INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-30 14:47 UTC

Phishing Campaign Targeting Financial Institution Customers via Credential Harvesting Pages

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0602
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Customers of multiple financial institutions; financial sector email platforms
Published	2026-06-29
Discovery Source	Gemini

Executive Summary

According to a SecurityWeek report, a phishing campaign is targeting customers of multiple financial institutions using personalized spear-phishing emails and counterfeit login pages designed to steal credentials and personal information. This report is single-sourced; no corroboration from CISA, affected institutions, or named threat intelligence providers has been identified in the available data. If confirmed, the business risk includes unauthorized account access, fraudulent transactions, and reputational harm to financial institutions whose brand identity is being impersonated.

Technical Analysis

According to SecurityWeek (single source, unconfirmed by independent authorities), this campaign uses spear-phishing emails (T1566.001) and spear-phishing links (T1598.003) paired with credential harvesting pages (T1056.003) to collect account credentials and personal information from financial institution customers. Attackers leverage stolen or valid accounts (T1078) and may harvest session cookies (T1539) to bypass authentication controls. The attack chain aligns with CWE-287 (improper authentication), CWE-384 (session fixation), and CWE-1021 (UI redress/clickjacking). No malware families, C2 infrastructure, IOCs, or named threat actors are identified in the source material. No CVE is associated with this campaign. Source quality score is 0.44; treat all specifics as unconfirmed pending corroboration from CISA, FS-ISAC, or affected institution advisories.

Action Checklist

1. Containment, Monitor and restrict inbound email traffic exhibiting financial-institution impersonation patterns; configure email gateway rules to flag or quarantine messages with spoofed sender domains mimicking known financial brands, per NIST SC-7 (Boundary Protection) for inbound traffic filtering.
2. Detection, Review email gateway logs and user-reported phishing submissions for indicators of spoofed financial institution domains and lookalike URLs; enable or verify DMARC/DKIM/SPF enforcement on your own domains to reduce impersonation risk; correlate authentication logs per NIST AU-2 (Event Logging) for anomalous login attempts originating from unfamiliar geographies or user agents following email delivery events.
3. Eradication, No specific IOCs, malware, or infrastructure have been identified in the source material; eradication steps cannot be scoped to this campaign specifically. Enforce MFA on all externally-exposed financial applications per CIS 6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.4 (Require MFA for Remote Network Access); rotate credentials for any accounts suspected of compromise per D3-CRO (Credential Rotation).
4. Recovery, Validate that MFA enforcement is active for all customer-facing and employee-facing portals per CIS 6.3 and CIS 6.5; audit account access logs per NIST AU-6 (Audit Record Review, Analysis, and Reporting) for sessions that authenticated successfully from anomalous sources during the suspected campaign window; apply D3-MFA (Multi-factor Authentication) controls to reduce residual exposure.
5. Post-Incident, Conduct a tabletop review of phishing response playbooks; assess user security awareness training coverage for spear-phishing recognition; review account management controls per NIST AC-2 (Account Management) for dormant or over-privileged accounts that may have been targeted; verify CIS 5.3 (Disable Dormant Accounts) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) compliance to reduce the blast radius of future credential-harvesting campaigns.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal, compliance, and executive leadership if authentication logs confirm any customer or employee accounts successfully authenticated to harvesting infrastructure, if financial transaction anomalies are identified in the campaign window, or if the institution's own domains were spoofed in delivery — any of these conditions may trigger mandatory breach notification obligations under GLBA, PCI DSS Requirement 12.10, or applicable state laws.
Recovery Notes	Before returning affected accounts to unrestricted use, verify that MFA is enforced and confirmed active (not merely enrolled) on all externally-exposed portals, that all session tokens and OAuth grants issued during the campaign window have been revoked for harvested accounts, and that no unauthorized payee additions, wire instructions, or account detail changes were made during the window of unauthorized access. Monitor authentication logs for the 30 days following containment for reuse of harvested credentials from new IP ranges or user agents, as threat actors frequently stage harvested credential sets for use weeks after initial collection. If the campaign is confirmed multi-institution, share sanitized IOCs (lookalike domains, sending IP ranges, email subject line patterns) through FS-ISAC or your sector's threat sharing channel to benefit peer institutions.

Forensic Artifacts	Email gateway message trace logs with full raw headers (Return-Path, X-Originating-IP, Authentication-Results, DKIM-Signature) for all inbound messages matching financial brand display names with mismatched envelope-From domains during the campaign window — documents the sending infrastructure and spoofing technique used. | Browser history and web proxy/DNS logs on endpoints that received campaign emails, specifically outbound HTTP/S connections to lookalike credential-harvesting domains (e.g., subdomains or TLD variations of Chase, Wells Fargo, Bank of America, or other targeted brands) in the 0–120 minute window following email delivery — confirms which users clicked and submitted credentials. | IdP authentication logs (Azure AD sign-in logs or on-prem Windows Security Event IDs 4624/4625/4648) filtered to the campaign delivery window, with source IP, user-agent string, and geographic location fields preserved — identifies which harvested accounts were used for unauthorized access and from which attacker-controlled infrastructure. | OAuth application consent grant logs for the campaign window (Azure AD: Get-AzureADAuditSignInLogs filtered for 'Consent to application' operations) — credential-harvesting pages in financial-sector campaigns increasingly include OAuth phishing steps that establish persistent delegated access to email or account data independent of the user's password. | DMARC forensic (ruf) report XML files and email authentication failure logs showing third-party use of your institution's sender domains in campaign delivery — establishes whether your own domain identity was weaponized and supports regulatory disclosure and inter-institution notification decisions.

Per-Action IR Details

Containment — Monitor and restrict inbound email traffic exhibiting financial-institution impersonation patterns; configure email gateway rules to flag or quarantine messages with spoofed sender domains mimicking known financial brands, per CIS 9.2 email allowlisting guidance (note: CIS 9.2 is not present in the loaded knowledge base — treat this as a gap; no mapped control from the verified reference set applies directly to inbound email gateway filtering for phishing containment).

NIST Phase: Containment

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

Compensating: Export your email gateway's message trace logs (Exchange: Get-MessageTrace -RecipientAddress * -StartDate -EndDate | Where-Object {$_.Subject -match 'bank|secure|verify|account'}) and build a blocklist of observed lookalike sender domains (e.g., 'wellsfarg0.com', 'chase-secure.net'). Without an enterprise gateway, deploy a free MX-layer tool such as rspamd or SpamAssassin with custom regex rules matching financial brand display names paired with mismatched envelope-From domains. A 2-person team can implement DNS-based blocklisting of observed phishing domains via RPZ (Response Policy Zones) on a local BIND/Unbound resolver within 2 hours.

Evidence: Before activating quarantine rules that will suppress future delivery and alter the observable mail flow baseline, capture: (1) a full export of raw email headers (including Received, Return-Path, X-Originating-IP, DKIM-Signature, and Authentication-Results fields) for all flagged messages in the campaign window; (2) MTA/SMTP connection logs showing originating IP addresses and HELO/EHLO strings used by the sending infrastructure; (3) any end-user reported phishing submissions with original attachments or embedded URL snapshots intact. These artifacts document the pre-containment campaign fingerprint and are needed to build IOC feeds for ongoing detection.

Detection — Review email gateway logs and user-reported phishing submissions for indicators of spoofed financial institution domains and lookalike URLs; enable or verify DMARC/DKIM/SPF enforcement on your own domains to reduce impersonation risk; correlate authentication logs per NIST AU-2 (Event Logging) for anomalous login attempts originating from unfamiliar geographies or user agents following email delivery events.

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), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, run this PowerShell query against Azure AD / on-prem AD sign-in logs to surface credential-harvesting victims: Get-AzureADAuditSignInLogs -Filter "status/errorCode eq 0" | Where-Object {$_.location.countryOrRegion -notin @('US','CA')} | Select-Object createdDateTime, userPrincipalName, ipAddress, clientAppUsed. For DMARC verification without commercial tooling, use the free 'mxtoolbox.com/dmarc' lookup or run 'dig TXT _dmarc.yourdomain.com' to confirm p=reject or p=quarantine is published. Correlate email delivery timestamps against authentication log events within a 30-minute window to identify users who clicked and authenticated.

Evidence: This is an analysis step that does not alter live state, so no volatile pre-capture is required before executing it. However, preserve and timestamp the following before any remediation actions that could alter authentication state: (1) raw email gateway logs showing delivery events, recipient addresses, and embedded URL domains for the campaign window; (2) authentication logs (Azure AD sign-in logs, on-prem Windows Security Event ID 4624/4625 from domain controllers) filtered to the 24–72 hour window following observed email delivery; (3) browser history or web proxy logs showing outbound connections to credential-harvesting domains (e.g., URLs matching financial brand names with mismatched TLDs or subdomains like 'secure-login.bankname-verify.com'); (4) DMARC aggregate (rua) and forensic (ruf) report XML files showing third-party spoofing of your own domains.

Eradication — No specific IOCs, malware, or infrastructure have been identified in the source material; eradication steps cannot be scoped to this campaign specifically. Enforce MFA on all externally-exposed financial applications per CIS 6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.4 (Require MFA for Remote Network Access); rotate credentials for any accounts suspected of compromise per D3-CRO (Credential Rotation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), NIST AC-3 (Access Enforcement)

Compensating: For teams without an enterprise IAM platform, enforce MFA using free tiers of Azure AD Conditional Access (available with Azure AD Free for MFA-per-user mode) or Duo Security's free tier (up to 10 users). For credential rotation without a PAM tool, generate a forced password reset via PowerShell: Set-ADUser -Identity -ChangePasswordAtLogon $true, then immediately invalidate all active sessions using: Revoke-AzureADUserAllRefreshToken -ObjectId . Maintain a rotation log with username, timestamp, and initiating analyst for audit chain-of-custody.

Evidence: CRITICAL — Before revoking sessions or rotating credentials for any suspected victim account, capture the following volatile authentication state evidence: (1) all active session tokens and refresh token metadata for targeted accounts (Azure AD: Get-AzureADAuditSignInLogs for the account; on-prem: klist sessions or Mimikatz-equivalent read of LSASS for live Kerberos tickets — use a read-only tool such as Volatility on a memory image if host compromise is suspected); (2) the full list of IP addresses, user-agent strings, and geographic locations associated with authenticated sessions initiated after the phishing emails were delivered — this identifies which accounts were successfully harvested and from which attacker infrastructure; (3) any OAuth application consent grants made during the campaign window (Azure AD: Get-AzureADUserOAuth2PermissionGrant), as credential-harvesting pages sometimes include OAuth phishing to establish persistent access beyond simple password theft.

Recovery — Validate that MFA enforcement is active for all customer-facing and employee-facing portals per CIS 6.3 and CIS 6.5; audit account access logs per NIST AU-6 (Audit Record Review, Analysis, and Reporting) for sessions that authenticated successfully from anomalous sources during the suspected campaign window; apply D3-MFA (Multi-factor Authentication) controls to reduce residual exposure.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AC-12 (Session Termination)

Compensating: Without an enterprise SIEM to baseline normal authentication geography, use a free geolocation lookup against your authentication log IP addresses: feed unique IPs from the campaign window into ipinfo.io's free API (curl ipinfo.io//json) and flag any successful logins from countries outside your institution's normal operating footprint. Verify MFA coverage by pulling a user report from your IdP (Azure AD: Get-MsolUser -All | Where {$_.StrongAuthenticationMethods.Count -eq 0}) and prioritizing accounts that received phishing emails but have no MFA method registered. Monitor for 'impossible travel' events manually by sorting successful auth events by user and timestamp and flagging cases where the same account authenticated from two geographically distant IPs within under 1 hour.

Evidence: Before restoring full account access or removing any account flags placed during containment, confirm you have preserved: (1) a timestamped snapshot of all successful authentication events (Event ID 4624, Logon Type 3 or 10) for harvested accounts during the campaign window, including workstation name, source IP, and authentication package fields — these establish the forensic baseline of attacker access scope; (2) financial transaction logs or application-layer activity logs for the same accounts covering the campaign window, to identify whether harvested credentials were used for fraudulent transactions (relevant for regulatory notification threshold assessment); (3) confirmation that all OAuth grants and app permissions created during the campaign window have been reviewed and revoked where unauthorized, as these can survive a password rotation.

Post-Incident — Conduct a tabletop review of phishing response playbooks; assess user security awareness training coverage for spear-phishing recognition; review account management controls per NIST AC-2 (Account Management) for dormant or over-privileged accounts that may have been targeted; verify CIS 5.3 (Disable Dormant Accounts) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) compliance to reduce the blast radius of future credential-harvesting campaigns.

NIST Phase: Post Incident

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

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For tabletop execution without a dedicated GRC platform, use a structured free template from CISA's Tabletop Exercise Packages (CTEPs) — specifically the 'Phishing' scenario package available at cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages (recommend human validation of current URL). To audit dormant accounts without a PAM tool, run: Search-ADAccount -AccountInactive -TimeSpan 45.00:00:00 -UsersOnly | Export-CSV dormant_accounts.csv. For spear-phishing awareness gaps specific to this campaign pattern (financial institution impersonation), simulate the attack vector using GoPhish (free, open-source) with a lookalike financial domain landing page to measure click and credential-submission rates before and after training.

Evidence: Post-incident documentation must include: (1) a final incident timeline correlating phishing email delivery timestamps to authentication anomaly timestamps to any confirmed account compromise or fraudulent transaction events — this is the evidentiary record for regulatory reporting if PII or financial account data was accessed; (2) the complete list of accounts that received campaign emails, segmented by those that clicked, those that authenticated to the harvesting page, and those with confirmed unauthorized access — required for breach notification threshold analysis under GLBA, state breach notification laws, or PCI DSS Requirement 12.10; (3) lessons-learned documentation noting whether DMARC/DKIM/SPF enforcement gaps on your own domains contributed to impersonation success, and whether existing email gateway rules failed to catch the observed lookalike domain patterns — these gaps feed directly into playbook and detection rule updates.

Detection Guidance

No IOCs, C2 infrastructure, or malware hashes are available from the source material; IOC-based detection is not possible from current data. Behavioral detection guidance based on mapped MITRE techniques: monitor authentication systems for successful logins immediately preceded by email delivery events from external senders (T1566.001 + T1598.003 + T1078 correlation); alert on session cookie reuse from new IP addresses or

user agents following authentication (T1539); review proxy and DNS logs for user navigation to lookalike financial institution domains. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) and AU-12 (Audit Record Generation) to ensure authentication and email delivery events are captured with sufficient fidelity. Use D3-LAM (Local Account Monitoring) to flag local account activity anomalies post-authentication. Activate D3-SFA (System File Analysis) on endpoint authentication stores if credential theft to disk is suspected. Corroborate against FS-ISAC feeds and CISA advisories for campaign-specific IOCs as they become available.

Framework Mappings

MITRE-ATTACK

- **T1056.003** — Web Portal Capture
- **T1598.003** — Spearphishing Link
- **T1539** — Steal Web Session Cookie
- **T1566.001** — Spearphishing Attachment
- **T1078** — Valid Accounts

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **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
- **IA-8** — Identification and Authentication (Non-Organizational Users)

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

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1056.003	Web Portal Capture	Collection
T1598.003	Spearphishing Link	Reconnaissance
T1539	Steal Web Session Cookie	Credential-Access
T1566.001	Spearphishing Attachment	Initial-Access
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
gemini	https://www.securityweek.com/new-phishing-campaign-targets-financia...	T2
Email Security for Financial Institutions - Spambrella	https://www.spambrella.com/email-security-for-financial-institution...	T3
A Guide to Email Cybersecurity for Banks - Register.bank	https://register.bank/insights/email-cybersecurity-guide-banks/	T3
Email Encryption for Banks: Compliance Guide 2026 - Virtru	https://www.virtru.com/blog/email-encryption/for-banks	T3

Generated 2026-06-30 14:47 UTC by TJS Security Command Center