BTEC AAQ IT Unit 2 Cyber Security and Incident Management

A1 – Cyber Security Threats

Rons Tech Hub

Cyber Security Threats (Overview)

Cyber threats can come from inside or outside an organisation.

They can damage systems, steal data, or stop services working.

Understanding threats helps us protect systems better.

Rons Tech Hub

Rons Tech Hub

Internal Threats (What are they?)

Internal threats come from people inside the organisation.

This includes employees, contractors, or visitors.

They can be accidental or deliberate.

Employee Sabotage

Employees may damage systems on purpose or by accident.

This can include stealing devices, data, or software.

It can cause serious disruption to the organisation.

Unauthorised Software

- Installing unknown software can break systems.
- It may cause legal issues or licence problems.
- It can also be used for spying or illegal activity.

Rons Tech Hub

Damage to Systems

- Systems can be damaged by fire, floods, or power loss.
- Attacks such as terrorism can also cause damage.
- These events can stop systems from working.

Rons Tech Hub

Weak Security Practices

Poor security makes systems easy to attack.

This includes unsafe websites and weak device security.

Visitors must also be checked properly.

Human Error

- People can lose or share data by mistake.
- This often happens due to poor training.
- Not following rules increases risk.

Rons Tech Hub

Weak Monitoring

Problems may go unnoticed without monitoring.

Security issues might not be reported.

A weak security culture increases risk.

Rons Tech Hub

External Threats (Overview)

- External threats come from outside the organisation.
- These are often carried out by hackers or criminals.
- They aim to steal, damage, or disrupt systems.

Rons Tech Hub

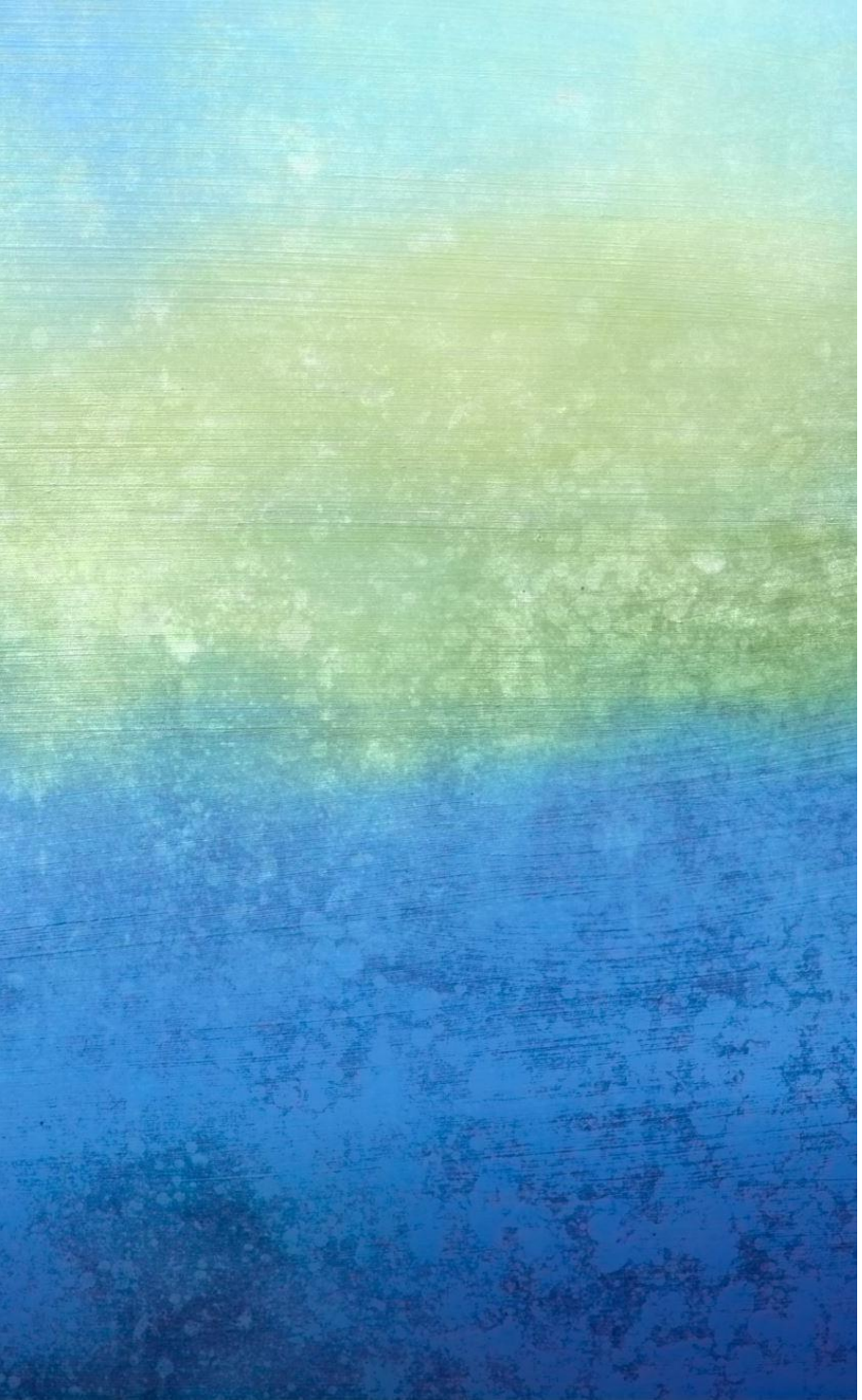
Malware (Malicious Software)

Malware is harmful software designed to damage systems.

It spreads through files, emails, or websites.

It can steal data or take control of devices.

Rons Tech Hub



Rons Tech Hub

Types of Malware

Viruses and worms spread between systems.

Trojans and rootkits hide inside software.

Browser hijackers change your web settings.

Spyware

Spyware secretly collects user information.

Keyloggers record what you type.

It can track activity on devices.

Rons Tech Hub

Rons Tech Hub

Adware

- Adware shows unwanted adverts.
- Some are legal, but others are harmful.
- It can slow down systems or track users.

Rons Tech Hub

Ransomware

Ransomware locks or encrypts your files.

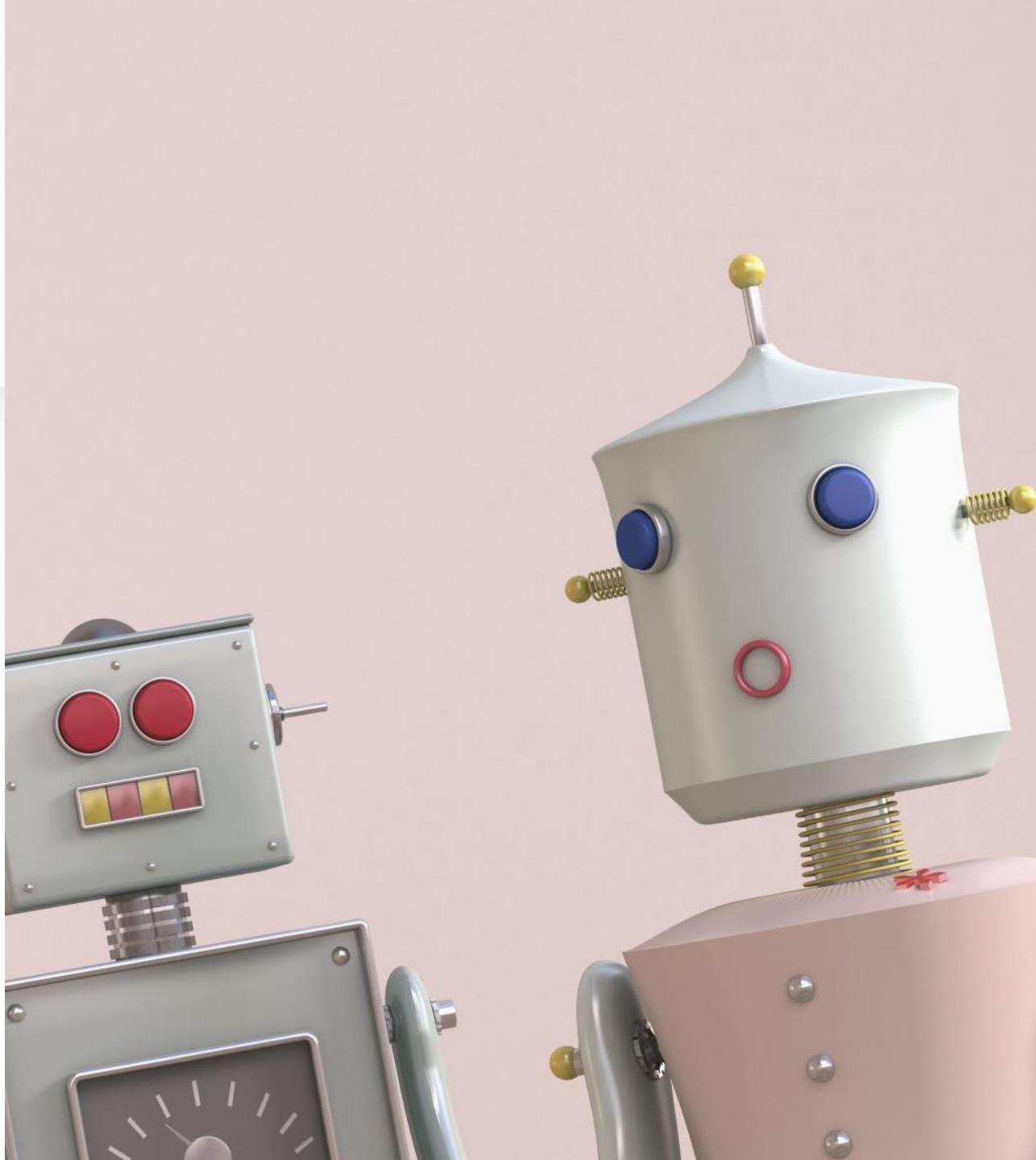
You must pay money to get access back.

Some versions threaten to leak your data.

Rons Tech Hub

Bots

- Bots are infected devices controlled remotely.
- They can be used in cyber-attacks.
- Large groups of bots are called botnets.



Rons Tech Hub

Hacking

- Hackers break into systems without permission.
- They may steal or change data.
- Targets include businesses and governments.

DoS and DDoS Attacks

- These attacks flood systems with traffic.
- This makes services slow or unavailable.
- DDoS uses many devices at once.

Rons Tech Hub

Rons Tech Hub

Data Attacks

- Data can be stolen, changed, or deleted.
- Attacks can target databases or websites.
- This affects both private and public data.

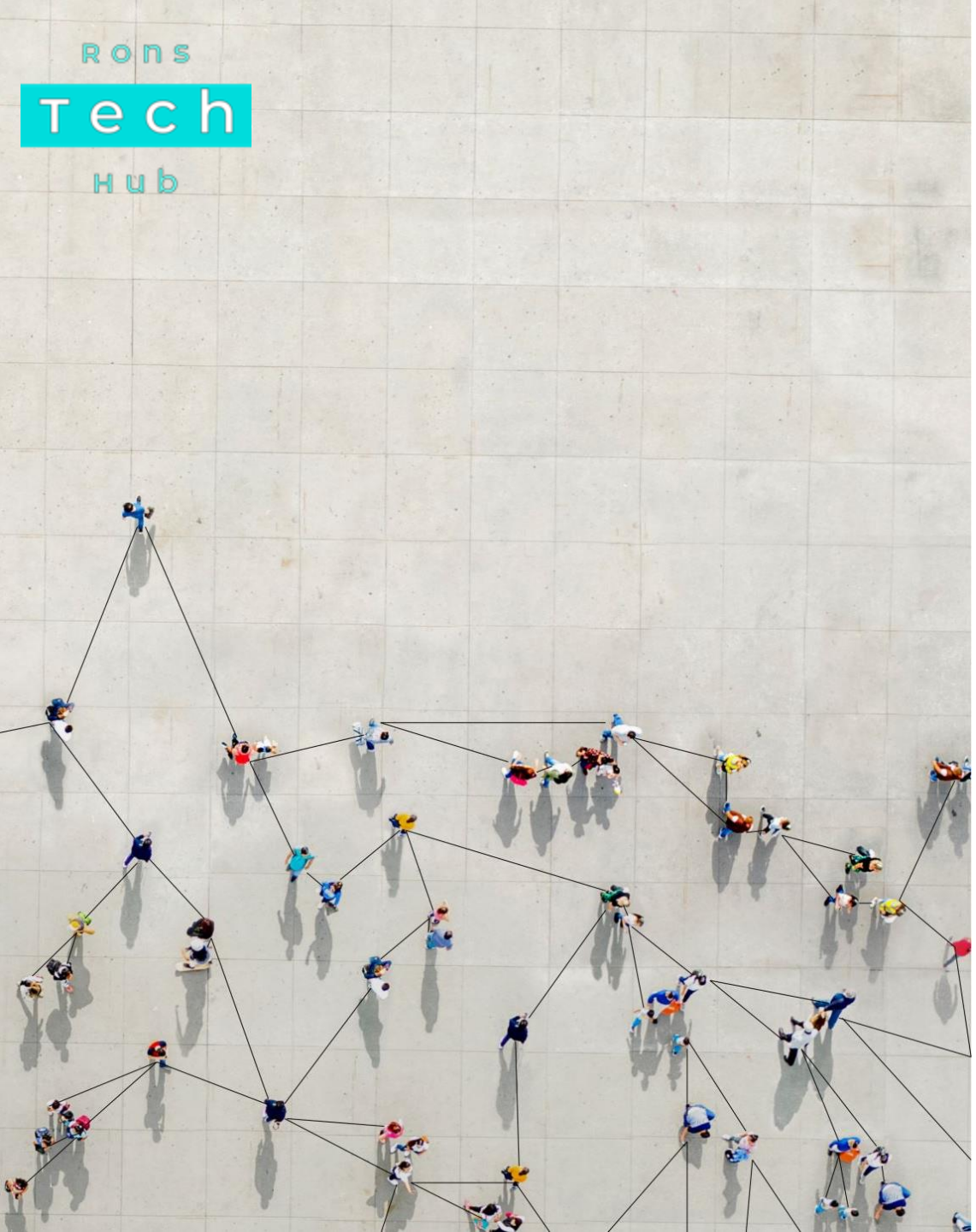
Rons Tech Hub

Sabotage

Attackers may damage systems or data.

They can create fake content like images or videos.

AI is now often used to create realistic fakes.



Social Engineering

- Attackers trick people into giving information.
- This relies on human behaviour, not technology.
- It is one of the most common threats.

Rons Tech Hub

Phishing Attacks

Phishing uses fake emails or messages.

It tries to steal passwords or personal data.

Variants include vishing and smishing.

RONS Tech Hub

Advanced Social Engineering

Spear phishing targets specific people.

Whaling targets high-level staff.

Impersonation involves pretending to be someone trusted.

Physical Security Threats

Attackers may enter secure areas without permission.

This includes tailgating or pretending to be staff.

Devices can also be stolen or accessed.

Rons Tech Hub

Rons Tech Hub

Device Risks

- Unattended devices can be accessed easily.
- Shoulder surfing means watching someone type.
- Lost or stolen devices are a major risk.

Impact Overview

- Cyber attacks can cause serious damage.
- Organisations may lose money, data, or trust.
- The impact can be long-term.

Rons Tech Hub

RONS Tech Hub

Operational Loss

Systems may stop working.

Services may become unavailable.

Data may not be accessible.

Rons Tech Hub

Financial Loss

- Businesses can lose money and profits.
- They may need to pay compensation.
- Legal fines can also be applied.

Reputational Damage

- Customers may lose trust in the organisation.
- Negative reviews can spread online.
- This can reduce future sales.

Rons Tech Hub

Intellectual Property Loss

Important ideas or designs can be stolen.

This includes plans and research data.

Competitors may gain an advantage.

Rons Tech Hub

Changing Threats

- Cyber threats change over time.
- New attacks are created regularly.
- Organisations must stay updated.

Rons Tech Hub

Rons Tech Hub

National Cyber Security Centre (NCSC)

Provides UK cyber security advice and updates.

Shares threat reports and alerts.

Helps organisations stay protected.

National Institute of Standards and Technology (NIST)

- Provides cyber security guidance and standards.
- Shares updates on new threats.
- Used worldwide by organisations.

RONS Tech Hub

Open Web Application Security Project (OWASP)

- Focuses on web application security.
- Publishes the OWASP Top 10 risks.
- Helps developers improve security.

Rons Tech Hub

Find More Resources

Acing Unit 2 is easier with the right support. Explore everything at:

www.ronstechhub.com

Search "RonsTechHub" on all major social platforms.

Rons Tech Hub