5 telltale signs of a social engineering attack

The message arrives unexpectedly

Unsolicited messages—especially those appearing to come from regulators, suppliers, or IT—should be treated with caution.

The requested action seems unusual

Be alert if asked to bypass protocol, share operational data, install unapproved software, or override access controls.

The requested action seems risky

If completing the action could impact nuclear safety, system availability, or compliance, stop and escalate it.

An unusual attachment or URL

Malicious links or files may be disguised as inspection reports, safety updates, or compliance documents—verify before opening.

There is a sense of urgency

Threat actors may reference shutdowns, audit failures, or safety breaches to push fast action—slow down and validate.

Stay Vigilant. Stay Cyber Aware.