EvilTokens

The New Microsoft 365 Phishing Threat

How attackers are using REAL Microsoft login pages
to steal your access tokens

IT Security Awareness Briefing | April 2026

systech

Why This Is Different

This isn't the phishing you've been trained to spot.

Old Phishing (Spoofed Pages)

- Fake login page mimics Microsoft
- URL is wrong (e.g. micros0ft-login.com)
- SSL cert doesn't match
- Password & MFA code captured by attacker proxy
- Trained users can spot the fake URL

EvilTokens (Real Pages)

- **REAL Microsoft login page**
- **URL is microsoft.com/devicelogin**
- Valid SSL certificate from Microsoft
- Your real MFA prompt fires — and you approve it
- **Even trained users get fooled**

The victim sees no red flags. The URL is real. The page is real. The MFA prompt is real.

What Is Device Code Flow?

A legitimate Microsoft feature being weaponized

Designed For:

Smart TVs, IoT devices, and printers that can't display a full login screen. Instead of typing credentials on the device, you enter a short code on your phone or laptop to authorize it.

The Legitimate Flow:

1. Device generates a short code
2. You visit microsoft.com/devicelogin
3. You enter the code & sign in with MFA
4. Device gets an access token

How Attackers Abuse It:

1. Attacker generates a device code tied to THEIR session
2. Sends you a phishing email with the code
3. You go to REAL Microsoft page & enter it
4. You complete YOUR real MFA challenge
5. **Microsoft gives the ATTACKER your tokens**

Result: Attacker gets a 90-day refresh token. No password stolen. No MFA bypassed. They just got YOU to authorize THEM.

The EvilTokens Attack Chain

1

Phishing Lure

Victim gets email: fake DocuSign, SharePoint share, voicemail, or payroll notice

2

Real Microsoft Page

Link goes to microsoft.com/devicelogin — a 100% legitimate Microsoft URL

3

Enter Code + MFA

Victim enters the attacker's code and completes their normal MFA prompt

4

Tokens Harvested

Attacker receives access token + 90-day refresh token for the victim's account

What The Attacker Gets:

Full Email Access

Read, send, delete emails as the victim

OneDrive / SharePoint

Access all files and shared documents

Teams Data

Read chats, channels, and meeting data

SSO Impersonation

Lateral movement across all M365 services

By The Numbers

EvilTokens campaign scope as of March 2026

340+

Microsoft 365 orgs compromised

1,000+

Domains hosting EvilTokens pages

90 days

Refresh token lifetime (attacker persistence)

Feb 2026

EvilTokens PhaaS launched

Most Targeted Roles & Sectors:

Finance & HR

Invoice approvals, payroll changes

Logistics & Sales

Shipping notices, purchase orders

Construction

Fake bid solicitations

Healthcare & Legal

Sensitive document lures

What The Lures Look Like

Phishing emails and documents your users will see

DocuSign / Adobe Sign

"Please review and sign this document." Displays a verification code and a "Continue to Microsoft" button.

Shared OneDrive File

"Someone shared a file with you." Opens a fake SharePoint page with the device code pre-filled.

Voicemail / eFax

"You have a new voicemail from +1 (555)..." Links to a page that requires Microsoft sign-in to listen.

Payroll / Invoice

"Action required: Review your updated pay stub." Urgent tone targets finance and HR teams.

Password Expiry

"Your password will expire in 24 hours." Creates urgency to click and "verify" via device code.

Calendar Invite / QR

Meeting invite or QR code that redirects to the Microsoft device login page.

All lures direct users to the REAL microsoft.com/devicelogin — that's what makes them so effective.

Defense: Admin Actions

What IT needs to do right now in Entra ID

Block Device Code Flow

Create a Conditional Access policy:
Conditions > Authentication Flows > Device Code Flow > Block Access. Apply to All Users. Exclude break-glass accounts only.
Use Report-Only mode first, then enforce.

Monitor Sign-In Logs

Filter Entra sign-in logs by Authentication Protocol = "Device Code."
Look for device code flow from unexpected IPs or locations.
KQL: SigninLogs | where AuthenticationProtocol == "deviceCode"

Revoke Tokens Immediately

If compromised: Revoke all refresh tokens for the user in Entra.
Password reset alone is NOT enough — refresh tokens survive resets.
Also check for newly registered devices under the user's account.

Require Compliant Devices

Use Conditional Access to require Intune-compliant or Entra-joined devices for access. This prevents token use from unmanaged machines.
Especially important for your CJIS-scoped tenants.

CJIS Note: For law enforcement tenants, blocking device code flow aligns with CJIS Security Policy 5.6.2.2 — verify audit logging is capturing these events.

What To Tell Your Users

Training points for end-user awareness

1

Never enter a code you didn't generate

If someone emails or messages you a code and tells you to go to microsoft.com/devicelogin, stop. You should only use that page for devices YOU are setting up, like a conference room TV or printer.

2

"Real Microsoft page" doesn't mean safe

The whole point of this attack is that the login page IS real. The danger is in WHY you're there. If you didn't initiate a device setup, don't enter any code — even on a legitimate Microsoft page.

3

Be suspicious of urgency + codes

Lures use time pressure: "Sign your document now," "Verify your password before it expires." If an email gives you a code AND creates urgency, that's the red flag.

4

When in doubt, call IT

If you get a request that involves entering a code at microsoft.com/devicelogin and you didn't initiate it yourself, contact your helpdesk immediately. Don't approve, don't enter the code.

Key Takeaways

- EvilTokens uses REAL Microsoft pages — old "check the URL" training won't save you.
- MFA is still important, but it does NOT stop this attack. The victim completes MFA themselves.
- The attacker gets a 90-day refresh token that survives password resets.
- Block device code flow in Conditional Access for all users who don't need it.
- Monitor Entra sign-in logs for device code flow authentications from unknown locations.
- Train users: never enter a code at microsoft.com/devicelogin unless they initiated the device setup.