

Device Code Attacks end at the browser.

A fake meeting invite, a real Microsoft sign-in page and a code the victim types in themselves: that is all it takes to hand an attacker a signed-in Microsoft 365 session, with no password stolen and the victim's own MFA satisfied. Cybereinforce blocks that sign-in step in the browser, by default, for every organisation on every plan.

Every plan

on by default from day one,
nothing to configure

0 rules

used from your rule allowance;
applied by the platform

Any lure

email, Teams, SMS, QR code or
phone call

Every block

logged with its reason and visible
to your SOC

HOW A DEVICE CODE ATTACK HAPPENS

1

The lure

A meeting invitation, a shared document or a security review arrives with a short code and an instruction to "confirm your device".

2

The real Microsoft page

The victim opens Microsoft's own device sign-in page and types the code. The address bar is genuine. **This is the step Cybereinforce stops.**

3

The attacker is signed in

The code was the attacker's. When the victim approves MFA, Microsoft issues the session tokens to the attacker.

4

Quiet persistence

The attacker reads mail, Teams and SharePoint, and can register their own device so later activity looks trusted.

Why a SOC rarely sees it in time

Everything in the sign-in logs looks right, which is exactly what makes analysts trust it.

Domain	login.microsoftonline.com
MFA	satisfied
Device ID / name	present
Device trust type	Azure AD registered

No malware, no attachment and no look-alike domain to find. By the time it is understood, the attacker may have been reading mail for days. (Illustrative values.)

The Cybereinforce answer: stop the sign-in step

- ✓ **Lure-proof.** Lures change every day; the device-code sign-in page does not. However the victim reaches it, the browser stops there.
- ✓ **Managed centrally.** A platform protection, not a rule anyone can delete by accident.
- ✓ **Look-alike sign-in pages.** Copies of the device login on other domains are caught by our look-alike and lure detections, new domains included.
- ✓ **Your call.** Organisations that rely on legitimate device-code sign-ins can permit them for themselves through the Whitelist.

For the CISO

One of the most effective Microsoft 365 takeover techniques is closed in every protected browser, with nothing for users to learn.

For the SOC

A lure that reached your staff becomes a visible, investigable block event, in the console and in Microsoft Sentinel.

For IT

No conditional-access project and no rule to maintain. It arrives with the extension and stays current.

Close the door on Device Code Attacks.

Start a trial and open the device-code sign-in page yourself: you will see the block page instead.

[Start free trial →](#)