Malware, social engineering and technical vulnerabilities

5.3.1 · Issues and impact · revision notes

The threats to digital systems: malware (viruses, worms, Trojans, ransomware and key loggers), the technical vulnerabilities hackers exploit (unpatched software and out-of-date anti-malware) and social engineering. On Paper 1, expect definitions, 'Explain' questions based on a scenario such as a suspicious message, and 6-mark 'Discuss' questions.

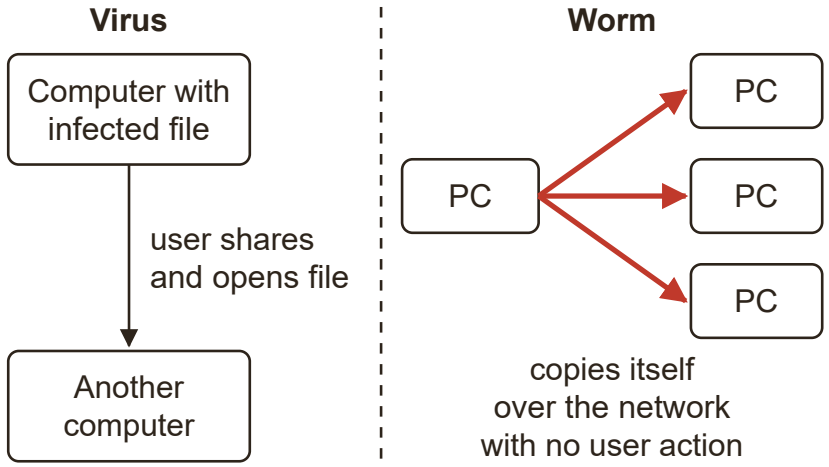
Key facts

- **Malware**: software designed to damage, disrupt, gain unauthorised access or steal data.
- **Worm**: standalone; copies itself across networks with no user action.
- **Ransomware**: encrypts files and demands payment for the key.
- **Unpatched software**: known, published security flaws left unfixed.
- **Social engineering**: manipulating people into giving away information or access (phishing, pretexting, baiting, quid pro quo, shoulder surfing).
- **Virus**: hides in a host file; spreads when infected files are run and shared.
- **Trojan**: disguised as genuine software; the user installs it; does not copy itself.
- **Key logger**: records key presses to steal passwords and card details.
- **Out-of-date anti-malware**: its signature database cannot recognise new malware.

Notes

Malware

- **Malware** (malicious software) is software designed to damage or disrupt a system, gain unauthorised access to it or steal data. A **cyberattack** is any attempt to do this.
- **Virus**: attaches itself to a host program or file. When the file is run, the virus runs and copies itself into other files. It spreads when infected files are shared, so it needs a user to act.
- **Worm**: a standalone program that copies itself and spreads across a network automatically, often by exploiting security flaws, with no user action. It can use up bandwidth and slow networks down.



A virus needs a user to share or run an infected file. A worm spreads by itself across a network.

- **Trojan**: disguised as useful, genuine software, so the user installs it. It then carries out hidden harmful actions, such as opening a 'back door' for an attacker. It does not copy itself.
- **Ransomware**: encrypts the victim's files and demands payment for the key. Paying does not guarantee that the files will be recovered.
- **Key logger**: records every key the user presses and sends it to the attacker, who picks out passwords and card numbers. It can be software or a small hardware device.

Technical vulnerabilities

- **Unpatched software**: when a security flaw is found, the software maker releases a fix called a **patch**. Once the flaw is public, attackers target computers that have not installed the patch.
- **Out-of-date anti-malware**: anti-malware recognises malware using a database of signatures of known malware. If it is not updated, new malware is not recognised and can infect the computer.

Social engineering

- **Social engineering** means manipulating people into giving away confidential information or access. It exploits trust, fear, urgency, curiosity and helpfulness rather than technical flaws.
- **Phishing**: fake emails, texts or websites that pretend to be from a trusted organisation, to get you to reveal details, click a malicious link or open an infected attachment.
- **Pretexting**: the attacker invents a believable story (the pretext), e.g. pretending to be from IT support or the bank, to persuade the victim to hand over information.
- **Baiting**: tempting the victim with something, such as a USB stick with an intriguing label left in a car park or a 'free' download, that carries malware.
- **Quid pro quo**: offering something in return, e.g. free 'technical support' in exchange for login details.
- **Shoulder surfing**: watching someone, directly or with a camera, as they type a PIN or password.
- Social engineering works because a genuine user hands over access, so it gets past firewalls, encryption and passwords. People are often the weakest link in security. Grade 7+ only

How to answer each type of question

Identify or describe a type of malware — 1 to 2 marks — Grade 4

1. Pick out the key clue: needs a host? spreads itself? disguised? encrypts files? records keys?
2. For 'Describe', say how it gets onto the system and what it does.
3. Use the exact name, e.g. Trojan, not 'virus'.

Example. Describe what a key logger does. (2 marks)

Model answer. It records every key the user presses (1) and sends the record to the attacker, who can find passwords or card numbers in it (1).

Explain the difference between two types of malware — 2 marks — Grade 5

1. Say how the first type spreads or gets onto a system.
2. Give the contrasting point for the second type, joined with 'whereas'.

Example. Explain **one** difference between a Trojan and a worm. (2 marks)

Model answer. A Trojan is disguised as useful software, so it relies on the user choosing to install it (1), whereas a worm spreads itself from computer to computer across a network without any user action (1).

Explain how a technical vulnerability is exploited

2 marks **Grade 6**

1. Say what the weakness is: a known flaw left unfixed, or a signature database that is out of date.
2. Explain how an attacker uses it, e.g. ready-made tools for a known flaw, or new malware that is not detected.

Example. A dental practice has not installed any operating system updates on its computers for two years. Explain why this makes the computers vulnerable to a cyberattack. (2 marks)

Model answer. Without the updates, security flaws that the patches would have fixed are still present on these computers (1). The flaws are publicly known, so attackers can use ready-made tools or malware to exploit them and get into the system (1).

Identify and explain social engineering in a scenario

3 marks **Grade 6**

1. Name the technique from the clues in the scenario.
2. Pick out features of the message or call that show it is an attack.
3. Explain what each feature does to the victim, e.g. creates panic so they do not stop to check.

Example. Priya receives a phone call from someone who says they work in her bank's fraud team. They tell her that her account has been hacked and ask her to confirm her online banking password so that they can 'secure' it.
(a) Identify the social engineering technique being used. (1 mark)
(b) Explain why this technique often works. (2 marks)

Model answer.

(a) Pretexting: the caller has invented a story to get information (1).
(Phishing by phone is also acceptable.)
(b) The caller pretends to be from a trusted organisation, so Priya believes the request is genuine (1). They create fear and urgency by saying her account has been hacked, so she acts quickly without checking (1).

6-mark 'Discuss' the threats to an organisation

6 marks **Grade 8**

1. Look for the weak points in the context: email, personal devices, remote access, old software.
2. Link each threat (malware, vulnerability or social engineering) to how it could happen here.
3. Explain the impact on the organisation's data and work.
4. Conclude with which threats are most serious and why.

Example. A university lets students connect their own laptops to its network, and its staff can log in to university systems from home. Discuss the threats to the university's systems from malware, technical vulnerabilities and social engineering. (6 marks)

Model answer. Marked in levels: the top level covers a range of threats, each developed and linked to the university, with a conclusion. A strong answer might say: Students' own laptops may have unpatched software or out-of-date anti-malware, so a worm on one laptop could spread by itself across the university network. Ransomware could encrypt research and student records, stopping teaching and exams until the files are restored. Staff working from home could receive phishing emails pretending to be from the IT department; if they type their password into a fake login page, an attacker could log in remotely as them. A key logger on a home computer could capture staff passwords. An attacker could also use pretexting, phoning the help desk and pretending to be a lecturer who is locked out. Overall, the biggest threats come from devices and people the university does not fully control, so one infected laptop or one tricked member of staff could give access to the whole system.

Don’t lose marks

- Calling all malware 'viruses'.
- Saying a Trojan copies itself, or that a worm needs the user to open a file.
- Saying unpatched software 'has a virus': it has a known, unfixed security flaw.
- Saying anti-malware stops social engineering: it cannot stop someone typing their password into a fake website.
- Naming a technique without explaining how it works in the scenario.

More tips

Memory tricks

- Virus = needs a host and a human. Worm = wriggles through the network on its own. Trojan = a gift with a hidden danger, like the wooden horse.
- Ransomware holds your files to ransom: they stay encrypted until you pay.
- Phishing red flags: urgent, unexpected, generic greeting, odd sender or link address, asks for a password or payment.
- Pretexting = a pretend story; baiting = bait to take; quid pro quo = 'something for something'.

Exam technique

- Name the exact type of malware or technique, then say how it gets in and what harm it does.
- In scenario questions, quote the clues from the message or situation, e.g. 'act now' shows urgency.
- Only describe ways of protecting a system if the question asks for them.

What each grade needs

What you need to be able to do, from the first marks up to the top grade.

Grade 3 — **Define malware and give examples**
Malware is software designed to cause harm, e.g. viruses, worms, Trojans, ransomware and key loggers.

Grade 4 — **Describe the five types of malware**
Say how each one gets onto a system and what it does once it is there.

Grade 4 — **Describe common social engineering techniques**
Phishing, pretexting, baiting, quid pro quo and shoulder surfing.

Grade 5 — **Explain how viruses differ from worms**
A virus needs a host file and a user action to spread; a worm spreads itself across networks.

Grade 6 — **Explain how unpatched software is exploited**
Attackers use known, published security flaws that have not been fixed on that computer.

Grade 6 — **Spot and explain signs of phishing**
Urgency, an unexpected request, a generic greeting and a link to the wrong web address.

Grade 7 — **Explain why social engineering beats technical defences**
A genuine user hands over access, so firewalls, encryption and passwords are bypassed.

Grade 8 — **Discuss the threats facing an organisation**
Link each threat to the organisation's systems and data, and explain the likely impact.

Free notes, Full packs, practice papers and mock exams at chhetriacademy.com. Written for this site; not taken from past papers. Stuck? 1-to-1 tutoring with a free 30-minute trial lesson.