

Security Update

Jim Gluck
Sr. Director, Cybersecurity

Operating Committee
February 5, 2026

Important Security Alerts

- **Malicious QR Codes Used in Nation-state Attack:** FBI issues [intelligence](#) on current threat.
- **Securing OT:** Agencies issue [joint guidance](#) on securing connectivity in operational technology.
- **Password Manager Phishing Alert:** Article describes [phishing campaign](#) highlighting vault maintenance to steal master passwords.

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:
Jim Gluck, jim.gluck@pjm.com

Security Update



Member Hotline

(610) 666 – 8980

(866) 400 – 8980

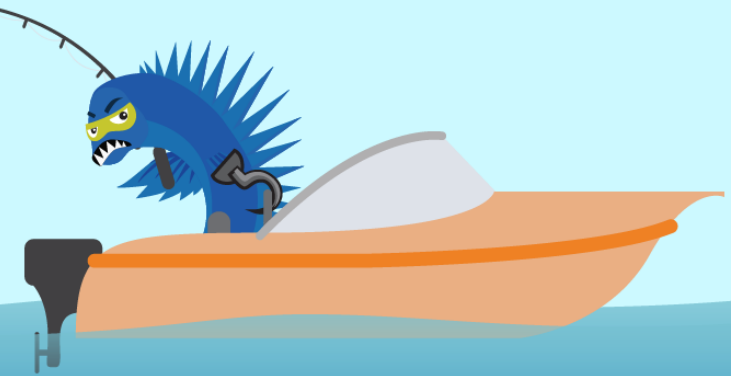
custsvc@pjm.com

**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