NEWS 18 December 2025

OAuth Device Code Phishing Campaigns Surge Targets Microsoft 365

Alessandro Mascellino
News Reporter
Email Alessandro Follow @a_mascellino

A surge in phishing campaigns abusing Microsoft's OAuth device code authorization flow has been observed with multiple threat clusters using the technique to gain unauthorized access to Microsoft 365 accounts.

According to a new advisory published today by Proofpoint, both state-aligned and financially motivated actors are leveraging social engineering to trick users into approving malicious applications, enabling account takeover, data theft and further compromise.

The attacks rely on the OAuth 2.0 device authorization grant, a legitimate process designed to help users sign in on devices with limited input capabilities.

Once a victim enters a device code generated by an attacker-controlled application on Microsoft's trusted verification page, the threat actor receives a valid access token. That token can then be used to control the compromised M365 account.

QR Codes, Embedded Buttons and Hyperlinks

The researchers noted unusually widespread campaigns that relied on QR codes, embedded buttons or hyperlinked text to initiate the attack chain. Lures often claimed to involve document sharing, token reauthorization or security verification.

Read more on OAuth authentication abuse: Russian Threat Actors Target NGOs with New OAuth Phishing Tactics

One campaign detected on December 8 used a fake shared document titled "Salary Bonus + Employer Benefit Reports 25." Victims were sent emails from attacker-controlled addresses and directed to localized websites branded to match their organization.

Users were then prompted to enter a code on Microsoft's device login page, inadvertently granting access to their accounts.

Proofpoint linked the growth of these campaigns to readily available phishing tools that simplify device code abuse. Two tools stood out:

- SquarePhish2, an updated phishing framework that uses QR codes and automates the OAuth device grant flow
- Graphish, a free phishing kit shared on vetted hacking forums that supports adversary-in-the-middle attacks and OAuth-based authorization abuse

Both tools are designed to be user-friendly and require limited technical skill, making them accessible to a wide range of threat actors.

Financial and State-Aligned Activity

Proofpoint said a financially motivated actor tracked as TA2723 began using device code phishing in October 2025, spoofing salary documents and shared files to lure victims.

The company also observed state-aligned activity, particularly from Russia-linked actors, adopting the technique as part of a broader shift toward passwordless phishing.

One suspected Russia-aligned group, UNK_AcademicFlare, targeted government, academic and transportation sectors in the US and Europe using compromised email accounts and spoofed OneDrive links to deliver device code phishing workflows.

According to Proofpoint, the expansion of these campaigns shows how quickly threat actors adapt legitimate authentication features for malicious ends.

The company said organizations should strengthen OAuth controls and train users not to enter device codes received from untrusted sources.

"Proofpoint assesses that the abuse of OAuth authentication flows will continue to grow with the adoption of FIDO compliant MFA controls."

You may also like

NEWS 17 May 2023
Social Engineering Risks Found in Microsoft Teams

NEWS 27 September 2022
Microsoft Sway Pages Weaponized to Perform Phishing and Malware Delivery

NEWS 22 January 2025
Tycoon 2FA Phishing Kit Upgraded to Bypass Security Measures

NEWS 22 July 2025
Widespread Net RFQ Scam Targets High-Value Goods

NEWS 25 March 2024
New Tycoon 2FA Phishing Kit Raises Cybersecurity Concerns

What's Hot on Infosecurity Magazine?

Read | Shared | Watched | Editor's Choice

1

NEWS 5 February 2026
New Hacking Campaign Exploits Microsoft Windows WinRAR Vulnerability

2

NEWS 3 February 2026

Hundreds of Malicious Crypto Trading Add-Ons Found in Moltbot/OpenClaw

3

NEWS 4 February 2026

Two Critical Flaws in n8n AI Workflow Automation Platform Allow Complete Takeover

4

NEWS 5 February 2026

Smartphones Now Involved in Nearly Every Police Investigation

5

NEWS 4 February 2026

AI Drives Doubling of Phishing Attacks in a Year

6

NEWS 4 February 2026

SolarWinds Web Help Desk Vulnerability Actively Exploited