Cybersecurity Station Prompt

Version 1: 2025-04-06

**Subject:** URGENT: Ransomware Incident—Immediate Decryption Needed

**From:** Abhinav Piratla, Head of Cyber Defense

Hello Team,

I’m reaching out regarding a critical ransomware incident that has just hit our company. A hacker group known only as **Phantom** has infiltrated our systems and locked down vital data. We have two choices: either pay a substantial ransom or decrypt the files ourselves. Failure to do so will result in **permanent data loss.**

**Here’s what we know so far:**

We have found an **“Ransomware Data”** folder left by the hackers with the demand for ransom. It has a number of files and it looks like the **ReadMe.pdf** file is the place to start

**Key Information:**

• The Phantom.pdf file appears to hold a poem that might reveal a **hidden word**, a **number**, and a **phrase** crucial to understanding how to unlock everything.

• There’s also a DecryptMe\_Caesar.pdf that seems to be encrypted with a Caesar cipher; once you figure out the **shift value**, apply it to uncover more information.

• Finally, DecryptMe\_AES.pdf likely requires a specific **passphrase** to perform AES decryption.

Retrieve our **Company Data**, from the password protected **.dmg file**, within the next approximately **40 minutes**, before we are forced to pay the ransom or lose our data forever. Please move swiftly and coordinate all findings with your team.

Stay focused, follow any hints in the ReadMe and Phantom files, and proceed **methodically** through each stage of decryption. Let’s do everything possible to save our systems without paying these criminals a dime.

Thank you for your immediate attention,

**Abhinav Piratla**

Head of Cyber Defense