Your notes

Cambridge National IT: revision notes

Cyber-security and legislation

Contents

1. Threats
2. Impacts
3. Prevention
4. Legislation
5. Key terms
6. Quick questions
7. What to do next

Threats

- **Malware** (viruses, worms, trojans, spyware and ransomware), **hacking** (gaining unauthorised access to a system), social engineering (**phishing**, blagging and shoulder surfing), denial of service attacks, and data theft or interception.
- Human error is a big risk too, such as losing a laptop or sending data to the wrong person.
- Attackers' motives include money, stealing data, causing disruption, spying, revenge, or just the challenge.

Impacts

- Loss or theft of data, financial loss (fines, compensation and lost sales), damage to reputation, disruption to services, and identity theft for individuals.

Prevention

- Physical measures: locks, biometric access, CCTV and security staff.
- Logical measures: strong passwords and two-factor authentication, **firewalls**, anti-**malware**, **encryption**, user access levels, software updates and backups.
- Policies and training: acceptable use policies, staff training on spotting **phishing**, and disaster recovery plans.

Legislation

- **Data Protection Act 2018** and the UK GDPR: rules for handling personal data, and rights for people (to see, correct and erase their data). Organisations can be fined for breaking them. In Guernsey, the Data Protection (Bailiwick of Guernsey) Law, 2017 does the same job.
- **Computer Misuse Act 1990**: makes unauthorised access, unauthorised access to commit further crimes, and unauthorised changes to data (such as spreading **malware**) illegal.

- Copyright, Designs and Patents Act 1988: protects original work, including software, images and music, from being copied without permission.
- **Freedom of Information Act 2000**: gives people the right to ask public bodies, such as councils and schools, for the information they hold.

Your notes

Key terms

Hacking	Gaining unauthorised access to a computer system.
Malware	Malicious software, such as viruses and ransomware.
Phishing	Fake messages designed to trick people into giving away their details.
Encryption	Scrambling data so it can only be read with the right key.
Firewall	Hardware or software that blocks unauthorised network traffic.
Biometrics	Using body features, such as fingerprints, to identify a person.
Data Protection Act 2018	The UK law that controls how personal data is used.
Computer Misuse Act 1990	The UK law that makes hacking and spreading malware illegal.
Freedom of Information Act 2000	The UK law that lets people request information held by public bodies.

Quick questions

Cover the answers and test yourself: remembering is what makes it stick.

1. What is hacking?
2. Which of these is a physical security measure?
3. Which of these is a logical security measure?
4. What does the Freedom of Information Act 2000 allow?
5. What can happen to an organisation that breaks data protection law?
6. What is ransomware?
7. Which law protects software and music from being copied?
8. What is one impact of a data breach on a company?

Answers

1. Gaining unauthorised access to a computer system
2. A lock on the server room door
3. A firewall
4. People to request information held by public bodies
5. It can be fined
6. Malware that encrypts files and demands payment
7. The Copyright, Designs and Patents Act 1988
8. Damage to its reputation

What to do next

Practise 12 questions on this topic

Try 4 exam questions, with mark schemes

Read the lesson, one step at a time

Free revision for GCSE and KS3 at lycolearn.co.uk. Some notes are for one exam board only, and say so in brackets.

Your notes