

# IT Security for Users

ECDL 5.0 / BCS IT User – Level 1  
Using Microsoft Windows



The  
Chartered  
Institute  
for IT

SAMPLE

© 1995-2010 Cheltenham Courseware Pty. Ltd.

All trademarks acknowledged. E&OE.

No part of this document may be copied without written permission from Cheltenham Courseware unless produced under the terms of a courseware site license agreement with Cheltenham Courseware.

All reasonable precautions have been taken in the preparation of this document, including both technical and non-technical proofing. Cheltenham Courseware and all staff assume no responsibility for any errors or omissions. No warranties are made, expressed or implied with regard to these notes. Cheltenham Courseware shall not be responsible for any direct, incidental or consequential damages arising from the use of any material contained in this document. If you find any errors in these training modules, please inform Cheltenham Courseware. Whilst every effort is made to eradicate typing or technical mistakes, we apologise for any errors you may detect. All courses are updated on a regular basis, so your feedback is both valued by us and will help us to maintain the highest possible standards.

**Sample versions of courseware from Cheltenham Courseware:**

(Normally supplied in Adobe Acrobat format): If the version of courseware that you are viewing is marked as NOT FOR TRAINING, SAMPLE, or similar, then it cannot be used as part of a training course, and is made available purely for content and style review. This is to give you the opportunity to preview our courseware, prior to making a purchasing decision. Sample versions may not be re-sold to a third party.

**For current license information:**

This document may only be used under the terms of the license agreement from Cheltenham Courseware. Cheltenham Courseware reserves the right to alter the licensing conditions at any time, without prior notice. Please see the site license agreement available at: [www.cheltenhamcourseware.com.au/agreement](http://www.cheltenhamcourseware.com.au/agreement)

**Contact Information**

**UK / Ireland**

Email: [info@cctglobal.com](mailto:info@cctglobal.com)

Web: [www.cctglobal.com](http://www.cctglobal.com)

**Australia / Asia Pacific / Europe (ex. UK/Ireland) / Rest of the World**

Email: [info@cheltenhamcourseware.com.au](mailto:info@cheltenhamcourseware.com.au)

Web: [www.cheltenhamcourseware.com.au](http://www.cheltenhamcourseware.com.au)

**USA / Canada**

Email: [info@cheltenhamcourseware.com](mailto:info@cheltenhamcourseware.com)

Web: [www.cheltenhamcourseware.com](http://www.cheltenhamcourseware.com)



SYSTEM PERFORMANCE SECURITY .....	5
UNWANTED MESSAGES .....	5
<i>What is spam?</i> .....	5
<i>Protecting against spam</i> .....	5
MALICIOUS PROGRAMS .....	6
<i>Computer viruses</i> .....	6
<i>Malware</i> .....	6
<i>Spyware</i> .....	6
<i>Worms</i> .....	7
<i>Trojans</i> .....	7
<i>Adware</i> .....	7
<i>Rogue diallers</i> .....	7
<i>How malicious programs can enter your computer</i> .....	7
<i>Risks associated with opening email attachments</i> .....	8
<i>Protecting your computer against malicious programs</i> .....	9
<i>Updating your anti-virus software</i> .....	9
<i>Protecting against malicious programs</i> .....	9
INFILTRATION .....	10
<i>What is a hacker?</i> .....	10
<i>How do hackers attack?</i> .....	10
<i>What is a firewall?</i> .....	11
HOAXES .....	11
<i>Hoaxes</i> .....	11
<i>How to spot a hoax message</i> .....	12
INFORMATION SECURITY.....	13
IDENTITY/AUTHENTICATION.....	13
<i>Risks of unauthorised access</i> .....	13
<i>User IDs and passwords</i> .....	13
<i>Keep your passwords and PIN number secret</i> .....	13
<i>Change your passwords and PIN number regularly</i> .....	13
<i>Changing your password or PIN number</i> .....	13
<i>How to change your password or PIN number on a Windows XP computer</i> .....	14
<i>How to change your password or PIN number on a Windows Vista computer</i> .....	17
CONFIDENTIALITY .....	19
<i>Passwords and PINs</i> .....	19
<i>Data protection and privacy Issues</i> .....	19
<i>Logging off or locking your computer</i> .....	19
IDENTITY THEFT.....	19
<i>What is Phishing?</i> .....	19
<i>Understanding and avoiding identity theft</i> .....	20
<i>Avoid inappropriate disclosure of information</i> .....	20
TECHNOLOGY SECURITY.....	21
NETWORKS .....	21
<i>What is a public network?</i> .....	21
<i>Network security</i> .....	21
<i>Network encryption</i> .....	21
<i>Wireless networks</i> .....	21
<i>Default passwords</i> .....	21
<i>Internet security settings</i> .....	21
CONNECTIVITY .....	22
<i>What is Bluetooth connectivity?</i> .....	22
<i>Bluetooth settings</i> .....	22

PORTABLE DEVICES .....	22
<i>Loss or theft of portable devices</i> .....	22
<i>Portable storage devices</i> .....	23
GUIDELINES AND PROCEDURES .....	24
GUIDELINES AND PROCEDURES .....	24
<i>Dealing with security problems</i> .....	24
<i>Responsibilities for dealing with security problems</i> .....	24
<i>Security rights and obligations</i> .....	24
PRIVACY .....	24
<i>What is a Privacy Policy?</i> .....	24
DATA SECURITY .....	26
SECURITY .....	26
<i>Locking computer hardware</i> .....	26
BACKUPS .....	26
<i>Why backup?</i> .....	26
<i>Backup media</i> .....	27
<i>Off-site backups</i> .....	27
STORAGE .....	27
<i>Storing your personal data</i> .....	27
<i>Storing your software</i> .....	27

SAMPLE

## System Performance Security

### Unwanted Messages

---

#### What is spam?

- Spam is the bulk sending of unsolicited and often fraudulent email messages, normally trying to sell a commercial product or service. There are companies which will sell lists of email addresses by the million. If you are a regular Internet user, then the chances are that the providers of these lists will pick up your email address (using a variety of sneaky techniques). As more and more companies buy in these lists and use them in their marketing campaigns, you will receive more and more spam emails, offering you an increasingly bizarre range of products and services! In many countries the sending of spam is now against the law!
- Increasingly unscrupulous marketing companies are using pop-up windows within your Web browser to display unwanted messages. There are now many anti-pop-up programs available to help block this newer type of spam.

#### Protecting against spam

- Internet service providers now devote considerable resources to managing the spam problem. Most now offer a spam filtering service which will scan and quarantine any spam emails sent to your email address. In addition popular email software such as Microsoft Outlook and Mozilla Thunderbird include anti-spam features which filter out spam emails as they are downloaded from the internet.
- Many popular anti-virus software packages now also include an anti-spam capability.



## Malicious Programs

---

### Computer viruses

- Viruses are small programs which hide themselves on your disks (both diskettes and your hard disk). Unless you use virus detection software, the first time that you know that you have a virus is when it activates. Different viruses are activated in different ways.

**BEWARE:** Viruses can destroy all your data.



### Malware

- The word Malware is a combination of the words "malicious" and "software". Malware is software designed to install itself and run without your consent and without your knowledge. Sometimes when you download free programs from an internet site, they come bundled with hidden programs that you did not ask for and will not want. Often these hidden programs send back marketing information to companies. Sometimes they may have more sinister purposes, such as sending your credit card details to criminals intending to steal from you.
- When installing free programs you find on the net always read the licensing terms, as often the malware content is hidden away within this long document.

### Spyware

- This is different from a virus. Details such as your online browsing habits can be sent, without your knowledge, to marketing companies, or even criminal organizations that will try to get information such as your credit card details or access passwords.

## Worms

- A computer worm is a self-replicating computer program that sends copies of itself to other computers via a network. It can copy itself from computer to computer without your knowledge.
- A worm is different from a virus because it has no need to hide itself within another program. Many worms can reduce your available bandwidth due to their copying activities, but otherwise do not actually damage your files. However there are also destructive worms that will attack or compromise your data.

---

## Trojans

- A Trojan horse (often just called a 'Trojan') is a type of software which you normally expect to do one thing, but in fact it does something else that you did not intend.
- A Trojan is not a computer virus and does not try and copy itself across your network. It is basically just a program which you need to run. The name comes from the classical story of the wooden Trojan Horse.

---

## Adware

- Adware or advertising supported software are "free" software programs which download and display adverts while the software is being used. The adverts provide an income for the author of the program. Sadly hackers have hijacked this concept and often use adware to install malicious programs onto a victim's computer.

---

## Rogue diallers

- A Rogue Dialler is a program which modifies the settings of any dial-up network connections on your computer. The rogue dialler will change the telephone number for the connection to one provided by the attacker, this will normally be a premium rate number. From that point on, whenever you dial-up to the Internet the call will be routed via the premium rate number, making money for the attacker at your expense.
- Rogue diallers are becoming less common as broadband replaces dial-up as the preferred Internet connection method.

---

## How malicious programs can enter your computer

- Malicious programs use a variety of methods to enter your computer system:

**Infected Web site:** Also known as a "drive-by download", it is a web site which has had malware installed into it. When you then visit and view the infected site the malware downloads itself onto your computer without your knowledge. This method of attack normally relies on exploiting known bugs in your web browser, keeping your web browser software up-to-date with the latest version can reduce this threat.

**Internet Download:** Any files downloaded from the Internet are a potential hazard. Make sure you only download files from known reputable web sites.

**USB Storage Device:** Portable USB flash drives have become a popular way of transporting files from one computer to another. They can also contain malicious programs or documents; make sure that you have anti-virus software installed on your computer before inserting a USB device from an unknown source.

**CD/DVD-ROM/Floppy disk:** Any device capable of storing files has the potential to contain malicious software and should be scanned with anti-virus software before use.

---

### **Risks associated with opening email attachments.**

- If an email you receive contains an attachment, you should be very cautious about opening that e-mail, especially if the email is from someone you do not know or someone you have never received an email from before.
- Sometimes an email can appear to be from somebody you know, when in actual fact, it has been sent maliciously, and at first glance only appears to be from somebody you know. Spammers are very good at disguising the source of an email. If in doubt, do not open email attachments.
- The risk associated with opening email attachments is real. It is a very common method used to spread viruses and other forms of malware such as trojans, worms spyware and adware. If you have details of your bank accounts and credit cards contained within your computer, be especially cautious.
- If you have a good virus checking program installed on your computer, it should automatically scan and verify the contents of any email attachments you receive. However you cannot rely solely on your anti-virus program to protect you. It is up to you to exercise common sense when dealing with email attachments.
- Even if an email attachment originated from a friend or family member, it may still contain malware buried within it. A friend's computer may have been infected without their knowledge and by sending an e-mail attachment to you they are inadvertently helping to spread the infection. Remember by its very nature, malware hides itself within a computer and most people are completely unaware that their machines have become infected.
- If a friend, family member or colleague has a computer which does not have a good virus checker installed, or which is not kept up to date, then simply refuse to accept e-mail attachments from them, until they install a decent virus checking program. The risk is just too great.
- If a colleague has sent you an attachment in the form of an Excel or Microsoft Word document it is important to realise that a word or spreadsheet document can also contain computer viruses, called macro viruses.
- Think before opening email attachments. It is common practice for criminals to send out mass emails after some large natural disaster, appealing for money or donations and these should be treated with extra caution. You need to be absolutely sure that the appeal came from a reputable source. If

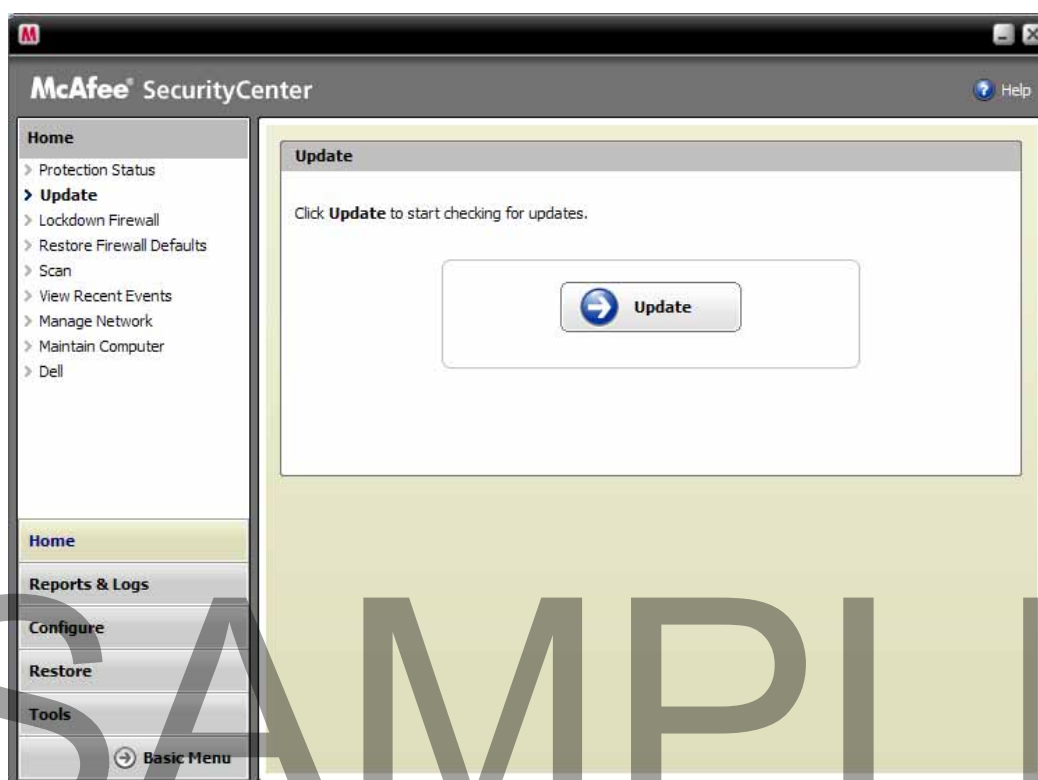
the appeal contains an attachment of some sort, be especially careful.

## Protecting your computer against malicious programs

- To help keep your computer safe from infection by malicious programs you should always ensure that you have up-to-date anti-virus and anti-spyware software installed. The software should be used to scan any files you receive from an unknown source.
- Most new anti-virus programs now also include anti-spyware features.

## Updating your anti-virus software

- It is important to remember to update your virus checker on a regular basis, so that it knows about more recent viruses. Many anti-virus programs have an auto-update feature which allows them to update themselves automatically as required. You can also run a manual update, as illustrated below for the McAfee anti-virus program.



## Protecting against malicious programs

- The safest way to use a computer is to not connect it to a Local Area network or the Internet. This is called a 'stand-alone' computer, providing that you do not use disks on that PC which have been used in other computers; this type of computer is virtually immune from any form of intrusion.
- Unfortunately it is the ability to connect to other computers or indeed the Internet, which makes the modern computer so versatile and so useful.

- Always make sure that all computers require an ID and password to access them. Make sure that all relevant 'security patches' from Microsoft have been applied.
- Make sure that the password is long enough, contains a random mixture of numbers and letters, and that the passwords are changed on a regular basis.
- There are many examples, where people have used passwords which relate to something personal, such as a partner's first name, the dog's or cat's name, etc. For a determined, serious computer hacker, these are easy to guess. If you have a system, where lots of different passwords are required to access the system, then security often breaks down and computer users will sometimes keep a list of these passwords in their desk. This defeats the whole object. If you forget your network access password, the network administrator should be able to assign you with a new one.



## Infiltration

---

### What is a hacker?

- A hacker is a person who tries to gain unauthorised access to a computer system.

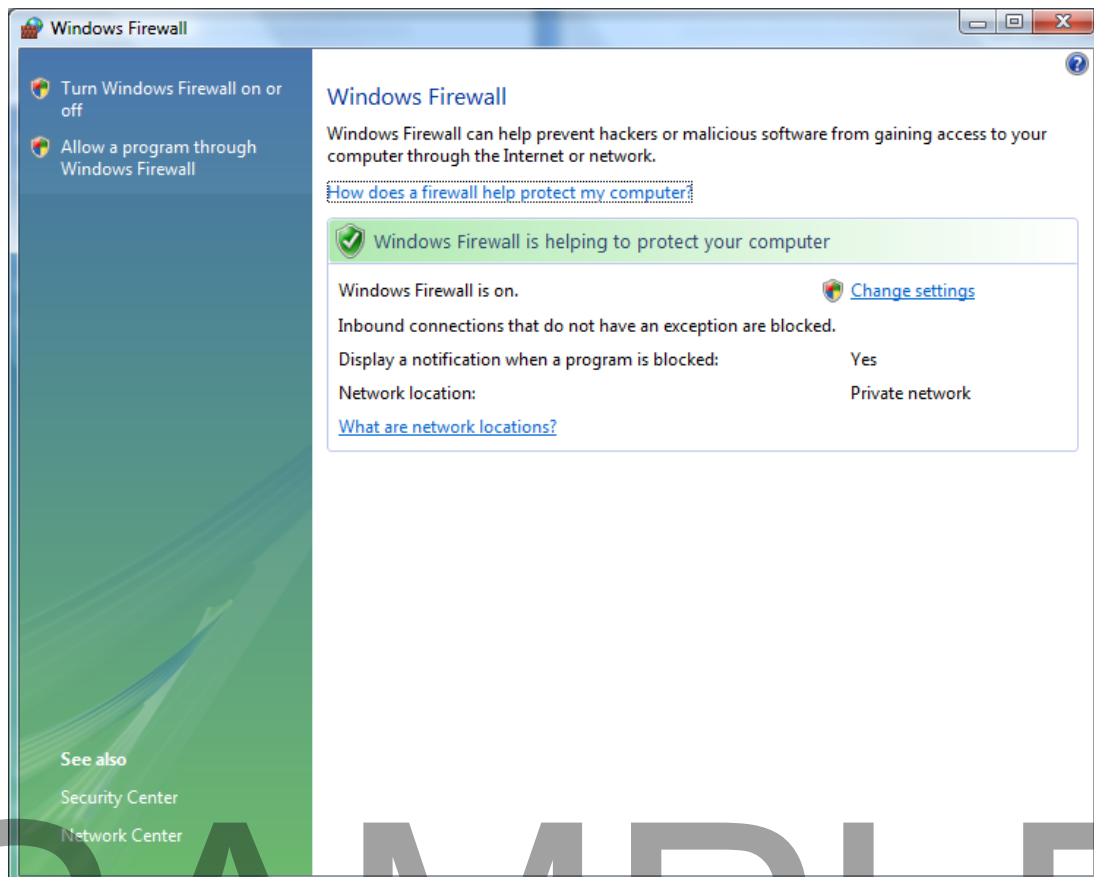
---

### How do hackers attack?

- Hackers will often attempt to exploit known bugs in commonly used software to gain access to a computer system through its network or Internet connection.
- They may attempt to infiltrate the computer by trying frequently used passwords to log-in. When first installed many software packages will be configured to use a standard default password. A hacker will know this default password and log into the system, so you should always set your own secure log-in password.

## What is a firewall?

- A firewall is a system that secures your network from access by unauthorized users. A firewall can be implemented via software, hardware or by a combination of the two. If you are using broadband for Internet access, it is vital that some sort of firewall is in place to stop people trying to hack into your computer.
- A firewall consists of software and/or hardware protection against invasion via a network connection. In most large companies any connection to the Internet automatically goes through a firewall which would have been installed and customized by the companies' technical IT team. In most cases you will be unaware of the firewalls existence.



## Hoaxes

### Hoaxes

- A hoax is an attempt to trick or deceive you into believing something which the perpetrator knows is not true. Hoaxes can take many forms such as chain letters, scams, false alarms, scares, virus hoaxes are just simple misunderstandings. The Internet has become a main source of hoaxes and scams.

## How to spot a hoax message

- A hoax message may contain one or more of the following signs:

The phrase **Forward this to everyone**. The more urgent the request the more suspicious the message.

The phrase '**This is not a hoax**' normally means the complete opposite.

Frequent use of uppercase letters and multiple exclamation points!!!!

Look for logical inconsistencies.

Read the text carefully and look for signs of subtle jokes.

Was the message actually written by the person who sent it?

SAMPLE

# Information Security

## Identity/Authentication

---

### Risks of unauthorised access

- Many computer systems can contain information which is personal or sensitive. This information has value and is therefore a potential target of unauthorised access. This can lead to theft of data or modification of the information.

### User IDs and passwords

- A User ID is normally used to logon to a computer, or computer network. It uniquely identifies you to the network. In addition you use a password which is only known to you. The password guarantees that no one can access the network and impersonate you (in theory). Once you have logged on (i.e. connected) to the rest of your computer network, you will have been assigned access rights to the network. Your network administrator will have defined these access rights. The idea of access rights is that you only have the ability to connect to, or share, devices which you have authority to use. In other words, the network administrators often have access rights to just about every computer, printer, modem etc on the network. You on the other hand may have access rights to print to only certain, specified printers and you may be able to access only certain data held on the network.

### Keep your passwords and PIN number secret

- Passwords and PIN numbers are used to protect your information from unauthorised access. It is important that you do not share them with anyone.

### Change your passwords and PIN number regularly

- Make sure that you change your PIN or password regularly as this will minimise the damage if your password or PIN should become known to a third-party.

### Changing your password or PIN number

- Your password is the only thing which will prevent someone else logging into a computer using your user ID and impersonating you. It is important to choose a password which cannot be easily guessed by other people. Ideally a password should be at least 8 characters long & contain a mixture of words and numbers. It is also recommended that you change your password regularly; some computer systems will require you to change your password

periodically. Never share your password with others.

- When choosing a PIN number try to make sure that the number is random and not something which can be easily guessed like a date of birth or a sequence of numbers like 1234.

---

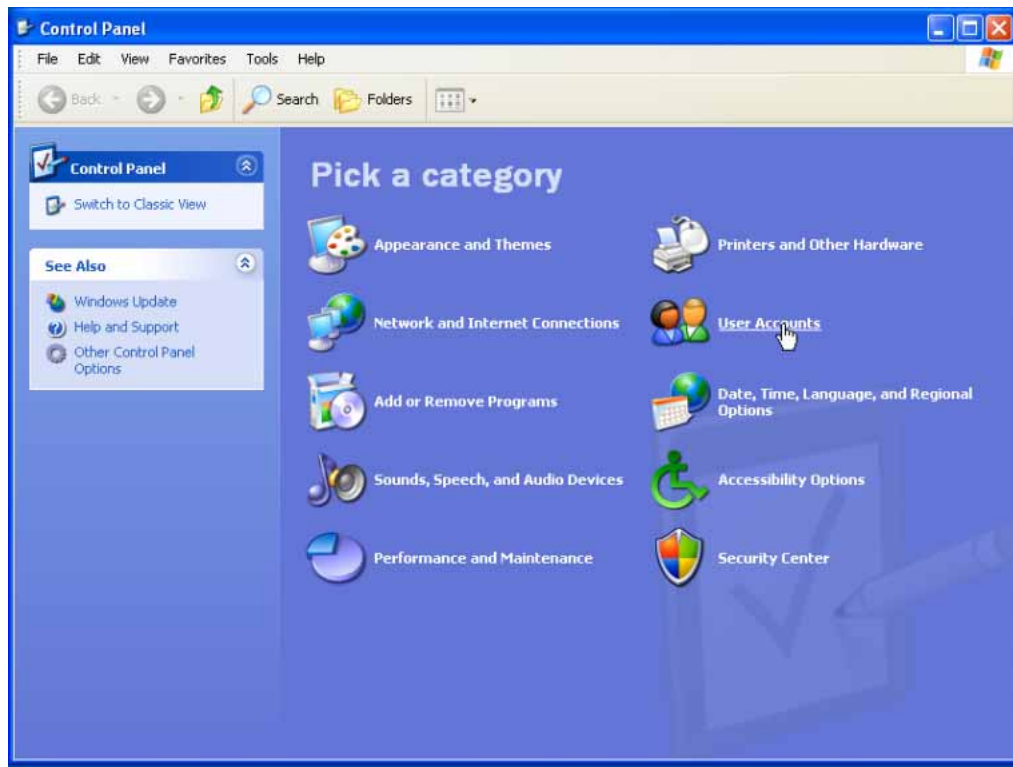
### How to change your password or PIN number on a Windows XP computer

- Click on the **Start** button to display the **Start** menu.
- Click on **Control Panel**. The **Control Panel** window will be displayed.



- The **Control Panel** window will be displayed. Click on **User Accounts**.

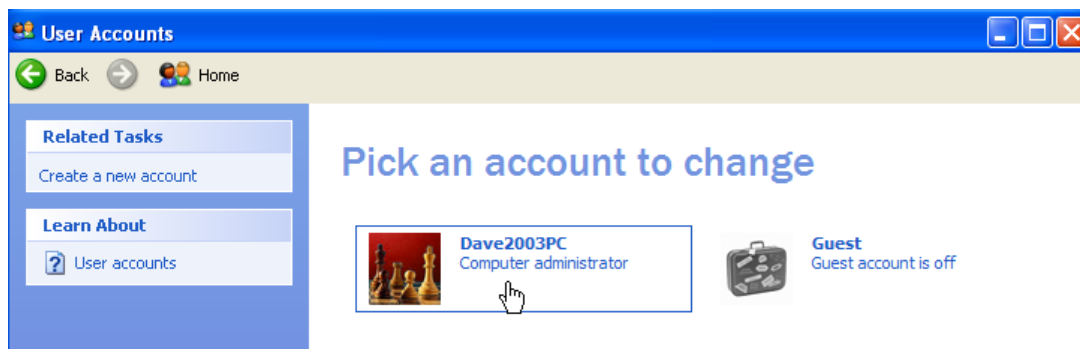
SAMPLE



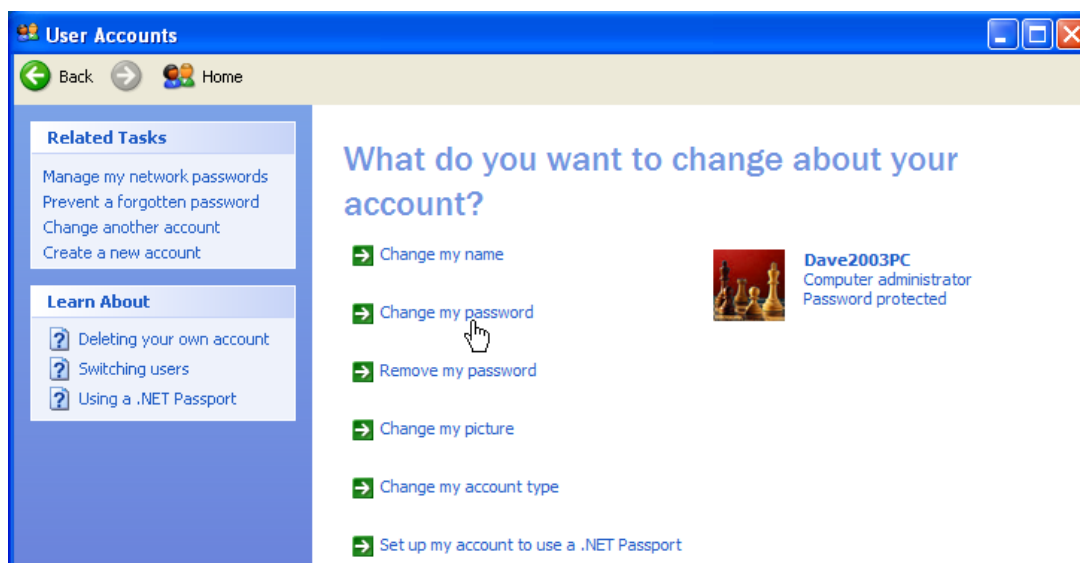
- The User Accounts options will be displayed. Click on **Change an account** from the Pick a task list.



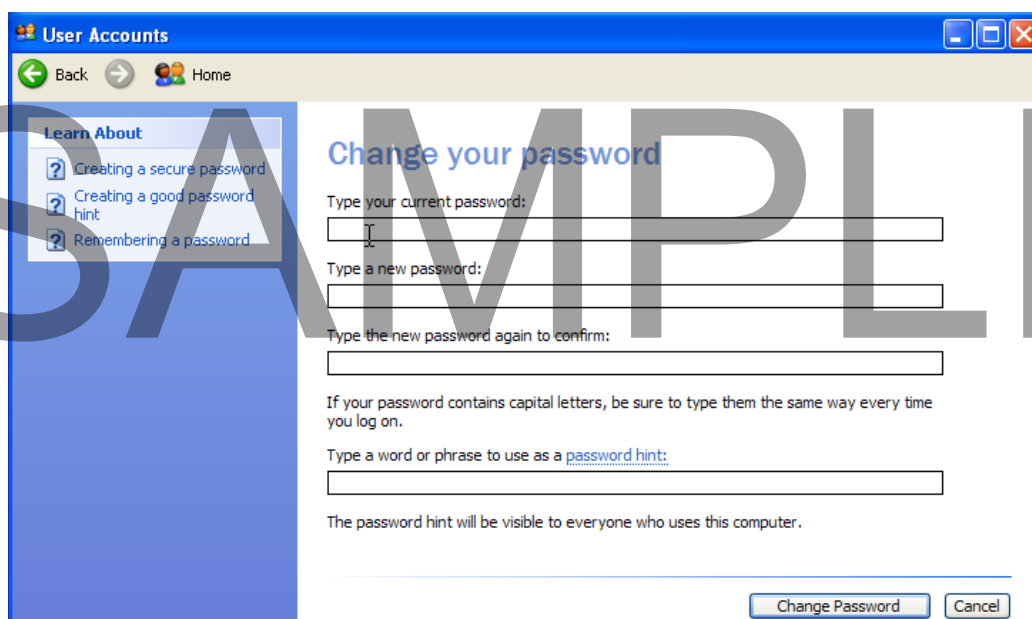
- Click on the user name whose password you wish to change.



- Click on **Change my password**.



- Fill in the form. You will need to enter your current password, followed by your new password twice. You also have the option of entering a password hint to help you remember the password.



- Click on the **Change password** button at the bottom of the window to apply the changes.

SAMPLE

## END OF THE SAMPLE PREVIEW.

This sample represents approximate half of the full course. Please see the Table of Contents at the beginning of this document to see the full list of topics covered.

To purchase the rights to duplicate the full version of this manual at your training centre, please visit our web site at:

[http://www.cctglobal.com/ecdl\\_bcs/samples.htm](http://www.cctglobal.com/ecdl_bcs/samples.htm)

A courseware licence allows you to make unlimited copies for use at your training centre and also includes the HTML versions of the courses for use on your local Intranet.



This sample allows you to preview our courseware and must not be used for training.

# SAMPLE