Help Desk Vishing and Fake Passkey Enrollment: AiTM Session Theft Driving Bulk SharePoint Exfiltration and Extortion

September 8th, 2026

Campaign	Help desk impersonation vishing paired with fake passkey or authenticator enrollment pages that operate as adversary-in-the-middle (AiTM) infrastructure. Multiple sources have also recently described the similar tradecraft against Microsoft 365 and Entra ID tenants.
Threat Actor	Financially motivated, primarily native English speaking operators associated with the broader The Com ecosystem (Scattered Spider, ShinyHunters, and affiliated extortion brands such as BlackFile, Pink, Helix, Redact, and Cinder). Treat any single-actor label as provisional; overlap between crews and shared phishing kits is likely.
Attack Type	Voice phishing to a targeted user, often on a personal phone with a spoofed caller ID, guiding the user through an MFA update on a lookalike domain. Attacker enrolls in a new authenticator or replays the session from a virtual private server (VPS) or proxy infrastructure, and proceeds to bulk collection from SharePoint, OneDrive, and Exchange for extortion.
Targeting	Often senior staff selected by title and access (VPs, directors, executives, operation leads). Observed and reported sectors include healthcare and pharmaceuticals, financial services, professional services, construction and engineering, technology, and food and beverage. Actors show prior knowledge of the target MFA stack and migration plans.
SRA Observed Activity	Multiple SRA incident response engagements over recent months across several client environments. In a recent healthcare sector case, a senior operations executive was walked through a fake passkey enrollment, a new MFA device was enrolled, a staff warning email was deleted, and well over 100,000 SharePoint files were accessed in a sync-like burst.
Impact	Bulk theft of SharePoint, OneDrive, Exchange, and Box content followed by extortion demands.

Executive Summary

Attackers are calling hand-picked employees, posing as the internal IT help desk, and walking them through a fake MFA or passkey enrollment. The enrollment page captures the live session, the attacker registers their own authenticator, and within hours entire SharePoint libraries are copied for extortion. Push, SMS, and code-based MFA do not stop this, and because the intrusion runs entirely through legitimate cloud services with no malware, endpoint tooling stays quiet.

This tradecraft belongs to the English-speaking extortion ecosystem. Mandiant's M-Trends 2026 ranks vishing as the second most common initial access vector overall and the leading vector for cloud

compromises, and CISA and FBI advisory AA23-320A (updated July 2025) describes the same help desk impersonation and MFA reset abuse by Scattered Spider. Through 2026, the lure shifted from password resets to passkey enrollment, using Microsoft's own passkey registration campaigns as the pretext. Okta (O-UNC-066), Google Threat Intelligence Group (UNC6671), and Arctic Wolf (PREY-0058) have each reported the pattern since July 2026: passkey-themed lure domains, operator-driven phishing panels that adapt to the victim's MFA method, calls to personal mobile numbers with spoofed help desk caller ID, and session replay from VPS or residential proxy infrastructure that mirrors the victim's location. Attribution across these clusters remains fluid.

The controlling factors are the help desk reset process, phishing-resistant authentication enforced through Conditional Access, and detection built around new MFA registrations followed by unusual bulk file activity. Prioritize help desk verification hardening and a phishing-resistant MFA rollout.

SRA-Observed Activity

The following reflects what SRA incident responders observed across client engagements:

- Targeted users received calls on personal devices from fake IT help desk numbers. In some cases caller ID was spoofed to display the client's name followed by IT Support.
- Callers walked the user through an MFA update on a fake domain, commonly structured as clientname[.]passkey[.]com or similar, which also functioned as AiTM infrastructure.
- After session theft and MFA enrollment, device registration and inbox rule creation varied case by case. When a device was registered, it did not follow the client's naming convention.
- Actors demonstrated prior knowledge of the target's name, personal number, domain, and MFA stack, including the organization's current MFA vendor and its planned migration to a new authenticator.
- Post-compromise activity moved directly to data. In one case the actor deleted a staff warning email about fake help desk calls, then generated more than 100,000 SharePoint FileAccessed events consistent with a client-side clone of the library. The initial sign-in came from a benign residential address in the user's home city and the session was then replayed from VPS hosting.
- Across engagements the actor consistently pivoted to VPS-hosted virtual machines rather than commercial VPN services. Providers seen include BL Networks, HostPapa, H4Y Technologies, Heymman Servers, BlueVPS, and GTT ranges flagged for fraud. HostPapa recurs across multiple cases.

Safeguards/Recommendations

- **Harden Help Desk Verification:** Treat MFA reset or enrollment request as a high-risk transaction. Never enroll or reset MFA on an inbound call. Require callback to the directory number of record, a second verification factor that cannot be socially engineered by voice, and manager attestation for executives and privileged accounts.
- **User Education:** State plainly that IT will never call a personal phone to walk a user through an MFA or passkey change. A real passkey enrollment uses the device's own system prompt, not a website that asks for codes. Warn that lure links combine the company name with passkey, MFA, or SSO wording.
- **Deploy Phishing-Resistant MFA:** Roll out FIDO2 security keys, passkeys in Microsoft Authenticator, or Windows Hello for Business and enforce them through Conditional Access authentication strengths, starting with administrators, executives, and high-access roles.

- **Restrict Security Info Registration:** Create a Conditional Access policy on the Register security information user action that requires a compliant or managed device or a trusted location. Pair with Entra ID Protection to block registration during risky sign-ins.
- **Block Device Code Flow:** Use the Conditional Access authentication flows condition to block device code flow tenant-wide, with documented exceptions only. Requiring a compliant device closes most remaining device code phishing paths.
- **Control Device Registration:** Limit who can register or join devices and require an authentication strength or trusted for the Register or join devices user action.
- **Enable Token Protection and Continuous Access Evaluation:** Bind tokens to managed devices where licensing allows, enforce compliant network checks, and enable CAE for Exchange and SharePoint so a replayed session from hosting or proxy infrastructure is revoked in near real time.
- **Reduce Data Blast Radius:** Review broad SharePoint and OneDrive access for executive accounts and confirm unified audit logging is enabled.

Indicators of Compromise

Indicator	Type	Source	Context
193.149.176[.]91	IPv4	SRA IR	BL Networks, session replay
142.111.185[.]146	IPv4	SRA IR	GTT Communications, fraud risk flagged
192.158.233[.]196	IPv4	SRA IR	H4Y Technologies LLC
192.210.198[.]89	IPv4	SRA IR	HostPapa, provider recurs across cases
212.162.151[.]145	IPv4	SRA IR	Heymman Servers Corporation
91.236.230[.]122	IPv4	SRA IR	BlueVPS OU, September 2026
setpasskey[.]com	Domain	Okta, Arctic Wolf	Passkey lure root, per-target subdomains
assignpasskey[.]com	Domain	Okta, Arctic Wolf	Passkey lure root, per-target subdomains
passkeydeploy[.]com	Domain	Okta, Arctic Wolf	Passkey lure root, per-target subdomains
deploypasskey[.]com	Domain	Okta	Passkey lure root, per-target subdomains
passkeyadd[.]com	Domain	Okta	Passkey lure root, per-target subdomains
mfaregister[.]com	Domain	Arctic Wolf	MFA lure root
registermymfa[.]com	Domain	Arctic Wolf	MFA lure root
passkey-mfa[.]com	Domain	Arctic Wolf	Passkey lure root
oskeysetup[.]com	Domain	Arctic Wolf	Passkey lure root
nowsso[.]com	Domain	Arctic Wolf	SSO lure root
oursso[.]com	Domain	Arctic Wolf	SSO lure root
AS57724	ASN	Okta, GTIG	DDoS-Guard, lure hosting
AS59692	ASN	Okta	IQWeb FZ-LLC, lure hosting
AS51852	ASN	GTIG	Private Layer, replay infrastructure
AS201814	ASN	GTIG	MEVSPACE, replay infrastructure
AS11878	ASN	GTIG	Tzulo, replay infrastructure
AS25369	ASN	GTIG	Hydra Communications, replay infrastructure

References

- Welcome to BlackFile: Inside a Vishing Extortion Operation
- Cloud Data Theft and Extortion via IT Help Desk Vishing and Residential Proxies
- Impersonating IT support: how threat actors turn a remote session into enterprise-wide access
- Behind the scenes of a vishing operation
- Vishing actors target Entra passkey enrollment | Okta Threat Intelligence