

Security Update

Matt Mossholder,
Lead Security Architect

Tech Change Forum
August 10, 2026

Disclaimer: While materials are current at the time of publishing, applicable requirements may change. PJM Governing Documents control.

Important Security Alerts

- CISA publishes [advisory](#) regarding new techniques used in ongoing exploits of critical infrastructure.
- CISA and international partners urge improved [router hygiene](#) to mitigate state-sponsored targeting.
- Autonomous AI agent [escaped sandbox](#) and breached AI service provider to achieve goal.

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.
- Share this info with your security team.

Presenter/SME:
Matt Mossholder,
matt.mossholder@pjm.com

Security Update



Member Hotline

(610) 666 – 8980

(866) 400 – 8980

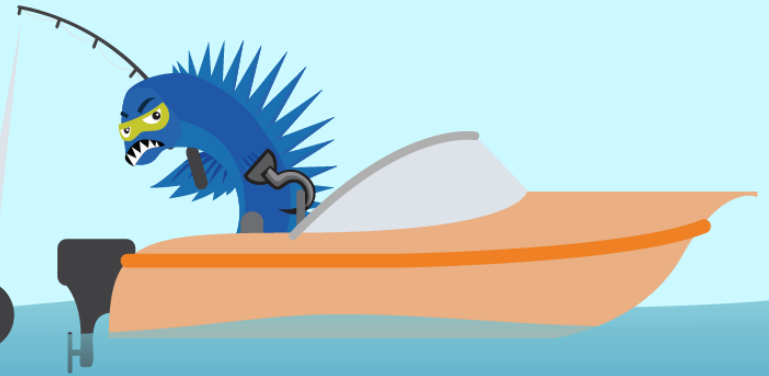
custsvc@pjm.com

**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