

Security Update

Matt Mossholder
Lead Security Architect

Tech Change Forum
September 15, 2025

Important Security Alerts

- **New social engineering playbook:** A threat group's [use of advanced deception tactics](#) to exploit organizations.
- **State-sponsored attacks against networks:** [Advisory](#) on tactics used to compromise and infiltrate networks.
- **Weaponized AI used in sophisticated attacks:** [Report](#) of large-scale theft and extortion using AI-driven automation

Monitored Threats

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

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.

Facilitator:

Tawnya Luna, Tawnya.Luna@pjm.com

Secretary:

Murat Odemis, Murat.Odemis@pjm.com

SME/Presenter

Matt Mossholder, Matt.Mossholder@pjm.com

PJM 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.
(610) 666-2244 / it_ops_ctr_shift@pjm.com

