INTELLIGENCE BRIEFING
Security Command Center

TLP:CLEAR
2026-06-12 14:15 UTC

Phishing Attack on Eversource Energy Exposes Personal Information of Thousands.

DATA BREACH | CRITICAL

SCC Item ID	SCC-DBR-2026-0165
Type	Data Breach
Severity	CRITICAL
Affected Products	Eversource Energy, energy provider serving Connecticut, Massachusetts, and New Hampshire customers
Published	2026-06-10
Discovery Source	Gemini

Executive Summary

A phishing attack against Eversource Energy resulted in unauthorized access to personal information belonging to approximately 3,049 customers across Connecticut, Massachusetts, and New Hampshire. The attack compromised employee credentials or account access, enabling adversaries to reach customer PII through legitimate internal systems. For energy sector organizations, this incident underscores the direct business risk of social engineering against employees with access to customer data, including potential regulatory notification obligations and reputational harm.

Technical Analysis

Attack vector: spear-phishing email targeting Eversource employees, consistent with MITRE T1566 (Phishing) and T1566.001 (Spearphishing Attachment or Link). Likely execution path: credential harvesting or account compromise (T1078, Valid Accounts), followed by unauthorized access to cloud or internal data stores containing customer PII (T1530, Data from Cloud Storage). Weakness classifications: CWE-1390 (Weak Authentication) and CWE-1021 (Improper Restriction of Rendered UI Layers, relevant if credential-harvesting pages were involved). No CVE applies; this is a human-factor incident with no exploitable software vulnerability. No patch is available or applicable. Affected data scope: personal information of approximately 3,049 customers. Threat actor attribution: unconfirmed. Incident associated with 2026 per Claim Depot reporting. Source quality is T3 across all references; no direct Eversource breach notification document is available in provided sources.

Action Checklist

1. Containment: Audit all employee accounts with access to customer PII repositories; suspend or reset credentials for any accounts that received phishing emails or show anomalous login activity. Enforce session termination for active sessions on affected accounts per NIST AC-12 (Session Termination).

2. Detection: Query email gateway logs for messages matching known phishing indicators (lookalike sender domains, credential-harvesting link patterns). Review AU-2 (Event Logging) sources including identity provider sign-in logs, cloud storage access logs, and VPN authentication logs for anomalous access patterns tied to T1078 (Valid Accounts) and T1530 (Data from Cloud Storage). Apply D3-LAM (Local Account Monitoring) to identify accounts accessing customer data outside normal business hours or from unusual source IPs.

3. Eradication: Reset credentials for all confirmed and suspected compromised accounts. Enforce password uniqueness per CIS 5.2 and disable any dormant accounts per CIS 5.3. Revoke and rotate API keys or service account credentials with access to customer data stores per D3-CRO (Credential Rotation). Review and restrict data access control lists to least-privilege per NIST AC-6 (Least Privilege) and CIS 3.3 (Configure Data Access Control Lists).

4. Recovery: Validate that customer PII repositories show no unauthorized access beyond the identified incident window using AU-6 (Audit Record Review, Analysis, and Reporting). Confirm MFA enforcement is active on all employee accounts with customer data access per CIS 6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.5 (Require MFA for Administrative Access). Monitor for secondary phishing waves targeting the same employee population.

5. Post-Incident: Conduct a phishing simulation exercise to benchmark employee susceptibility. Document control gaps, particularly around MFA gaps and email filtering effectiveness. Map findings to NIST AC-17 (Remote Access) and AU-13 (Monitoring for Information Disclosure). Initiate required breach notifications under applicable state privacy laws for Connecticut, Massachusetts, and New Hampshire. Update the incident response playbook to reflect phishing-to-data-access attack chains targeting critical infrastructure.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately if post-containment log review reveals access to customer PII beyond the 3,049 records initially identified, if any compromised account held administrative privileges over the customer data platform, or if evidence of data exfiltration (bulk download, API export, email forwarding rule) is confirmed — all of which trigger mandatory breach notification obligations under CT CRDPA, MA MGL c.93H, and NH RSA 359-C with strict notification windows.
Recovery Notes	After credential rotation and MFA enforcement are confirmed, conduct a 30-day heightened monitoring period on all accounts with customer PII access, specifically watching for anomalous off-hours access, bulk record queries, and new email forwarding rules that could indicate a secondary phishing wave or persistent access via a previously overlooked account. Validate the completeness of the affected customer list by auditing the customer PII repository access log against every account that received the phishing email — not only those flagged for anomalous login — before finalizing breach notification counts for CT, MA, and NH regulators. Do not close the incident until MFA enrollment is verified at 100% for all in-scope accounts and the email gateway's lookalike-domain detection rules have been tested and confirmed active.

Forensic Artifacts	M365/Exchange message trace logs: full delivery records for the phishing campaign including sender domain, recipient list, URL payload, and delivery timestamps — confirms the initial access vector and total employee exposure scope for the Eversource incident | Identity provider (Azure AD/Okta) sign-in audit logs: per-account records of authentication source IP, device, geolocation, risk score, and session duration during the incident window — primary evidence for mapping which employee credentials were harvested and when adversary access began | Customer PII repository access logs (SharePoint audit log or CRM audit trail): record-level access events showing which customer accounts (CT, MA, NH) were viewed, searched, or exported during the unauthorized session — the definitive artifact for scoping the 3,049 affected customer count and supporting state breach notifications | OAuth token and refresh token issuance logs from the IdP: documents whether the adversary established persistent access via token theft beyond the initial credential-harvesting session, which would extend the incident window and affect notification scope | Email forwarding rule audit log (M365 Unified Audit Log event `Set-Mailbox` or `New-InboxRule`): reveals whether compromised employee mailboxes were configured to forward communications to external attacker-controlled addresses, a common persistence technique in phishing-to-data-breach chains targeting utility sector employees

Per-Action IR Details

Containment — Audit all employee accounts with access to customer PII repositories; suspend or reset credentials for any accounts that received phishing emails or show anomalous login activity. Enforce session termination for active sessions on affected accounts per NIST AC-12 (Session Termination).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-12 (Session Termination), NIST AC-2 (Account Management), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Export Azure AD or Okta sign-in logs via PowerShell (`Get-AzureADAuditSignInLogs`) or the portal's CSV export; filter for accounts that received the phishing email (cross-reference Exchange message trace by sender domain) and flag any login from a new ASN or country within 48 hours of email receipt. Force sign-out all sessions via `Revoke-AzureADUserAllRefreshToken` per account, or equivalent IdP bulk-revoke CLI. A 2-person team can prioritize accounts with access to the Eversource customer PII repository first.

Evidence: Before suspending or resetting any credential, capture: (1) active session tokens and OAuth refresh tokens from the identity provider (Azure AD sign-in log export, Okta System Log JSON) showing source IP, user agent, and session start time; (2) concurrent session list per affected account; (3) cloud storage or CRM access logs showing which customer PII records were viewed or exported during the anomalous session window. These are volatile — IdP session records may be overwritten or expire. Snapshot them before the revoke action destroys the live session context.

Detection — Query email gateway logs for messages matching known phishing indicators (lookalike sender domains, credential-harvesting link patterns). Review AU-2 (Event Logging) sources including identity provider sign-in logs, cloud storage access logs, and VPN authentication logs for anomalous access patterns tied to T1078 (Valid Accounts) and T1530 (Data from Cloud Storage). Apply D3-LAM (Local Account Monitoring) to identify accounts accessing customer data outside normal business hours or from unusual source IPs.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting)

Compensating: Use Microsoft 365 Message Trace (free with M365) to query all inbound messages from lookalike domains (e.g., `eversource-support[.]com`) over the 30 days preceding the incident. Cross-reference with Azure AD

sign-in logs filtered for `RiskState: atRisk` or `RiskLevel: high`. For VPN, parse authentication logs with `grep` or PowerShell for failed-then-succeeded login sequences from the same account within 10 minutes. Write a Sigma rule targeting cloud storage access events (e.g., SharePoint file-download events with >50 records in a single session) and run it against exported logs using `sigma-cli` with the generic log backend.

Evidence: Capture before any account action: (1) full email header and body of the phishing message(s) from Exchange/M365 quarantine or delivery logs, including the credential-harvesting URL and redirector chain; (2) identity provider sign-in log entries for affected accounts covering 72 hours before and after phishing delivery, noting impossible-travel or new-device flags; (3) cloud storage audit logs (SharePoint/OneDrive audit log, or equivalent CRM access log) showing file/record-level access to Eversource customer PII datasets — specifically any bulk download, export, or search query touching CT, MA, or NH customer records; (4) VPN or remote-access authentication logs with source IP and geolocation for the incident window.

Eradication — Reset credentials for all confirmed and suspected compromised accounts. Enforce password uniqueness per CIS 5.2 and disable any dormant accounts per CIS 5.3. Revoke and rotate API keys or service account credentials with access to customer data stores per D3-CRO (Credential Rotation). Review and restrict data access control lists to least-privilege per NIST AC-6 (Least Privilege) and CIS 3.3 (Configure Data Access Control Lists).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), CIS 5.2 (Use Unique Passwords), CIS 5.3 (Disable Dormant Accounts), CIS 3.3 (Configure Data Access Control Lists)

Compensating: Run `Get-MsolUser -All | Where {$_.LastDirSyncTime -eq $null -and $_.WhenCreated -lt (Get-Date).AddDays(-45)}` to identify dormant cloud accounts for immediate disable. For API key rotation, enumerate service principals with access to customer data stores via `Get-AzADServicePrincipal` and force secret rotation through the Azure portal or `az ad sp credential reset`. For ACL review, export SharePoint site permissions or CRM role assignments to CSV and remove any role granting access to customer PII for accounts not operationally required — document each removal in a change log.

Evidence: Before resetting credentials or rotating API keys, capture: (1) a full dump of current ACL/role assignments for the customer PII repository (SharePoint permission report or CRM role export) to establish the pre-eradication access baseline; (2) service account last-activity timestamps and any API call logs showing data queries made under those credentials during the incident window; (3) dormant account list with last-login timestamps as evidence of the access control gap. These records are needed for breach notification documentation and regulatory response for CT, MA, and NH.

Recovery — Validate that customer PII repositories show no unauthorized access beyond the identified incident window using AU-6 (Audit Record Review, Analysis, and Reporting). Confirm MFA enforcement is active on all employee accounts with customer data access per CIS 6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.5 (Require MFA for Administrative Access). Monitor for secondary phishing waves targeting the same employee population.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Generate a 30-day access report from the customer PII repository (SharePoint audit log export or CRM audit trail) and diff it against the confirmed-compromised account list to identify any access events outside the declared incident window — flag anomalies for manual review. Verify MFA enrollment status for all accounts with customer data access using `Get-MsolUser -All | Select UserPrincipalName, StrongAuthenticationMethods` and treat any account with an empty `StrongAuthenticationMethods` field as a gap requiring immediate remediation. Set up a free Microsoft 365 alert rule or Sigma rule on the email gateway to flag messages from domains registered within the past 30 days targeting the same employee distribution lists.

Evidence: Capture before declaring recovery complete: (1) a post-remediation snapshot of the customer PII repository access log covering the full incident window plus 7 days post-containment, confirming no residual unauthorized sessions; (2) MFA enforcement policy export from the IdP confirming conditional access policies are applied to all roles with customer data access; (3) email gateway alert configuration confirming lookalike-domain monitoring is active. Worth noting this touches active incident response and regulatory notification timelines — verify recovery completeness with your legal and compliance team before closing the incident.

Post-Incident — Conduct a phishing simulation exercise to benchmark employee susceptibility. Document control gaps, particularly around MFA gaps and email filtering effectiveness. Map findings to NIST AC-17 (Remote Access) and AU-13 (Monitoring for Information Disclosure). Initiate required breach notifications under applicable state privacy laws for Connecticut, Massachusetts, and New Hampshire. Update the incident response playbook to reflect phishing-to-data-access attack chains targeting critical infrastructure.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-17 (Remote Access), NIST AU-13 (Monitoring For Information Disclosure), CIS 8.2 (Collect Audit Logs)

Compensating: Use the free GoPhish framework to run a targeted phishing simulation against the employee groups with customer PII access, using lure themes consistent with the Eversource incident (utility billing, account verification). Document click and credential-submission rates as the susceptibility baseline. For breach notification, map the 3,049 affected customers to their state of record from the confirmed-access log and prepare separate notification packages for CT (CRDPA), MA (MGLC. 93H), and NH (RSA 359-C) — each has different notification windows and required content. Update the IR playbook with a specific detection rule: any employee account accessing more than 100 customer PII records in a single session within 24 hours of receiving an external email from an unknown sender domain triggers an automatic escalation to the SOC.

Evidence: Preserve for post-incident documentation and regulatory submission: (1) the complete email gateway log export showing phishing message delivery scope (all recipients, timestamps, delivery status) to support notification list accuracy; (2) the identity provider sign-in audit log covering the full incident window as the authoritative record of unauthorized access scope for the 3,049 affected customers; (3) the pre- and post-remediation ACL snapshots showing the access control gap that enabled lateral movement from compromised employee credentials to customer PII. Worth noting this step involves legal obligations under CT, MA, and NH breach notification statutes — timing and content of notifications should be reviewed by qualified legal counsel.

Detection Guidance

Focus detection on three phases of the attack chain. Phase 1, Phishing delivery: query email gateway and security awareness platform logs for messages with lookalike Eversource domains, credential-harvesting URLs, or HTML attachment payloads consistent with T1566.001. Phase 2, Account compromise: pull identity provider (IdP) and SSO authentication logs for login anomalies: impossible travel, new device or IP, off-hours access, or MFA bypass events tied to T1078 (Valid Accounts). Phase 3, Data exfiltration: review cloud storage and CRM access logs for bulk download, unusual query volumes, or access to customer PII fields outside normal job function, consistent with T1530 (Data from Cloud Storage). Apply D3-SFA (System File Analysis) to detect modifications to authentication configuration files. Alert on AU-5 (Response to Audit Logging Process Failures) conditions; if logging gaps exist in cloud storage access, that absence itself is a detection signal. No confirmed IOCs are available in provided sources.

Framework Mappings

MITRE-ATTACK

- **T1566** — Phishing
- **T1530** — Data from Cloud Storage
- **T1078** — Valid Accounts
- **T1566.001** — Spearphishing Attachment

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC6.3** — Authorizes, modifies, or removes access

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566	Phishing	Initial-Access
T1530	Data from Cloud Storage	Collection
T1078	Valid Accounts	Defense-Evasion
T1566.001	Spearphishing Attachment	Initial-Access

Sources

Source	URL	Tier
Eversource Energy Notifies Customers of Data Breach | JD Supra	https://www.jdsupra.com/legalnews/eversource-energy-notifies-custom...	T3
Privacy Policy | Eversource	https://www.eversource.com/residential/about/privacy-policy	T3
Eversource EV Rebate Program Exposed Massachusetts Customer ...	https://mtlynch.io/eversource-resource-innovations-exposure/	T3
[PDF] testimony of eversource energy - Connecticut General Assembly	https://cga.ct.gov/2026/psdata/TMY/2026SB-00403-R000310-Pace,%20Vin...	T3
Eversource Data Breach Impacts 3049 Customers - Claim Depot	https://www.claimdepot.com/data-breach/eversource-energy-2026	T3

Generated 2026-06-12 14:15 UTC by TJS Security Command Center