Here is the **complete sentence-by-sentence breakdown** of the document **“Symptoms of Infection Notes.docx”**, formatted as **professional study notes** aligned with **CompTIA A+ 220-1102 | Objective 2.4 – Security**. This version is optimized for direct pasting into **Microsoft Word**—numbered topics, no extra spacing, and all key information retained.

**🦠 Symptoms of Malware Infection – Study Notes - CompTIA A+ 220-1102 | Objective 2.4 – Security**

**1. General Behavior Changes**

* A malware infection often causes a computer to **start behaving strangely**.
* These behavioral changes vary but are early indicators that the system is compromised.

**2. System Performance – Sluggishness**

* One of the first signs is that the system **runs slower than normal**.
* For example:
  + A **worm** consumes **CPU** and **network resources** while spreading.
  + Receiving **spam** can also tax system performance.
* Many forms of malware consume system resources, leading to slowdowns.

**3. Freezing and Lock-Ups**

* If the system **locks up**, becomes **unresponsive**, or **freezes frequently**, this may indicate malware.
* Frequent **blue screens of death (BSOD)** are also a red flag.
* A virus might accidentally **overwrite critical system files**, leading to crashes and lockups.

**4. Crashes and Reboots**

* If your computer **crashes often** or **restarts unexpectedly**, this can be a symptom of infection.
* Malware that corrupts system files may cause **instability and reboot loops**.

**5. File and Application Access Issues**

* Infected systems may block access to **files, folders, or applications**.
* Malware can change **file permissions**, preventing users from:
  + Running files
  + Deleting or modifying files
* This helps the malware **maintain persistence**.

**6. Strange Noises and Visual Errors**

* The computer may emit **unusual noises** or display **unusual error messages**.
* Screens might show **distorted graphics** or error content.
* Printing might produce **gibberish symbols** instead of normal text.
* These anomalies may occur due to how the malware interferes with software or drivers.

**7. Icon and File Changes**

* Unexpected **new icons appear** on the desktop, or known icons **disappear**.
* This can happen when malware:
  + Installs additional programs
  + Deletes or hides existing files

**8. Use of Double File Extensions**

* Malware may use **double file extensions** to disguise itself.
* In Windows, known file extensions (e.g., .exe, .txt) are **hidden by default**.
* A malicious file might appear as textfile.txt but be textfile.txt.exe.
* Clicking this file may unknowingly execute malware.

**9. Antivirus Disabled**

* If your **antivirus software won’t launch**, this is a common symptom.
* Malware often targets **security software** to:
  + Prevent detection
  + Extend its presence on the system
* Disabling antivirus tools helps the malware stay **undetected and persistent**.

**10. File or Folder Corruption**

* You may notice **corrupted files or folders**, or **new unknown files** appearing.
* Malware can:
  + **Delete, modify, or duplicate** files
  + **Spread infected files** across the network
* This behavior is part of malware’s effort to maintain a foothold.

**11. System Restore Disabled**

* Malware may **disable System Restore** to prevent you from rolling back to a clean state.
* Just like with antivirus disabling, this helps it remain on the system longer.
* Without System Restore, users cannot easily undo the infection.

**12. Summary: Recognizing Malware**

* If your system starts acting **odd or unexpected**, malware may be present.
* Recommended actions include:
  + **Booting into Safe Mode**
  + **Scanning with a trusted antivirus tool**
  + Using an **external rescue drive** for scanning and recovery