CYBER SECURITY

0478/0984 COMPUTER SCIENCE SYLLABUS

CAMBRIDGE INTERNATIONAL EXAMINATIONS (CIE)

Syllabus Overview

5.3 Cyber security

Candidates should be able to:	Notes and guidance
1 Describe the processes involved in, and the aim of carrying out, a range of cyber security threats	• Including: – brute-force attack – data interception – distributed denial of service (DDoS) attack – hacking – malware (virus, worm, Trojan horse, spyware, adware, ransomware) – pharming – phishing – social engineering

5.3 Cyber security continued

Candidates should be able to:	Notes and guidance
2 Explain how a range of solutions are used to help keep data safe from security threats	• Including: – access levels – anti-malware including anti-virus and anti-spyware – authentication (username and password, biometrics, two-step verification) – automating software updates – checking the spelling and tone of communications – checking the URL attached to a link – firewalls – privacy settings – proxy-servers – secure socket layer (SSL) security protocol

Hacking

- When a person tries to get unauthorized access to and corrupt data
- There are various ways in which a hacker can get access to your computer data

Did you know?

Did you know that not all hackers are criminals. There is a type of hackers called the ‘white hat’ hackers which are employed by companies to prevent the criminal hackers.

Malware

- Malware is a malicious code/software program used to harm a computer system or damage data

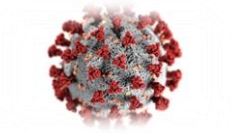
- Examples of malware are: Virus, worms, Trojans horse, spyware

- Generally, criminal hackers download the malware into the computer in order to get access to your device or harm your computer storage

- How a malware could be downloaded on a computer?
  - User clicks on a link from an untrusted email/website
  - When link is clicked the malware is downloaded

You only need to know, from the types of malwares, how virus and spyware work. But you just need to be aware of the other examples (worm, Trojan horse adware, ransomware)

Virus



- A type of malware
- A virus is a coded program which that is able to replicate itself to damage a computer system.
- The harm could be in the form of: deleting files, damaging programs, or even reformatting the hard drive of a computer.
- Other virus programs could keep replicating themselves and use up the storage space in a computer.
    - This may lead to the slowing down of a computer system

Spyware

- A type of malware
- Spyware records key logs from keyboard
- Key-logs are sent back to the creator of the spyware (Third party)
- The key-logs are analysed
- Common pattern in the key-logs shows password
- This allows the hacker to get access to the computer

Antimalware programs

- Luckily, there are programs that limit from malware attacks such as anti-spyware and anti-virus programs.

ANTISPYWARE	***ANTIVIRUS***
• Scans the computer for a spyware • Alerts the user for presence of a spyware • Removes the Spyware • Checks the files for spyware before being downloaded	• Scans computer for a virus • Alerts user of virus being present • Quarantines the Virus • Removes the virus • Checks the data before being downloaded

Internet Security

- Internet, just like the real world, has criminals individuals and associations which try to steal personal information from people and take their properties (e.g. bank account, passwords, locations etc...)
- Everyone using the internet should be aware of how to avoid these criminals.

Phishing

- Exciting looking email is sent to a user
- The user is encouraged to click on the link that is provided
- Redirects user to an exciting looking email

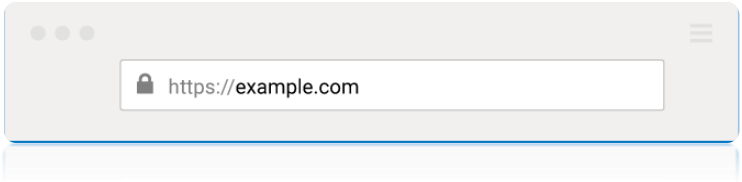
Pharming

- An exciting looking website is presented
- Offers desirable prizes and discounts that attracts victims.
- May have a similar website presentation to a well-known company
- Asks for sensitive information

How to ensure a website is secure?

- Checking the URL

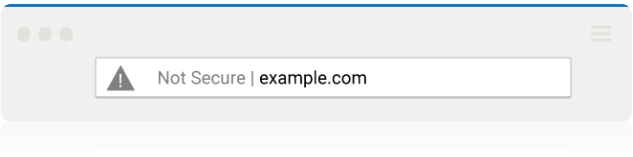
Authentic Websites



- Closed padlock

HTTPS (Hyper Text Transfer Protocol Secure)

Unauthentic Websites



- No padlock

Checking the spelling and tone of communication

Authentic Websites

- Website is continuously updated
- Accurate Grammar and spelling

Unauthentic Websites

- Website is not up to date
- Inaccurate Grammar and spelling

SSL (Secure Socket Layer)

- Security protocol
- Encrypts data sent
- Digital certificates is sent to the browser
- Contains the public key
- The website is authenticated
- Once the certificate is authenticated everything runs.

The SSL uses **Encryption** when it sends data. As the encryption algorithm is used, the original data (**plain text**) is scrambled into **cypher** text. An **encryption key** is used to encrypt data and a decryption key is required to **decrypt** the data sent.

In an Exam

If you mention that SSL stands for Secure Socket Layer **AND** it is a Security protocol you get 2 marks!
You can use this technique to answer similar exam questions.

DDOS (Distributed Denial of Service attacks)

- The DOS is made to deny people access to a website
- Many requests are sent at the **same time**
- The webserver is unable to respond
- The server fails as a result

The Denial-of-Service attacks are stopped by firewalls and proxy servers.

FIREWALL

- Monitors traffic coming into and out of the computer system
- Checks that the traffic meets any rules set/criteria
- Blocks the traffic that does not meet the criteria
- Can set a blacklist and block the IP address
- Close certain ports

Proxy Server

- Prevents direct access to the webserver
- If an attack happens it hits the proxy server instead.
- Directs invalid traffic away from webserver
- Traffic is examined by proxy server.
- If the traffic is valid the data would be obtained by user.
- If the traffic is invalid request, then data is denied by the proxy server.
- The proxy server can block requests from IP addresses.

Authentication

- Strong Password (small letters, capital letters, numbers, symbols)
    - Do not use the same password for all accounts
    - Do not personalize the password
    - Make password have more characters
    - Make password harder to guess

- Biometrics (storing unique features of an individual)
    - Physical features (finger print, face ID, Retina scan etc.…) cannot be copied and used by criminals.

- Two step verification
    - Extra data sent to device making it more difficult for hackers to guess.

*Prevent data loss (due to sudden shut of power supply, disasters, sudden shut down of computers) by saving your data and having a backup storage.