Below is the **comprehensive sentence-by-sentence study note breakdown** of the document **“Ransomware Notes.docx”**. It is formatted cleanly and professionally for **direct pasting into Microsoft Word**—numbered topics, aligned bullet points, minimal spacing, and all critical information retained.

**🔐 Ransomware – Study Notes CompTIA A+ 220-1102 | Domain 2.0 – Security | Objective 2.4**

**1. Definition of Ransomware**

* Ransomware is a type of **malware** that **restricts access** to a victim’s computer or files until a **ransom** is paid.
* This is typically done by **encrypting files**, **changing passwords**, or **locking the system**.
* The attacker demands payment, usually through **cryptocurrency like Bitcoin**, to restore access.

**2. Common Behavior of Ransomware**

* You may reboot your system and see a **lock screen** with a message such as:

“Your computer has been locked. Pay $200 through Bitcoin at this link.”

* The attacker promises to send a **decryption key or unlock code** once payment is received.
* This is a form of **blackmail and extortion**.
* However, **paying the ransom does not guarantee** access will be restored.

**3. Expert Advice: Do Not Pay the Ransom**

* Cybersecurity experts advise **not to pay** because:
  + In many cases, the **unlock key is never delivered**.
  + Paying may only **fund and encourage further attacks**.
* Victims often **lose their money and still have no data access**.

**4. Importance of Backups**

* Ransomware is particularly harmful if you do **not have backups** of your files.
* If you maintain regular **backups**:
  + You can **restore your system** without paying the ransom.
  + You can **roll back** to a clean system state prior to the infection.

**5. Real-World Example: City of Atlanta (2018)**

* In 2018, the **city of Atlanta** was attacked by **SamSam ransomware**.
* The ransomware **spread across multiple city systems**.
* The city chose **not to pay** the ransom.
* Instead, they incurred:
  + **$6 million** in services, contracts, and software upgrades.
  + **$11 million** in hardware upgrades.
* Total cost: **$17 million**, making it one of the most expensive government-related cyberattacks in 2018.

**6. Other Ransomware Targets**

* Hospitals and healthcare providers have been targeted, with **patient records encrypted** and held hostage.
* **Personal data** such as **family photos or important documents** can also be targeted.

**7. Attack Vector and Exploitation**

* Ransomware exploits a **vulnerability** in software to gain initial access to a system.
* Once access is obtained, it proceeds to:
  + **Encrypt user files**, or
  + Lock the system or user account.
* After encryption, there is **no way to decrypt** without:
  + **Paying the ransom**, or
  + **Restoring from a known good backup**.

**8. Final Recommendations**

* To mitigate ransomware risks:
  + Perform **regular backups**.
  + Apply **security patches and updates** to eliminate vulnerabilities.
  + Use **endpoint protection** with behavior-based detection.