PJM Security Update

Matt Mossholder,
Lead Security Architect

Tech Change Forum
July 13, 2026

Important Security Alerts

- CISA publishes directive to agencies with procedure for risk-based vulnerability remediation.
- White House issues executive order targeting transition to post-quantum cryptography (PQC) by 2030/2031.
- Researchers demonstrate fake AI agent skills able to bypass security scanners.

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.

Contact

Presenter/SME:
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!

pjm

BE ALERT TO MALICIOUS PHISHING EMAILS

Report suspicious email activity to PJM.

Call (610) 666-2244 or email it_ops_ctr_shift@pjm.com