

MFA Is Not Enough: How Attackers Are Hijacking Microsoft 365 Without Your Password



ARTICLE 06.17.26 GUI COZZI

For years, the cybersecurity community has championed multi-factor authentication (MFA) as the single most impactful control organizations can implement to protect their accounts. And that guidance remains sound, but it comes with a critical caveat: not all MFA is created equal, and attackers have found ways around it.

The FBI issued an urgent Public Service Announcement in May 2026 warning about a new Phishing-as-a-Service (PhaaS) platform called **Kali365** that is specifically engineered to bypass MFA in Microsoft 365 environments, without ever stealing your password.

This is a threat your organization needs to understand and act on now.

What Is Kali365 and Why Should You Care?

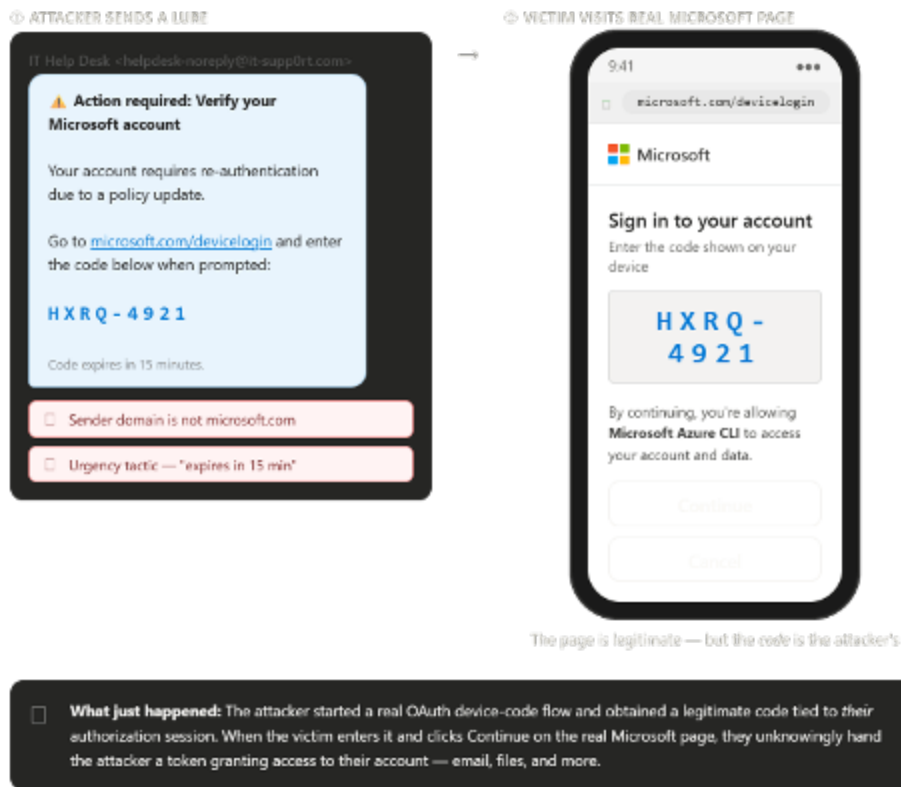
Kali365 is a subscription-based attack toolkit distributed through Telegram that enables cybercriminals (even those with limited technical skills) to compromise Microsoft 365 accounts at scale. Its capabilities include AI-generated phishing lures, automated campaign management, real-time victim tracking dashboards, and most dangerously, OAuth token capture.

What makes Kali365 particularly alarming is the attack method it exploits: device code flow phishing. This technique abuses a legitimate Microsoft authentication mechanism, allowing attackers to hijack a user's authenticated session entirely by bypassing the MFA process.

How the Attack Works

The attack chain is deceptively simple and exploits user trust in Microsoft's own infrastructure:

- **Lure** – A victim receives a phishing email impersonating a familiar cloud service (think DocuSign, SharePoint, or Microsoft Teams). The email contains a device code and instructs the recipient to visit a legitimate Microsoft verification page to enter it.
- **Authorization** – The victim navigates to a real Microsoft URL (*microsoft.com/devicelogin*) and enters the code. Because the page is genuine, nothing looks suspicious. The victim may also complete an MFA prompt at this stage believing they are authenticating into a trusted service.



- **Token Theft** – In the background, the attacker's device captures the resulting OAuth access token and refresh token. These tokens represent a fully authenticated session as no password required, and no further MFA is needed.
- **Persistent Access** – With valid tokens in hand, the attacker gains access to Outlook, Teams, OneDrive, SharePoint, and other Microsoft 365 services. Refresh tokens can extend this access for days or weeks.

The victim completed MFA. The victim did nothing obviously wrong and the attacker now owns the account.

Why This Bypasses MFA

Traditional MFA protects the *password login flow*. Device code flow phishing sidesteps that flow entirely. The attacker is not trying to log in as you but instead tricking you into authorizing *their device* through a legitimate Microsoft interface. When the MFA prompt is complete, it is validating the attacker's session, not protecting against it.

This is why the FBI's advisory specifically warns that standard MFA protocols are insufficient against this attack vector, and why organizations relying solely on SMS codes, authenticator app push notifications, or even TOTP codes remain exposed.

Who Is at Risk?

Any organization using Microsoft 365 is potentially vulnerable if device code flow authentication is enabled, which is by default in most tenant configurations. Industries handling sensitive data or subject to regulatory oversight face compounded risk:

- Healthcare organizations – PHI exposure, HIPAA breach notification obligations
- Financial services firms – client data, wire transfer systems, fiduciary exposure
- Professional services – confidential client communications, privileged information

- Manufacturing and supply chain – operational systems accessible through M365 identities
- Higher education – FERPA-protected student records, research data

The broad availability of Kali365 through a low-cost Telegram subscription means even organizations that are not high-profile targets may be swept up in opportunistic campaigns.

What Your Organization Should Do

The FBI and Dean Dorton recommend the following immediate and near-term actions:

Immediate Priority: Restrict Device Code Flow

The core technical mitigation is to **disable or restrict device code flow authentication** in your Microsoft Entra ID (formerly Azure AD) environment through Conditional Access policies.

- **Audit first** – Before blocking device code flow broadly, identify any legitimate business processes that rely on it (certain legacy devices, printers, or kiosk scenarios may use it). Blocking without auditing can cause disruptions.
- **Create a Conditional Access policy** – To block device code flow for all users, with documented exceptions for verified legitimate use cases.
- **Protect emergency access accounts** – Exclude your break-glass accounts from this policy to prevent an accidental lockout scenario.
- **Block authentication transfer** – Implement policies that prevent authentication sessions from being transferred between devices.

Upgrade to Phishing-Resistant MFA

Against this attack technique, phishing-resistant MFA is not a complete defense because Device Code Phishing can trick a user into authorizing access through a legitimate device-code flow. However, it provides exceptional protection against Adversary-in-the-Middle phishing by binding authentication to the legitimate website or service, preventing stolen credentials or session interactions from being replayed through a proxy. It also significantly reduces the effectiveness of targeted phishing attacks, since attackers cannot simply persuade users to reveal a one-time code, approve a push notification, or share a password-equivalent factor.

Your organization should evaluate and migrate toward phishing-resistant authentication methods, including:

- **FIDO2 / Passkeys** – Hardware or platform-bound authenticators that cryptographically bind authentication to the legitimate site
- **Certificate-Based Authentication (CBA)** – Smart cards or device certificates that cannot be proxied
- **Windows Hello for Business** – Windows Hello for Business is a phishing-resistant MFA method that replaces passwords with device-bound cryptographic keys, so authentication succeeds only from the enrolled device using the user's biometric gesture or PIN.

Train Your Users With This Specific Scenario

Device code phishing succeeds in part because users are trained to complete MFA prompts. Update your security awareness training to include:

- What device code flow authentication looks like
- The rule: never enter a code on Microsoft's device login page unless you personally initiated the sign-in from a known device
- Skepticism toward any email requesting authentication through an unfamiliar workflow

Monitor for Indicators of Compromise

If you have a SIEM, MDR, or Microsoft Defender for Identity in place, configure alerting for:

- OAuth token grants from unexpected IP addresses or geographies
- Sign-ins during unusual hours tied to token-based authentication
- Unusual access patterns to Teams, OneDrive, or SharePoint following a device code flow event
- Active sessions originating from IP addresses not associated with known users

Review Third-Party App Permissions

Attackers with valid OAuth tokens can also grant persistent access to malicious third-party applications. Audit your Microsoft 365 tenant for:

- Unexpected OAuth application consents
- Apps with broad permissions (Mail.Read, Files.ReadWrite.All) granted by end users
- Applications you do not recognize in the Enterprise Applications list

How Dean Dorton Can Help

Our Cybersecurity Risk & Compliance team works with organizations across all industries including healthcare, financial services, manufacturing, and professional services to assess and strengthen Microsoft 365 security postures. Specific services relevant to this threat include:

- **Microsoft 365 Security & Tenant Assessment** – A comprehensive review of your Entra ID configuration, Conditional Access policies, MFA posture, and OAuth application inventory
- **Phishing-Resistant MFA Advisory** – Evaluating and planning a migration from legacy MFA methods to FIDO2 or certificate-based authentication
- **Managed Detection & Response (MDR)** – 24/7 monitoring for identity-based threats, including token abuse and anomalous sign-in activity
- **Security Awareness Training** – Updated training content that incorporates emerging social engineering techniques like device code phishing
- **Fractional CISO Services** – Ongoing strategic guidance for organizations that need expert cybersecurity leadership without a full-time hire

The Bottom Line

The Kali365 advisory is a timely reminder that attackers adapt faster than most organizations update their defenses. MFA is still a critical control. However, the threat landscape has evolved, and organizations that deployed MFA several years ago and never revisited their authentication architecture are not as protected as they believe.

Restricting device code flow and migrating to phishing-resistant MFA are not long-term roadmap items. They are actions that should be prioritized today.

If you would like to discuss your organization's Microsoft 365 security posture or schedule an assessment, [contact the Dean Dorton Cybersecurity Risk & Compliance team](#).

Reference: FBI IC3 Public Service Announcement I-052126-PSA, "Kali365 Phishing-as-a-Service Kit Hijacks Microsoft 365 Access Tokens," May 21, 2026. <https://www.ic3.gov/PSA/2026/PSA260521>