# CHAPTER 9

**INFORMATION SYSTEMS CONTROLS FOR SYSTEMS RELIABILITY – Part 2: Confidentiality and Privacy**

**SUGGESTED ANSWERS TO DISCUSSION QUESTIONS**

**9.1** **From the viewpoint of the customer, what are the advantages and disadvantages to the opt-in versus the opt-out approaches to collecting personal information? From the viewpoint of the organization desiring to collect such information?**

For the consumer, opt-out represents many disadvantages because the consumer is responsible for explicitly notifying every company that might be collecting the consumer’s personal information and tell the company to stop collecting his or her personal data. Consumers are less likely to take the time to opt-out of these programs and even if they do decide to opt-out, they may not know of all of the companies that are capturing their personal information.

For the organization collecting the data, opt-out is an advantage for the same reasons it is a disadvantage to the consumer, the organization is free to collect all the information they want until explicitly told to stop.

For the consumer, opt-in provides more control to protect privacy, because the consumer must explicitly give permission to collect personal data. However, opt-in is not necessarily bad for the organization that is collecting information because it results in a database of people who are predisposed to respond favorably to communications and marketing offers.

**9.2** **What risks, if any, does offshore outsourcing of various information systems functions pose to satisfying the principles of confidentiality and privacy?**

Outsourcing is and will likely continue to be a topic of interest. One question that may facilitate discussion is to ask the students if once a company sends some operations offshore, does the outsourcing company still have legal control over their data or do the laws of the off shore company dictate ownership? Should the outsourcing company be liable in this country for data that was lost or compromised by an outsourcing offshore partner?

Data security and data protection are rated in the top ten risks of offshore outsourcing by CIO News. Compliance with The Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act (SOX) are of particular concern to companies outsourcing work to offshore companies.

Since offshore companies are not required to comply with HIPAA, companies that contract with offshore providers do not have any enforceable mechanisms in place to protect and safeguard Protected Health Information; i.e., patient health information, as required by HIPAA. They essentially lose control of that data once it is processed by an offshore provider. Yet they remain accountable for HIPAA violations.

**9.3 Should organizations permit personal use of e-mail systems by employees during working hours?**

Since most students will encounter this question as an employee and as a future manager, the concept of personal email use during business hours should generate significant discussion.

Organizations may want to restrict the use of email because of the following potential problems:

* + Viruses are frequently spread through email and although a virus could infect company computers through a business related email, personal email will also expose the company to viruses and therefore warrant the policy of disallowing any personal emails.
  + The risk that employees could overtly or inadvertently release confidential company information through personal email. Once the information is written in electronic form it is easy and convenient for the recipient to disburse that information.

One question that may help facilitate discussion is to ask whether personal emails are any different than personal phone calls during business hours.

**9.4 What privacy concerns might arise from the use of biometric authentication techniques? What about the embedding of RFID tags in products such as clothing? What other technologies might create privacy concerns?**

Many people may view biometric authentication as invasive. That is, in order to gain access to a work related location or data, they must provide a very personal image of part of their body such as their retina, finger or palm print, their voice, etc. Providing such personal information may make some individuals fearful that the organization collecting the information can use it to monitor them. In addition, some biometrics can reveal sensitive information. For example, retina scans may detect hidden health problems – and employees may fear that such techniques will be used by employers and insurance companies to discriminate against them.

RFID tags that are embedded or attached to a person’s clothing would allow anyone with that particular tag’s frequency to track the exact movements of the “tagged” person. For police tracking criminals that would be a tremendous asset, but what if criminals were tracking people who they wanted to rob or whose property they wanted to rob when they knew the person was not at home.

Cell phones and social networking sites are some of the other technologies that might cause privacy concerns. Most cell phones have GPS capabilities that can be used to track a person’s movement – and such information is often collected by “apps” that then send it to advertisers. GPS data is also stored by cell phone service providers.

Social networking sites are another technology that creates privacy concerns. The personal information that people post on social networking sites may facilitate identity theft.

**9.5 What do you think an organization’s duty or responsibility should be to protect the privacy of its customers’ personal information? Why?**

Some students will argue that managers have an ethical duty to “do no harm” and, therefore, should take reasonable steps to protect the personal information their company collects from customers.

Others will argue that it should be the responsibility of consumers to protect their own personal information.

Another viewpoint might be that companies should pay consumers if they divulge personal information, and that any such purchased information can be used however the company wants.

**9.6 Assume you have interviewed for a job online and now receive an offer of employment. The job requires you to move across the country. The company sends you a digital signature along with the contract. How does this provide you with enough assurance to trust the offer so that you are willing to make the move?**

A digital signature provides the evidence needed for non-repudiation, which means you can enforce the contract in court, if necessary. The reason is that the digital signature provides the evidence necessary to prove that your copy of the contract offer is identical to the company’s and that it was indeed created by the company.

The digital signature is a hash of the contract, encrypted with the creator’s (in this case, the company’s) private key. Decrypting the signature with the company’s public key produces the hash of the contract. If you hash your copy of the contract and it matches the hash in the digital signature, it proves that the contract was indeed created by the company (because decrypting the digital signature with the company’s private key produced a hash sent by and created by the company). The fact that the two hashes match proves that you have not tampered with your copy of the contract – it matches, bit for bit, the version created by the company.

**SUGGESTED SOLUTIONS TO THE PROBLEMS**

**9.1 Match the terms with their definitions**:

|  |  |
| --- | --- |
| 1. \_d\_\_ Virtual Private Network (VPN) | a. A hash encrypted with the creator’s private key |
| 2. \_k\_\_ Data Loss Prevention (DLP) | b. A company that issues pairs of public and private keys and verifies the identity of the owner of those keys. |
| 3. \_a\_\_ Digital signature | c. A secret mark used to identify proprietary information. |
| 4. \_j\_\_ Digital certificate | d. An encrypted tunnel used to transmit information securely across the Internet. |
| 5. \_e\_\_ Data masking | e. Replacing real data with fake data. |
| 6. \_p\_\_ Symmetric encryption | f. Unauthorized use of facts about another person to commit fraud or other crimes. |
| 7. \_\_h\_ Spam | g. The process of turning ciphertext into plaintext. |
| 8. \_\_i\_ Plaintext | h. Unwanted e-mail. |
| 9. \_l\_\_ Hashing | i. A document or file that can be read by anyone who accesses it. |
| 10. \_m\_\_ Ciphertext | j. Used to store an entity’s public key, often found on web sites. |
| 11. \_r\_\_Information rights management (IRM) | k. A procedure to filter outgoing traffic to prevent confidential information from leaving. |
| 12. \_b\_ Certificate authority | l. A process that transforms a document or file into a fixed length string of data. |
| 13. \_q\_\_ Non-repudiation | m. A document or file that must be decrypted to be read. |
| 14. \_c\_\_ Digital watermark | n. A copy of an encryption key stored securely to enable decryption if the original encryption key becomes unavailable. |
| 15. \_o\_\_ Asymmetric encryption | o. An encryption process that uses a pair of matched keys, one public and the other private. Either key can encrypt something, but only the other key in that pair can decrypt it. |
| 16. \_n\_ Key escrow | p. An encryption process that uses the same key to both encrypt and decrypt. |
|  | q. The inability to unilaterally deny having created a document or file or having agreed to perform a transaction. |
|  | r. Software that limits what actions (read, copy, print, etc.) that users granted access to a file or document can perform. |

**9.2 Cost-effective controls to provide confidentiality require valuing the information that is to be protected. This involves classifying information into discrete categories. Propose a minimal classification scheme that could be used by any business, and provide examples of the type of information that would fall into each of those categories.**

There is no single correct solution for this problem. Student responses will vary depending on their experience with various businesses. One minimal classification scheme could be highly confidential or top-secret, confidential or internal only, and public. The following table lists some examples of items that could fall into each basic category.

|  |  |  |
| --- | --- | --- |
| **Highly Confidential**  **(Top Secret)** | **Confidential**  **(Internal)** | **Public** |
| Research Data | Payroll | Financial Statements |
| Product Development Data | Cost of Capital | Security and Exchange Commission Filings |
| Proprietary Manufacturing Processes | Tax data | Marketing Information |
| Proprietary Business Processes | Manufacturing Cost Data | Product Specification Data |
| Competitive Bidding Data | Financial Projections | Earnings Announcement Data |

**9.3** **Download a hash calculator that can create hashes for both files and text input. Use it to create SHA-256 (or any other hash algorithm your instructor assigns) hashes for the following:**

**a. A document that contains this text: “Congratulations! You earned an A+”**

**b. A document that contains this text: “Congratulations! You earned an A-”**

**c. A document that contains this text: “Congratulations! You earned an a-”**

**d. A document that contains this text: “Congratulations! You earned an A+” (this message contains two spaces between the exclamation point and the capital letter Y).**

**e. Make a copy of the document used in step a, and calculate its hash value.**

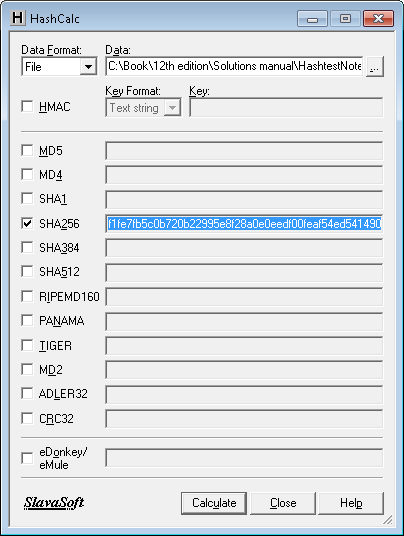
**Solution:** Slavasoft.com has a free hash calculator called “HashCalc” that will allow you to generate a number of different hashes, including SHA-256. It is an easy tool to install and use.

To use it, simply open the program and then point to the file that you wish to hash:

Step 1: Click on the button to find your file

Step 2: Select one or more hash values by clicking on the box to the left of that hash

Step 3: Click the “Calculate” button



The exact hash values will differ depending upon the program used to create the text documents (e.g., Word versus Notepad). Below are SHA-256 hashes of files created in Word for Windows 2007 on a computer running Windows 7:

Part a: 866af63d78f6546b95e48919e9007309b1cd646da384035c5e6f4790b90cbf24

Part b: b537d8ba8de6331b7db1e9d7a446fd447c0a2b259c562bf4bc0caa98e4df383d

Part c: 826a17a341d37aece1e30273997a50add1f832a8b7aac18f530771412e3f919a

Part d: 2250234c61a4ccd1a1dbf0da3ea40319baee3c27c172819c26ae2b0f906482a2

And here are the SHA-256 hash values of the same files created in NotePad:

Part a: 414b6e3799ccd6ff1fe7fb5c0b720b22995e8f28a0e0eedf00feaf54ed541490

Part b: 90f373ea52c567304a6630ecef072471727e9bfda1514a7ed4988fc7884ffc3b

Part c: 327194a7459ab8f7db9894bd76430d8e9c7c3ce8fbac5b4a8fbc842ab7d91ec4

Part d: 8c47c910a0aa4f8f75695a408e757504e476b2e02a4dd5dfb4a527f3af05df22

Notice how any change, no matter how small results in a different hash value:

* changing a “+” to a “-“ sign (compare hashes for parts a and part b)
* changing from uppercase “A” to lowercase “a” (compare hashes for parts b and c)
* inserting a space (compare hashes for parts a and d)

This is the reason that hashes are so important – they provide a way to test the “integrity” of a file. If two files are supposed to be identical, but they have different hash values, then one of them has been changed.

The solution to part e depends upon whether you are using a simple text editor like NotePad or a more powerful word processing program like Word. If you are using NotePad, then simply opening the file for part a and saving it with the name part e generates an exact copy of the original file, as evidenced by the identical hash values:

* NotePad file for part a: 414b6e3799ccd6ff1fe7fb5c0b720b22995e8f28a0e0eedf00feaf54ed541490
* NotePad file for part e: 414b6e3799ccd6ff1fe7fb5c0b720b22995e8f28a0e0eedf00feaf54ed541490

If you are using Word, then the “Save As” command will generate a document that has the same text, but a different hash value because Word incorporates system data when saving the file:

* Word document for part a: 866af63d78f6546b95e48919e9007309b1cd646da384035c5e6f4790b90cbf24
* Word document for part e: 03f77774bfab4cbb1b1660cb3cd7fc978818506e0ed17aca70daa146b54c06c1

But, if you right-click on the original document, select “Copy” and then paste it into the same directory, you get a file that is marked as a copy: “Problem 9-3 part a –Copy.docx” – which has the same SHA-256 value as the original: 866af63d78f6546b95e48919e9007309b1cd646da384035c5e6f4790b90cbf24

The point of this exercise is to show the power of using simple utilities like Notepad – you can play with a document and restore it. In contrast, playing with a document using more powerful programs like Word will leave tell-tale traces that the document was altered.

NOTE: simply opening a Word document to read it and then closing it or saving it (not Save As) will **not** alter the hash value.

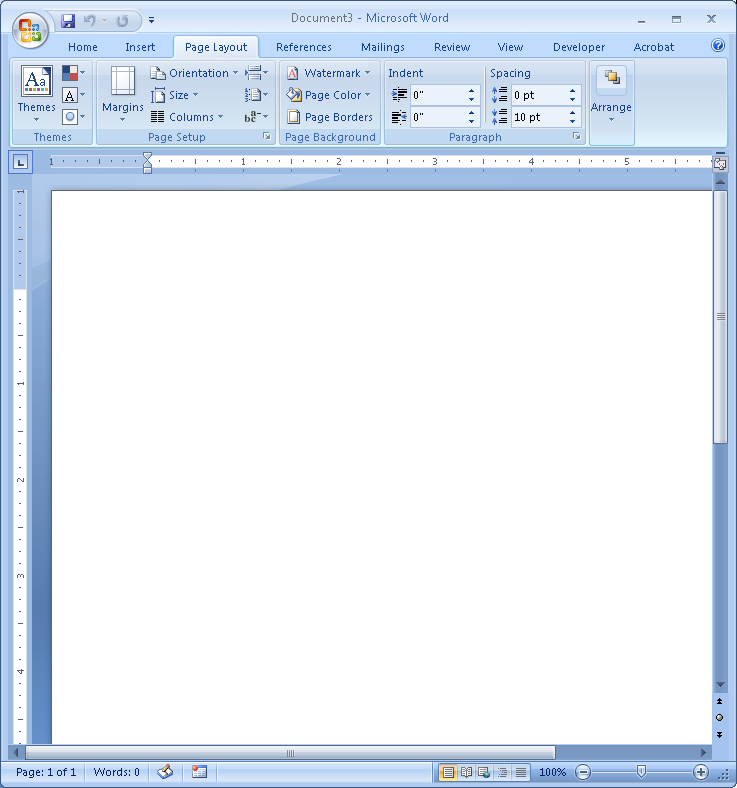
**f. Hash any multiple-page text file on your computer.**

no matter how large the file, the hash will be the same length as the hashes for parts a-e.

**9.4** **Accountants often need to print financial statements with the words “CONFIDENTIAL” or “DRAFT” appearing in light type in the background.**

**a. Create a watermark with the word “CONFIDENTIAL” in a Word document. Print out a document that displays that watermark.**

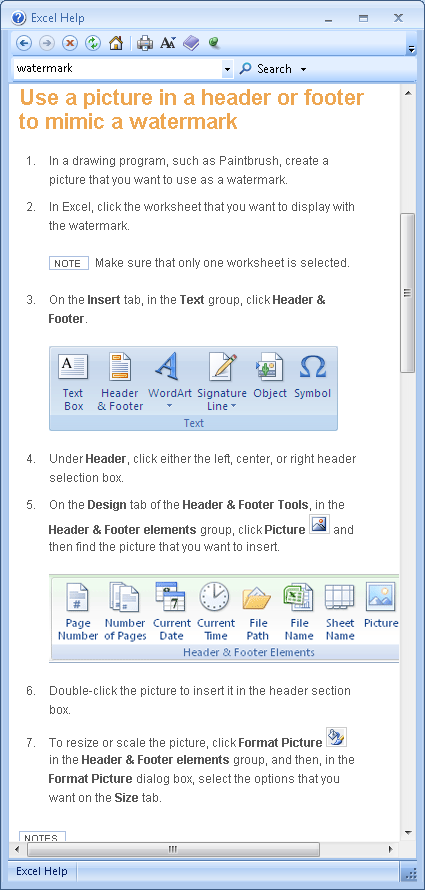
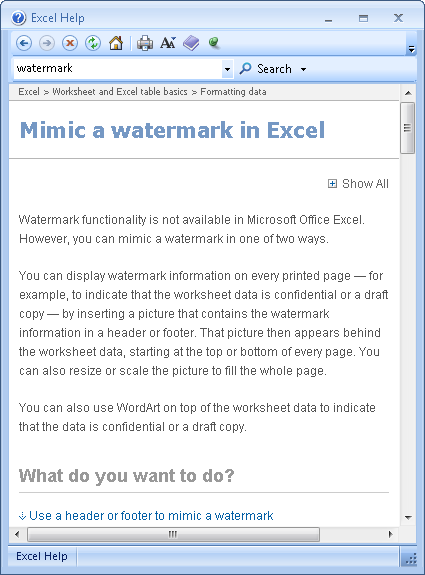
In Word, the Page Layout menu contains an option to create a watermark.



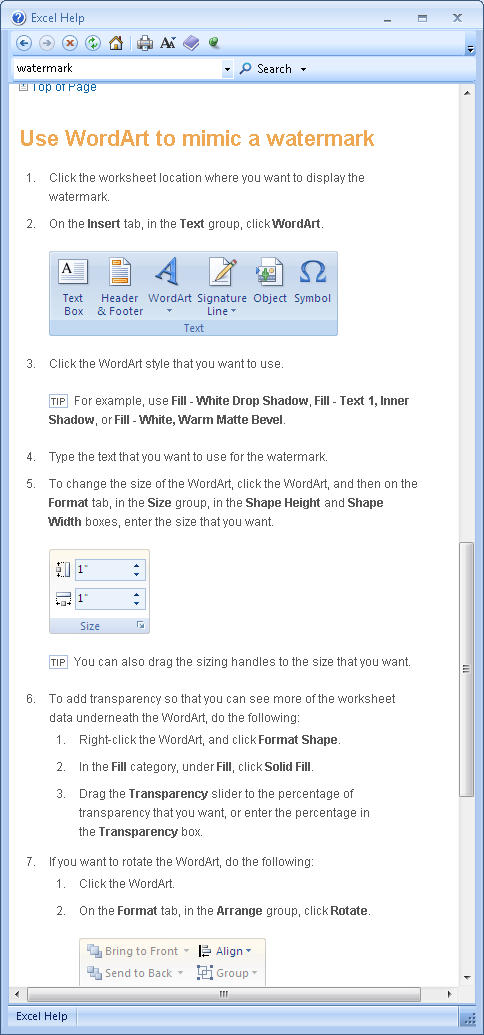
When you click on the Watermark choice, a drop-down menu presents an array of built-in options for using the word “Confidential” as a watermark.

**b. Create the same watermark in Excel and print out a spreadsheet page that displays that watermark.**

Excel does not have a built-in watermark facility. However, if you search for information about watermarks in Excel’s help function, you learn that you have two options:



.



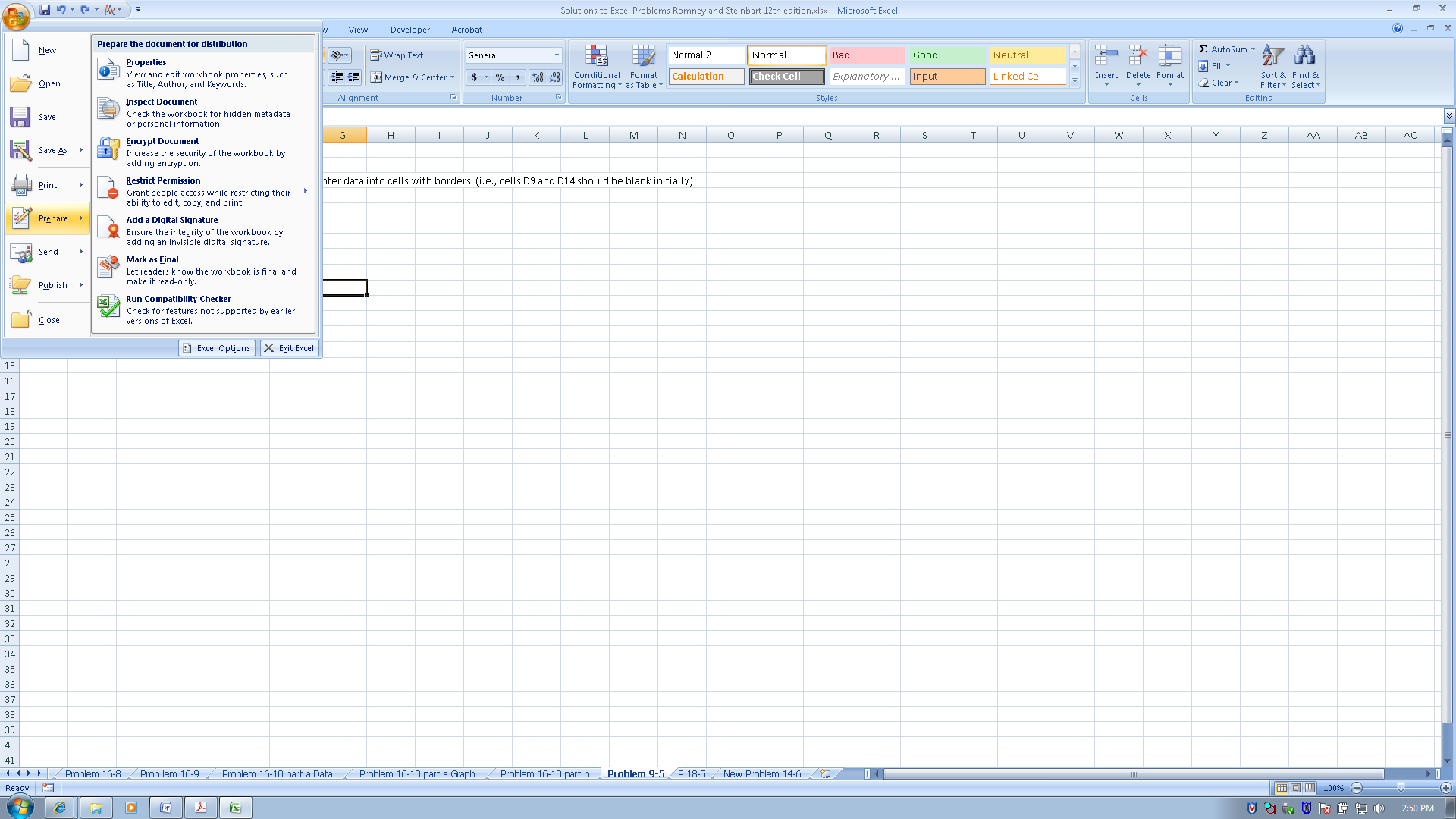
**c. Can you make your watermark “invisible” so that it can be used to detect whether a document containing sensitive information has been copied to an unauthorized location? How? How could you use that “invisible” watermark to detect violation of copying policy?**

If you make the text of the watermark white, then it will not display on the screen. To make the watermark visible in Word, on the Page Layout menu select the “Page Color” option and set the color to something dark to reveal the “invisible” white watermark. In Excel, you would select all cells and then change the fill color to something dark to reveal the “invisible” white watermark.

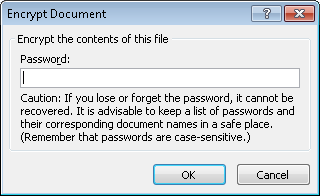
**9.5** **Create a spreadsheet to compare current monthly mortgage payments versus the new monthly payments if the loan were refinanced, as shown (you will need to enter formulas into the two cells with solid borders like a box: D9 and D14)**

1. **Restrict access to the spreadsheet by encrypting it.**

In Excel 2007, choose Prepare and then Encrypt Document.



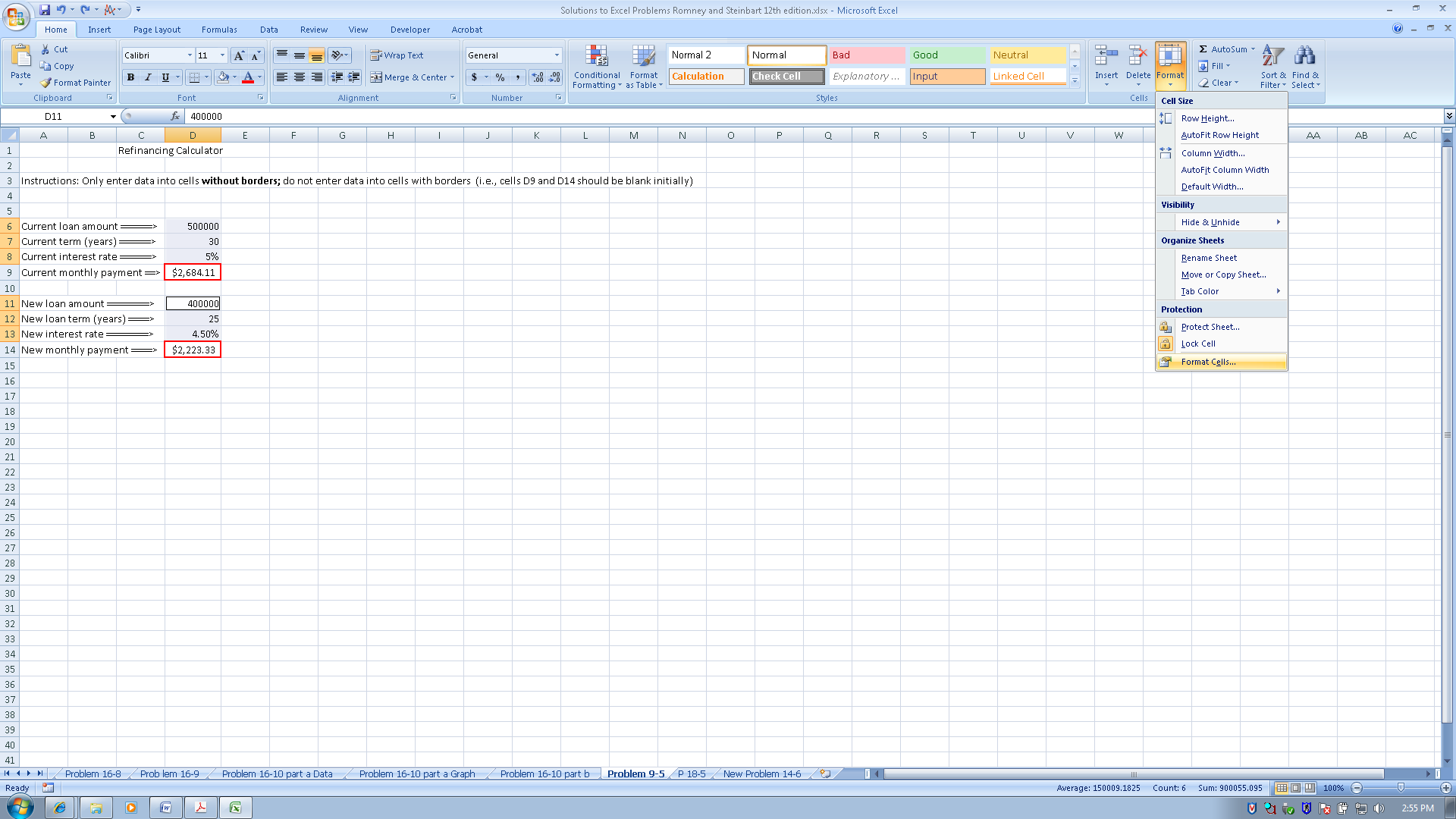
Then select a password, and be sure to remember it:



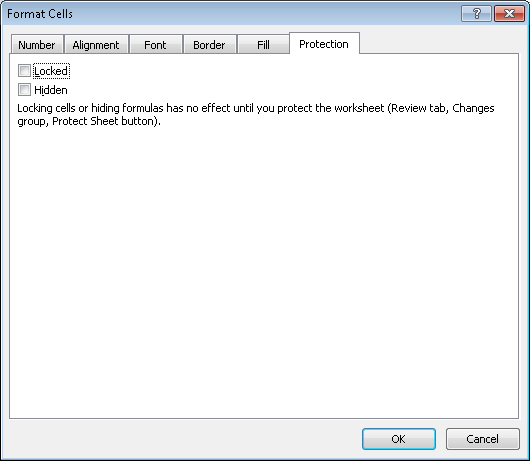
**Further protect the spreadsheet by limiting users to only being able to select and enter data in the six cells without borders.**

To protect the two cells that contain the formula (shown below with red boxed borders):

* 1. Select the cells that users are allowed to change (cells D6:D8 and D11:D13)
  2. Under the Format drop-down menu, select format cells

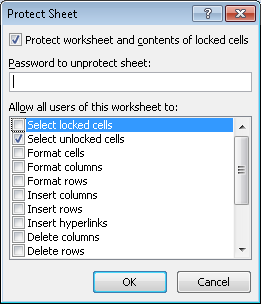


Then uncheck the box next to “Locked” as shown below, because these are going to be the only cells we do not protect in the next step.



Now, under the Format drop-down menu, select “Protect Sheet” and then

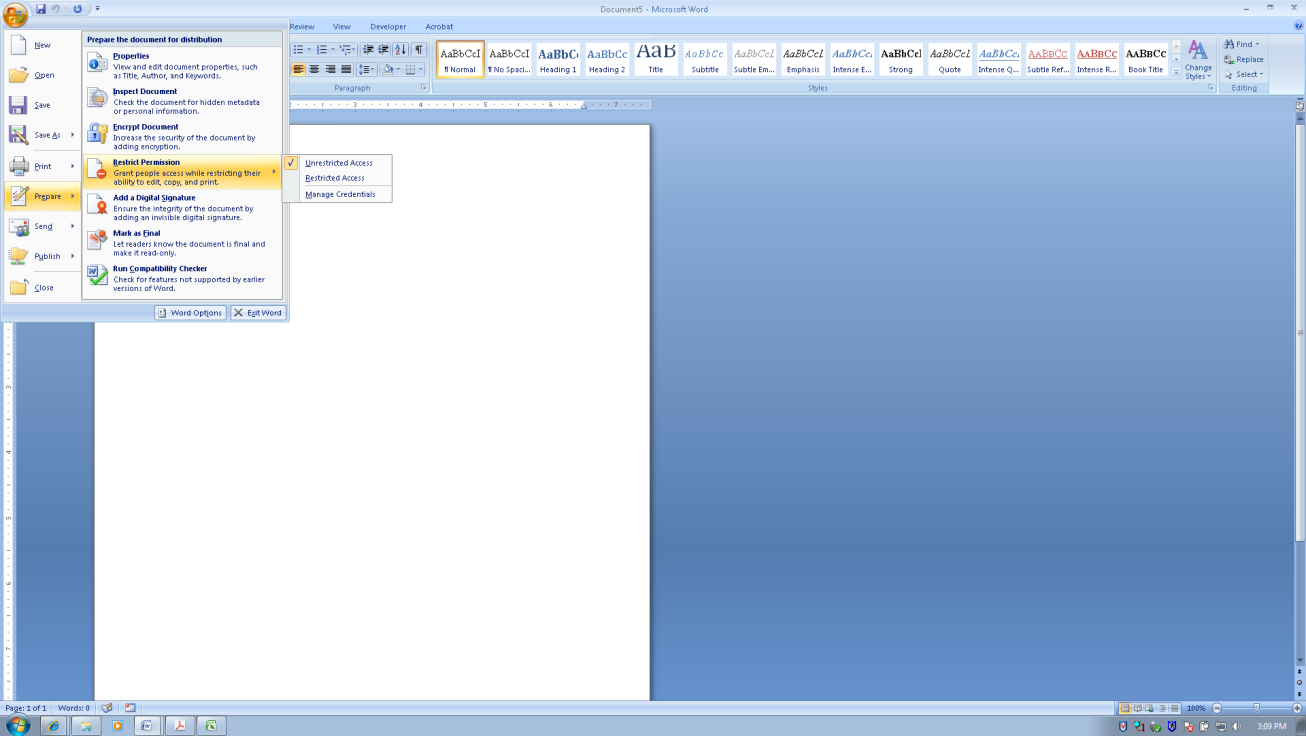
1. enter a password, and
2. uncheck the box “Select locked cells”. This will protect the entire sheet EXCEPT for the cells you unlocked in the previous step – users can only move between the six unlocked cells! BE SURE TO REMEMBER YOUR PASSWORD – it is the only way to unlock the spreadsheet.



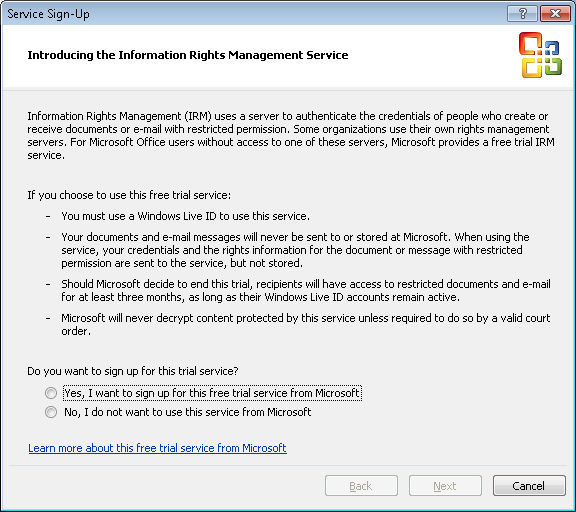
**9.6 Research the information rights management software that may be available for your computer. What are its capabilities for limiting access rights? Write a report of your findings.**

**Optional: If you can download and install IRM software, use it to prevent anyone from being able to copy or print your report.**

Solutions will vary depending upon the student’s computer and version of operating system. Windows, for example, has information rights management software but consumers must create a LiveID account to use it. The following screen shot shows how to access the Information Rights Management (IRM) software in Word 2007:



Choosing the “Manage Credentials” option calls up the dialogue for Microsoft’s Information Rights Management (IRM) software:



**9.7 The principle of confidentiality focuses on protecting an organization’s intellectual property. The flip side of the issue is ensuring that employees respect the intellectual property of other organizations. Research the topic of software piracy and write a report that explains:**

**a. What software piracy is.**

**b. How organizations attempt to prevent their employees from engaging in software piracy.**

**c. How software piracy violations are discovered.**

**d. The consequences to both individual employees and to organizations who commit software piracy.**

Solutions will vary. Key points to look for in the report:

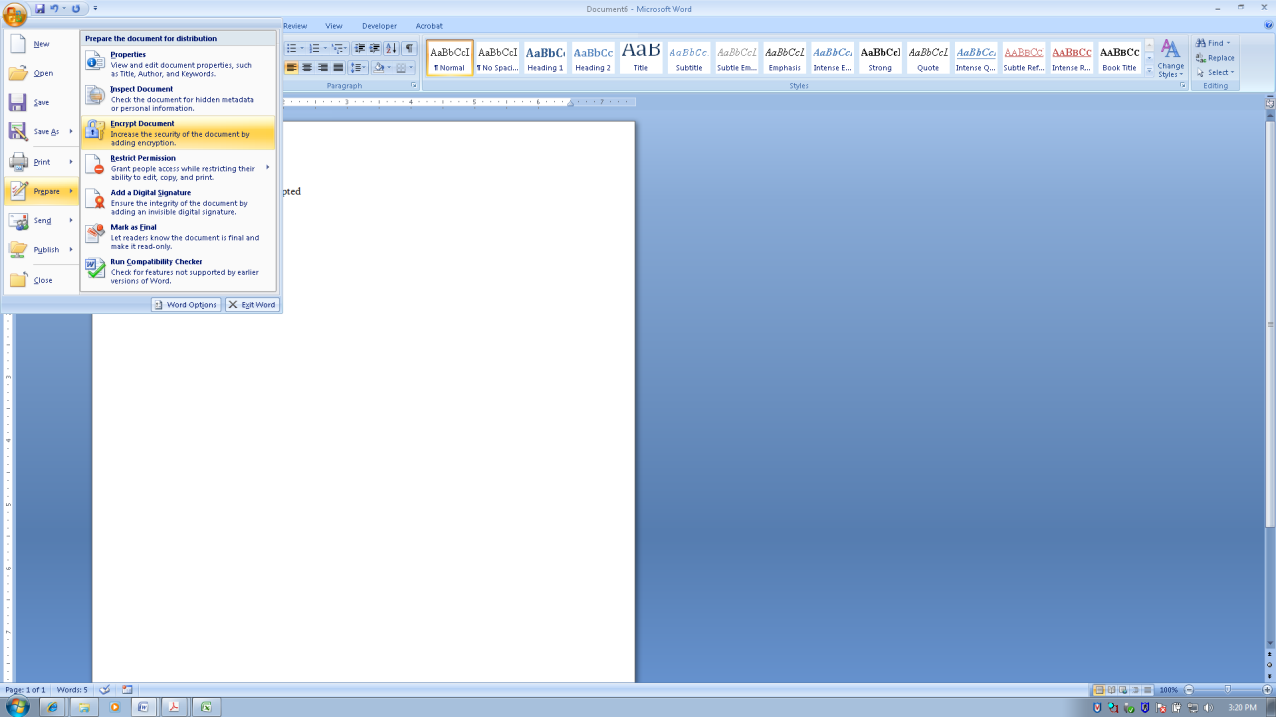
1. Definition of software piracy that clearly indicates it involves the illegal or unauthorized downloading and use of software in violation of the terms of the software license agreement.
2. Training and periodic audits of employees’ computers.
3. Most often by anonymous tips, either from disgruntled employees or a competitor.
4. Organizations discovered to have illegal copies of software have received large fines. It is possible that individuals convicted of software piracy could go to jail. The sites that people visit to obtain illegal copies of software often are not very secure, so people often find that they download and install not just the program they want, but also malware.

**9.8 Practice encryption.**

**Required:**

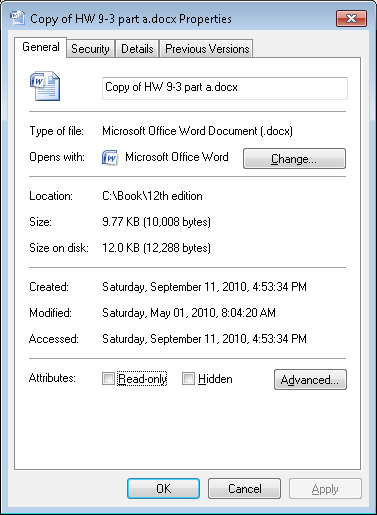
1. **Use your computer operating system’s built-in encryption capability to encrypt a file.**

**In Windows, if you are working with an open document, you can encrypt it by choosing that option under the “Prepare” menu:**

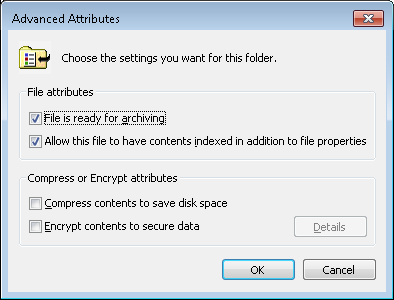


You will then be prompted for a password to protect that file.

You can also encrypt an existing file by right-clicking on its name in a directory list and then choosing Properties, which brings up this pop-up window:



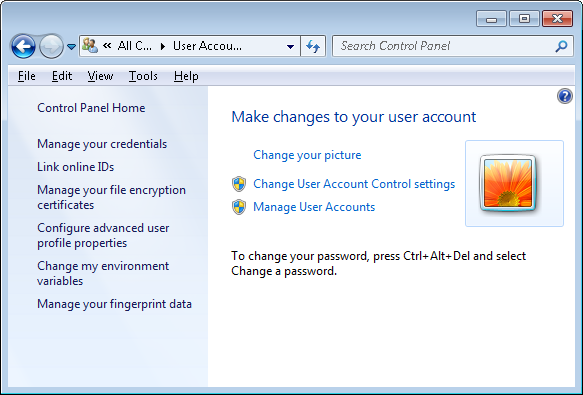
Clicking on the Advanced button brings up this dialog box:



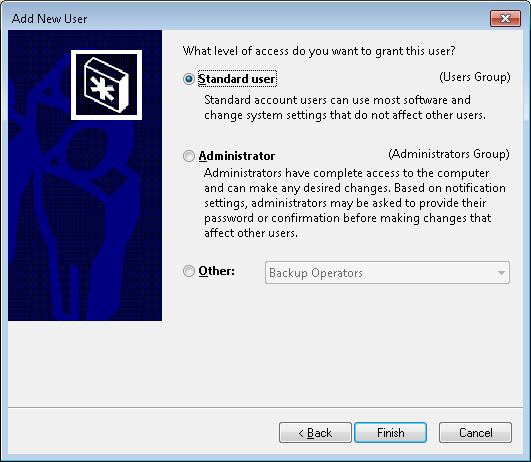
Select the box “Encrypt contents to secure data” and follow the directions.

**Create another user account on your computer and log in as that user.**

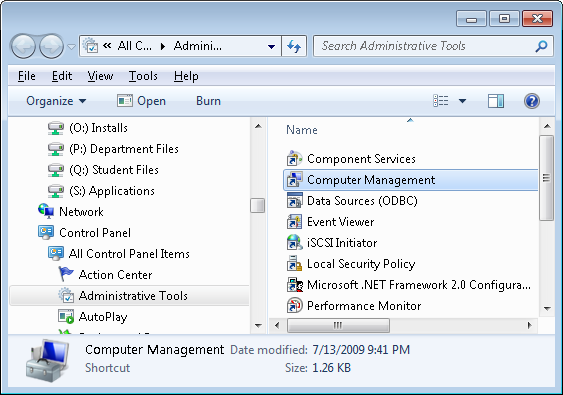
In Windows, there are two ways to create new user accounts. One way is to open the Control Panel and select the option “User Accounts”. This brings up the following screen:



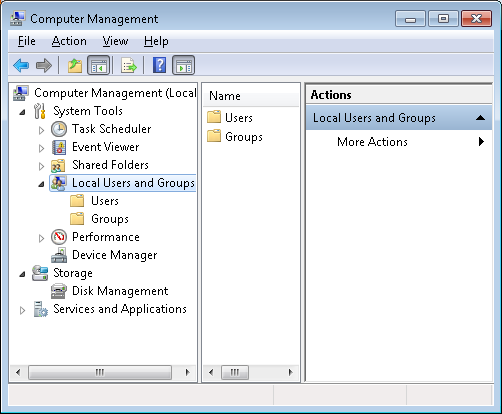
Select the “Manage User Accounts” and then click the “Add” button. You will then be prompted to give a name to your new user account and decide whether it is a standard user or an account with administrative rights. For purposes of this exercise, just create a standard user.



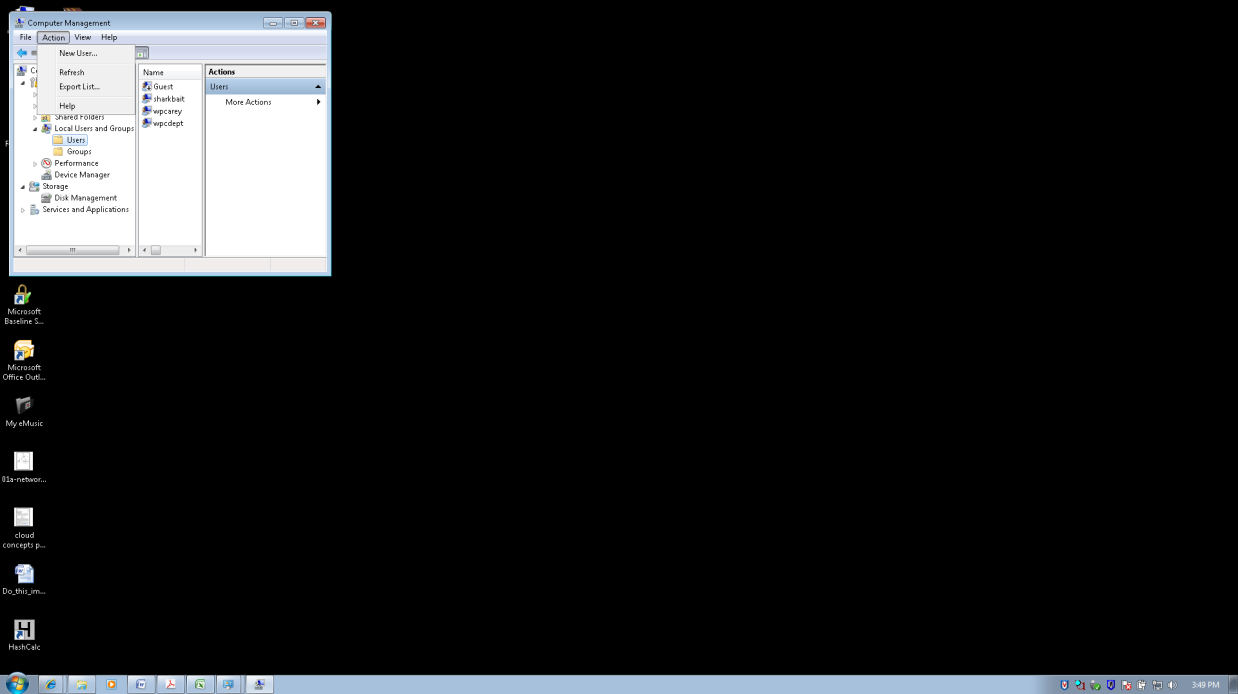
Method 2: Open the Control Panel, choose “Administrative Tools and then select “Computer Management”:



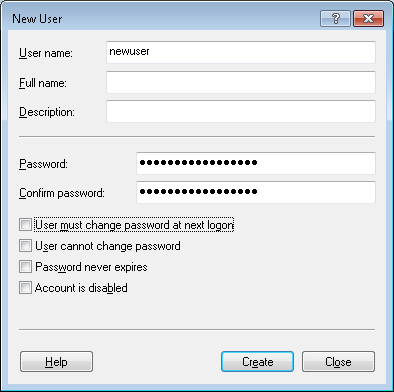
Double-click on Computer Management and then click on the Users and Groups:



Now, click on the “Users” folder in the left pane, and then click on the “Action” menu item at the top and select the option “New user”:



Fill in the screen, giving your new user a name and password. It will probably be easiest for this assignment to not force the new user to change passwords. Also, uncheck the box “Account is disabled” so that you can do the rest of this exercise.



**Which of the following actions can you perform?**

**1. Open the file**

**2. Copy the file to a USB drive.**

**3. Move the file to a USB drive.**

**4. Rename the file.**

**5. Delete the file**

ADDITIONAL NOTE TO INSTRUCTORS: Tell students to save the encrypted file in a shared directory that is accessible to all users who log onto that system. That way, even a standard user will be able to see the files.

Solutions may vary depending upon the computer’s operating system. In Windows, a standard user who did not create the encrypted file will not be able to open, copy, or move the encrypted file to a USB drive – but is able to rename or delete it. This demonstrates that encryption is not a total solution – if someone has physical access to a computer that has encrypted files on it, they may not be able to read that file but they can destroy it. Thus, physical access controls are also important.

In Windows, if a student creates another user account with Administrative privileges, that account will also not be able to open, copy or move the encrypted file to a USB drive – but can rename or delete it. One other difference is that a user with administrative privileges can also open up other user’s profiles.

**IMPORTANT NOTE TO INSTRUCTORS:** Tell students to delete the new user account that they created to do this problem after they finish the assignment.

**b. TrueCrypt is one of several free software programs that can be used to encrypt files stored on a USB drive. Download and install a copy of TrueCrypt (or another program recommended by your professor). Use it to encrypt some files on a USB drive. Compare its functionality to that of the built-in encryption functionality provided by your computer’s operating system.**

TrueCrypt is available at [www.truecrypt.org](http://www.truecrypt.org) – note that the name is TrueCrypt.

The article “Protect Your Portable Data—Always and Everywhere,” (by Simon Petravick and Stephen Kerr) in the June 2009 issue of the Journal of Accountancy discusses a number of encryption products.

Students will likely report that software like TrueCrypt offers many more features than their computer operating system’s built-in encryption functionality.

**9.9 Research the problem of identity theft and write a report that explains:**

**a. Whether the problem of identity theft is increasing or decreasing**

**b. What kind of identity theft protection services or insurance products are available. Compare and contrast at least two products.**

Students should report that the problem of identity theft is increasing. One issue, however, concerns how identity theft is defined. Some sources include things like stealing credit card or debit card numbers; others limit identity theft to impersonating someone to open a new credit card account, take out a loan, purchase a major item (like a car) on credit, etc. Regardless, the general trend is increasing.

An excellent source of detailed information for instructors is the FTC. If you go to the main web site ([www.ftc.gov](http://www.ftc.gov)) you will see a link to Identity Theft under the list “Quick Finder”:



Clicking that link brings you to a page with videos and documents about how to protect yourself, etc. Particularly interesting is the document “To buy or not to buy: Identity theft spawns new products and services to help minimize risk.”

The web site [www.insure.com](http://www.insure.com) provides a lot of information about different identity theft protection products (you can find it under the “Other Insurance” tab on the main page). Probably the most well-known product is LifeLock. Increasingly, many home insurance policies also offer riders for identity theft protection.

**9.10 Certificate authorities are an important part of a public key infrastructure (PKI). Research at least two certificate authorities and write a report that explains the different types of digital certificates that they offer.**

Solutions will vary depending upon the specific certificate authorities the student investigates. Students will most likely choose Verisign, GoDaddy, Entrust, Equifax, Deutsche Telekom, and Thawte.

These certificate authorities (CAs) issue several types of certificates. For example, the Verisign site has a white paper called “Beginners Guide to SSL certificates” that includes the following explanation:

**DIFFERENT TYPES OF SSL CERTIFICATE**

There are a number of different SSL Certificates on the market today.

1. The first type of SSL Certificate is a **self-signed certificate**. As the name implies, this is a certificate that is generated for internal purposes and is *not* issued by a CA. Since the web site owner generates their own certificate, it does not hold the same weight as a fully authenticated and verified SSL Certificate issued by a CA.

2. A **Domain Validated Certificate** is considered an entry-level SSL Certificate and can be issued quickly. The only verification check performed is to ensure that the applicant owns the domain (web site address) where they plan to use the certificate. No additional checks are done to ensure that the owner of the domain is a valid business entity.

3. A **fully authenticated SSL Certificate** is the first step to true online security and confidence building. Taking slightly longer to issue, these certificates are only granted once the organization passes a number of validation procedures and checks to confirm the existence of the business, the ownership of the domain, and the user’s authority to apply for the certificate.

*All VeriSign® brand SSL Certificates are fully authenticated.*

4. Even though an SSL Certificate is capable of supporting 128-bit or 256-bit encryption, certain older browsers and operating systems still cannot connect at this level of security. SSL Certificates with a technology called Server-Gated Cryptography (SGC) enable 128- or 256-bit encryption to over 99.9% of web site visitors. Without an SGC certificate on the web server, browsers and operating systems that do not support 128-bit strong encryption will receive only 40- or 56-bit encryption. Users with certain older browsers and operating systems will temporarily step-up to 128-bit SSL encryption if they visit a web site with an SGC-enabled SSL Certificate. For more information about SGC please visit: www.verisign.com/sgc.

5. A domain name is often used with a number of different host suffixes. For this reason, you may employ a Wildcard Certificate that allows you to provide full SSL security to any host of your domain—for example: host.your\_domain. com (where “host” varies but the domain name stays constant).

6. Similar to a Wildcard Certificate, but a little more versatile, the SAN (Subject Alternative Name) SSL Certificate allows for more than one domain to be added to a single SSL Certificate.

7. **Code Signing Certificates** are specifically designed to ensure that the software you have downloaded was not tampered with while en route. There are many cyber criminals who tamper with software available on the Internet. They may attach a virus or other malicious software to an innocent package as it is being downloaded. These certificates make sure that this doesn’t happen.

8. **Extended Validation (EV) SSL Certificates** offer the highest industry standard for authentication and provide the best level of customer trust available. When consumers visit a web site secured with an EV SSL Certificate, the address bar turns green (in high-security browsers) and a special field appears with the name of the legitimate web site owner along with the name of the security provider that issued the EV SSL Certificate. It also displays the name of the certificate holder and issuing CA in the address bar. This visual reassurance has helped increase consumer confidence in e-commerce.

**9.11** **Obtain a copy of COBIT (available at** [**www.isaca.org**](http://www.isaca.org)**) and read the control objectives that relate to encryption (DS5.8 and DS5.11). What are the essential control procedures that organizations should implement when using encryption?**

COBIT control objective DS5.8 addresses key management policies with respect to encryption. This should include procedures concerning:

* Minimum key lengths
* Use of approved algorithms
* Procedures to authenticate recipients
* Secure distribution of keys
* Secure storage of keys
* Key escrow
* Policies governing when to use encryption and which information should be encrypted (this probably requires the organization to classify and label all information assets so that employees can identify the different categories)
* Procedures for revoking compromised keys

COBIT control objective DS5.11 addresses the use of encryption during the transmission of information. This should include procedures concerning:

* Procedures to ensure information is encrypted prior to transmission
* Specification of approved encryption algorithms
* Access controls over incoming encrypted information
* Secure storage of encryption keys

**SUGGESTED SOLUTIONS TO THE CASES**

**Case 9-1** **Protecting Privacy of Tax Returns**

**The department of taxation in your state is developing a new computer system for processing individual and corporate income-tax returns. The new system features direct data input and inquiry capabilities. Identification of taxpayers is provided by using the Social Security number for individuals and federal tax identification number for corporations. The new system should be fully implemented in time for the next tax season.**

**The new system will serve three primary purposes:**

**1 Data will either be automatically input directly into the system if the taxpayer files electronically or by a clerk at central headquarters scanning a paper return received in the mail.**

**2 The returns will be processed using the main computer facilities at central headquarters. Processing will include four steps:**

**a. Verifying mathematical accuracy**

**b. Auditing the reasonableness of deductions, tax due, and so on, through the use of edit routines, which also include a comparison of current and prior years’ data.**

**c. Identifying returns that should be considered for audit by department revenue agents**

**d. Issuing refund checks to taxpayers**

**3 Inquiry services. A taxpayer will be allowed to determine the status of his or her return or get information from the last three years’ returns by calling or visiting one of the department’s regional offices, or by accessing the department’s web site and entering their social security number.**

**The state commissioner of taxation and the state attorney general are concerned about protecting the privacy of personal information submitted by taxpayers. They want to have potential problems identified *before* the system is fully developed and implemented so that the proper controls can be incorporated into the new system.**

**Required**

**Describe the potential privacy problems that could arise in each of the following three areas of processing, and recommend the corrective action(s) to solve each problem identified:**

**a. Data input**

**b. Processing of returns**

**c. Data inquiry**

**[CMA examination, adapted]**

a. Privacy problems which could arise in the processing of input data, and recommended corrective actions, are as follows:

|  |  |
| --- | --- |
| Problem | Controls |
| Unauthorized employee accessing paper returns submitted by mail. | Restrict physical access to room used to house paper returns and scanning equipment by   * Using ID badges or biometric controls * Logging all people who enter. |
| Unauthorized employee accessing the electronic files. | Multi-factor authentication of all employees attempting to access tax files. |
| Interception of tax information submitted electronically. | Encrypt all information submitted to the tax website. |

b. Privacy problems which could arise in the processing of returns, and recommended corrective actions, are as follows:

|  |  |
| --- | --- |
| Problem | Controls |
| Operator intervention to input data or to gain output from files. | Limit operator access to only that part of the documentation needed for equipment operation.  Prohibit operators from writing programs and designing the system.  Daily review of console log messages and/or run times.  Encryption of data by the application program. |
| Attempts to screen individual returns on the basis of surname, sex, race, etc., rather than tax liability. | Training about proper procedures  Multi-factor authentication to limit access to system.  Encrypt of tax return data stored in system |

c. Privacy problems which could arise in the inquiry of data, and recommended corrective actions, are as follows:

|  |  |
| --- | --- |
| Problem | Controls |
| Unauthorized access to taxpayer information on web site | Strong authentication of all people making inquiries via the web site using something other than social security numbers – preferably multi-factor, not just passwords.  Encryption of all tax return data while in storage  Encryption of all traffic to/from the web site |
| Unauthorized release of information in response to telephone inquiry | Training on how to properly authenticate taxpayers who make telephone inquiries  Strong authentication of taxpayers making telephone inquiries |
| Disclosure of taxpayer information through improper disposal of old files | Training on how to shred paper documents prior to disposal  Training on how to wipe or erase media that contained tax return information prior to disposal |

(CMA Examination, adapted)

**Case 9-2 Generally Accepted Privacy Principles**

**Obtain the practitioner’s version of Generally Accepted Privacy Principles from the AICPA’s web site (**[**www.aicpa.org**](http://www.aicpa.org)**). You will find it located under professional resources and then information technology. Use it to answer the following questions:**

1. **What is the difference between confidentiality and privacy?**

Privacy relates to information collected about identifiable individuals.

Confidentiality relates to the organization’s intellectual property and similar information it collects/shares with business partners.

Regulations exist concerning responsibilities for protecting privacy; no such broad regulations exist with respect to confidentiality.

1. **How many categories of personal information exist? Why?**

Two: personal information and sensitive personal information. Examples are provided on page 4 of the GAPP document (which is reproduced below and highlighted in yellow):

### *Personal Information*

*Personal information* (sometimes referred to as personally identifiable information) is information that is about, or can be related to, an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual. Individuals, for this purpose, include prospective, current, and former customers, employees, and others with whom the entity has a relationship. Most information collected by an organization about an individual is likely to be considered personal information if it can be attributed to an identified individual. Some examples of personal information are as follows:

• Name

• Home or e-mail address

• Identification number (for example, a Social Security or Social Insurance Number)

• Physical characteristics

• Consumer purchase history

Some personal information is considered sensitive. Some laws and regulations define the following to be sensitive personal information:

• Information on medical or health conditions

• Financial information

• Racial or ethnic origin

• Political opinions

• Religious or philosophical beliefs

• Trade union membership

• Sexual preferences

• Information related to offenses or criminal convictions

Sensitive personal information generally requires an extra level of protection and a higher duty of care. For example, some jurisdictions may require explicit consent rather than implicit consent for the collection and use of sensitive information.

Some information about or related to people cannot be associated with specific individuals. Such information is referred to as *nonpersonal information*. This includes statistical or summarized personal information for which the identity of the individual is unknown or linkage to the individual has been removed. In such cases, the individual’s identity cannot be determined from the information that remains because the information is deidentified or anonymized. Nonpersonal information ordinarily is not subject to privacy protection because it cannot be linked to an individual. However, some organizations may still have obligations over nonpersonal information due to other regulations and agreements (for example, clinical research and market research).

The difference is that sensitive personal information can, if misused, cause significant harm or embarrassment to the individual.

1. **In terms of the principle of choice and consent, what does GAPP recommend concerning opt-in versus opt-out?**

Sensitive personal information requires explicit consent (i.e., opt-in). Other personal information can be collected through either explicit (opt-in) or implicit (opt-out) consent.

1. **Can organizations outsource their responsibility for privacy?**

No. The section on “Outsourcing and Privacy” on page 3 specifically states that organizations cannot totally eliminate their responsibility for complying with privacy regulations when they outsource collection, use, etc. of personal information.

1. **What does principle 1 state concerning top management’s and the Board of Directors’ responsibility for privacy?**

It is top management’s responsibility to assign privacy management to a specific individual or team (management criterion 1.1.2). As an illustrative control for this criterion, the Board of Directors should review privacy policies at least annually.

1. **What does principle 1 state concerning the use of customers’ personal information when testing new applications?**

It must be rendered anonymous (all personally identified information removed).

1. **Obtain a copy of your university’s privacy policy statement. Does it satisfy GAPP criterion 2.2.3? Why?**

Answers will vary. The key point is the rationale provided as to why the policy is (not) clear and easy to understand.

1. **What does GAPP principle 3 say about the use of cookies?**

Organizations must develop programs and procedures to ensure that if customers want to disable cookies, that the organization complies with those wishes.

1. **What are some examples of practices that violate management criterion 4.2.2?**

* Surreptitious collection of data via secret cookies or web beacons
* Linking information collected with information collected from other sources without notifying individuals
* Use of a third party to collect information in order to avoid having to provide notice to people that the organization is collecting personal information about them.

1. **What does management criterion 5.2.2 state concerning retention of customers’ personal information? How can organizations satisfy this criterion?**

Organizations need a retention policy and must regularly inventory the information they store and delete it if no longer relevant.

1. **What does management criterion 5.2.3 state concerning the disposal of personal information? How can organizations satisfy this criterion?**

Organizations need to destroy media with sensitive information. Note that sometimes this requires destruction of an entire file or database (e.g., cannot just destroy one track on CD or DVD). If documents are released, personal information needs to be redacted.

1. **What does management criterion 6.2.2 state concerning access? What controls should organizations use to achieve this objective?**

Organizations need to authenticate the identity of people requesting access to their personal information. DO NOT use Social Security Numbers for such authentication.

1. **According to GAPP principle 7, what should organizations do if they wish to share personal information they collect with a third party?**

Organizations should

* Disclose that they intend to share information with third parties (management criterion 7.1.1)
* Provide third parties with the organization’s privacy policies (management criterion 7.1.2)
* Only share information with third parties that have systems in place to provide the same level of protection of privacy as the sharing organization (management criterion 7.2.2)
* Take remedial actions against third parties that misuse personal information disclosed to them (management criterion 7.2.4)

1. **What does GAPP principle 8 state concerning the use of encryption?**

Personal information must be encrypted whenever transmitted (management criterion 8.2.5) or stored on portable media (management criterion 8.2.6).

1. **What is the relationship between GAPP principles 9 and 10?**

Principle 9 stresses the importance of maintaining accurate records.

Principle 10 requires that a complaint resolution process must exist. One of the most frequent causes of complaints will likely be customers discovering, when provided access as per principle 6, errors and inaccuracies in their records which the organization fails to correct on a timely basis.