ADVISORY FOR ICM SECTOR

AI-Enabled Device Code Phishing Campaign

Published Date: 6 April 2026

Classification: TLP:CLEAR

Executive Summary

On 6 April 2026, Microsoft published an ongoing phishing campaign where the threat actor tricks victim into permitting threat actor's device or application to access a victim's M365 account. Conventional phishing campaigns steals usernames, passwords or deliver malware, but this campaign abuses legitimate Microsoft authentication process. Victims first receive an email lure requiring their login before accessing a file. Victims are directed to Microsoft's legitimate website (https://microsoft.com/devicelogin) and required to enter a device authentication code provided by the threat actor. After which, if victim is not already logged into M365, they will be asked to enter username, password and/or MFA to their Microsoft 365 account. The campaign appeared to incorporate AI-assisted automation to improve phishing effectiveness and scale credential abuse operations.

Once the authentication process is completed, the threat actor does not require victim's M365 credentials but receives valid access and refresh tokens associated with the victim's account, potentially allowing unauthorised access to Microsoft 365 services. Microsoft linked the activity to the emergence of "EvilTokens", a Phishing-as-a-Service (PhaaS) toolkit designed to automate device-code phishing operations. Given the widespread adoption of Microsoft 365 across various sectors including telecommunications operators, media organisations, enterprises, organisations are strongly encouraged to review identity and access security controls and monitor for suspicious device-code authentication activity.

Background

Device Code Authentication is a legitimate OAuth-based authentication mechanism commonly used to allow devices or applications. The typical sequence of activities triggered by a legitimate user is: user is prompted to visit a Microsoft login page on a secondary device and enter a short authentication code to complete the sign-in process.

Threat actors reverse this workflow by generating authentication codes on attacker-controlled systems and convincing victims to complete the authentication on Microsoft's legitimate login portal. Once the victim approves the login request, Microsoft issues authentication tokens tied to the victim's account directly to the attacker-controlled session.

According to Microsoft Threat Intelligence, the campaign leverages:

- AI-assisted phishing infrastructure
- Automated victim interaction workflows
- Dynamic device-code generation
- Cloud-hosted redirect infrastructure
- Real-time authentication processes

Observed phishing emails impersonate common business and collaboration workflows, including:

- Password expiry notifications
- Shared document requests
- Voicemail alerts
- Electronic-signature request
- Internal collaboration notifications

Victims are typically redirected through multiple cloud-hosted services before reaching Microsoft's legitimate device login page.

Detection and Mitigation

IMDA recommends organisations perform continual testing and validation of existing security controls to ensure detection and prevention against the AI-enabled device-code phishing activities identified in this advisory:

- Refer to the MITRE ATT&CK techniques in this advisory (Annex A):
  - Assess whether Device Code Authentication is operationally required within the environment.
  - Restrict Device Code Authentication flows to approved applications where feasible.
  - Strengthen Conditional Access Policies to restrict authentication from unmanaged devices and untrusted locations.
  - Implement phishing-resistant authentication mechanisms such as FIDO2 security keys, passkeys, or Windows Hello for Business where feasible.
  - Where available, enable Microsoft Defender XDR, Defender for Office 365 Safe Links and Microsoft Entra ID Protection to generate alerts for suspicious device-code authentication, malicious email links, risky sign-ins and abnormal token activity.
  - Review Microsoft Entra sign-in logs for Device Code Flow authentication and investigate unusual source IP addresses, locations, applications, device registrations and Microsoft Graph activity.
  - Monitor for impossible-travel anomalies, anonymous IP usage, and abnormal token activity.
  - Create, test and validate detection rules against the identified threat behaviours.
  - Enhance user awareness regarding device-code phishing techniques and unexpected requests involving microsoft.com/devicelogin.
  - Restrict user privileges to reduce the impact of initial compromise.
  - Revoke active sessions and refresh tokens if unauthorised activity is detected.
  - Review mailbox rules, OAuth application permissions, and suspicious device registrations following suspected compromise.

Annex A – MITRE ATT&CK Mapping

ATT&CK Tactic	ATT&CK ID	Technique	Observed Activity
Reconnaissance	T1589.001	Gather Victim Identity Information: Credentials	Validation of active Microsoft 365 accounts and tenants prior to phishing delivery.
Initial Access	T1566.002	Phishing: Spearphishing Link	Delivery of phishing emails containing malicious hyperlinks and fake collaboration requests.
Initial Access	T1566.001	Phishing: Spearphishing Attachment	Delivery of HTML and PDF attachments containing phishing lures.
Credential Access	T1528	Steal Application Access Token	Abuse of OAuth Device Code Authentication to obtain access and refresh tokens.

Credential Access	T1550.001	Use Alternate Authentication Material: Application Access Token	Use of stolen OAuth tokens to access Microsoft 365 services without passwords.
Defense Evasion	T1036	Masquerading	Abuse of Microsoft's legitimate authentication portal to appear trustworthy to victims.
Command and Control	T1102.003	Web Service: One-Way Communication	Use of legitimate cloud-hosted services such as Cloudflare Workers, AWS Lambda and Vercel for phishing infrastructure.
Persistence	T1098	Account Manipulation	Persistent access through valid refresh tokens and OAuth sessions.

References

- Microsoft Security Blog – AI-Enabled Device Code Phishing Campaign