



# PJM Security Update

Matt Mossholder,  
Lead Security Architect

Tech Change Forum  
June 15, 2026

## Important Security Alerts

- CISA releases [guidance](#) to help critical infrastructure sustain essential operations during geopolitical conflict.
- CISA releases [guidance](#) to securely deploy agentic AI in mission critical environments.
- Frontier AI model [helped to uncover](#) over 10,000 software vulnerabilities resulting in more vendor patches.

## Monitored Threats

- Exploitation of unpatched vulnerabilities
- Phishing and smishing attacks
- Use of deepfake and Adaptive AI technology
- Distributed Denial of Service attacks

## Contact PJM

- To report unusual events, notify your normal PJM contacts.
- To report connectivity issues, contact Member Relations.
- To report suspicious email, notify [SecurityAlertTm@pjm.com](mailto:SecurityAlertTm@pjm.com).
- Share this info with your security team.

Presenter/SME:  
Matt Mossholder,  
[matt.mossholder@pjm.com](mailto:matt.mossholder@pjm.com)

## PJM Security Update



### Member Hotline

(610) 666 – 8980

(866) 400 – 8980

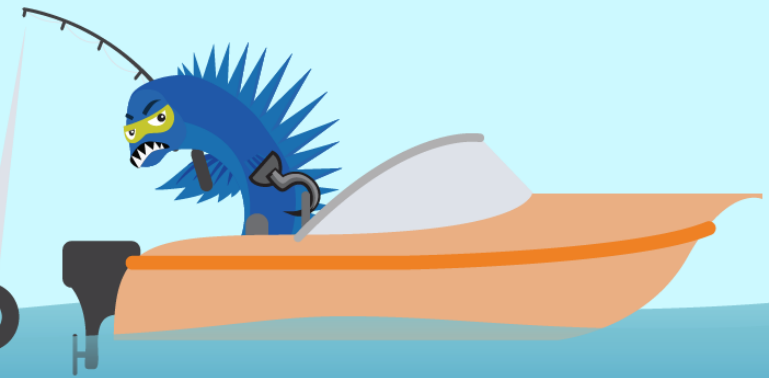
[custsvc@pjm.com](mailto:custsvc@pjm.com)

**PROTECT THE  
POWER GRID**

**THINK BEFORE  
YOU CLICK!**



**BE ALERT TO  
MALICIOUS PHISHING  
EMAILS**



**Report suspicious email activity to PJM.  
Call (610) 666-2244 or email [it\\_ops\\_ctr\\_shift@pjm.com](mailto:it_ops_ctr_shift@pjm.com)**