DIGITAL DEFENSE DIGEST

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

INSIDE THIS ISSUE

This monthly publication is provided by Black Belt Secure

BLACK BELT SECURE

OUR MISSION:

To empower businesses of all sizes with the knowledge and tools they need to thrive in today's increasingly complex cyber threat landscape. We are dedicated to providing cutting-edge cybersecurity solutions and expert guidance to help our clients

WHY MFA ALONE NO LONGER STOPS PHISHING

For a decade, "turn on MFA" was the single most effective piece of security advice a business could follow. That advice is now dangerously incomplete. Adversary-in-the-middle (AiTM) phishing — also called reverse-proxy phishing — doesn't try to guess your password or defeat your second factor. It sits invisibly between you and the real login page, relays every field you type, and steals the authenticated session token the instant you finish logging in.
The result: the attacker walks away with a live, already-authenticated session — no password cracking, no MFA fatigue bombing, no second guess required. Microsoft's 2025 Digital Defense Report attributes 80% of all MFA-bypass breaches to exactly this mechanism, and Microsoft separately disclosed a single AiTM campaign that hit 35,000 users across 13,000 organizations in 26 countries over just three days this spring.

The Stakes:

Proofpoint found that 59% of accounts compromised through phishing in 2025 had MFA enabled at the time of the attack. Obsidian Security's incident response data puts it even higher: MFA failed to stop the attack in 84% of the cases they investigated. MFA is still essential — but the type of MFA now determines whether it works at all.

The tools driving this shift are no longer nation-state exclusive. Phishing-as-a-Service (PhaaS) kits such as Evilginx, Tycoon 2FA, and Mamba 2FA operate as ready-made reverse proxies and rent for as little as $120 — putting session-token theft within reach of any low-skill criminal crew. Microsoft recorded a 146% year-over-year increase in AiTM attacks as this commodity tooling spread.

continued on page 2...

...continued from cover

THE STRATEGIC VIEW: HOW AITM PHISHING ACTUALLY WORKS

From a vCISO perspective, AiTM phishing is best understood not as a smarter phishing email, but as a real-time man-in-the-middle relay attack against the authentication process itself. It unfolds in four steps, and understanding each one clarifies exactly where a defense has to sit.

Step 1 — The Lure

A phishing email, SMS, or Teams message directs the victim to a link that looks identical to a familiar login page (Microsoft 365, Okta, a VPN portal). Increasingly, these lures are AI-generated and personalized using data scraped from LinkedIn or prior breaches, making them far harder to spot than the generic phishing of years past.

Step 2 — The Proxy

Instead of a static fake login page, the victim lands on a reverse proxy that faithfully forwards every request to the real site in real time. The victim is, in effect, logging into the genuine service — through the attacker's server.

Step 3 — The Capture

When the victim enters their password and completes MFA (SMS code, push approval, or authenticator app code), the proxy captures the resulting session cookie or token — the artifact that proves "this user is already authenticated" — the moment it is issued.

Step 4 — The Takeover

The attacker imports that session token into their own browser and is instantly logged in as the victim, with MFA already satisfied. From here, business email compromise, mailbox rule manipulation, and lateral movement typically follow within minutes.

$4.81M
AVG. COST OF A CREDENTIAL-BASED BREACH (IBM, 2025)

$3.9M
AVG. DAYS TO IDENTIFY & CONTAIN A STOLEN-CREDENTIAL BREACH

84%
OF INCIDENTS WHERE MFA FAILED TO STOP THE ATTACK (OBSIDIAN)

146%
YEAR-OVER-YEAR GROWTH IN AiTM ATTACKS (MICROSOFT)

WHY THIS MATTERS BEYOND IT

Because the attacker ends up with a legitimate, fully authenticated session, most conventional MFA — SMS codes, push notifications, and time-based one-time-password apps — provides no protection whatsoever against this technique. The control that matters is not whether MFA is present, but whether the authentication method can be phished in the first place.

FROM THE OPERATIONS CENTER: WHICH MFA METHODS ACTUALLY HOLD UP

Every month, Black Belt Secure's SOC evaluates the authentication methods in use across our client base against real-world AiTM activity. Here is how the common options stack up — and why only one category is considered phishing-resistant by CISA.

Authentication Method	Resistant to AiTM?	Common Weakness	Compliance / Insurance Standing
SMS one-time code	No	Session token stolen post-verification; also vulnerable to SIM-swapping	Does not satisfy NIST 800-171r3 3.5.3 or most 2026 carrier requirements
Push notification (app)	No	Relayed by proxy in real time; vulnerable to MFA-fatigue prompting	Accepted minimum for standard users; not for admins or CUI systems
TOTP authenticator code	No	Code is entered into the proxy and relayed instantly	Same limitations as push; commonly used but phishable
FIDO2 / WebAuthn security key	Yes	None known at scale; cryptographic challenge is bound to the origin domain	Meets NIST 800-171r3 3.5.3, CMMC Level 2, and top-tier carrier requirements
PKI-based (PIV / CAC / smart card)	Yes	Requires hardware issuance and lifecycle management	Standard for federal agencies and DIB contractors under OMB M-22-09

BEYOND MFA: SESSION AND TOKEN PROTECTIONS

Phishing-resistant MFA closes the door AiTM walks through at authentication — but a complete defense also limits what a stolen session can do if one ever slips through. Conditional Access policies that bind sessions to a managed device and a known IP range, shortened token lifetimes, and automated alerting on impossible-travel sign-ins all reduce the blast radius. Black Belt Secure layers these controls into every managed security engagement so a single compromised token cannot become a full account takeover.

PROACTIVE VALIDATION:

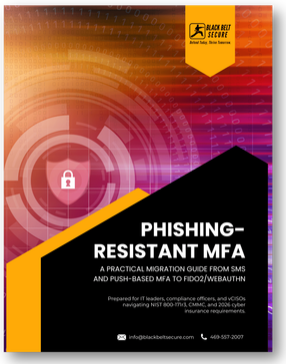
Our technical workflow includes a quarterly authentication audit – reviewing every account with administrative or CUI access to confirm it is protected by a phishing-resistant method, not merely "MFA enabled." This surfaces exposure before an auditor, an insurer, or an attacker does.

FREE WHITEPAPER:

Phishing-Resistant MFA: A Practical Migration Guide

A step-by-step guide to migrating from SMS and push-based MFA to FIDO2/WebAuthn — including a phased rollout plan by account tier, a NIST 800-171r3 and CMMC control mapping, and a rollout checklist for IT leaders and vCISOs.

Claim Your FREE Copy Today At: blackbeltsecure.com/reports



BLACK BELT SECURE
Defend Today, Thrive Tomorrow.

COMMUNITY CORNER & UPCOMING INITIATIVES

At Black Belt Secure, our mission extends beyond protecting networks. We are dedicated to cultivating the next generation of cybersecurity talent and supporting the organizations that serve our communities.

YOUR PHISHING-RESISTANT MFA ACTION PLAN

Migrating away from phishable MFA is not a weekend project, but it is achievable with a prioritized, phased approach. To move from "MFA enabled" to genuinely phishing-resistant, prioritize these five actions:

1. Inventory Every Authentication Method in Use
You cannot protect what you haven't mapped. Catalog every account — user, admin, service, and shared — and the MFA method each one relies on today.

2. Move Privileged and Admin Accounts to FIDO2 First
These accounts carry the most risk and the least tolerance for delay. Hardware security keys or platform passkeys should be the first migration wave, completed within 30–60 days.

3. Retire SMS and OTP-App MFA for CUI and Regulated Systems
Any system touching Controlled Unclassified Information, PHI, or cardholder data should move to phishing-resistant MFA to satisfy NIST 800-171r3 Practice 3.5.3 and CMMC Level 2.

4. Deploy Conditional Access and Session Token Protections
Bind sessions to managed devices, shorten token lifetimes, and enable automated alerting on impossible-travel or anomalous sign-ins as a second layer of defense.

5. Engage an MSSP for a Structured Rollout
A phased migration — with user training, help-desk support, and documented evidence for auditors and insurers — avoids the disruption and gaps that come with an ad hoc rollout.

COMING NEXT MONTH

Non-Profit & Government Sector Security Initiative

Launching in September: educational workshops and tailored resources to help nonprofits, schools, and local government agencies navigate NIST and FISMA compliance and grant eligibility.

SCHEDULE A FREE ASSESSMENT

Not sure which of your accounts are still protected by phishable MFA? Our no-obligation Authentication Gap Assessment delivers a prioritized finding report – in plain language – within 5 business days.

blackbeltsecure.com/assessment