The background is a solid pink color. In the top right corner, there is a decorative pattern of overlapping triangles in various shades of pink and magenta, creating a geometric, stepped effect.

BREAK! Be back at  
9:30am to continue  
the fun!



# Cybersecurity in the Pipeline Industry

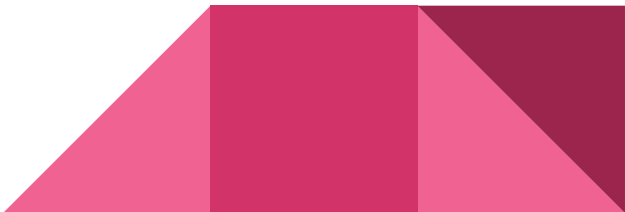
Pipeline Safety Seminar 2025

Source: "Generate an image that combines cybersecurity and natural gas pipelines" prompt, Gemini, 2.5 Flash, Google, 1 Aug. 2025.

# Why We're Here

- Pipelines are critical national infrastructure.
- Cyber threats are increasing in sophistication.
- A single point of failure can have massive real-world consequences.
- Empowering ourselves with knowledge is our first line of defense.

# Agenda

- Defining Types of Cyber Attacks
  - The Colonial Pipeline Cyber Attack
  - Cybersecurity: The Human Element
  - Future PHMSA Regulations
  - Conclusion
  - Q/A
- 

# Defining Types of Cyber Attacks



Source: "Generate an image that looks like a cyber attack" prompt, Gemini, 2.5 Flash, Google, 1 Aug. 2025.

# Phishing

- Phishing is a type of cyber attack where a malicious actor, pretending to be a trustworthy entity, tricks a person into revealing sensitive information. This is often done by sending fraudulent communications, such as emails, text messages, or instant messages, that appear to be from a legitimate company or person.
- The goal of a phishing attack is to get the victim to click a malicious link, download an attachment, or provide personal data like passwords, credit card numbers, or social security information. These attacks often create a sense of urgency or threat, for example, claiming there is a problem with an account that requires immediate action.

# Ransomware

- A ransomware attack is a type of cyberattack where malicious software, known as ransomware, encrypts a victim's files, making them inaccessible. The attacker then demands a ransom, usually in cryptocurrency, in exchange for a decryption key to restore access to the files.
- Ransomware typically spreads through phishing emails that contain malicious links or attachments, but it can also exploit vulnerabilities in network systems. Once inside a system, the ransomware quickly encrypts data, often displaying a message on the user's screen with instructions on how to pay the ransom.

# Malware

- Malware, or malicious software, is a broad term for any software intentionally designed to cause damage to a computer, server, client, or network. Attackers use malware to steal sensitive data, gain unauthorized access to systems, or disrupt normal operations.
- Malware can infiltrate a device in various ways, such as through phishing emails, malicious websites, or infected software downloads. Once a system is compromised, the malware can carry out a range of harmful activities, from logging keystrokes to encrypting files.



# Data Breach

- A data breach is a security incident where sensitive, confidential, or protected information is accessed, stolen, or disclosed by unauthorized individuals. This can affect personal data (e.g., social security numbers, credit card details) or corporate data (e.g., intellectual property, customer records).

# Stalkerware

- Stalkerware is a form of malware designed to secretly monitor a person's digital activity on their mobile device or computer without their knowledge or consent. It is a type of spyware, but it is specifically intended for use by someone the victim knows, such as an abusive partner, ex-partner, or family member, or disgruntled employee to track, harass, or control them.

# DDoS

- A DDoS (Distributed Denial-of-Service) attack is a type of cyberattack that aims to make a website, server, or online service unavailable to its intended users. This is achieved by overwhelming the target with a flood of malicious internet traffic from multiple sources.
- Unlike a single-source DoS attack, a DDoS attack is "distributed," meaning it uses a large network of compromised computers and devices (known as a botnet) to launch the attack simultaneously. This makes the attack much more powerful and difficult to defend against, as the traffic comes from a wide variety of sources, making it hard to distinguish between legitimate and malicious requests.
- For example, a pipeline operation or bill pay website/server for gas utilities.

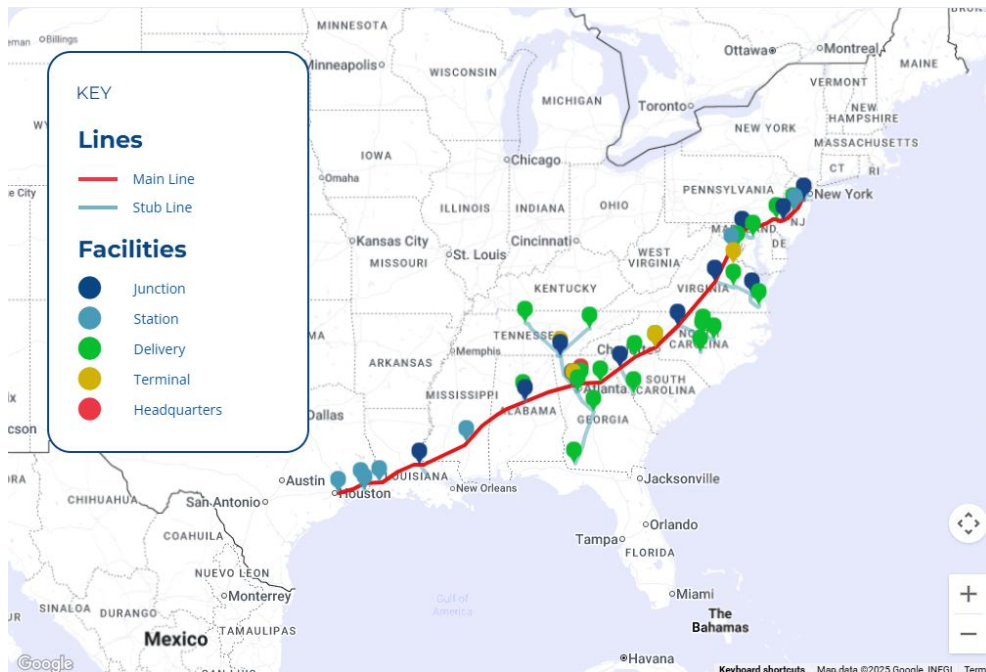
# The Colonial Pipeline Cyber Attack



Source: "Could you generate an image of a natural gas pipeline?" prompt, Gemini, 2.5 Flash, Google, 1 Aug. 2025.

# The Colonial Pipeline - At a Glance

- Largest refined products pipeline in the U.S.
- Transports ~100 million gallons of fuel daily.
- Serves the entirety of the U.S. East Coast.
- 5,582 miles of total pipeline.
- 27.7 million barrels of storage capacity



Source: "Our Operations | Energy Infrastructure | Colonial Pipeline." Colonial Pipeline Company, [www.colpipe.com/our-operations/](http://www.colpipe.com/our-operations/). Accessed 1 Aug. 2025.

# The Attack: What happened?

- **May 7, 2021: A Ransomware Attack**
  - An amateur ransomware group named "DarkSide" gained access to the company's network.
  - The initial point of entry was a legacy VPN account that lacked multifactor authentication (MFA).
  - The hackers stole data and encrypted critical billing and business systems.



# The Immediate Response

- **A Proactive Shutdown**
  - Colonial Pipeline proactively shut down its operational technology (OT) systems to prevent the ransomware from spreading.
  - This was a safety measure, but it immediately halted all fuel shipments.
  - The company paid a ransom of 75 bitcoin (worth ~\$4.4 million at the time).





# The Lasting Impact

- **The Ripple Effect**
  - **Economic:** Widespread fuel shortages and panic buying across the East Coast. Gas prices spiked to their highest level since 2014.
  - **National Security:** A Presidential state of emergency was declared. The incident highlighted the vulnerability of critical infrastructure.
  - **Operational:** The pipeline was shut down for six days. It took several more days for the system to return to normal operation.



Source: "File:2021-05-15 14 33 28 Out-of-service gas pumps due to panic buying after the Colonial Pipeline cyberattack at the Wawa along Air and Space Museum Parkway in Oak Hill, Fairfax County, Virginia.jpg." Wikimedia Commons. 26 Nov 2024, 14:16 UTC. <[link](#)> 1 Aug 2025, 11:24.



# The Aftermath & Recovery

- **A Glimmer of Hope**
  - The Department of Justice recovered a significant portion of the ransom payment which totaled to be 63.7 of the 75 bitcoins (about 84%). Unfortunately, the cryptocurrency value crashed late May, meaning the value of the recovered bitcoins were only worth around \$2.3 million, about half of the value.
  - The incident triggered a national discussion on cybersecurity for critical infrastructure.
  - It led to new cybersecurity regulations from the Transportation Security Administration (TSA).



# Brief Overview of the Regulations from the TSA

- **Under the Directive from the US TSA, a TSA-specified pipeline owner/operators must:**
  - Review their current activities against TSA recommendations for pipeline cyber security to assess cyber risks, identify any gaps, and develop remediation measures
  - Report the results of these actions to the TSA and the DHS Cybersecurity and Infrastructure Security Agency (CISA)
  - Report cybersecurity incidents to CISA
  - Designate a cybersecurity coordinator who is required to be available to TSA and CISA 24 hours a day, seven days a week, to coordinate cybersecurity practices and address any incidents that arise.

# Lessons Learned - The Technical

- **Multifactor Authentication (MFA):** The single most important lesson. A simple security measure that would have likely prevented the breach.
- **Network Segmentation:** The importance of separating IT (information technology) networks from OT (operational technology) networks.
- **Regular Audits:** Decommissioning old accounts and regularly auditing remote access.
- **Implementing Logs:** Adding a logging system of who, when, and from where people are accessing company systems.



# Lessons Learned - The Human

- **Our Role in Cybersecurity**
  - Cybersecurity isn't just an IT issue; it's a people issue.
  - The Colonial Pipeline attack started with a compromised password on an old account.
  - Every employee is a potential target and a crucial part of the defense.



# Cybersecurity: The Human Element



Source: "Generate an image of a creepy email personified to follow someone home from work" prompt, Gemini, 2.5 Flash, Google, 1 Aug. 2025.

# Introduction to Personal Cybersecurity

- **Your Digital Shield**
  - Cyber threats follow us from the office to our homes. Protecting ourselves and those living with us is a 24/7 job.



# Phishing: The Most Common Threat

- **Phishing: Don't Take the Bait**
  - Urgent or threatening language.
  - Requests for personal information.
  - Suspicious links or attachments.
  - Grammatical errors or awkward phrasing.
  - Unfamiliar sender addresses.



Source: "Generate an image of a construction worker phishing out an email of a sea of emails" prompt, Gemini, 2.5 Flash, Google, 1 Aug. 2025.

# The Golden Rule of Email

- **Stop. Look. Think.**
  - **Rule:** Before you click on any link or open any attachment, stop and think. Does this email look legitimate? Was I expecting this? When in doubt, delete it or contact your IT department for more information.
  - What are your company's procedures for handling these emails? Any experiences?



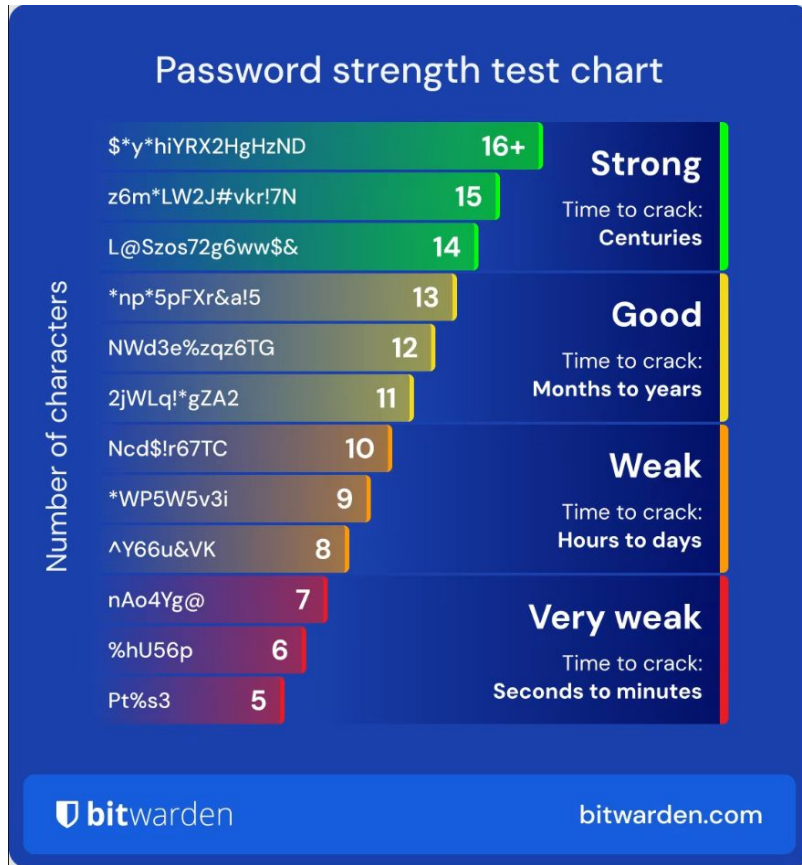


# Passwords & MFA

- **The Power of a Strong Password (and More)**
  - **Strong Passwords:** Use long, unique passphrases with symbols. Avoid common words, names, or birthdays.
  - **Password Managers:** Use a trusted and encrypted password manager to securely store unique passwords for all accounts.
  - **Multifactor Authentication (MFA):** Reiterate the lesson from Colonial Pipeline. MFA is a simple yet powerful barrier. Enable it on all personal and work accounts whenever possible.



# Password Fun Facts



- There are places online that you can check the strength of a password and how long it would take to crack.
- The shorter the password = the shorter amount of time it would take to crack.
- Use passwords with lots of symbols and phrases that don't make sense in a word string.
- Password managers make it really easy to generate random, strong passwords.

# Safe Browsing Habits

- **Navigating the Web Safely**
  - **Secure Websites:** Look for "https://" in the URL and the padlock icon.
  - **Public Wi-Fi:** Avoid conducting sensitive work or banking on public Wi-Fi. Use a VPN if you must.
  - **Software Updates:** Keep all software, operating systems, and antivirus programs up to date.
  - **Set Filters:** Some browsers can help filter out malicious websites and ads.
  - **Sponsored Search Results:** Just don't.



# Work & Home Security

- **Beyond the Screen**

- **Device Security:** Always lock your computer when you walk away.
- **Home Network:** Secure your home Wi-Fi with a strong password and change the default router name. Also limit access to your router.
- **Work Devices:** Never allow family members to use your work computer.




# Future PHMSA Regulations



Source: "Generate an Image of a pipeline safety investigator looking at cybersecurity regulations" prompt, Gemini, 2.5 Flash, Google, 1 Aug. 2025.

# PHMSA's Current Role

- **Rather than issuing its own cybersecurity regulations, PHMSA uses its existing authority to enhance pipeline security during inspections:**
    - **Inspecting control rooms:** PHMSA includes cybersecurity questions during inspections of pipeline control room operations, which are the "nerve centers" of the pipeline network.
    - **Reviewing response plans:** The agency checks that emergency response plans consider cyberattack threats and include measures to mitigate their impact.
    - **Enforcing integrity management:** PHMSA ensures cybersecurity is considered within integrity management plans, which focus on the overall safety and reliability of pipelines.
- 


# PHMSA's Current Role Continued

- **And...**
  - **Collaborating with other agencies:**  
PHMSA works with the Cybersecurity and Infrastructure Security Agency (CISA) and TSA on joint cybersecurity exercises for pipeline operators.



Source: "Can you generate an image of a natural gas pipeline operator exercising in their work uniform?" prompt, Gemini, 2.5 Flash, Google, 3 Sep. 2025.

# Outlook on Future Regulations

- **Future regulations could result from ongoing debate and congressional actions:**
    - **Possible new rulemaking:** Though no specific new cybersecurity rulemakings are currently scheduled by PHMSA, the agency is actively involved in safety enhancements.
    - **Authority debate:** There has been an industry debate over whether TSA or the Federal Energy Regulatory Commission (FERC) should be the lead agency for mandatory pipeline cybersecurity standards.
    - **Congressional oversight:** Congress continues to hold hearings and consider potential legislative changes related to pipeline security.
    - **Advocacy for broader requirements:** Some in the industry have advocated for broader, mandatory federal standards for natural gas pipelines, similar to those for the electric grid, and for expanded federal requirements for security.
- 



# Conclusion



Source: "Make a natural gas pipeline operator look elated about cyber security" prompt, Gemini, 2.5 Flash, Google, 1 Aug. 2025.

# Summary

- **Key Takeaways**

- The Colonial Pipeline attack was a wake-up call for the industry, emphasizing the link between cyber and physical security.
- Individual vigilance is our most important defense against threats like phishing and weak passwords.
- Proactively preparing for new regulations will ensure compliance and improve safety.

**Thank you!**



# Q/A



Source: "Can you generate an image of a natural gas pipeline operator pondering very hard in the thinking man pose? Include the uniform again." prompt, Gemini, 2.5 Flash, Google, 3 Sep. 2025.