

BCS IT User Syllabus IT Security for Users Level 1

Version 1.0

March 2009

CATEGORY	SKILL SET	REF.	TASK ITEM
1.1 System Performance Security	1.1.1 Unwanted Messages	1.1.1.1	Know what 'spam' is
		1.1.1.2	Understand that unwanted email and other messages, or 'spam', can be received on the computer
		1.1.1.3	Use anti-spam software to protect the computer from the risk of unwanted messages
	1.1.2 Malicious Programs	1.1.2.1	Understand what malicious programs are: viruses, worms, trojans, spyware, adware, rogue diallers
		1.1.2.2	Be aware of how malicious programs can enter the computer
		1.1.2.3	Use anti-virus and anti-spyware software to protect the computer from the risk of malicious programs
		1.1.2.4	Know that anti-virus software needs to be updated regularly
		1.1.2.5	Know how to protect yourself from malicious programs: do not open email attachments from unknown users, treat messages, files, software and attachments from unknown sources with caution
	1.1.3 Infiltration	1.1.3.1	Know what a hacker is
		1.1.3.2	Know how hackers can attempt to infiltrate the computer
		1.1.3.3	Understand that a firewall helps to protect the computer against the risk of infiltration
	1.1.4 Hoaxes	1.1.4.1	Know that you can receive hoaxes: virus hoaxes, chain letters, scams, false alarms, misunderstandings, scares
		1.1.4.2	Know how to check whether a message you have received is a hoax
	1.2 Information Security	1.2.1 Identity/Authentication	1.2.1.1
1.2.1.2			Know that an individual user name limits access to relevant levels of information when logging onto a computer
1.2.1.3			Understand that passwords and PIN numbers help to protect information from the risk of unauthorised access
1.2.1.4			Understand that you should change your password/PIN number regularly
1.2.1.5			Know how to change your password/PIN number
1.2.2 Confidentiality		1.2.2.1	Understand that you should not share your password/PIN number with others
		1.2.2.2	Understand that you should not write down your password/PIN number

CATEGORY	SKILL SET	REF.	TASK ITEM
		1.2.2.3	Know that you should respect the confidentiality of information you have access to
		1.2.2.4	Know that you should not leave your computer unattended without logging off or locking it, to prevent the risk of access to your data
	1.2.3 Identify Theft	1.2.3.1	Know what phishing is
		1.2.3.2	Understand identify theft and how to avoid it
		1.2.3.3	Avoid inappropriate disclosure of information
1.3 Technology Security	1.3.1 Networks	1.3.1.1	Understand what a public network is
		1.3.1.2	Know that unsecured networks can make information accessible to others
		1.3.1.3	Be aware that you should not send unencrypted confidential information across an unsecured network
		1.3.1.4	Understand that wireless networks may be visible or accessible to other users
		1.3.1.5	Be aware of the security risks when using default passwords and settings on networks, computers and programs
		1.3.1.6	Know that your internet security settings should be adjusted to prevent the risk of access to your network by other users
	1.3.2 Connectivity	1.3.2.1	Know what Bluetooth connectivity is
		1.3.2.2	Understand that Bluetooth settings should be adjusted to prevent the risk of unauthorised access to a Bluetooth device by others
	1.3.3 Portable Devices	1.3.3.1	Know that portable devices are vulnerable to loss or theft: laptop, notebook, PDA, mobile phone, multimedia player
		1.3.3.2	Know that USB and other removable storage devices can contain valuable and confidential information, and are vulnerable to loss or theft
		1.3.3.3	Ensure all portable and removable devices are stored safely and securely
1.4 Guidelines and Procedures	1.4.1 Guidelines and Procedures	1.4.1.1	Know where to find the relevant guidelines and procedures for the secure use of IT within your organisation
		1.4.1.2	Ensure you follow the guidelines and procedures for the secure use of IT
		1.4.1.3	Know who to approach if you are unsure of the procedure to follow
		1.4.1.4	Understand the IT security checks you should carry out
		1.4.1.5	Know how to report IT security threats or breaches

CATEGORY	SKILL SET	REF.	TASK ITEM
	1.4.2 Privacy	1.4.2.1	Know the privacy policy within your organisation
		1.4.2.2	Ensure you follow the privacy policy within your organisation
1.5 Data Security	1.5.1 Security	1.5.1.1	Know ways to prevent data theft like: locking computer and hardware using a security cable
	1.5.2 Backups	1.5.2.1	Be aware of the possibility of accidental file deletion
		1.5.2.2	Be aware of the possibility of data corruption
		1.5.2.3	Be aware of the possibility of computer malfunction and subsequent file loss
		1.5.2.4	Understand that you should back up your personal data to appropriate media
		1.5.2.5	Understand the importance of having a secure off-site backup copy of files
	1.5.3 Storage	1.5.3.1	Know how to store your personal data safely
		1.5.3.2	Know how to store software securely