INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-06 15:13 UTC

# Vishing Campaign by Threat Group 'Pink' (CL-CRI-1147) Targets IT Helpdesk Impersonation for Credential Theft and MFA Bypass

**THREAT CAMPAIGN** | **HIGH** | CVSS 7.5

| | |
|---|---|
| **SCC Item ID** | SCC-CAM-2026-0626 |
| **Type** | Threat Campaign |
| **Severity** | HIGH |
| **CVSS Base Score** | 7.5 |
| **Affected Products** | Organizations broadly; cloud collaboration platforms including Microsoft SharePoint and OneDrive |
| **Published** | 2026-07-06 |
| **Discovery Source** | Gemini |

## Executive Summary

A criminal threat group reported as 'Pink' (tracked as CL-CRI-1147) is reportedly conducting an active voice phishing campaign in which operators impersonate IT helpdesk staff to extract credentials and bypass multi-factor authentication controls. Upon successful social engineering, the group reportedly exfiltrates data from Microsoft SharePoint and OneDrive before issuing ransom demands. Specific attribution details are based on limited source corroboration and should be treated as low-to-medium confidence pending independent verification. However, the core threat pattern - helpdesk-impersonation vishing leading to cloud data theft and extortion - is consistent with established threat behavior and should be treated as credible. Organizations should prioritize defensive measures against this attack chain regardless of attribution certainty.

## Technical Analysis

Threat group 'Pink' (CL-CRI-1147) reportedly executes a multi-stage social engineering chain: operators call targets impersonating IT helpdesk personnel (T1566.004, Spearphishing Voice; T1598.004, Phishing for Information via Voice), manipulate victims into disclosing credentials (CWE-287, Improper Authentication; CWE-1390, Weak Authentication), and coach or trick them into completing or surrendering MFA tokens to bypass second-factor controls (T1621, MFA Request Generation; CWE-308, Use of Single-Factor

Authentication). Valid accounts obtained through this process (T1078) are then used to access and exfiltrate data from Microsoft SharePoint and OneDrive (T1530, Data from Cloud Storage). Ransom demands follow via email or web-based communication (T1567, Exfiltration Over Web Service). No CVE identifiers are associated with this campaign; the attack exploits human behavior and process gaps rather than software vulnerabilities. The source base for specific campaign attribution is general social engineering reference material (T1 and T3 vendor educational content); no vendor PSIRT, CISA advisory, or FBI alert corroborates the 'Pink' / CL-CRI-1147 designation in the provided material. Confidence in core TTPs is HIGH based on established vishing tradecraft; confidence in specific group attribution is LOW-MEDIUM.

## Action Checklist

1. Step 1: Containment. Immediately brief IT helpdesk staff and management that impersonation calls are an active reported threat vector; instruct helpdesk personnel to follow a strict callback verification protocol using a known-good directory number before performing any account resets, MFA changes, or credential-related actions. Evaluate suspending or restricting self-service credential reset flows for privileged accounts pending review.
2. Step 2: Detection. Review Microsoft 365 Unified Audit Logs and Azure AD Sign-In Logs for anomalous authentication events: successful logins following a failed MFA attempt sequence (T1621 indicator), logins from unexpected geographies or ASNs immediately after a helpdesk ticket, and bulk file access or download events in SharePoint and OneDrive (T1530 indicator). Query for large-volume file copy or sync events (>100 files in a short window) from accounts that recently had credentials or MFA reset. Cross-reference helpdesk ticket timestamps against authentication log timestamps. Enable or verify that NIST AU-2 event logging is active across identity and collaboration platforms per CIS 8.2.
3. Step 3: Eradication. For any account suspected of compromise: revoke all active sessions and refresh tokens immediately (Microsoft 365 admin: Revoke Sign-In Sessions); rotate credentials and re-enroll MFA using a phishing-resistant method (FIDO2 / hardware token preferred) via a verified out-of-band process; audit and remove any OAuth application grants or forwarding rules added during the suspected compromise window. Enforce NIST AC-2 account management review for all helpdesk-touched accounts in the prior 30 days.
4. Step 4: Recovery. Validate SharePoint and OneDrive activity logs to scope any data exfiltrated before session revocation; document files accessed and assess sensitivity for breach notification obligations. Confirm MFA re-enrollment is complete and phishing-resistant tokens are in place before restoring full account access. Monitor re-enrolled accounts under NIST AU-6 review cadence for a minimum of 14 days post-recovery. Apply NIST AC-17 remote access controls review to ensure no persistent backdoor access was established.
5. Step 5: Post-Incident. Conduct a tabletop exercise simulating a helpdesk-impersonation call to identify process gaps. Update helpdesk runbooks to require multi-step identity verification (e.g., manager callback + employee ID + time-based PIN) before any credential action, aligned to NIST IA controls. Evaluate deployment of phishing-resistant MFA org-wide per CIS 6.3 and CIS 6.5. Review and update security awareness training to include vishing scenarios. Assess whether multi-factor authentication hardening (NIST IA-2) and credential rotation procedures (NIST IA-4) are formalized and tested.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | URGENT |
| **Escalation Criteria** | Escalate immediately to legal counsel and executive leadership if UAL or OneDrive/SharePoint log review confirms bulk file access (>100 files) of data classified as PII, PHI, or financial records during the compromise window, as this triggers breach notification assessment obligations under GDPR (72-hour notification), HIPAA, or applicable state law; additionally escalate if any re-enrolled account shows renewed anomalous authentication patterns within the 14-day monitoring window, indicating CL-CRI-1147 operators have re-targeted the organization or established persistence not identified during eradication. Note: the 'Pink'/CL-CRI-1147 attribution rests on a single unverified source — escalation and public disclosure language should reflect this attribution uncertainty until corroborated. |
| **Recovery Notes** | Before restoring any compromised account to full production access, confirm via Azure AD Sign-In Logs that the re-enrolled account is successfully authenticating exclusively with a phishing-resistant method (FIDO2 or Windows Hello for Business) and that all conditional access policies apply without exception or bypass for that account. Run a 14-day enhanced monitoring period using daily UAL queries for SharePoint FileDownloaded, FileCopied, and AnonymousLinkCreated events on all re-enrolled accounts, with a designated analyst reviewing output each morning for anomalies. Because the 'Pink'/CL-CRI-1147 group reportedly issues ransom demands following exfiltration, assess whether any data confirmed exfiltrated in the scoping exercise meets breach notification thresholds and engage legal counsel before the applicable notification clock expires — do not conflate recovery of system access with closure of the data breach notification question. |
| **Forensic Artifacts** | Azure AD Audit Logs — 'Activity: User registered security info' and 'Activity: Reset password' events on compromised UPNs: these entries record the exact timestamp when CL-CRI-1147 operators re-registered attacker-controlled MFA methods and rotated credentials after a successful helpdesk vishing call, and are the primary artifact linking a helpdesk ticket to account takeover. \| Microsoft 365 Unified Audit Log — FileDownloaded, FileCopied, FileAccessedExtended, AnonymousLinkCreated, and SharingSet operations in SharePoint and OneDrive workloads for compromised UPNs: these records constitute the exfiltration evidence chain and are the basis for breach notification scoping; must be exported before the 90-day UAL retention window expires. \| Azure AD Sign-In Logs — entries showing 'Success' authentication result with 'MFA requirement satisfied by claim in the token' or 'MFA skipped — user registered for MFA by admin' immediately following a helpdesk-ticket-timestamped credential reset: this pattern is the authentication-layer signature of a successful CL-CRI-1147 vishing-to-access conversion and the primary detection indicator for this campaign. \| Exchange Online Inbox Rules export (Get-InboxRule) and OAuth permission grants (Get-AzureADUserOAuth2PermissionGrant) for compromised accounts: CL-CRI-1147 operators establishing mail forwarding to external addresses and OAuth grants with Files.ReadWrite.All scope represent the persistence and data-staging artifacts; these are volatile in the sense that the attacker may remove them upon detecting a response, and must be captured before session revocation. \| OneDrive sync engine logs at %localappdata%\Microsoft\OneDrive\logs\SyncEngine on endpoints assigned to compromised users: these logs capture file sync events to attacker-controlled devices that may not generate a UAL 'FileDownloaded' event, potentially revealing exfiltration volume and file names not visible in the cloud-side audit trail. |

### Per-Action IR Details

**Step 1: Containment — Immediately brief IT helpdesk staff and management that impersonation calls are an active reported threat vector; instruct helpdesk personnel to follow a strict callback verification protocol using a known-good directory number before performing any account resets, MFA changes, or**

**credential-related actions. Suspend self-service credential reset flows for privileged accounts pending review.**

**NIST Phase:** Containment

**Reference:** NIST 800-61r3 §3.3 — Containment Strategy: Stop the bleeding by eliminating the social-engineering vector before eradication or recovery actions are taken on potentially compromised accounts.

**Controls:** NIST AC-2 (Account Management), NIST AC-7 (Unsuccessful Logon Attempts), CIS 6.2 (Establish an Access Revoking Process), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

**Compensating:** For teams without an ITSM platform with enforced callback workflows: create a shared Teams/Slack pinned message with a read-receipt acknowledgment requiring all helpdesk staff to confirm they have read the advisory. Publish the known-good internal directory as a printed laminated reference at each helpdesk station. Use a free Google Form or Microsoft Forms one-pager as a mandatory verification checklist before any credential action — fields: caller name, employee ID, manager name, manager callback number confirmed (Y/N), ticket number. Suspend SSPR (Self-Service Password Reset) in Azure AD for privileged accounts via Azure AD portal > Password Reset > Properties > select group scope; this requires no additional licensing.

**Evidence:** Before suspending SSPR or modifying helpdesk procedures, capture a point-in-time snapshot of: (1) Azure AD audit logs (portal.azure.com > Azure Active Directory > Audit Logs, category: UserManagement and Authentication) filtered for the prior 72 hours — export to CSV before any policy change alters log retention context; (2) current list of accounts that had MFA methods modified or passwords reset in the prior 30 days via Microsoft Graph or Azure AD audit log filter 'Activity: Reset password' and 'Activity: Update user'; (3) active helpdesk ticket queue snapshot to correlate call-based requests against subsequent authentication events. These records establish a pre-containment baseline and are critical for scoping which accounts may already be compromised by CL-CRI-1147 operators before the callback protocol was enforced.

**Step 2: Detection — Review Microsoft 365 Unified Audit Logs and Azure AD Sign-In Logs for anomalous authentication events: successful logins following a failed MFA attempt sequence (T1621 indicator), logins from unexpected geographies or ASNs immediately after a helpdesk ticket, and bulk file access or download events in SharePoint and OneDrive (T1530 indicator). Query for large-volume file copy or sync events (>100 files in a short window) from accounts that recently had credentials or MFA reset. Cross-reference helpdesk ticket timestamps against authentication log timestamps. Enable or verify that NIST AU-2 event logging is active across identity and collaboration platforms per CIS 8.2.**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.2 — Detection and Analysis: Correlate identity-platform telemetry against helpdesk activity records to determine whether CL-CRI-1147 operators have already achieved authenticated access to Microsoft 365 tenant resources.

**Controls:** NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

**Compensating:** Without a SIEM, run the following directly against Microsoft 365 using PowerShell with the ExchangeOnlineManagement and AzureAD modules (free): (1) Unified Audit Log query — `Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-30) -EndDate (Get-Date) -Operations FileDownloaded,FileCopied,FileAccessed -ResultSize 5000 | Export-Csv UAL_FileEvents.csv`; (2) Sign-in anomaly pivot — export Azure AD Sign-In logs via portal (Azure AD > Sign-ins > Download CSV, last 30 days), then filter in Excel or PowerShell for 'Result: Success' records where 'MFA Result' contains 'MFA requirement satisfied by claim in the token' immediately preceded by failed MFA attempts on the same UPN — this pattern is characteristic of MFA fatigue or MFA bypass following vishing-obtained OTP; (3) SharePoint/OneDrive bulk access — filter UAL export for `>100 FileDownloaded` or `FileCopied` events per UPN within any 60-minute window. Cross-reference UPN against your helpdesk ticket log by timestamp. Use free Sigma rule 'win_susp_aad_signin_brute_force' adapted to M365 log schema as a detection template.

**Evidence:** This is a read-only analysis step — no live state is altered. However, before enabling any new logging or changing audit policies (the 'enable or verify AU-2' sub-action), export a current snapshot of: (1) Microsoft 365 Unified Audit Log (Compliance Center > Audit > Search) for the past 30 days, all workloads, exported to CSV — UAL records are only retained 90 days on E3 and can be overwritten if storage limits are hit; (2) Azure AD Sign-In Logs (retained 30 days by default — export immediately as this window is finite); (3) SharePoint Online access logs via `Get-SPOSite`

and Unified Audit Log filtered on SiteCollectionAdminAdded, SharingInvitationCreated, AnonymousLinkCreated — these indicate post-compromise data staging by CL-CRI-1147 operators preparing for exfiltration to an external location before ransom demand; (4) OneDrive sync client logs on endpoints (%localappdata%\Microsoft\OneDrive\logs) for any recently reset accounts — these may show mass sync activity not visible in UAL.

**Step 3: Eradication — For any account suspected of compromise: revoke all active sessions and refresh tokens immediately (Microsoft 365 admin: Revoke Sign-In Sessions); rotate credentials and re-enroll MFA using a phishing-resistant method (FIDO2 / hardware token preferred) via a verified out-of-band process; audit and remove any OAuth application grants or forwarding rules added during the suspected compromise window. Enforce NIST AC-2 account management review for all helpdesk-touched accounts in the prior 30 days.**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication: Remove all attacker-established persistence mechanisms (OAuth grants, mail forwarding rules, MFA registrations added by CL-CRI-1147) and revoke authentication state before re-enrolling victims on phishing-resistant credentials.

**Controls:** NIST AC-2 (Account Management), NIST AC-12 (Session Termination), NIST AC-17 (Remote Access), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

**Compensating:** Session revocation and OAuth audit without enterprise tooling: (1) Revoke sessions via Azure AD portal (Users > select user > Revoke Sessions) or PowerShell: `Revoke-AzureADUserAllRefreshToken -ObjectId `; (2) Enumerate OAuth app grants: `Get-AzureADUserOAuth2PermissionGrant -ObjectId ` — flag any grants to unfamiliar application IDs, particularly those with Mail.Read, Files.ReadWrite.All, or Contacts.Read scopes which align with CL-CRI-1147's data exfiltration objective; (3) Enumerate mail forwarding rules (common CL-CRI-1147 persistence): `Get-InboxRule -Mailbox | Select Name,ForwardTo,ForwardAsAttachmentTo,RedirectTo,DeleteMessage` — remove any rule forwarding to external addresses; (4) Audit MFA registrations added in the compromise window: Azure AD > Users > Authentication Methods — remove any phone-based OTP or authenticator app registrations added without a verified out-of-band request. Re-enroll only via FIDO2 or hardware token using in-person or verified video verification.

**Evidence:** CRITICAL — before revoking sessions or rotating credentials, capture the following volatile state which is destroyed the moment sessions are revoked: (1) Current active sign-in sessions for the compromised account via Azure AD Sign-In Logs — note the IP addresses, ASNs, device IDs, and conditional access policy results for the attacker's authenticated session; (2) Microsoft Cloud App Security (MCAS/Defender for Cloud Apps) activity log if available — shows real-time file access chain the attacker's session is actively performing in SharePoint/OneDrive; (3) Export the full OAuth application permission grant list and inbox rule configuration for the account BEFORE revocation — these may be removed by the attacker's automated scripts upon detecting session termination; (4) Azure AD audit log entry for MFA registration events on the compromised UPN — specifically 'Activity: User registered security info' and 'Activity: User registered all required security info' which confirm when CL-CRI-1147 re-registered attacker-controlled MFA on the account; (5) SharePoint Online file version history for any files in recently accessed document libraries — attacker may have exfiltrated and deleted files, and version history is the only recovery path.

**Step 4: Recovery — Validate SharePoint and OneDrive activity logs to scope any data exfiltrated before session revocation; document files accessed and assess sensitivity for breach notification obligations. Confirm MFA re-enrollment is complete and phishing-resistant tokens are in place before restoring full account access. Monitor re-enrolled accounts under NIST AU-6 review cadence for a minimum of 14 days post-recovery. Apply NIST AC-17 remote access controls review to ensure no persistent backdoor access was established.**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery: Restore affected accounts to verified-clean state only after confirming eradication of all CL-CRI-1147 persistence mechanisms, and establish a minimum 14-day enhanced monitoring window for re-enrolled accounts accessing SharePoint and OneDrive.

**Controls:** NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-11 (Audit Record Retention), NIST AC-17 (Remote Access), NIST AC-2 (Account Management), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 6.3 (Require MFA for Externally-Exposed Applications)

**Compensating:** Data exfiltration scoping without a DLP platform: (1) Use Microsoft 365 Compliance Center Audit Log search (free with M365 Business or E3) — filter for `FileDownloaded`, `FileCopied`, `FileAccessedExtended`, and `SharingSet` operations on the compromised UPN, export to CSV, and sort by timestamp to reconstruct the exfiltration timeline; (2) Check for anonymous sharing links created during the compromise window: `Get-SPOSite -Limit ALL | Get-SPOSiteGroup` and UAL filter for `AnonymousLinkCreated` — CL-CRI-1147 may have staged data via anonymous links rather than direct download; (3) For the 14-day monitoring period without SIEM, schedule a daily PowerShell task (Windows Task Scheduler) running `Search-UnifiedAuditLog` for the re-enrolled account filtered on all SharePoint/OneDrive operations, outputting to a dated CSV reviewed by a designated analyst each morning; (4) Verify no new conditional access policy exclusions were added for the account — Azure AD > Conditional Access > Policies, review each policy for named user exclusions added in the compromise window.

**Evidence:** Before restoring full account access (the live-state change in this step), confirm and document: (1) Complete SharePoint Online file access inventory for the compromised account covering the full compromise window — use UAL `FileAccessed` and `FileDownloaded` operations cross-referenced against your data classification inventory to identify PII, PHI, or financial data that may trigger breach notification obligations under GDPR, HIPAA, or state breach notification laws; (2) OneDrive sync history from the endpoint assigned to the compromised user (%localappdata%\Microsoft\OneDrive\logs\SyncEngine) — this may show files synced to an attacker-controlled device during the compromise window even if UAL shows no download event (sync is logged differently); (3) Azure AD Conditional Access sign-in log for the re-enrolled account confirming phishing-resistant MFA (authentication method = FIDO2 or Windows Hello for Business) is enforcing successfully before access is restored — do not restore access if the sign-in log shows fallback to SMS OTP or authenticator app push; (4) Confirm no new service principal credentials or app registrations were created under the compromised account's permissions during the window — Azure AD > App Registrations > filter by owner UPN.

**Step 5: Post-Incident — Conduct a tabletop exercise simulating a helpdesk-impersonation call to identify process gaps. Update helpdesk runbooks to require multi-step identity verification (e.g., manager callback + employee ID + time-based PIN) before any credential action, aligned to NIST IA controls. Evaluate deployment of phishing-resistant MFA org-wide per CIS 6.3 and CIS 6.5. Review and update security awareness training to include vishing scenarios. Assess whether D3-MFA (Multi-factor Authentication hardening) and D3-CRO (Credential Rotation) procedures are formalized and tested.**

**NIST Phase:** Post Incident

**Reference:** NIST 800-61r3 §4 — Post-Incident Activity: Document lessons learned from the CL-CRI-1147 campaign, update helpdesk verification runbooks to close the social-engineering gap exploited in this campaign, and institutionalize phishing-resistant MFA deployment to eliminate the credential and MFA bypass vector used.

**Controls:** NIST AC-2 (Account Management), 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), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

**Compensating:** Tabletop execution without a formal IR retainer or facilitator: use the free CISA Tabletop Exercise Packages (CTEPs) as a scenario framework base — the 'Ransomware' CTEP is directly applicable given CL-CRI-1147's ransom demand end-state; adapt inject 3 (credential compromise) to specifically simulate a vishing call impersonating internal IT helpdesk. For phishing-resistant MFA rollout without enterprise MDM: deploy FIDO2 hardware tokens (e.g., YubiKey 5 series) for privileged accounts first using Azure AD's free FIDO2 support — no Entra ID P1/P2 license required for FIDO2 registration. For vishing-specific security awareness content, use free SANS Security Awareness materials or CISA's 'Vishing Guidance' publication as training source material. Document the updated helpdesk verification runbook in a version-controlled repository (GitHub private repo or SharePoint with version history) so procedural changes are auditable.

**Evidence:** No live system state is altered in this phase. The evidence focus is institutional: (1) Retain the complete incident timeline, UAL exports, Azure AD audit log exports, and compromised account file access inventory for a minimum of 12 months (or per your documented retention policy under NIST AU-11) to support potential regulatory

notification, legal hold, or future threat intelligence correlation with additional CL-CRI-1147 campaign activity; (2) Preserve the pre-remediation OAuth grant list, inbox rule export, and MFA registration audit as forensic artifacts documenting attacker persistence techniques — these are directly useful for contributing indicators to threat intelligence sharing platforms (ISAC, CISA reporting) and corroborating or disputing the single-source 'Pink'/CL-CRI-1147 attribution; (3) Document the tabletop exercise findings, updated runbook version, and training completion records as evidence of due diligence — this documentation directly supports breach notification defense and regulatory audit responses if the incident involved regulated data.

## Detection Guidance

Focus detection on identity and collaboration platform telemetry. In Microsoft 365 Unified Audit Log, query for: (1) MFA modification events (operation: 'Update user' with StrongAuthenticationMethods property change) followed within 60 minutes by a successful login from a new IP or device; (2) bulk SharePoint/OneDrive download events, filter for FileDownloaded or FileSyncDownloadedFull operations exceeding an organizational baseline (e.g., >50 files per hour per user); (3) successful authentications immediately following a series of MFA push denials or timeouts on the same account (T1621 MFA fatigue pattern). In Azure AD Sign-In Logs, flag sign-ins with risk level 'medium' or higher coinciding with a helpdesk ticket in your ITSM system. Behavioral indicators: a user's account performing SharePoint bulk operations at unusual hours (nights, weekends) shortly after a helpdesk interaction; forwarding rules or inbox rules created shortly after a helpdesk-assisted credential reset (T1078 post-compromise persistence). NIST AU-6 mandates periodic review of these logs; consider increasing review frequency to daily for privileged and SharePoint-admin accounts during elevated threat periods. Account management reviews (NIST AC-2) and user account permissions audits (NIST AC-6) should be applied to any account touched by helpdesk within the alert window.

## Framework Mappings

### MITRE-ATTACK

- **T1567** — Exfiltration Over Web Service
- **T1621** — Multi-Factor Authentication Request Generation
- **T1598.004** — Spearphishing Voice
- **T1566.004** — Spearphishing Voice
- **T1078** — Valid Accounts
- **T1530** — Data from Cloud Storage
- **T1486** — Data Encrypted for Impact

### NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IA-8** — Identification and Authentication (Non-Organizational Users)

- **IR-4** — Incident Handling
- **AT-2** — Literacy Training and Awareness

**OWASP-TOP10-2021**

- **A07:2021** — Identification and Authentication Failures

**CIS-V8**

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

**SOC2-TSC**

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

**HIPAA-SECURITY**

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(5)(i)** — Security Awareness and Training

**NIST-CSF-2**

- **RS.MI-01** — Incidents are contained

**ISO-27001-2022**

- **A.5.29** — Information security during disruption
- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1567 | Exfiltration Over Web Service | Exfiltration |
| T1621 | Multi-Factor Authentication Request Generation | Credential-Access |
| T1598.004 | Spearphishing Voice | Reconnaissance |
| T1566.004 | Spearphishing Voice | Initial-Access |
| T1078 | Valid Accounts | Defense-Evasion |
| T1530 | Data from Cloud Storage | Collection |

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1486 | Data Encrypted for Impact | Impact |

## Sources

| Source | URL | Tier |
|---|---|---|
| 8 Types of Social Engineering Attacks - Arctic Wolf | https://arcticwolf.com/resources/blog/top-social-engineering-attack... | T3 |
| What is Social Engineering? \| IBM | https://www.ibm.com/think/topics/social-engineering | T1 |
| 10 Types of Social Engineering Attacks \| CrowdStrike | https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineer... | T1 |
| 10 Types Of Social Engineering Attacks & How To Stop Them | https://www.huntress.com/social-engineering-guide/types-of-social-e... | T1 |
| 8 Ways Organisations Prevent Social Engineering Attacks | https://blogs.stickmancyber.com/cybersecurity-blog/8-ways-organisat... | T3 |



Generated 2026-07-06 15:13 UTC by TJS Security Command Center