

Security Update

Joe Callis

Cybersecurity Operations Center

System Operations Subcommittee

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.
- **Hydro plant targeted by hacktivists:** Operations [were disrupted](#) after attackers manipulated operational parameters.

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.

Presenter:
Joe Callis

Joseph.Callis@pjm.com

Security Update

A green speech bubble containing a white question mark, positioned above a blue speech bubble containing three horizontal lines, representing a question or inquiry.

?

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