Principles of Security Technologies (COS6025-B)
COURSEWORK (50%)

Analytical Report: Malware Attack Lifecycle and Response Simulation
DEADLINE: 3:00pm Friday 24th April

This assignment requires you to produce a professional analytical report on a malware attack scenario, using a combination of:

- Secondary research (e.g. academic papers, threat intelligence reports, MITRE ATT&CK database), and
- Conceptual simulation (e.g. describing what *would* be observed in a controlled lab).

You are not expected to execute or analyse malware directly. Instead, you will demonstrate your understanding of the malware analysis process, security technologies, and the ethical implications of threat research.

Your report must address each section below, clearly labelled:

1. Attack Overview and Context (15%)

- Select one real-world malware family or attack case (e.g. WannaCry, Emotet, Stuxnet, Trickbot, or similar).
- Summarise its background: target environment, delivery mechanism, and impact.
- Identify the threat actor tactics using frameworks such as MITRE ATT&CK.
- Explain why this malware type is significant for cybersecurity professionals.

Suggested sources:
MITRE ATT&CK, CISA advisories, NCSC threat briefings, academic or vendor reports (e.g. Symantec, FireEye, CrowdStrike).

2. Simulated Malware Analysis Process (30%)

- Describe how analysts would perform static and dynamic analysis on this malware in a virtual lab, including:
  - Typical tools (e.g. PEiD, strings, ProcMon, Wireshark, RegShot)
  - Expected findings from file inspection, network monitoring, or process tracing
- Include sample or mock outputs (e.g. fabricated log entries or screenshots from sandbox reports). *Any simulated logs or screenshots must be clearly labelled as illustrative examples.*
- Explain the difference between what static and dynamic analysis reveal.

You may use existing public sandbox reports (e.g. from Any.Run, Hybrid Analysis, or Malpedia) as evidence, without running malware yourself.

3. Detection and Mitigation (20%)

- Explain how SIEM, IDS/IPS, or endpoint detection technologies could identify or block this malware.
- Suggest secure software design or patching strategies that would have reduced the risk.
- Where possible, relate to secure SDLC principles (input validation, least privilege, patch management, secure configuration).

4. Ethical, Legal, and Social Considerations (20%)

- Discuss ethical issues of malware analysis (handling malicious code, data privacy, responsible disclosure).
- Reflect on the societal implications of surveillance or monitoring technologies used to detect malware.
- Consider relevant governance or compliance frameworks (e.g. GDPR, NCSC guidance, ACM Code of Ethics).

5. Presentation and Academic Quality (15%)

- Clear structure and academic writing style.
- Use of diagrams/figures (attack chain, analysis workflow, etc).
- Consistent referencing style throughout the report.
- Logical flow and professional presentation.

Submission Requirements

- **Word count:** 2,000 words (±100), excluding references
- **File format & naming:** Submit as a PDF via Canvas, named StudentName–Coursework
- **Safety & ethics:** Do not download, execute, or distribute live malware or executable samples
- **Research quality:** Use rigorous academic and professional sources (e.g. peer-reviewed literature, threat intelligence reports, MITRE ATT&CK, NCSC guidance) and provide critical analysis, not just description
- **Critical thinking:** Demonstrate evaluation of detection, response, and mitigation approaches, linking theory to real-world or simulated scenarios
- **High-mark standard (80%+):** Show original insight, critical discussion, and ethical/societal reflection, supported by high-quality sources
- **Referencing:** Include at least 12 academic references and use a consistent, approved referencing style (e.g. Harvard or IEEE); clearly distinguish your own analysis from cited work

The report must be submitted to CANVAS by **3:00pm on Friday 24th April 2026**. Late submissions (without acceptable extenuating circumstances) will receive a mark of zero.

This coursework brief is used alongside the marking criteria to determine your overall mark. It is essential to read both in conjunction with each other. Please check the mark scheme of the coursework uploaded to Canvas.

Please note that using any AI text generator tools (e.g. ChatGPT or any similar tool) will be detected by Turnitin on the instructors' side. The similarity score generated by Turnitin (seen by both students and instructors) is different from the AI score (seen only by the instructors). Using AI tools for this coursework goes against the principles of academic integrity and will be reported to the university as academic misconduct.