Enabling the information society

BCS IT User Syllabus
IT Security for Users Level 2

Version 1.0

June 2009

CATEGORY	SKILL SET	REF.	TASK ITEM
ITS2.1 System Performance Security	ITS2.1.1 Unwanted messages	ITS2.1.1.1	Be able to describe how unwanted email and other messages, or 'spam', can be received on the computer
		ITS2.1.1.2	Use and manage anti-spam software to protect the computer from the risk of unwanted messages
	ITS2.1.2 Malicious programs	ITS2.1.2.1	Be able to describe what malicious programs are and how they can enter the computer: viruses, worms, trojans, spyware, adware, rogue diallers
		ITS2.1.2.2	Know how to gain protection from malicious programs: do not open email attachments from unknown users, treat messages, files, software and attachments from unknown sources with caution
		ITS2.1.2.3	Be able to describe how anti-virus software can protect hardware, software and data
		ITS2.1.2.4	Configure and use anti-virus and anti-spyware software to protect the computer from the risk of malicious programs
		ITS2.1.2.5	Be able to update anti-virus software, and know how often this should be done
	ITS2.1.3 Infiltration	ITS2.1.3.1	Know what a hacker is and describe how a hacker can attempt to infiltrate the computer
		ITS2.1.3.2	Be able to describe how a firewall can protect the computer against the risk of infiltration
		ITS2.1.3.3	Adjust firewall settings to minimise security risk
	ITS2.1.4 Hoaxes	ITS2.1.4.1	Be able to describe what hoaxes are, and how to check whether a received message is a hoax: virus hoaxes, chain letters, scams, false alarms, misunderstandings, scares
	ITS2.1.5 Software	ITS2.1.5.1	Be able to describe how setting up and using security software can further protect the computer from Internet threats such as malicious web pages, zero day exploits, drive-by downloads
		ITS2.1.5.2	Be able to describe how security software patches and updates can protect software
		ITS2.1.5.3	Know how to download security software patches and updates
		ITS2.1.5.4	Be aware of the threats to software and data when downloading software from the Internet

CATEGORY	SKILL SET	REF.	TASK ITEM
		ITS2.1.5.5	Know and use the methods available to protect software and data when downloading software from the Internet
ITS2.2 System and Information Security and Integrity	ITS2.2.1 Information Security	ITS2.2.1.1	Be able to describe how information can be at risk from theft, from unauthorised access
		ITS2.2.1.2	Be able to describe how malicious programs and hackers can threaten information and system security
	ITS2.2.2 Networks	ITS2.2.2.1	Be able to describe how unsecured networks can make information accessible to others
		ITS2.2.2.2	Know how to ensure that unencrypted confidential information is not sent across an unsecured network
		ITS2.2.2.3	Know how to ensure that a wireless network is not accessible to other users
		ITS2.2.2.4	Be able to describe how a proxy server can protect computers on a network
		ITS2.2.2.5	Be able to adjust internet security settings to prevent the risk of access to the network by other users
		ITS2.2.2.6	Be able to describe how access controls can minimise the security risk to systems and data on networks
		ITS2.2.2.7	Be able to describe the security risks when using default passwords and settings on networks, computers and programs
	ITS2.2.3 Confidentiality	ITS2.2.3.1	Use access controls to keep data confidential
		ITS2.2.3.2	Know that it is important to respect the confidentiality of any accessible information
		ITS2.2.3.3	Know that the computer should not be left unattended without logging off or locking it, to prevent the risk of unauthorised access to data
ITS2.3 Access to Information Sources	ITS2.3.1 Identity/Authentication	ITS2.3.1.1	Be able to describe how an individual user name limits access to relevant levels of information when logging onto a computer
		ITS2.3.1.2	Be able to describe how passwords and PIN numbers help to protect information from the risk of unauthorised access
		ITS2.3.1.3	Be able to describe what makes a password strong or weak

CATEGORY	SKILL SET	REF.	TASK ITEM
		ITS2.3.1.4	Be able to describe why passwords/PIN numbers should be changed regularly
		ITS2.3.1.5	Be able to describe why passwords/PIN numbers should not be shared with others or written down
		ITS2.3.1.6	Be able to manage passwords/PIN numbers: change regularly, select strong passwords
	ITS2.3.2 Identify theft	ITS2.3.2.1	Be able to describe phishing
		ITS2.3.2.2	Know how to avoid being affected by phishing
		ITS2.3.2.3	Be able to describe identity theft
		ITS2.3.2.4	Know how to avoid being affected by identity theft
		ITS2.3.2.5	Be able to describe the threat to information security associated with an online identity or profile
		ITS2.3.2.6	Know steps that can be taken to keep a personal identity secure: whether to use a real name or a pseudonym, what an avatar is and how this can protect a personal identity
		ITS2.3.2.7	Be aware of how to keep personal information secure within an online profile: what information to include, who should be given access to this information, when to withhold personal information
		ITS2.3.2.8	Avoid inappropriate disclosure of information
	ITS2.3.3 Bluetooth	ITS2.3.3.1	Be able to describe what Bluetooth connectivity is, and why information on Bluetooth devices is vulnerable to unauthorised access
		ITS2.3.3.2	Be able to adjust Bluetooth settings to prevent the risk of unauthorised access to a Bluetooth device by others
	ITS2.3.4 Portable Devices	ITS2.3.4.1	Be able to describe why portable devices are vulnerable to loss or theft: laptop, notebook, PDA, mobile phone, multimedia player
		ITS2.3.4.2	Be able to describe why USB and other removable storage devices are vulnerable to loss or theft of valuable and confidential information
		ITS2.3.4.3	Be able to describe how information stored on USB and other removable devices can be protected: passwords, safe and secure storage

CATEGORY	SKILL SET	REF.	TASK ITEM
ITS2.4 Guidelines and Procedures	ITS2.4.1 Security	ITS2.4.1.1	Know and apply the guidelines and procedures for the secure use of IT set by employers or organisations
		ITS2.4.1.2	Know the legal requirements within security procedures for organisations
		ITS2.4.1.3	Know who to approach if unsure of a security procedure to follow
		ITS2.4.1.4	Know how to use products to ensure information security within organisations
		ITS2.4.1.5	Understand and carry out relevant IT security checks
		ITS2.4.1.6	Know how to report IT security threats or breaches
	ITS 2.4.2 Privacy	ITS2.4.2.1	Understand and follow the privacy policy within an organisation
ITS2.5 Data Security	ITS2.5.1 Security	ITS2.5.1.1	Be able to describe ways to prevent physical data theft like: locking computer and hardware using a security cable
		ITS2.5.1.2	Be able to describe how different access levels can protect data on a network
		ITS2.5.1.3	Be able to describe how the use of risk assessment can help to minimise common security risks
	ITS2.5.2 Backups	ITS2.5.2.1	Be able to describe the possible consequences of accidental file deletion: on a personal computer, on a network
		ITS2.5.2.2	Be aware of the consequences of data corruption
		ITS2.5.2.3	Be aware of the consequences of computer malfunction and subsequent system and file loss
		ITS2.5.2.4	Select and use effective back up procedures for data, and know the importance of doing so
		ITS2.5.2.5	Be able to describe the importance of having a secure, off-site backup copy of data
		ITS2.5.2.6	Select and use effective back up procedures for systems, and know the importance of doing so
	ITS2.5.3 Storage	ITS2.5.3.1	Know how to store data safely and securely
		ITS2.5.3.2	Be aware that it is important to control access to software, to ensure it is not accessed by unauthorised users
		ITS2.5.3.3	Know how to store software safely