1.2 Security - Security Unit Study Guide

1. Describe common security problems and their impacts
2. Explain good security practices (preventative measures)
3. Explain solutions to common security problems (corrective measures)
4. Select the appropriate security software based on the risks a user faces
5. Explain how biometric technology works, using technical language
6. Discuss the ethical issues related to encryption and biometric

Security refers to the protection of hardware, software, machines and networks from unauthorized access. Security measures include restricted access to machines and networks for certain employees or to prevent access by hackers. The degree of security of information systems largely determines society's confidence in the information contained in the systems.

Internet threats and security

- Internet security: for example, firewall, proxy server, SSL (secure sockets layer), encryption, public and private keys, digital signatures
- Internet threats: for example, global viruses, hackers, spam, phishing, pharming, spyware, adware

General Information Links:

- http://itgsopedia.wikispaces.com/1.2+Security
- http://www.itgstextbook.com/chapter5-security.html

Practice using these terms in all your answers. These are the words that qualify as technical language:

access levels	anti-virus	asymmetric key encryption	authentication	backdoor
biometric enrolment	biometric template	biometrics	botnet	brute force attack
CAPTCHA	Certificate Authority	ciphertext	Computer Misuse Act	cracking
Denial of Service attack	dictionary attack	digital signatures	Distributed Denial of Service	DNS poisoning
drive-by download	encryption	encryption key	EVSSL	false negative
false positive	full disk encryption	hacking	home directory	https
identity theft	key escrow	key logger	key pair	macro virus
malware	multi-factor authentication	one time password	packet sniffer	passphrase
password	pharming	phishing	physical security	plaintext
private key	public key	root user	rootkit	secret key encryption
Secure Socket Layer	security token	security update	smishing	social engineering
spam	spam bot	spam filters	spyware	symmetric key encryption
system administrator	Transport Layer Security	Trojan horse	unauthorised access	virus
virus definition file	vishing	vulnerability scanner	web bug	WEP
worm	WPA	WPA2	zombie	