

# PJM Security Update

Matt Mossholder  
Lead Security Architect

Tech Change Forum  
October 14, 2025

## Important Security Alerts

- **ChatGPT used to steal emails:** Using [AI to create a summary](#) of messages can lead to silent exfiltration of messages
- **Salesforce compromise leads to data theft and extortion:** [FBI advisory](#) on the threat actor tactics being used.
- **Open-source package manager packages compromised:** Attacker [uploaded compromised packages to NPM](#) to steal secrets from developers' machines

## 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](mailto:SecurityAlertTm@pjm.com).
- Share this info with your security team.

Facilitator:

Tawnya Luna, [Tawnya.Luna@pjm.com](mailto:Tawnya.Luna@pjm.com)

Secretary:

Murat Odemis, [Murat.Odemis@pjm.com](mailto:Murat.Odemis@pjm.com)

SME/Presenter

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.**  
(610) 666-2244 / [it\\_ops\\_ctr\\_shift@pjm.com](mailto:it_ops_ctr_shift@pjm.com)

