


# Colonial Pipeline Attack

Joseph Koduah






# What happened?

- A criminal extortion group executed a ransomware attack on the Colonial Pipeline that force Colonial Pipeline Company to shut down the pipeline.
- 



# Who was involved?

- Colonial Pipeline Company
  - East Coast; Texas, Louisiana, Mississippi, Tennessee, Alabama, Georgia, North Carolina, South Carolina, Virginia, Pennsylvania, New Jersey, Delaware, and Maryland.
  - FBI
- 





# Where did this occur?

- The ransomware attack started in Houston, Texas.
- 





# How did this happen?

- “Colonial Pipeline Co. was breached due to a leaked password, an inactive VPN account and a lack of multifactor authentication.” - (Back to Basic)
- 





# What were the consequences/impacts? (individuals, legal, ethical, social, society, environment)

- The attack forced the pipeline to be shutdown. This shocked the east coast due to shortage of fuel.
  - The aftermath cause gas prices to rise above 5\$/ gal in some states.
- 




# What are your suggestions to prevent this from happening again?

- To have a monitoring system that tracks suspicious activity and acts immediately.
  - Enforce a multi-layer security system.
- 



# Do you think this could happen again and why?

- It's possible for this attack to happen again, but the chances are rare. This attack showed the US how seriously we should take cyber attacks. They should enforce a multi-layer security system.
- 



# Work cited

- “15 Biggest Cybersecurity Attacks in 2021.” *Privacy Affairs*, 8 Aug. 2022, <https://www.privacyaffairs.com/cybersecurity-attacks-in-2021/>.
- “Back to Basics: A Deeper Look at the Colonial Pipeline Hack.” GovTech, GovTech, 8 July 2021, <https://www.govtech.com/sponsored/back-to-basics-a-deeper-look-at-the-colonial-pipeline-hack>.