Cambridge (CIE) IGCSE ICT

Your notes

Security

Contents

Hacking

What is a hacking?

- Hacking is a generic term used to describe the act of gaining **unauthorised access** to computer **systems or networks** to gain **control**, **steal information**, or **cause damage**
- A hacker is a **criminal** who **exploits technical vulnerabilities** to break into computer systems and networks
- Hackers **seek out opportunities** that make this possible, these include:
  - **Unpatched software**
  - **Out-of-date anti-malware**
  - **Weak passwords**

What are the effects of hacking?

- Hacking can cause a number of issues for an organisation or individual, these include:
  - **Data breaches**
  - **Installation of malware**
  - **Data loss**
  - **Identify theft**
  - **Financial loss**

How can hacking be prevented?

- Hacking can be prevented by a number of methods, some of these include:
  - Using **strong passwords**
  - Using **two-factor authentication**
  - Installing **anti-malware software**
  - Using **firewalls**

Phishing

What is a phishing?

- Phishing is a form of social engineering
- It involves sending **fraudulent, legitimate-looking emails** to a large number of email addresses, claiming to be from a **reputable company** or trusted source to try and **gain access** to your details

- Phishing often tries to coax the user to click on a login button to enter their details

What are the effects of phishing?

- The creator of the email can gain unauthorised access to personal data such as login information, bank accounts and more
- Phishing can lead to identity theft or fraudulent activity on credit cards and bank accounts

How can phishing be prevented?

- Phishing can be prevented by:
  - **Anti-spam filters** to avoid fraudulent emails arriving in a user's inbox
  - **Training staff** to recognise fraudulent emails and to avoid opening attachments from unrecognised senders
  - **User access levels** to prevent staff from being able to open files-types such as executable (**.exe)** files and batch (**.bat**) files

Pharming

What is a pharming?

- Pharming is typing a website address into a browser and it is redirected to a 'fake' website to trick a user into typing in sensitive information such as passwords
- An attacker attempts to alter DNS settings or change a users browser settings to redirect users to the fraudulent website

What are the effects of pharming?

- The creator of the malicious content can gain unauthorised access to personal data such as login information, bank accounts and more
- Pharming can lead to identity theft or fraudulent activity on credit cards and bank accounts

How can pharming be prevented?

- Pharming can be prevented by:
  - **Keeping anti-malware software up to date**
  - **Checking URLs regularly**
  - **Make sure the padlock icon is visible**

Smishing & vishing

What is a smishing & vishing?

- Smishing (**SMS phishing**) is a **form of phishing** where attackers **use SMS** to **trick individuals into sharing sensitive information** or downloading malicious content.

- Vishing (**voice phishing**) is also a **form of phishing** involving **fraudulent phone calls** where attackers **impersonate legitimate companies** to get personal information

What are the effects of smishing and vishing?

- These attacks can result in unauthorised access to personal data such as login information and bank accounts
- They can lead to identity theft

How can pharming be prevented?

- Pharming can be prevented by:
  - **Keeping anti-malware software up to date**
  - **Checking URLs regularly**
  - **Make sure the padlock icon is visible**

Viruses & malware

Why is malware a threat?

- Malware (**mal**icious soft**ware**) is the term used for any software that has been created with malicious intent to cause harm to a computer system
- Examples of issues caused by malware include
  - Files being **deleted**, **corrupted** or **encrypted**
  - Internet connection becoming **slow** or **unusable**
  - Computer **crashing** or **shutting down**
- Malware can exist in many forms, each designed to perform its role in different ways

Malware	What it Does
Computer virus	▪ A program which can **replicate itself** on a user's computer. It contains code that will cause **unwanted and unexpected events** to occur ▪ Examples of issues a user may experience are ▪ **Corrupt** files ▪ **Delete** data ▪ **Prevent** applications from running correctly
Trojan	▪ Sometimes also called a **Trojan Horse** ▪ Trojans **disguise** themselves as **legitimate software** but contain malicious code in the background

Spyware	▪ Software which will allow a person to **spy** on the users' **activities** on their devices ▪ This form of software will be embedded into other software such as games or programs that have been downloaded from **illegitimate sources** ▪ Spyware can **record** your screen, log your **keystrokes** to gain access to **passwords** and more

How can malware be prevented?

- To protect against the threat of malware:
    - **Ensure code is written correctly**
    - **Keep anti-malware software up to date**
    - **Install a firewall**
    - **Educate users**

Card fraud

Why is card fraud a threat?

- Card fraud is a threat as fraudsters will try to gain illegal access to credit and debit cards
- The main way this is achieved is through:
    - **Shoulder surfing (shouldering)**
    - **Card cloning**
    - **Keylogging**

Shoulder Surfing

- **Observing a person's private information** over their shoulder e.g. cashpoint machine PINs
- This can be prevented by users ensuring they have **covered over their PIN** when entering it

Card cloning

- This is the **copying of the data from a user's credit or debit card** by scanning the magnetic strip through a skimmer machine
- Card cloning can be prevented by ensuring a **card with a chip** is being used and the chip can not be cloned, though the data on it can still be read

Keylogging

- This is software installed to **detect and store keystrokes** from the keyboard and send the data back to the criminal

- Data such as passwords and other secure data can be collected this way
- To prevent key logging, users should **frequently scan their system** using anti-virus software and use cloud **password software** to prevent having to enter their details manually

Your notes

Protection of Data

How can data be kept securely?

- Data can be held securely by storing it in an **encrypted format** and ensuring **authentication** is being used
- This goes a long way to ensuring that **only trusted sources** can access the data
- There are a number of ways to store data securely, these include:
  - **Biometrics**
  - **Digital certificate**
  - **Secure socket layer (SSL)**
  - **Encryption**
  - **Firewall**
  - **Two-factor authentication**
  - **Usernames & passwords**

Biometrics

What are biometrics?

- Biometrics are a way of authenticating a user by using their **unique human characteristics**
- Some of the ways biometrics can be used are:
  - **Fingerprint scans**
  - **Retina scans**
  - **Facial recognition**

What are the benefits of using biometrics?

- Biometric data is unique to the person and can not be copied, meaning that the data is always with the person
- Passwords can be easily copied, forgotten, guessed or cracked
- It is difficult to copy or forge biometric data
- Biometrics eliminates the possibility of attacks such as shoulder surfing and key-logging software
- Biometrics of a high degree of accuracy as there is no known way to copy a person's retina pattern for example

What are the drawbacks of using biometrics?

- Collecting biometric data can be intrusive, for example, scanning eyes
- Scans be not be recognised, an example of could be fingerprint scans with dirty hands
- Retina and iris recognition is very expensive to install
- Low light can provide an issue for facial recognition as well as hats and glasses
- people may be uncomfortable having their most unique characteristics being stored in a database

Digital certificate

What is a digital certificate?

- A digital certificate is a digital file used to prove who stores the public key
- The public key works alongside a private key to encrypt and decrypt the data so that all content is secure
- Digital certificates are given by trusted companies to ensure they are real and safe

What is included in a digital certificate?

- Digital certificates contain a lot of information, some of this includes:
  - **Public key**: The key associated with the holder
  - **Subject information**: Details about the holder
  - **Issuer information**: This identifies the certificate authority (CA)
  - **Validity period**: The start and end date for the certificate to remain valid
  - **Serial number**: A unique number to identify the certificate
  - **Signature algorithm**: The algorithm used by the CA to sign the certificate
  - **Digital signature**: The CA's signature to prove the certificate was issued by them

Secure Socket Layer (SSL)

What is SSL?

- Secure Socket Layer (**SSL**) is a **security protocol** which is used to **encrypt data** transmitted **over the internet**
- This helps to prevent **eavesdropping** and other forms of **interception**
- SSL is widely used to protect **online transactions**, such as those involving credit card information or other sensitive data
- It works by sending a **digital certificate** to the user's browser
- This contains the **public key** which can be used for **authentication**

- Once the certificate is authenticated, the transaction will begin

Worked Example

(i)) Identify a security solution that could be used to protect a computer from a computer virus, hacking and spyware.

Each security solution must be different

Threat	Security solution
Phishing	
DDoS attack	
Hacking	

[3]

(ii) Describe how each security solution you identified in (i) will help protect the computer.

[6]

Answers

(i)

Threat	Security solution
Phishing	Monitoring communication
Brute force attack	Authentication
Hacking	Firewall/Biometrics

(ii) **Two** marks for each description

- **Monitoring communication**
  - Checking for spelling & grammar errors
  - Reading tone, is the user being rushed? // is the user made to panic?
- **Authentication**
  - Checks the user is they say they are
  - Captcha proves they are not a bot
  - Passwords lockout after a set number of attempts
- **Firewall**
  - Monitors traffic coming into and out of the computer system
  - Checks that the traffic meets any criteria/rules set
  - Blocks any traffic that does not meet the criteria/rules set // set blacklist/whitelist
- **Biometrics**

- Data needed to enter is unique to individual
- … therefore it is very difficult to replicate
- Lock out after set number of attempts

Encryption

What is encryption?

- Encryption is a method of converting plain text into **ciphered text** to be stored
- Encryption uses complex mathematical algorithms to scramble the text
- Asymmetric encryption, also known as private key, public key encryption is often used for web pages and other communication

What form of attack would this prevent?

- Encryption plays a role in all forms of attack on a network
- It is important to note that it **does not prevent the attacks** from occurring but it does stop the attacker from gaining access to the information

Firewall

What is a firewall?

- A firewall is a **barrier** between a network and the internet
- A firewall prevents **unwanted traffic** from entering a network by filtering requests to ensure they are **legitimate**
- It can be both **hardware** and **software** and they are often used together to provide stronger security to a network
  - Hardware firewalls will protect the whole network and prevent unauthorised traffic
  - software firewalls will protect the individual devices on the network, monitoring the data going to and from each computer

What form of attack would this prevent?

- **Hackers**
- **Malware**
- **Unauthorised Access to a Network**
- **DOS/DDOS attacks**

Two-factor authentication

What is two-factor authentication (2FA)?

- 2FA is a security measure that **requires users to provide two separate forms** of **identification** to **verify their identity**

- The purpose of 2FA is to **add an extra layer** of security beyond just a username and password
- It usually involves a combination of something the **user knows (password),** something the user has such as a **smartphone** using **SMS** or an **authenticator application**
- **The two stages of two-factor authentications are:**
    1. the user enters a username and password / pin number
    2. The user enters a 1 time unique pin number sent to their mobile device

Username & Password

What are passwords?

- Passwords are a **digital lock** to prevent unauthorised access to an account
- They are often stored as an **encrypted/ciphered** text entry in a database, ensuring that even with unauthorised access to a database, a hacker would not be able to gain access to the individual passwords of users
- **Strong passwords** and **regular password changes** are important to maintain security
- To maintain a strong password, it is recommended to use a **combination of uppercase** and **lowercase letters**, **numbers**, and **special characters**

What form of attack would this prevent?

- **Data Interception and Theft**
- **Physical Security Issues**
- **SQL Injection**

What are the advantages and disadvantages of using passwords?

Advantages	Disadvantages
▪ Strong passwords are difficult to crack ▪ Regularly changing passwords increases the security ▪ Using a range of passwords over the system will prevent or slow unauthorised access to the full system	▪ Passwords that are too complex can be harder to remember ▪ Too many passwords are hard to remember ▪ It is harder to choose unique passwords if a user is forced to regularly update them ▪ Hackers can break most passwords using brute force attacks

Copyright

What is copyright?

- Copyright is covered under a law called the **Copyright Designs & Patents Act**
- This protects the **intellectual property** of an individual or a company
- It makes it illegal to copy, modify or distribute software or other intellectual property without the relevant **permission**
- If **original work** is original, **copyright** will be automatically applied and will not expire until 25 - 70 years from the death of the creator depending on the type of work
- If an individual believes that their work has been copied it is their responsibility to take action under the **Copyright Designs and Patents Act**
- Many sites online offer free downloads of copyrighted **software/videos** which prevents the intellectual copyright holder from earning their income on the work they have created
  - E.g. If someone downloaded videos from Netflix and shared them with others, they would be breaching the act
- The act covers videos and audio where **peer-to-peer streaming** prevents a copyright owner from receiving an income

What is prohibited under the Copyright, Designs & Patents Act?

Primary breaches:

- Copying an original work
- Issuing a copy of the original work to the public
- Renting/lending a copy of the original work to the public
- Performing, showing or playing the original work in public
- Making an adaptation of the original work

Secondary breaches:

- Importing a copy of the original work
- Possessing or dealing with a copy of the original work
- Providing means to make copies of the original work
- Permitting the use of premises for making copies of the original work
- Provision of props/equipment for a performance of a copy of the original work

Software piracy

- Software piracy is the **illegal copying and distribution** of software
- Companies often take a lot of **steps to prevent software piracy**, some of these methods include:
  - **Product key / license:** Often a unique string or letters and numbers supplied with the software to activate it
  - **Agreement of terms and conditions:** Users will be asked to click to agree to the license agreement before being able to install the software
  - **Holograms:** Holograms are often used on the packaging of software and they indicate that the copy is genuine as they are too difficult and costly for pirates to implement
  - Some older software would only run if the **CD ROM or memory stick was physically in** the device using it

Worked Example

Describe methods that software producers use to prevent software copyright from being broken. **[4]**

Answer: One mark for naming the method then one mark for each reason

Serial numbers/product keys
When software is being installed, users are often asked to enter a unique number which proves the software is original

Serial numbers and product keys are supplied with the original copy of the software

Holograms
Holograms are often used on the packaging of software and they indicate that the copy is genuine

Software without a hologram on the packaging is usually an illegal copy as they are too difficult and costly for pirates to implement

Licence agreements
Licence agreements are part of the software installation process and they inform the user exactly how they are legally allowed to use the product

Users are required to 'agree to terms of use' before they can complete the installation
Any breach of this can mean prosecution and fines