأ إحدى محاولات الخداع عبر الإنترنت بإرسال رسالة بريد إلكتروني التي تبدو مثل ملاحظة مالية من أحد المصادر الموثوق بها، كأحد البنوك، أو شركة بطاقات الاعتماد، أو تاجر ذي سمعة طيبة عبر الإنترنت. وفي هذه الرسالة، يتم توجيه المستلمين إلى أحد مواقع الويب غير الآمنة، حيث يتم مطالبتهم بتوفير معلومات شخصية، مثل رقم الحساب أو كلمة المرور، ثم يتم استخدام هذه المعلومات غالبا لسرقة الهوية.

ومن الميزات الفريدة في (Internet Explorer 9) إمكانية تطبيق (عامل تصفية Smart Screen) الذي يساعد على كشف مواقع الويب التي تقوم بالخداع، ولتشغيل عامل التصفية هذا، اتبع الخطوات الآتية:

1. افتح متصفح الإنترنت.
2. انقر على لائحة (أدوات/ *Tools*).
3. انقر على (عامل تصفية SmartScreen/ *SmartScreen Filter*)، فتظهر لائحة، انقر منها على (تشغيل عامل تصفية SmartScreen/ *Turn on SmartScreen Filter*)، ثم أغلق المتصفح.

### 6.1.5 خطر إصابة الحاسوب بالبرامج الخبيثة/الضارة The danger of infecting the computer with malware

يجب الحذر عند تنزيل الملفات المرفقة مع الرسائل الإلكترونية، وعدم فتحها؛ أو فتح الرسائل الواردة من مرسلين مجهولين، وذلك لإمكانية احتوائها على البرامج الخبيثة التي قد تسبب ضررا كبيرا لحاسوبك، حيث يتم تنشيط تلك البرامج الماكرة بمجرد فتح الرسائل أو فتح مرفقاتها، وبخاصة في الحالتين الآتيتين:

- إذا قمت بفتح مرفقات رسالة، وتحتوي تلك المرفقات على وحدات ماكرو.
- إذا قمت بفتح مرفقات رسالة، وتحتوي تلك المرفقات على ملفات (تنفيذية/ *Executable*).

لذا يجب التأكد دائما من أن برنامج مكافحة الفيروسات يعمل بشكل مناسب على جهازك، وأنه يتم تحديثه باستمرار. وإذا كنت تشك دائما بالملفات المرفقة فاحفظها على قرص تخزين مؤقت، ثم قم بتفحصها من الفيروسات قبل فتحها.

**تمرين (1-5)**

اختر الإجابة الصحيحة من بين البدائل الأربعة المذكورة لكل سؤال مما يلي: *(انظر الإجابات في ملحق الإجابات ص 70)*.

1. أي مما يأتي ينبغي استخدامه لإرسال بريد إلكتروني آمن؟
أ- صحة العناوين. ب- فك التشفير. ج- التشفير. د- التوقيع الرقمي.

2. ما السبب في استخدام التوقيع الرقمي؟
أ- لفك تشفير البريد الإلكتروني. ب- لتمكين وحدات الماكرو.
ج- للتحقق من مرسل البريد الإلكتروني. د- للسماح بإرفاق ملف مع البريد الإلكتروني.

3. ما الذي يبين لمستلم البريد الإلكتروني أن الرسالة قد أنشئت بوساطة مرسل معروف؟
أ- التوقيع الرقمي. ب- الشهادة الرقمية. ج- الجهاز الرقمي. د- الاتصال الرقمي.

4. ماذا يطلق على قيام شخص بإرسال بريد إلكتروني مدعيا أنه شخص آخر من أجل سرقة المعلومات؟
أ- تزوير العناوين. ب- فك التشفير. ج- الخداع. د- التشفير.

5. أي مما يلي يستخدم أسماء الشركات المرخصة للحصول على بيانات أمنية شخصية؟
أ- الخداع. ب- استراق النظر. ج- برامج الدعاية. د- البرامج الجذرية.

6. أي الحالات التالية يكون حاسوبك فيها عرضة للبرامج الخبيثة الضارة بشكل أكبر؟
أ- عند استعادة النسخ الاحتياطي للبيانات. ب- عند إنشاء نسخ احتياطية من البيانات.
ج- عند فتح مرفق البريد الإلكتروني. د- عند إنشاء بريد إلكتروني.

7. ماذا يطلق على رسائل البريد الإلكتروني الوهمية التي تطلب منك التحقق من تفاصيل حسابك المصرفي؟
أ- اختراق الحماية. ب- القرصنة الأخلاقية. ج- الخداع. د- الإزعاج الإلكتروني.

8. لماذا يجب عليك أن لا تفتح مرفقات بريد إلكتروني غير مرغوب فيه؟
أ- لتوفير مساحة أكبر على القرص الصلب. ب- لأنه قد يحتوي على برامج خبيثة.
ج- لعدم احتوائه على توقيع رقمي. د- لأنك قد تحتاج إلى مفتاح التشفير لفتحه.

9. أي مما يلي يمكن أن يحتوي على فيروسات أو برامج ضارة؟
أ- التواقيع الرقمية. ب- الشهادات الرقمية. ج- الجدران النارية. د- رسائل البريد الاحتيالية.

10. أي مما يلي يعد من خصائص الخداع؟
أ- سيوجهك البريد الإلكتروني إلى موقع ويب غير صحيح.
ب- سيوقف الجدار الناري جميع رسائل البريد الإلكتروني .
ج- سيتطلب فتح البريد الإلكتروني كلمة مرور.
د- سوف يكون البريد الإلكتروني من مرسل معروف.

11. أي مما يلي يعد من الممارسات الجيدة عند استخدام البريد الإلكتروني؟

أ- إعادة توجيه الرسالة التي تحتوي على برنامج تنفيذي. ب- فتح الرسالة التي تحتوي على برنامج تنفيذي.

ج- حذف الرسالة التي تحتوي برنامج تنفيذي. د- إرسال بريد إلكتروني يحتوي على برنامج تنفيذي.

12. ما الهدف من تشفير البريد الإلكتروني؟

أ- الحد من البريد الإلكتروني من مصادر غير معروفة.

ب- التأكد من أن البريد الإلكتروني لا يحتوي على برامج ضارة.

ج- إمكانية فتح البريد الإلكتروني في أي متصفح.

د- ضمان أن الشخص المقصود بالرسالة يمكنه وحده قراءة البريد الإلكتروني.

13. أنشئ توقيعا رقميا للمستند المساهمون.docx، نصه (مدرب الحاسوب).

## 2.5 المراسلة اللحظية/الفورية (Instant Messaging (IM

### 1.2.5 مفهوم المراسلة اللحظية/الفورية، واستخداماتها The term: Instant Messaging (IM) and its uses

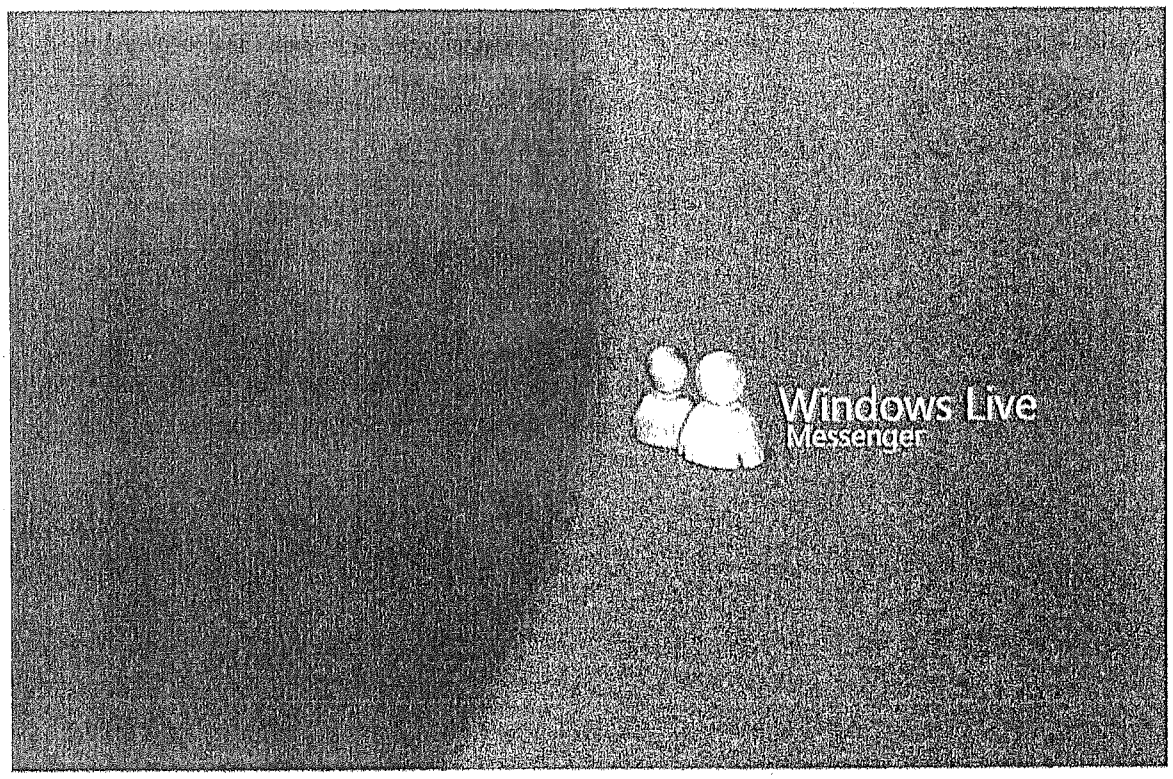
الرسائل اللحظية/الفورية هي شكل من أشكال التواصل النصي بين شخصين أو أكثر في وقت حقيقي عبر الإنترنت. ويمكن استخدام المراسلة اللحظية لإجراء دردشة ذات نص قصير مع الأصدقاء وزملاء العمل، مع إمكانية مشاركة الروابط والملفات.

بعض برامج المراسلة اللحظية تحتوي أيضا على (بروتوكول نقل الصوت عبر الإنترنت/ VoIP) وكاميرا ويب، الأمر الذي يتيح إمكانية التواصل البصري والصوتي أيضا بين المشتركين في هذه الخدمة.

توفر الرسائل الفورية إمكانية الاتصال المباشر مع الآخرين، بخلاف البريد الإلكتروني الذي يتطلب إرسال الرسالة، ثم الانتظار لحين قراءتها من قبل المستقبل ثم الرد عليها. لذلك لا يمكن القيام باتصال مباشر بين المستخدمين من خلال البريد الإلكتروني من هنا انتشرت خدمة الرسائل الفورية التي توفر اتصالا مباشرا قليل التكلفة بين المشتركين بهذه الخدمة، التي تحقق العديد من الفوائد، مثل:

- تعد اتصالا حقيقيا في الوقت، وليس فيه انتظار، وكأن الشخص المرسل إليه جالس أمامك، حيث يتم كتابة الرسالة وإرسالها للطرف الآخر لتصله مباشرة، ويقوم بالرد عليها في اللحظة نفسها. وهناك إمكانية استخدام كاميرات الويب للتواصل بالصوت والصورة بين المشتركين في هذه الخدمة من خلال التحدث المباشر مع بعضهم البعض، وهو ما يعرف بالدردشة.
- معرفة من هم متصلون بالإنترنت ومن ليسوا كذلك، ويمكن أيضا من خلال هذه الخدمة إرسال الرسائل للمشتركين في حالة عدم اتصالهم (*Off Line*) في لحظة إرسال الرسالة، وبمجرد دخوله للخدمة يتم إعلامهم بوجود الرسالة.
- تعد هذه الخدمة قليلة التكلفة إذا ما قورنت مع غيرها من طرق الاتصال.
- القدرة على مشاركة الصور والملفات المختلفة أثناء عملية الاتصال.

ومن البرامج التي توفر هذه الخدمة برنامج MSN Messenger، وبرنامج Yahoo Messenger، وبرنامج Skype.




### 2.2.5 الثغرات الأمنية في المراسلة اللحظية The security vulnerabilities of IM

على الرغم من الفوائد الكبيرة للمراسلة اللحظية، إلا أنه ينبغي أن تكون على دراية بأنك حين تستخدم المراسلة اللحظية فإن فيها بعض العيوب الأمنية التي يمكن أن يستغلها المخترقون والقراصنة، لذا ينبغي الانتباه إلى هذه العيوب والعمل على تفاديها، ومن أهم هذه العيوب الأمنية ما يلي:

- إمكانية وصول (البرامج الخبيثة/ *Malware*).
- إمكانية وصول برامج (المداخل الخلفية/ *Backdoor*).
- إمكانية الوصول إلى الملفات، وسرقة البيانات أو العبث بها..

### 3.2.5 أساليب ضمان السرية أثناء استخدام المراسلة اللحظية Methods of ensuring confidentiality while using IM

لضمان السرية أثناء استخدام المراسلة اللحظية، عليك العمل بما يأتي:

- استخدام (التشفير / *Encryption*)، وبخاصة عند إرفاق ملفات تتضمن معلومات قيمة.
- (عدم الإفصاح عن المعلومات المهمة/ *Non-disclosure of important information*).
- (الحد من مشاركة الملفات/ *Restricting file sharing*).

**تمرين (5-2)**

اختر الإجابة الصحيحة من بين البدائل الأربعة المذكورة لكل سؤال مما يلي: *(انظر الإجابات في ملحق الإجابات ص 70).*

1. ما المقصود بالمراسلة الفورية؟
أ- شكل من أشكال التواصل النصي بين شخصين أو أكثر في وقت حقيقي عبر الإنترنت.
ب- استخدام الإنترنت والتقنيات المرتبطة به في إيذاء الأشخاص الآخرين، من خلال سلوك عدواني متكرر ومتعمد.
ج- إنشاء نسخة من البيانات الهامة خوفا من ضياعها.
د- استدراج الناس لإقامة علاقات صداقة معهم للقيام بأنشطة غير أخلاقية.

2. أي مما يلي ليس شائع الاستعمال في الرسائل الفورية؟
أ- الدردشة مع عدد من الاشخاص في وقت واحد. ب- إمكانية إرفاق الملفات مع الرسائل.
ج- إجراء المعاملات المصرفية. د- الاتصالات تكون في وقت حقيقي.

3. أي مما يلي يزيد من خطر وصول المستخدمين غير المصرح لهم إلى ملفاتك الخاصة؟
أ- التشفير. ب- المراسلة الفورية. ج- الشهادة الرقمية. د- التوقيع الرقمي.

4. أي مما يلي يعد ثغرة أمنية معروفة في الرسائل الفورية؟
أ- التشفير. ب- البرمجيات الخبيثة. ج- الشهادة الرقمية. د- التوقيع الرقمي.

5. أي مما يلي يساعد على ضمان السرية عند استخدام المراسلة الفورية؟
أ- تقييد مشاركة الملفات. ب- تمكين وحدات الماكرو.
ج- ضبط إعدادات الحفظ التلقائي. د- ضبط إعدادات الإكمال التلقائي.

## 6 الإدارة الآمنة للبيانات Secure Data Management

### 1.6 النسخ الاحتياطي وتأمين البيانات Securing and Backing Up Data

#### 1.1.6 طرق ضمان الأمن المادي للأجهزة Ways of ensuring physical security of devices

هناك طرق كثيرة لضمان الأمن المادي/الفيزيائي للأجهزة الإلكترونية التي تستعملها وتقوم بتخزين بياناتك عليها، وفيما يلي أهم هذه الطرق:

- (تسجيل الدخول إلى موقع الأجهزة والمعدات والتفاصيل/ *Log equipment location and details*)، فلا يمكن لأي شخص غير مصرح له بالدخول أن يدخل إلى موقع تلك الأجهزة دون تسجيل الدخول الصحيح. كما ينبغي الاحتفاظ بسجل عن موقع كل جهاز مع التفاصيل الخاصة به كالأرقام التسلسلية ونحو ذلك.
- (استخدام أسلاك حماية/ *Use cable locks*) وذلك لتتجنب سرقتها من قبل الآخرين.
- تنفيذ تدابير (التحكم بالوصول/ *Access control*)، مثل البطاقات الممغنطة، والفحوصات الحيوية/البيومترية التي تحدثنا عنها سابقا، والتي دونها لا يستطيع أحد دخول الموقع الذي فيه الأجهزة.

#### 2.1.6 أهمية النسخ الاحتياطي The importance of having a back-up procedure

النسخ الاحتياطي يعني إنشاء نسخة من البيانات الهامة خوفا من ضياعها، وتتم عملية النسخ الاحتياطي في الكثير من المؤسسات كالبنوك والمصانع والمؤسسات العسكرية والشركات الكبيرة بطريقة تلقائية، حيث تحفظ البيانات بشكل مركزي على الشبكة، ويفضل أن تضع جميع البيانات التي تريد عمل نسخة احتياطية لها في مجلد واحد، يحتوي التاريخ الذي تمت فيه عملية النسخ الاحتياطي.

والسبب الرئيسي للنسخ الاحتياطي هو منحك الثقة بأن البيانات يمكن استرجاعها في حال فقدانها، وإعطاؤك القدرة على استعادة البيانات في حال فشل الوصول إلى الشبكة، أو خطأ مستخدم، أو إخفاق معدات الحاسوب المادية أو برامجه، أو التعرض للحريق، الأمر الذي قد يتسبب بخسارة الشركة.

وهناك نوعان من النسخ الاحتياطي هما:

- (النسخ الاحتياطي الكامل/ *Complete Backup*): أن تقوم بتخزين البيانات الموجودة كاملة مرة واحدة كل أسبوع أو شهر أو غير ذلك بشكل دوري. وهذا النوع من النسخ الاحتياطي يحتاج إلى فترات طويلة من الزمن بسبب كمية البيانات والمعلومات الهائلة التي سوف يتم تخزينها.
- (النسخ الاحتياطي التراكمي أو التزويدي/ *Incremental Backup*): أن تقوم بإجراء نسخ احتياطي للملفات التي تم تعديلها بعد آخر نسخ احتياطي، ويتم في هذه الحالة تعديل سمات الملفات بحيث يظهر أنه جرى لها نسخ احتياطي. ويعد هذا النوع فعالا ولا يحتاج إلى فترات زمنية كبيرة لتخزين البيانات، لأنه يقوم فقط بتخزين البيانات التي لم يتم تخزينها سابقا، وليس كل البيانات كما هو الحال في النسخ الاحتياطي الكامل.

ومن أهم العناصر التي ينبغي نسخها نسخا احتياطيا ما يلي:

- البيانات.
- السجلات المالية.
- محفوظات استعراض الويب، والإشارات المرجعية المفضلة.

### 3.1.6 ميزات النسخ الاحتياطي The features of a back-up procedure

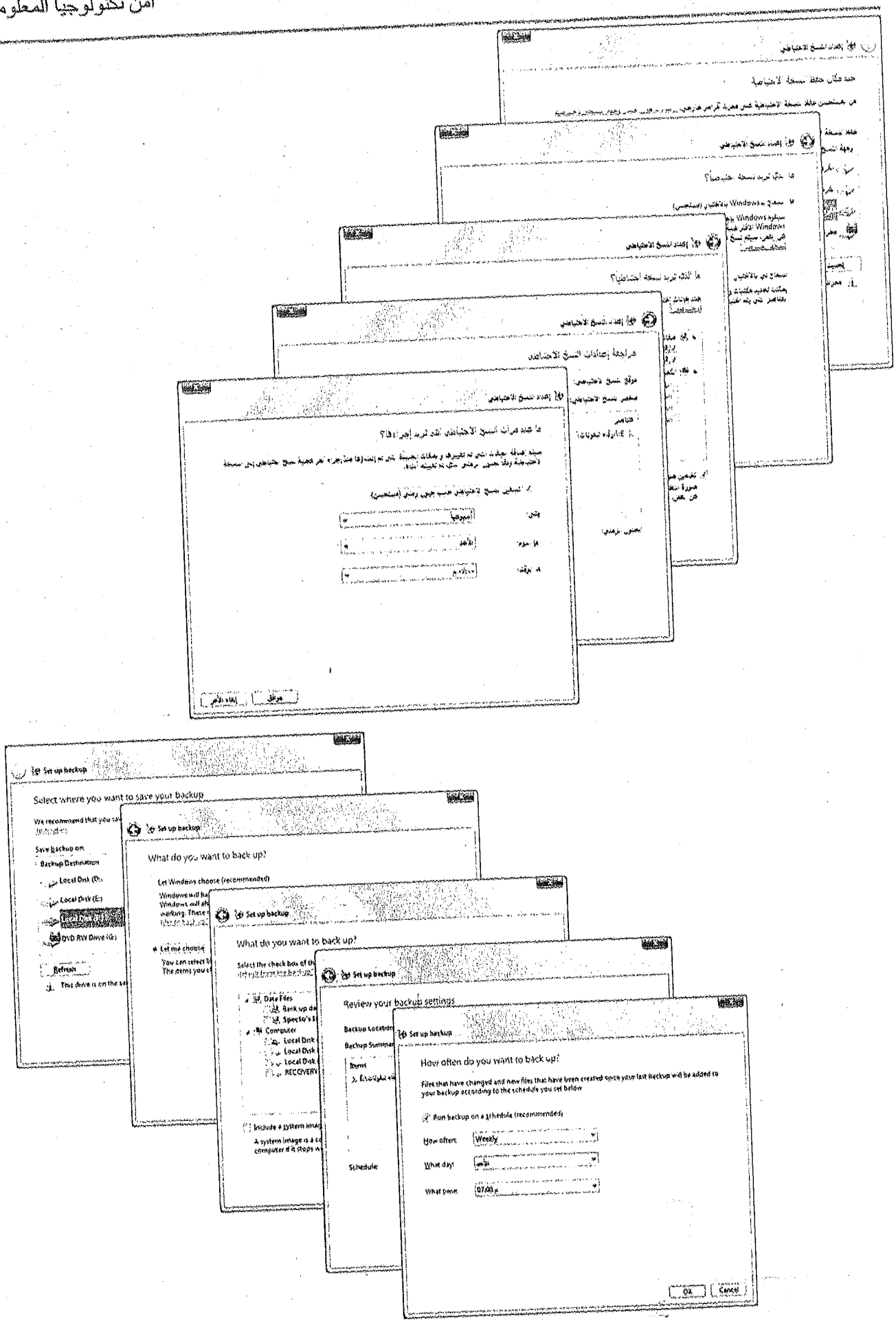
لضمان فاعلية النسخ الاحتياطي للبيانات، ينبغي مراعاة ما يلي:

- (التكرار/ *Regularity/Frequency*): وذلك من خلال القيام بعملية النسخ الاحتياطي بشكل منتظم، لأنه بإمكانك تعيين كم مرة تريد إجراء النسخ الاحتياطي.
- (الجدولة/ *Schedule*): بإمكانك تحديد جدول زمني ومواعيد محددة بدقة لعملية النسخ الاحتياطي.
- (موقع التخزين/ *Storage location*): بإمكانك تحديد موقع لتخزين البيانات عليه، حيث يتم وضع النسخة الاحتياطية إما داخل الجهاز نفسه على القرص الصلب ولكن في مكان مختلف، أو على وحدات التخزين المختلفة القابلة للنقل والإزالة، ويفضل وضع النسخ الاحتياطية بعيدا عن الحاسوب في مكان آخر مثل القرص الصلب الخارجي ونحوه خوفا من فقدان الأصل والنسخ الاحتياطية معا.

### 4.1.6 إجراء النسخ الاحتياطي للبيانات Back up data

لإجراء نسخ احتياطي لمحتويات مجلد ملفات العمل الخاص بك، اتبع الخطوات الآتية:

1. انقر على زر (ابدأ/ *Start*)، ومن اللائحة التي ستظهر، انقر على (لوحة التحكم/ *Control Panel*) لفتحها.
2. أسفل رابط (النظام والأمان/ *System and Security*)، انقر على رابط (إجراء نسخ احتياطي للكمبيوتر/ *Back up your computer*)، فتفتح نافذة (النسخ الاحتياطي والاستعادة/ *Backup and Restore*).
3. انقر على زر (إعداد النسخ الاحتياطي/ *Set up Backup*)، فيظهر معالج النسخ الاحتياطي.
4. في الخطوة الأولى، حدد مكان حفظ النسخة الاحتياطية (محرك أقراص أم الشبكة)، ثم انقر على زر (التالي/ *Next*).
5. في هذه الخطوة إما أن تبقي على الخيارات الافتراضية، وفي هذه الحالة سيقوم ويندوز بتحديد البيانات التي ينبغي نسخها، أو انقر على زر (السماح لي بالاختيار/ *Let me choose*)، وفي هذه الحالة تستطيع اختيار البيانات التي تريد نسخها دون سواها.
6. انقر على زر (التالي/ *Next*).

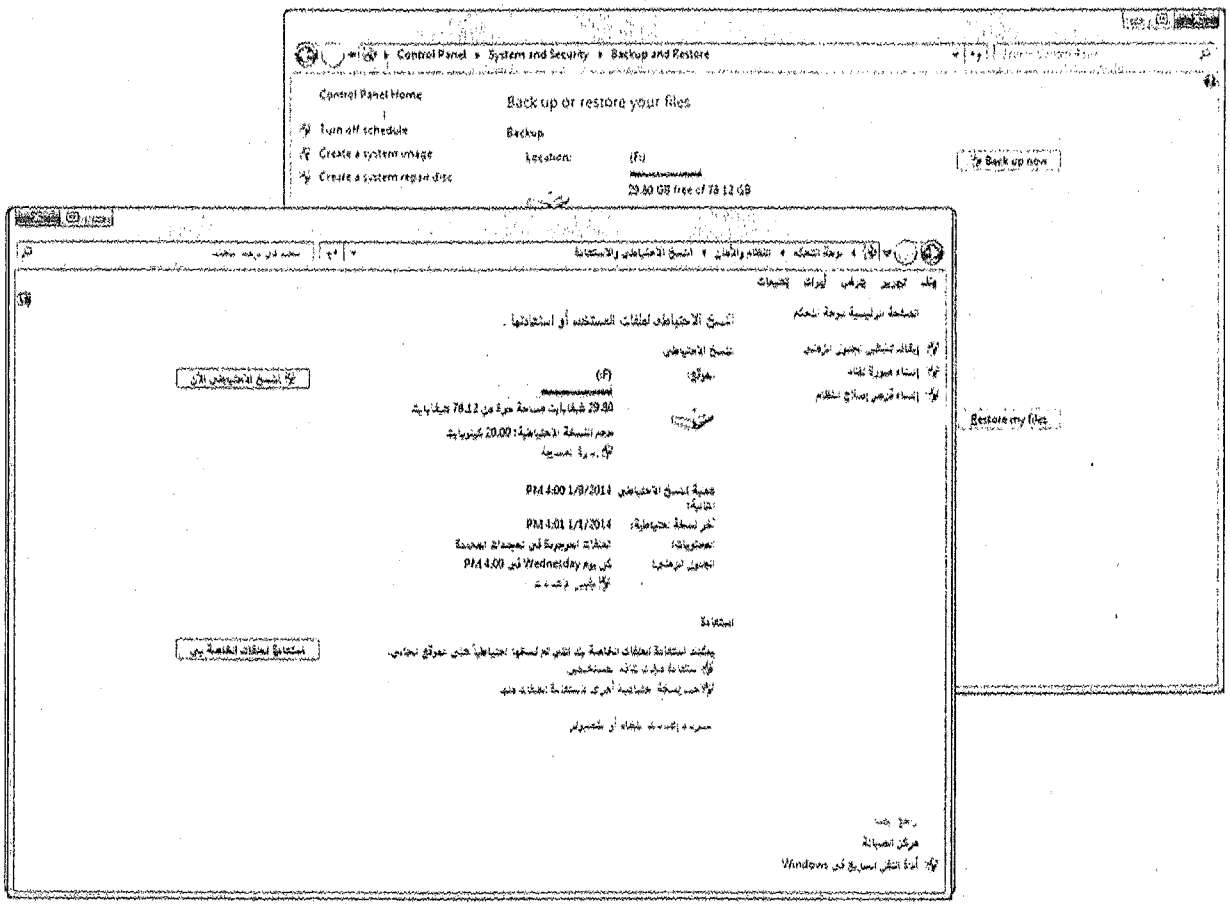

Set up backup
Select where you want to save your backup
Save backup on:
Backup Destination
Local Disk (C:)
Local Disk (E:)
DVD RW Drive (G:)
Refresh
What do you want to back up?
Let Windows choose (recommended)
Let me choose
Data Files
Computer
Local Disk
RECOVERY
Include a system image
Review your backup settings
Backup Location
Backup Summary
Items
Schedule
How often do you want to back up?
Files that have changed and new files that have been created since your last backup will be added to your backup according to the schedule you set below
Run backup on a schedule (recommended)
How often:
Weekly
What day:
What time:
07:00
OK
Cancel

7. حدد البيانات التي تريد نسخها.
8. انقر على زر (التالي/ *Next*).
9. لتحديد الجدول الزمني للنسخ الاحتياطي، انقر على (تغيير الجدول/ *Change Schedule*).
10. حدد اليوم والوقت وعدد مرات النسخ الاحتياطي التي تريد إجراءها، ثم انقر على زر (موافق/ *OK*).
11. انقر على زر (حفظ الإعدادات، وتشغيل النسخ الاحتياطي/ *Save Settings and Backup*)، وانتظر حتى تتم عملية النسخ الاحتياطي.
12. أبق نافذة (النسخ الاحتياطي والاستعادة/ *Backup and Restore*) مفتوحة إلى الدرس القادم.

### 5.1.6 استعادة وتقييم البيانات التي تم نسخها نسخا احتياطيا Restoring and validating backed up data

في كل مرة تقوم بها بعمل نسخة احتياطية باستخدام برنامج النسخ الاحتياطي الموجود في نظام التشغيل، سيتم إنشاء مجلد نسخ احتياطي منفصل في موقع تخزين النسخ الاحتياطي. ولاسترجاع الملفات التي قمت بنسخها في الدرس السابق، اتبع الخطوات الآتية:

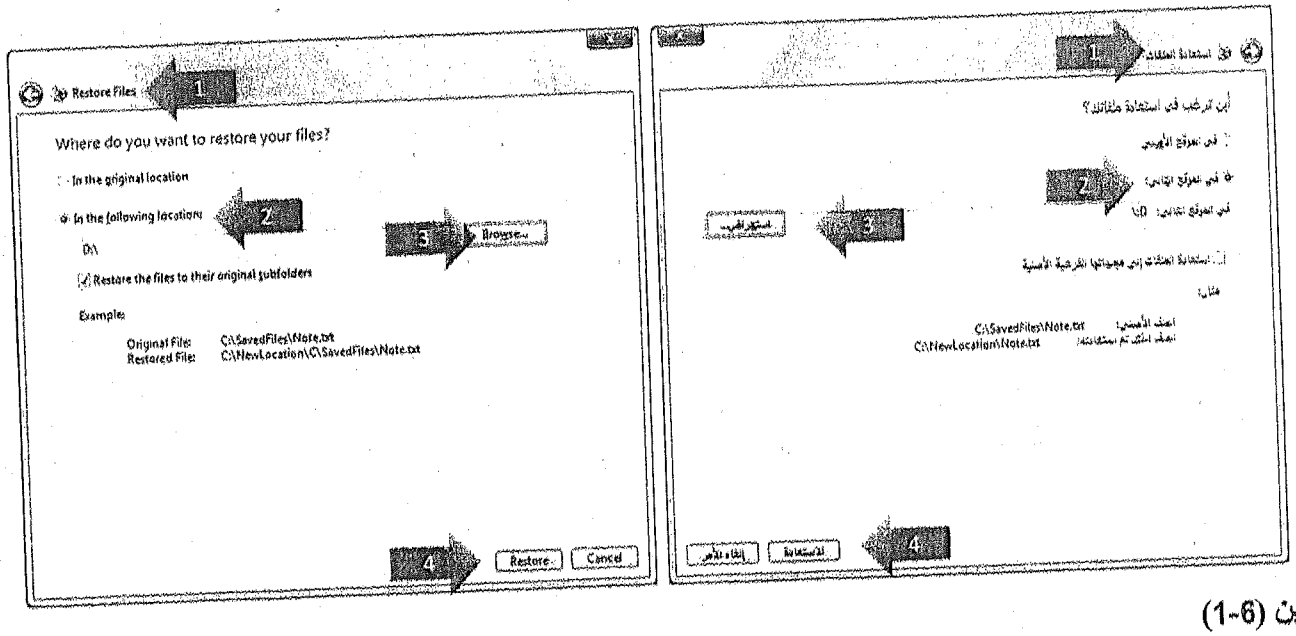
1. افتح نافذة (النسخ الاحتياطي والاستعادة/ *Backup and Restore*)، إذا لزم الأمر.
2. انقر على (استعادة الملفات الخاصة بي/ *Restore My Files*)، فتظهر نافذة (استعادة الملفات/ *Restore Files*).




3. لتحديد الملفات التي تريد استعادتها، انقر على زر (بحث/ *Search*)، أو زر (استعراض المجلدات/ *Browse for Folders*)، أو زر (استعراض الملفات/ *Browse for Files*)، وحدد تلك الملفات، ثم انقر على زر (التالي/ *Next*).

4. حدد أين ترغب في استعادة ملفاتك، هل هو في موقعها الأصلي أم في موقع آخر، ثم انقر على زر (الاستعادة/ *Restore*).

5. بعد الانتهاء من استعادة الملفات، انقر على زر (إنهاء/ *Finish*).




**تمرين (6-1)**

اختر الإجابة الصحيحة من بين البدائل الأربعة المذكورة لكل سؤال مما يلي: *(انظر الإجابات في ملحق الإجابات ص 70).*

1. أي مما يلي يمكن استخدامه لضمان الأمن المادي لحاسوبك؟
   أ- استخدام برامج مراقبة المحتوى.
   ب- تحديث برامج مكافحة الفيروسات.
   ج- إزالة مغناطيسية وسائط التخزين القابلة للإزالة.
   د- استخدام أسلاك حماية.

2. أي مما يلي ينبغي القيام به للاستفادة منه في حالة فقدان البيانات؟
   أ- إجراء النسخ الاحتياطي.
   ب- إعادة تهيئة القرص الصلب.
   ج- المراسلة الفورية.
   د- الاحتفاظ بسجل عن كل جهاز مع تفاصيله الخاصة.

3. أي مما يلي من ميزات إجراء النسخ الاحتياطي للبيانات؟
   أ- يتضمن تسجيل الدخول إلى موقع الأجهزة والمعدات والتفاصيل.
   ب- إمكانية إزالة مغناطيسية وسائط التخزين القابلة للإزالة.
   ج- إمكانية قرصنة البطاقات الائتمانية أثناء عملية النسخ الاحتياطي.
   د- إمكانية تحديد جول زمني ومواعيد محددة بدقة لعملية النسخ الاحتياطي.

4. أنشئ مصنفا جديدا يتضمن ميزانية للبيت، ثم احفظه على سطح المكتب باسم الميزانية.xlsx، ثم قم بإجراء النسخ الاحتياطي له في مجلد ملفات العمل الخاص بك.

5. قم باستعادة النسخ الاحتياطي للمصنف الميزانية الذي قمت به في السؤال السابق.

## 2.6 التدمير الآمن Secure Destruction

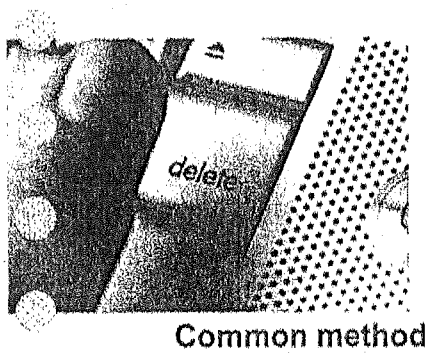
### 1.2.6 أسباب حذف البيانات من محركات الأقراص أو من الأجهزة بشكل دائم The reason for permanently deleting data from drives or devices

عندما لا تعود بحاجة أبدا إلى البيانات التي قمت بتخزينها، ينبغي أن تحذفها من أنظمة المعلومات؛ وذلك للتأكد من أنه لا يمكن الوصول إليها من قبل شخص آخر.

ولا تنس أن ملفات النسخ الاحتياطي موجودة في مجلد النسخ الاحتياطي في موقع النسخ الاحتياطي الذي اخترته. وعبر الزمن ستحتل هذه النسخ الاحتياطية مساحة كبيرة من قرص النسخ الاحتياطي. ولهذا وفي فترات زمنية معقولة يجب عليك أن تقوم بالتخلص من هذه الملفات الموجودة في النسخ الاحتياطية القديمة تخلصا كليا، وذلك للمحافظة على السرية والخصوصية، ولتفريغ مساحة على موقع النسخ الاحتياطي.

ولأسباب أمنية لا تحذف البيانات من محركات الأقراص أو من الأجهزة بشكل دائم إلا إذا كنت متأكدا من أن هذه البيانات لا يمكن استرجاعها.

### 2.2.6 الفرق بين حذف البيانات وتدميرها بشكل دائم Distinguish between deleting and permanently destroying data

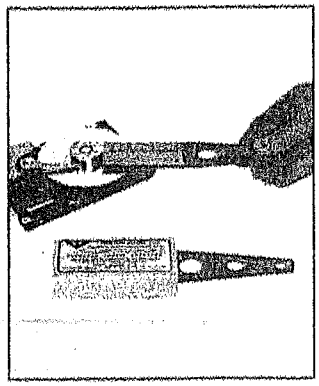



إن حذف البيانات بنقلها إلى (سلة المحذوفات/ *Recycle Bin*) لا يدمر البيانات بشكل دائم؛ لأنه – كما هو معلوم - يمكن استعادتها بسهولة.

أما حذف البيانات بشكل دائم - من خلال التقطيع/التمزيق أو إزالة المغنطة من وسائط التخزين التي عليها تلك البيانات أو الضغط على مفتاحي Shift + Delete أثناء تحديد الملفات - فإن هذا يضمن أن هذه البيانات لا يمكن استرجاعها.

### 3.2.6 وسائل تدمير البيانات بشكل دائم Common methods of permanently destroying data

- (التمزيق/التقطيع/ *Shredding*)، وذلك بتكسيرها وتقطيعها وبخاصة إذا كانت هذه البيانات مخزنة على أقراص مدمجة أو على أقراص رقمية، لأنه يتوافر آلات خاصة لتكسيرها فلا يمكن قراءتها ولا استرجاع ما تحتويه من بيانات.
- (تدمير محرك الأقراص أو الوسائط/ *Drive/Media destruction*) تدميرا ماديا بحيث لا يمكن إصلاحها.
- (استخدام أدوات تدمير البيانات/ *Using data destruction utilities*) التي تعمل على تدمير البيانات الموجودة على محرك الأقراص أو وسائط التخزين الأخرى.
- (إزالة المغنطة/ *Degaussing*) من وسائط التخزين؛ لأنه يترك المجالات المغناطيسية على القرص في أنماط عشوائية تجعل البيانات السابقة غير قابل للاسترداد.



**تمرين (6-2)**

اختر الإجابة الصحيحة من بين البدائل الأربعة المذكورة لكل سؤال مما يلي: *(انظر الإجابات في ملحق الإجابات ص 70).*

1. أي مما يلي هو أهم سبب لحذف البيانات بشكل دائم من الجهاز؟
أ- للتأكد من أن البيانات لا يمكن إلغاء حذفها وفي الوقت نفسه لا يمكن استردادها.
ب- لضمان مسح سطح المكتب، وتنظيفه أولا بأول.
ج- لضمان أن البيانات يمكن استردادها فقط من قبل المستخدمين المصرح لهم بذلك.
د- للتأكد من طلب مفتاح التشفير لاسترداد البيانات.

2. أي العبارات الآتية صحيحة فيما يتعلق بالفرق بين حذف البيانات وتدميرها؟
أ- عند حذف البيانات تضمن أنه لا يمكن الوصول إليها من قبل شخص آخر.
ب- عند تدمير البيانات تضمن أنه يمكن الوصول إليها من قبل شخص آخر.
ج- سوف يتم تخزين البيانات في سلة المحذوفات في حال حذفها.
د- تدمير البيانات يعني حذفها إلى سلة المحذوفات.

3. أي مما يلي هو وسيلة من وسائل تدمير البيانات بشكل دائم؟
أ- نقل البيانات إلى سلة المحذوفات.
ب- التلاعب بملف البيانات.
ج- إزالة مغناطيسية وسائط التخزين القابلة للنقل.
د- تعديل البيانات.

4. أي مما يلي لا يضمن تدميرا دائما للبيانات؟
أ- تكسير القرص المدمج.
ب- إعادة تهيئة القرص الصلب.
ج- إزالة مغناطيسية القرص الصلب.
د- نقل البيانات إلى سلة المحذوفات.

## ملحق إجابات الأسئلة، والمراجع

- **إجابات أسئلة التمرين (1-1) الموجود ص (3):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | أ- الجريمة الإلكترونية. |
| 2. | ج- الخداع. |
| 3. | ب- الاختراق المصرح به للنظام. |
| 4. | أ- مزودو الخدمة. |
| 5. | ب- معرفة نص كلمة المرور. |
| 6. | ج- الشهادات الرقمية. |
| 7. | أ- البيانات التي تمت معالجتها. |
| 8. | د- الاختراق الأخلاقي. |

- **إجابات أسئلة التمرين (1-2) الموجود ص (6):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | د- منع القرصنة الأخلاقية. |
| 2. | د- التشفير. |
| 3. | ب- الثقة بمصادر المعلومات، وأنها معلومات صحيحة وكاملة. |
| 4. | أ- حماية المعلومات الشخصية من الوصول غير المصرح به. |
| 5. | ج- هذه الإرشادات مهمة لأنها توفر معيارا للمستخدمين كي يتبعوه. |
| 6. | أ- الكمال. |
| 7. | ب- لتشجيع الوصول الخارجي إلى الشبكة. |
| 8. | أ- 1995. |
| 9. | د- السرية. |

- **إجابات أسئلة التمرين (1-3) الموجود ص (9):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | أ- التلاعب بالأشخاص واستغلالهم. |
| 2. | د- تعطيل الجدار الناري. |
| 3. | ب- استخدام تقنية استعادة المعلومات من مواد مهملة. |
| 4. | أ- سرقة الهوية. |
| 5. | ب- القيام بمكالمات صوتية ومرئية مع الأصدقاء باستخدام شبكة الانترنت. |
| 6. | ب- انتحال الشخصية لتحقيق مكاسب ذاتية. |
| 7. | ب- استرجاع المعلومات من قرص صلب تم التخلص منه. |

- **إجابات أسئلة التمرين (1-4) الموجود ص (16):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | ب- سيمنعك من استخدام كافة ميزات ذلك الملف. |
| 2. | ب- البيانات لا تزال عرضة للتهديدات ممن يملكون مفتاح فك التشفير. |

- **إجابات أسئلة التمرين (2-1) الموجود ص (17):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | ب- البرمجيات الخبيثة. |
| 2. | ج- البرامج الخبيثة. |
| 3. | ب- حصان طروادة. |
| 4. | د- البرمجيات الجذرية. |
| 5. | ج- المداخل الخلفية. |

- **إجابات أسئلة التمرين (2-2) الموجود ص (19):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | أ- برامج التجسس. |
| 2. | ب- شبكات الروبوت. |
| 3. | أ- لا يتطلب الأمر عملا بشريا لتكرار الفيروس نفسه. |
| 4. | د- هي نوع من البرمجيات الخبيثة التي تقوم بجمع معلومات عن عادات مستخدمي المتصفح دون موافقتهم. |
| 5. | ج- ذاتية التكرار. |

- **إجابات أسئلة التمرين (2-3) الموجود ص (25):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | ج- قد يمنع ميزات أمنية لتطبيقات أخرى. |

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 2. | ب- الحجر. |
| 3. | ب- لإصلاح الأخطاء أو المخاطر الأمنية في التطبيق. |
| 4. | أ- تحمي أنظمة الحاسوب من البرامج الخبيثة. |
| 5. | ب- تتطلب تحديثات منتظمة. |
| 6. | ب- يمكن استعادتها من الحجر إذا لزم الأمر. |
| 7. | ج- تحديث برنامج مكافحة الفيروسات. |

- **إجابات أسئلة التمرين (3-1) الموجود ص (28):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | د- توفر وصولا خاصا آمنا إلى الشبكة. |
| 2. | ب- الشبكة المحلية LAN. |
| 3. | ج- الشبكة الواسعة WAN. |
| 4. | د- الشبكة الافتراضية الخاصة VPN. |
| 5. | أ- السماح للعامة أن يصلوا وأن يعدلوا جميع البيانات على الشبكة. |
| 6. | د- عدد من أجهزة الحاسوب المرتبطة معا في الغرفة نفسها. |
| 7. | ب- الجدار الناري. |

- **إجابات أسئلة التمرين (3-2) الموجود ص (30):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | ب- لربط الحاسوب بشبكة سلكية. |
| 2. | د- هي أقل عرضة للتهديدات الأمنية من الشبكة السلكية. |
| 3. | د- سوف تكون هناك حاجة إلى وصول مستتر للوصول إلى الملفات على الشبكة. |

- **إجابات أسئلة التمرين (3-3) الموجود ص (34):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | ب- استخدام كلمات مرور. |
| 2. | د- الوصول المحمي بالدقة اللاسلكية WPA. |
| 3. | د- التنصت اللاسلكي من الأطراف غير المصرح لهم. |
| 4. | أ- سوف تحتاج إلى كلمة المرور للوصول إلى الشبكة. |
| 5. | أ- سيتمكن المستخدمون غير المصرح لهم من الوصول إلى ملفات تعريف ارتباط الإنترنت المخزنة في المتصفح. |
| 6. | أ- تعيين كلمة مرور. |

- **إجابات أسئلة التمرين (3-4) الموجود ص (37):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | د- إنشاء حساب يتطلب اسم مستخدم وكلمة مرور. |
| 2. | أ- اسم مستخدم، وكلمة مرور. |
| 3. | ج- يجب تغييرها بانتظام. |
| 4. | ج- لحماية الحواسيب من الاستخدام غير المسموح به. |
| 5. | د- Pass@Word456. |
| 6. | ب- المسح الضوئي للعين. |

- **إجابات أسئلة التمرين (4-1) الموجود ص (48):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | ج- تأكد أن موقع الويب هو موقع ويب آمن. |
| 2. | د- مواقع محركات البحث. |
| 3. | ب- https. |
| 4. | ب- تزوير العناوين. |
| 5. | ج- تزوير العناوين. |
| 6. | ب- الشهادات الرقمية. |
| 7. | ب- الشهادة الرقمية. |
| 8. | د- عند تسجيل الدخول إلى الشبكة الخاصة الافتراضية VPN. |
| 9. | أ- ستنتهي من تعبئة النماذج عبر الإنترنت بشكل أسرع. |
| 10. | ب- الكوكيز. |
| 11. | ب- متصفح الإنترنت. |
| 12. | ب- بيانات الإكمال التلقائي. |
| 13. | ج- برامج تصفية الإنترنت. |
| 14. | ج- ضمان عدم تقييد المحتوى المشروع. |

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 2. | ب- الحجر. |
| 3. | ب- لإصلاح الأخطاء أو المخاطر الأمنية في التطبيق. |
| 4. | أ- تحمي أنظمة الحاسوب من البرامج الخبيثة. |
| 5. | ب- تتطلب تحديثات منتظمة. |
| 6. | ب- يمكن استعادتها من الحجر إذا لزم الأمر. |
| 7. | ج- تحديث برنامج مكافحة الفيروسات. |

- **إجابات أسئلة التمرين (3-1) الموجود ص (28):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | د- توفر وصولا خاصا آمنا إلى الشبكة. |
| 2. | ب- الشبكة المحلية LAN. |
| 3. | ج- الشبكة الواسعة WAN. |
| 4. | د- الشبكة الافتراضية الخاصة VPN. |
| 5. | أ- السماح للعامة أن يصلوا وأن يعدلوا جميع البيانات على الشبكة. |
| 6. | د- عدد من أجهزة الحاسوب المرتبطة معا في الغرفة نفسها. |
| 7. | ب- الجدار الناري. |

- **إجابات أسئلة التمرين (3-2) الموجود ص (30):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | ب- لربط الحاسوب بشبكة سلكية. |
| 2. | د- هي أقل عرضة للتهديدات الأمنية من الشبكة السلكية. |
| 3. | د- سوف تكون هناك حاجة إلى وصول مستتر للوصول إلى الملفات على الشبكة. |

- **إجابات أسئلة التمرين (3-3) الموجود ص (34):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | ب- استخدام كلمات مرور. |
| 2. | د- الوصول المحمي بالدقة اللاسلكية WPA. |
| 3. | د- التنصت اللاسلكي من الأطراف غير المصرح لهم. |
| 4. | أ- سوف تحتاج إلى كلمة المرور للوصول إلى الشبكة. |
| 5. | أ- سيتمكن المستخدمون غير المصرح لهم من الوصول إلى ملفات تعريف ارتباط الإنترنت المخزنة في المتصفح. |
| 6. | أ- تعيين كلمة مرور. |

- **إجابات أسئلة التمرين (3-4) الموجود ص (37):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | د- إنشاء حساب يتطلب اسم مستخدم وكلمة مرور. |
| 2. | أ- اسم مستخدم، وكلمة مرور. |
| 3. | ج- يجب تغييرها بانتظام. |
| 4. | ج- لحماية الحواسيب من الاستخدام غير المسموح به. |
| 5. | د- Pass@Word456. |
| 6. | ب- المسح الضوئي للعين. |

- **إجابات أسئلة التمرين (4-1) الموجود ص (48):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | ج- تأكد أن موقع الويب هو موقع ويب آمن. |
| 2. | د- مواقع محركات البحث. |
| 3. | ب- https. |
| 4. | ب- تزوير العناوين. |
| 5. | ج- تزوير العناوين. |
| 6. | ب- الشهادات الرقمية. |
| 7. | ب- الشهادة الرقمية. |
| 8. | د- عند تسجيل الدخول إلى الشبكة الخاصة الافتراضية VPN. |
| 9. | أ- ستنتهي من تعبئة النماذج عبر الإنترنت بشكل أسرع. |
| 10. | ب- الكوكيز. |
| 11. | ب- متصفح الإنترنت. |
| 12. | ب- بيانات الإكمال التلقائي. |
| 13. | ج- برامج تصفية الإنترنت. |
| 14. | ج- ضمان عدم تقييد المحتوى المشروع. |

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 15. | ب- للتصفح على موقع ويب غير مألوف. |

- **إجابات أسئلة التمرين (4-2) الموجود ص (51):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | أ- خشية سرقتها أو سوء استخدامها. |
| 2. | د- رقم هاتفك الخلوي. |
| 3. | أ- الهويات المزيفة. |
| 4. | ج- استدراج الناس لإقامة علاقات صداقة معهم للقيام بأنشطة غير أخلاقية. |

- **إجابات أسئلة التمرين (5-1) الموجود ص (57):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | ج- التشفير. |
| 2. | ج- للتحقق من مرسل البريد الإلكتروني. |
| 3. | أ- التوقيع الرقمي. |
| 4. | ج- الخداع. |
| 5. | أ- الخداع. |
| 6. | ج- عند فتح مرفق البريد الإلكتروني. |
| 7. | ج- الخداع. |
| 8. | ب- لأنه قد يحتوي على برامج خبيثة. |
| 9. | د- رسائل البريد الاحتيالية. |
| 10. | أ- سيوجهك البريد الإلكتروني إلى موقع ويب غير صحيح. |
| 11. | ج- حذف الرسالة التي تحتوي برنامج تنفيذي. |
| 12. | د- ضمان أن الشخص المقصود بالرسالة يمكنه وحده قراءة البريد الإلكتروني. |

- **إجابات أسئلة التمرين (5-2) الموجود ص (60):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | أ- شكل من أشكال التواصل النصي بين شخصين أو أكثر في وقت حقيقي عبر الإنترنت. |
| 2. | ج- إجراء المعاملات المصرفية. |
| 3. | ب- المراسلة الفورية. |
| 4. | ب- البرمجيات الخبيثة. |
| 5. | أ- تقييد مشاركة الملفات. |

- **إجابات أسئلة التمرين (6-1) الموجود ص (65):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | د- استخدام أسلاك الحماية. |
| 2. | أ- إجراء النسخ الاحتياطي. |
| 3. | د- إمكانية تحديد جول زمني ومواعيد محددة بدقة لعملية النسخ الاحتياطي. |

- **إجابات أسئلة التمرين (6-2) الموجود ص (67):**

| رقم السؤال | الإجابة الصحيحة |
|---|---|
| 1. | أ- للتأكد من أن البيانات لا يمكن إلغاء حذفها وفي الوقت نفسه لا يمكن استردادها. |
| 2. | ج- سوف يتم تخزين البيانات في سلة المحذوفات في حال حذفها. |
| 3. | ج- إزالة مغناطيسية وسائط التخزين القابلة للنقل. |
| 4. | د- نقل البيانات إلى سلة المحذوفات. |

## المراجع


- الرخصة الدولية لقيادة الحاسوب، الإصدار الخامس، عرفات رشاد ياسين، 2010، المطابع المركزية.
- تعليمات Windows 7، شركة ميكروسوفت، 2009م.
- تعليمات Microsoft Office 2010، شركة ميكروسوفت، 2010م.
- http:office.microsoft.comar-sadefault.asxp?ofcresset=1
- http:ar.wikipedia.org