

Standard Module - IT Security This quick reference guide is for Microsoft Internet Explorer 9.0 and Word 2010

Quick Reference



Security Concepts

Data Threats 1.1

- Distinguish between data and information. 1.1.1
 - · Data is unprocessed information for data processing. Data may be a collection of unprocessed numbers, text, or images.

Information is the processed output of data making it meaningful to the person who receives it.

- Understand the term cybercrime. 1.1.2
 - · Cybercrime is an illegal activity that uses the Internet or a computer. Examples include identity theft and social engineering.

Understand the difference between: 1.1.3

- · Hacking involves using computer expertise to gain access to a computer system without authorisation. The hacker may wish to tamper with programs and data on the computer, use the computer's resources, or just prove they can access the computer.
- Password cracking involves recovering passwords from data that has been stored in or transmitted by a computer system. This can be attempted manually by quessing the password, or by using software.
- · Software cracking involves disabling or removing certain features in software that are deemed undesirable by the software cracker, for example, copy protection, serial numbers, hardware keys, date checks.
- · Ethical hacking involves attacking a computer security system with permission from its owners to find vulnerabilities that a malicious hacker could exploit.

1.1.4 Recognise threats to data from force maieure.

- Force majeure is a 'superior force' or an unforeseen event that can threaten data like:
 - Fire
 - Floods
 - War
 - Earthquake

1.1.5

Recognise threats to data from:

- · Employees Could steal company data such as new product information
- · Service providers Could lose, destroy, or steal valuable company data
- · External individuals Could gain access to a computer system and steal/delete data

Value of Information 1.2

- Understand the reasons for protecting personal 1.2.1 information like:
 - · Avoiding identity theft · Avoiding fraud
- 1.2.2 Understand the reasons for protecting commercially sensitive information like:
 - * Preventing theft or misuse of client details
 - Preventing theft or misuse of financial information
- 1.2.3 Identify measures for preventing unauthorised access to data like:
 - Encryption is the process of encoding data to make it unintelligible to any unauthorised person who tries to read the data.

· Passwords are a string of characters used for authentication, to prove identity or gain access to a resource

- Understand basic characteristics of information 1.2.4 security like:
 - · Confidentiality Ensures information is protected against unauthorised access or disclosure
 - · Integrity Refers to the trustworthiness of information resources
 - · Availability Refers to the availability of information resources
- Identify the main data/privacy protection, retention 1.2.5 and control requirements in your country.
 - In EU countries the 1995 European Data Protection Directive applies.
- 1.2.6 Understand the importance of creating and adhering to guidelines and policies for ICT use.
 - They provide a standard for users to follow and ensure that there is a clear position on how ICT should be used to ensure the protection of the organisation's data.

Personal Security 1.3

- 1.3.1 Understand the term social engineering
 - · Social engineering involves manipulating people into performing actions or divulging confidential information, rather than by hacking to obtain the information.

Certification Test Goals

This module sets out essential concepts and skills relating to the ability to understand the main concepts underlying the secure use of ICT in daily life and to use relevant techniques and applications to maintain a secure network connection, use the Internet safely and securely, and manage data and information appropriately.

Successful candidates will be able to:

- · Understand the key concepts relating to the importance of secure information and data, physical security, privacy and identity theft.
- · Protect a computer, device or network from malware and unauthorised access
- · Understand the types of networks, connection types and network specific issues including firewalls.
- Browse the World Wide Web and communicate on the Internet securely.
- · Understand security issues related to communications including e-mail and instant messaging.
- Back up and restore data appropriately and safely, and securely dispose of data and devices.

Understand its implications like: 1.3.1

- · Information gathering Gathering information that may be confidential or valuable
- Fraud Using gathered information to commit an act of fraud
- · Data access It facilitates unauthorised computer system access - potentially revealing confidential information

Identify methods of social engineering like: 132

- · Phone calls Misleading someone about your identity in a phone call to gain valuable information
- · Phishing Misleading someone about your
- identity online to gain valuable information Shoulder surfing - Using direct observation

to get information 1.3.3 Understand the term identity theft.

· Identity theft involves assuming another person's identity for personal gain. This can lead to the theft or misuse of personal, business or legal information.

Identify methods of identity theft like: 1.3.4

- · Information diving The practice of recovering information from discarded material
- Skimming Using a scanner device to skim information, often from a credit/debit card
- Pretexting Gaining personal information
- through deception **File Security**

1.4

Understand the effect of enabling/disabling 1.4.1 macro security settings.

- · Enabling a macro will ensure that the macro will run but may harm your computer if the source of the file is unknown.
- · Disabling a macro will ensure the macro will not run but may prevent you from using all the features in a file.

© 2012, ECDL Foundation. This Quick Reference may be used by candidates to assist in preparation for this ECDL module test. ECDL Foundation does not warrant that use of this guide will ensure passing of the test. Screen shots used with permission from Microsoft.

1.4.2 Set a password for files like:

Documents:

- Click File.
- · Click Info.
- · Click Protect Document.
- · Click Encrypt with Password.

Save	Information about Security S	iettings
🗃 Open	C\Uses\farenriDektrg\SecuritySettings.docx	
📬 Osse	(C) Permissions	
Ho (Anyone can open, copy, and Protect	change any part of this o
Recent	Document -	
New	Mark as final Let readers know the document is final and make it read-only.	
Friet Save & Send	Encrypt with Password Require a password to open this document	that it contains: thor's name
save & seno Help	Restrict Egiting Control what types of changes people can make to this document.	
Cythens	Bratict Permission by People Grant people access while removing	• me of this file.
Exe	their ability to edit, copy, or print.	The second life.
	Add a Digital Signature Ensure the integrity of the document by adding an invisible digital signature.	

- $\cdot\,$ Choose a password and click OK.
- Reenter the password and click OK. Compressed files:

• On the Home tab, select Encrypt.

- Select the files, folders to zip.
- · Click Zip
- · Choose a password and reenter the password.
- Click OK.

Spreadsheets:

- Click File.
- Click Info.
- Click Protect Workbook.

Click Encrypt with Password.

🖬 Save 🔛 Save As 🎯 Open		n about Income and sktop/Income and Expenditure.als	
Close by/o	07713	Permissions Anyone can open, copy, and char	ge any part of this workbo
New		nal s know the workbook is final if read-only.]
Print Save & Send		th Password password to open this	i it contains: r's name
Help	Control un	ment Sheet hat types of changes people can se current sheet.	
Coptions	Prevent un	orkbook Structure wanted changes to the structure Rbook, such as adding sheets.	of this file.
	Grant pets	minution by People ple access while removing their dif, copy, or print,	
	2 Ensure the	ital Signature - integrity of the workbook by invisible digital signature.	

- Choose a password and click OK.
- Reenter the password and click OK.
- 1.4.3 Understand the advantages and limitations of encryption.

Advantages:

- Encrypted data cannot be read without a key
- · Only an authorised receiver can read the message Limitations:
- If the encrypted key is lost it leaves the data unusable

2 Malware

2.1 Definition and Function

- 2.1.1 Understand the term malware.
 - Malware is malicious software that is designed to install itself on a computer without the owner's consent.
- 2.1.2 Recognise different ways that malware can be concealed like:
 - Trojan Destructive program that masquerades as an application
 - Rootkit Used to enable continued access to a
 - computer while actively hiding its presence
 - Back door Used to bypass system security

2.2 **Types**

2.2.1 Recognise types of infectious malware and understand how they work like:

- Viruses Computer programs that can replicate themselves and cause damage to a computer
- Worms Self-replicating malware that uses a computer network to send copies of itself to other computers

- 2.2.2 Recognise types of data theft, profit generating/ extortion malware and understand how they work like:
 - Adware Software package that automatically plays, displays, or downloads advertisements to a computer
 - Spyware Malware that collects information on user browser habits without their consent
 - Botnets Can infect and control computers
 without consent
 - Keystroke logging Involves the capturing of information that is typed on a keyboard
 - Dialers Malicious programs that install onto a computer and attempts to dial premium telephone lines at other locations

2.3 Protection

- 2.3.1 Understand how anti-virus software works and its limitations.
 - Anti-virus software uses scans to detect and block viruses before they infect your system.
 - Anti-virus software needs to be kept up to date with definition files. It cannot always stop attacks to system vulnerabilities or security flaws.
- 2.3.2 Scan specific drives, folders, files using

anti-virus software

- Launch the Anti-Virus Application.
 - Select the Drives, Folders, Files to scan.
- Click Scan.
- 2.3.2 Schedule scans using anti-virus software.
 - Launch the Anti-Virus Application.
 - Select the Schedule Scan options and select the Scan Frequency, Date/Time.
 - Click on the Scan button.

2.3.3 Understand the term quarantine and the effect of quarantining infected/suspicious files.

 Quarantining a file moves the file to a safe location on a drive that is managed by the anti-virus software.

The file can still be restored from quarantine if required.

2.3.4 Understand the importance of downloading and installing software updates, anti-virus definition files.

 Installing software updates and anti-virus definition files can fix a flaw or security risk in an application and update against new security risks.

3 Network Security

- 3.1.1 Understand the term network.
 - A group of two or more computer systems linked together by communications channels to allow for sharing of resources and information.
- 3.1.1 Recognise the common network types like:
 Local Area Network (LAN) A network that connects computers in close proximity, usually in the same building
 - Wide Area Network (WAN) A network that connects computers over a long distance, using telephone lines and satellite communications
 - Virtual Private Network (VPN) A network that allows users to privately share information between remote locations, or between a remote location and a business' home network
- 3.1.2 Understand the role of the network administrator.
 - Network administrators are involved in managing the authentication, authorisation and accounting within a network.
 - Tasks include maintaining staff access to required data on the network and ensuring network usage is in line with ICT policy.

3.1.3 Understand the function of a firewall.

 Used to protect a network from intrusions from outside sources.

3.1.3 Understand the limitations of a firewall.

- Does not always provide automatic notification if your network is hacked
- · Cannot protect against an attack generated
- from within the network

 May restrict some legitimate traffic
- 3.2 Network Connections

3.2.1 Recognise the options for connecting to a network like:

 Cable - Involves connecting to a network using physical cables

• Wireless - Connections that allow you to wirelessly connect to a network without the need for a cable

3.2.2 Understand how connecting to a network

has implications for security like: • Computers connected to the network may be

((0))

- infected with malware.Connecting to a network may open your
- system up to potential for unauthorised data access.
- Connecting to a network may increase the challenge of maintaining privacy.

3.3 Wireless Security

- 3.3.1 Recognise the importance of requiring a password for protecting wireless network access.
 - Requiring a password ensures that only authorised users can access the network and data.
- 3.3.2 Recognise different types of wireless security like:
 - Wired Equivalent Privacy (WEP)
 - Wi-Fi Protected Access (WPA)
 - Media Access Control (MAC)
- 3.3.3 Be aware that using an unprotected wireless network can allow wireless eavesdroppers to access your data.
 - · On an unprotected wireless network other
 - people may be able to access your data.
- 3.3.4 Connect to a protected/unprotected wireless network.

· Click Network and Sharing Center.

· Double click on the desired network.

· Enter the wireless network password

Understand the purpose of a network account

and how it should be accessed through a user

• For security reasons, a user name and

password should be required for a user to

 \cdot Adequate letter, number and special characters

Identify common biometric security techniques

Recognise good password policies, like:

· Click Connect to a network.

(protected network only).

• Click Start.

· Click Control Panel.

· Click Connect.

Access Control

name and password.

access a network.

Not sharing passwords

· Changing them regularly

Adequate password length

used in access control like:

Be aware that certain online activity

Purchasing – e.g. Online shopping

(purchasing, financial transactions) should

only be undertaken on secure web pages:

Financial Transactions - e.g. Online banking,

Fingerprint scanning

Secure Web Use

Web Browsing

fund transfers

3.4

3.4.1

3.4.2

3.4.3

4

4.1

4.1.1

mix

4.1.2 Identify a secure website:

Check the web page URL for "https"

(=) 🕘 🛃 https://www

Check for the Lock Symbol in the browser window

4.1.3 Be aware of pharming.

- Pharming An attack that redirects a website's traffic to a fake website
- 4.1.4 Understand the term digital certificate. Validate a digital certificate.
 - A digital certificate is used to provide 3rd party verification that the sender of a message is who they claim to be. The file contains a public key and other authentication information to allow it to be validated.
- 4.1.5 Understand the term one-time password.
 - A one-time password is a password that is valid for only one login session or transaction.
- 4.1.6 Select appropriate settings for enabling, disabling autocomplete, autosave when completing a form.

Autocomplete:

- · Click on the Tools button on the Command bar.
- Select Internet Options.
- <complex-block>
- Click the Settings button beside AutoComplete.
- Check/uncheck the AutoComplete options as



Click OK

Autosave:

- Click on the Tools button on the Command bar.
- Select Internet Options.
- · Select the Content tab.
- Click the Settings button beside AutoComplete.
- Check/uncheck the AutoComplete options for saving user names and passwords as required.

toComplete Setting	gs	
utoComplete lists por ped or visited before	ssible matches from entr e.	ries you've
Use AutoComplete fr	or	
Address bar		
Browsing hist	ory	
Favorites		
Fgeds		
Use Windows	Search for better resul	ts
Eorms		
User names and p	passwords on forms	
Ask me befor	e saving passwords	
	Delete AutoComple	te history
	ОК	Cancel

4.1.7 Understand the term cookie.

- Cookie A small piece of text stored by the web browser running on your computer
- The cookie can store information like pages visited on a site or information given to the site. When the user revisits, the cookie allows the website to recognise the user.
- 4.1.8 Select appropriate settings for allowing, blocking cookies.
 - Click on the Tools button on the Command bar.
 - · Select Internet Options.
 - · Select the Privacy tab.
 - · Click the Advanced button.

ieneral	Security	Privacy	Content	Connections	Programe	Advanced
Setting						
Select	a setting fo	r the Inte	met zone.			
1.7	Med	ium				
-	-50 -60 -80	acy policy ooks third used to co estricts fin	party cool intact you st-party co	ses that do not tes that save in without your es okies that save you without you	formation t plicit conse information	hat can nt i that
	Ş9H	lm	port	Adyanced	i) De	fiult
Locatio	n —	100000				
	er allow w sical (ocati		request ys	NF .	Qea	r Sites
Popup	Blocker -					
U Tur	n on Pap u	p Booker			Sg	tings
InPrive	he				-	
Disa	ble joolba	rs and ext	ensions wh	nen InPrivate D	rowsing sta	8
			_	C C C	-	

· Check/uncheck the Cookies options as required.

	ow cookies are handled in the Internet es automatic cookie handling.
Cookies	
Verride automatic cooki	ie handling
First-party Cookies	Third-party Cookies
Accept	Accept
O Block	🔘 Block
© Prompt	Prompt
Always allow session	cookies

Click OK.

- Block cookies if you are browsing on an unfamiliar website.
- 4.1.9 Delete private data from a browser like: browsing history, cached internet files, passwords, cookies, autocomplete data.
 - Click on the Tools button on the Command bar.
 Select Internet Options.
 - · Select the General tab.
 - Click the Delete button beside Browsing history.

General	Security	Deixener	Content	Connections	Programs	Advance
	Security	Privacy	Content	Connections	Programs	Auvance
Home p	age					
1	To cre	ate home	page tabs,	type each add	ress on its o	wn line.
	http	e / hananar d	nongle cor	m/a/ecdl.org/S	envicel onin	250 .
	uus s		i o o gi e i e o	n/u/ccunorg/	enneerogii	
						-
						
		Use <u>c</u> u	irrent	Use de <u>f</u> ault	Use	<u>b</u> lank
Browsi	ng history					-
1				ory, cookies, s	aved passw	ords,
	and w	eb form in	formation.			
	V Del	ete brows	ing history	on exit		
			F	0.1.1		
				Delete	Set	tings
Search	-					
C) Chang	e search o	defaults.		Set	tings
r						
Tabs -						
Tabs -		e how we	bpages are	displayed in	Set	tings
Tabs -	Chang tabs.	e how we	bpages are	displayed in	Set	tings
Tabs -	tabs.	e how we	bpages are	displayed in	Set	tings
Appea	tabs.					
Appea	tabs.		bpages are guages	displayed in Fo <u>n</u> ts		tings
Appea	tabs.					

Check/uncheck the Browsing history options as required.



- 4.1.10 Understand the purpose, function and types of content-control software like:
 - Internet filtering software Designed to filter and monitor access to websites
 - Parental control software Used to restrict the length of time spent on the Internet and restrict access to certain content

4.2 Social Networking

- 4.2.1 Understand the importance of not disclosing confidential information on social networking sites.
 - Examples of confidential information include passwords, PIN numbers, certain company information, client details.
 - Disclosing such information could lead to personal information, company information, client information or finances being stolen or misused.

4.2.2 Be aware of the need to apply appropriate

- social networking account privacy settings.
 Making your account public will allow anybody to view your personal details
- Ensure that personal details are hidden
 Understand potential dangers when using
 social networking sites like:
 - Cyber bullying Involves using the Internet and related technologies to harm other people, in a deliberate, repeated, and hostile manner
- Grooming Involves using the Internet and related technologies to befriend a person, in the negative context of preparing them to accept inappropriate behaviour
 - Misleading/ dangerous information can be posted by users
 - False identities may be assumed by social network users to contact other users
 - Fraudulent links or message may be sent to ellicit information from you

5 Communications

5.1 E-Mail

- 5.1.1 Understand the purpose of encrypting, decrypting an e-mail.
 - Encryption and decryption help to ensure only the intended recipient can read an e-mail.

5.1.2 Understand the term digital signature.

- A digital signature is an encrypted code that demonstrates the authenticity of a message.
- 5.1.3 Create and add a digital signature.
 - Click File.
 - Click Info.
 - Click Protect Document.
 - Click Add a Digital Signature.



- Click OK.
- · Select Create your own digital ID and click OK.
- Enter your Name, E-Mail Address, Organisation and Location details.
- · Click Create.
- Enter a Purpose for signing this document.
- Click Sign.
- 5.1.4 Be aware of the possibility of receiving fraudulent and unsolicited e-mail.
 - A fraudulent or unsolicited e-mail may contain a virus or malware, or may be trying to gain information from you and should not be opened.
- 5.1.5 Understand the term phishing.
 - Phishing involves misleading someone about your identity online to gain valuable information.
- 5.1.5 Identify common characteristics of phishing like:
 - Using names of legitimate companies, people, false web links.
- 5.1.6 Be aware of the danger of infecting the computer with malware:
 - By opening an e-mail attachment that contains a macro
 - · By opening an executable file

5.2 Instant Messaging

5.2.1 Understand the term instant messaging (IM) and its uses.

- Instant messaging is a form of real-time text-based communication between two or more people.
- IM can be used to have short text chats with colleagues/friends, to share links or files. Some IM
- programs also have VoIP and web camera functions. 5.2.2 Understand the security vulnerabilities of IM like:
 - Malware access
 - Backdoor access
 - · Access to files
- 5.2.3 Recognise methods of ensuring confidentiality while using IM like:
 - Encryption
 - Non-disclosure of important information
 - Restricting file sharing

6 Secure Data Management

- 6.1 Securing and Backing Up Data
- 6.1.1 Recognise ways of ensuring physical security of devices like:
 - Log equipment location and details
 - Use cable locks
 - Implement access control measures such as swipe cards, biometric scans
- 6.1.2 Recognise the importance of having a back-up procedure in case of loss of data, financial records, web bookmarks/history.
 - Back-up procedures will ensure that data can be recovered in the event it is lost.

- Examples of items to back-up include:
 Data
 - Financial records
 - · Web bookmarks/history
- 6.1.3 Identify the features of a back-up procedure like: Regularity/frequency – Set up how often you want a back-up to occur
 - Schedule Set up a back-up schedule
 - Storage location Set up a location to store your
 - back-up to like an external hard drive **Back up data.**
- 6.1.4 Back up data • Click Start.
 - Click Backup and Restore.
 - Set up Backup.
 - Chasses a backup.
 - Choose a back-up location (drive/network) and click Next.

and the second sec		
 Bat See Look Sept. Control Panel Huma Control a system intege Control a system report duc. 	Back up or restore your files British Working Harting has not been sit up. Ration Window caudi not find a backup for this company.	2 States of Section 1.
	Statut gydraf sdiryg i rydwi corpute	
Ten stor Action Center Sy Windows Easy Transfer		

• Choose what data to back up or accept the recommended default settings.

		-
0	😸 Set up backup	
	What do you want to back up?	
	Let Windows choose (recommended)	
	Windows will back up data files saved in libranes, on the desitop, and in default Windows folders. These items will be backed up on a regular schedule. <u>How does Windows choose what files to back</u> up	
	Let me choose	
	You can select libraries and folders and whether to include a system image in the backup. The items you choose will be backed up on a regular schedule.	
	Nest	

· Choose the back-up schedule.



- Save Settings and Backup.
- 6.1.5 Restore and validate backed up data. • Click Restore My Files.
 - Choose what you want to restore by using Search, Browse for Files or Browse for Folders to add files/folders to restore.

Ein Edit Ymw Ioolt Help			
Control Panel Home	Back up or rest	ore your files	
🚱 Create a system image	facture		
🖗 Create a system repair disc	Location	(8) 134.43 MB free of 334.65 MB	S Back up new
	~	Beckup size: 46.73 KB @Manage space	
	Next backup:	Not scheduled	
	Lethoka	19/08/2011 12:00	
	Contents	Files in selected folders	
	Schedule	None, Select Back up now to nut backup manually. Si Type on schedule	
		SChange settings	
	Restore		
	current location.		Enters my files
	Statut at un		
See abs	Sylateri aprila	e backup to restore files hore	
Action Center	Excessor exiters	settings or your computer	

- Click Restore My Files.
- Choose what you want to restore by using Search, Browse for Files or Browse for Folders to add files/folders to restore.
- · Click Next.
- Choose to restore in the original location or in the following location to choose a new location.

3 to feature files		
ge fielder rins		
Where do you want to restore your files?		
In the griginal location		
C in the following location:		
C many states	Inge.	
	angle.	
	Retire	

Click Restore.

6.2 Secure Destruction

- 6.2.1 Understand the reason for permanently deleting data from drives or devices.
 - To ensure it is completely unrecoverable for security reasons

6.2.2 Distinguish between deleting and permanently destroying data.

- Deleting data by moving it to the recycle bin does not permanently destroy the data.
- Permanently deleting data by shredding or degaussing ensures that it cannot be recovered.

6.2.3 Identify common methods of permanently destroying data like:

- Shredding Shredding disks like CD/DVD
 Drive/media destruction Physical destruction
- of a drive or media • Degaussing - Leaves the magnetic domains on a disk in random patterns rendering previous data unrecoverable
- Using data destruction utilities Software/utility to carry out the destruction of data on a drive

For more information, visit:

www.icdl.org

© 2012, ECDL Foundation Ltd. This Quick Reference may be used by candidates to assist in preparation for this ECDL module test. ECDL Foundation does not warrant that use of this guide will ensure passing of the test. Screen shots used with permission from Microsoft.