ANOTHER
MANAGED IT SERVICES

WHITEPAPER

Hook, Line and Sinker:

How Modern Phishing Bypasses Microsoft 365 Security and How to Stop It

May 2026

Executive Summary

Modern phishing attacks have evolved beyond simply stealing passwords. Attackers now focus on capturing authenticated user sessions and abusing legitimate Microsoft authentication features to gain access to Microsoft 365 accounts without directly needing user credentials.

A session is the trusted connection created after a successful sign-in. Once authenticated, Microsoft issues a session token — a piece of code that keeps the user signed in without repeatedly requesting a password or multi-factor authentication (MFA). If an attacker steals this token, they can often access the account as though they were the legitimate user.

Two techniques increasingly seen in real-world attacks are Adversary-in-the-Middle (AiTM) phishing and device code abuse.

AiTM phishing uses convincing fake Microsoft login pages placed between the user and the real Microsoft sign-in service. The user signs in and completes MFA normally, but the attacker captures the authenticated session after login, allowing continued access even if the password is later changed.

Device code attacks abuse a legitimate Microsoft authentication feature designed for devices with limited input capability, such as smart TVs or conference room systems. Victims are prompted to enter a verification code into a genuine Microsoft login page, unknowingly approving an authentication request initiated by the attacker.

Both methods are difficult to detect because they operate within trusted Microsoft authentication workflows rather than exploiting vulnerabilities or guessing passwords. As a result, traditional password-focused security controls are less effective.

Reducing risk requires stronger control over authentication behaviour and session trust. Recommended protections include restricting unused authentication methods, enforcing phishing-resistant MFA, limiting access to managed or compliant devices, and monitoring sign-in and application consent activity for unusual behaviour.

These attack techniques highlight a significant shift in identity security. Protecting passwords alone is no longer sufficient; organisations must also secure and monitor authenticated sessions after login.

Adversary-in-the-Middle (AiTM) Attacks

Adversary-in-the-Middle (AiTM) attacks are a modern form of phishing designed to bypass multi-factor authentication (MFA).

Instead of just stealing usernames and passwords, attackers place a fake login page between the user and the real Microsoft sign-in system. When the user logs in, their details and MFA approval are passed through to Microsoft in real time, making the process look completely normal.

Once authentication is completed, Microsoft issues a session cookie, which acts like a "logged-in pass." The attacker captures this cookie and can then reuse it to access the account without needing the password or MFA again.

With this stolen session, attackers can impersonate the user inside Microsoft 365, access emails and files, and potentially carry out further actions such as data theft, setting up mailbox rules, or maintaining ongoing access to the account.

Device Code Flow Attacks

As phishing defences have improved, attackers have adapted by moving away from fake login pages toward abusing legitimate Microsoft authentication features.

Traditional AiTM attacks can sometimes be detected because they rely on spoofed Microsoft 365 login pages, which may show suspicious domains or unusual behaviour – Microsoft uses consistent login domains.

To avoid this weakness, attackers increasingly use device code authentication, a real Microsoft feature designed for devices like smart TVs or IoT systems that cannot easily enter passwords or MFA codes. In normal use, a user is given a code on one device and enters it on another trusted device to sign in.

In a phishing scenario, the attacker generates a valid device code and tricks the victim into entering it on an official Microsoft login page. This causes Microsoft to issue a legitimate authenticated session to the attacker.

Because the process uses genuine Microsoft infrastructure and real authentication flows, it is harder to detect than fake login pages. Victims are often unaware they are approving access, especially since the code is presented simply as an "authentication code", without clear context about what it authorises.

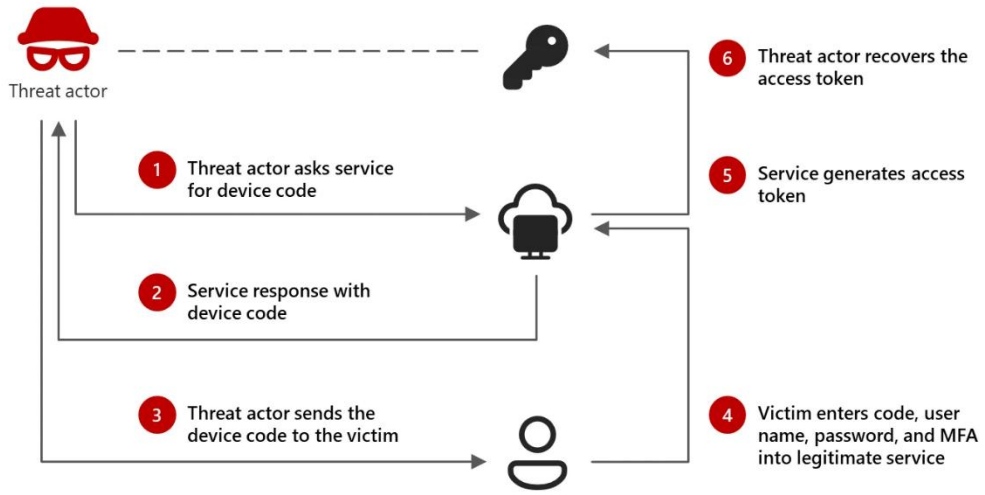
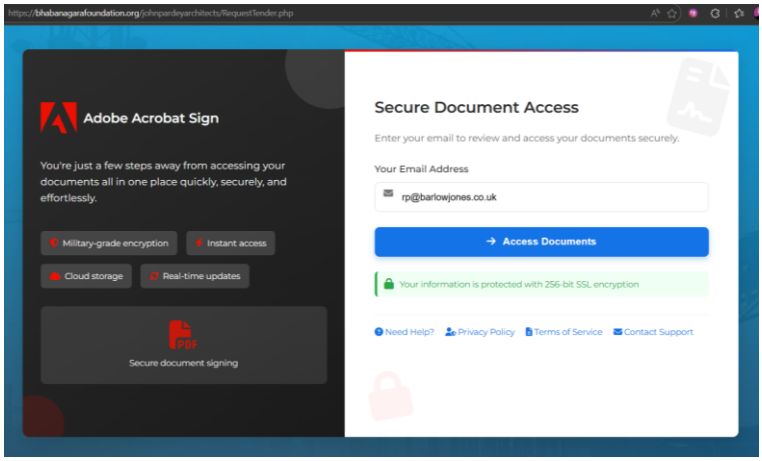


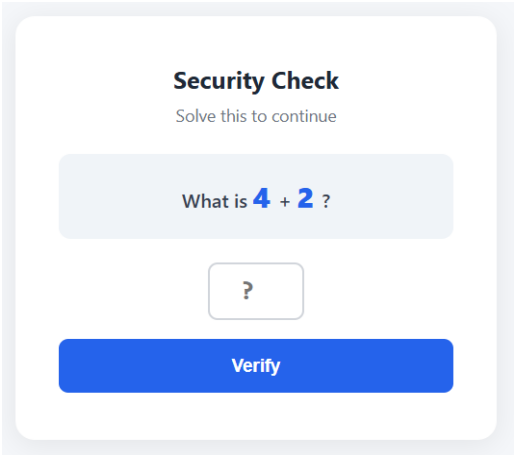
Figure 1 - Device code phishing attack cycle (Source: Microsoft)

How Device Code Flow Attacks Work

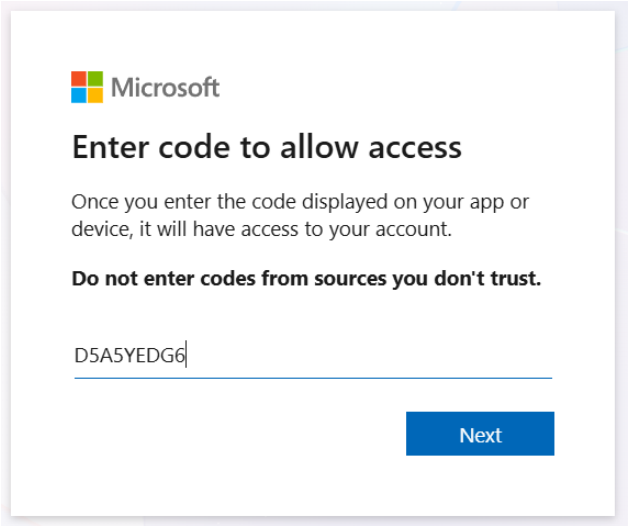
In a typical attack flow, the victim is first directed to a convincing attacker-controlled page after clicking a link in a phishing email. Common lure content includes requests to review shared documents or project updates.

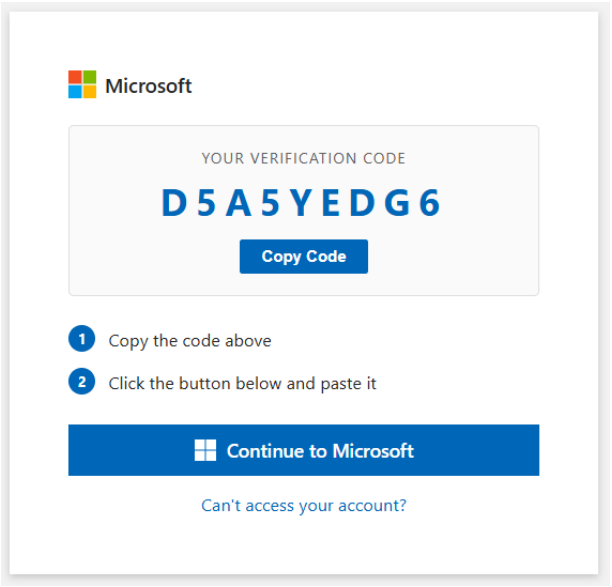
Before presenting the device code, the attacker may request the victim's email address and require completion of a simple CAPTCHA-style challenge. This step is not part of the authentication process but is used to filter out automated security scanners and reduce detection by phishing analysis tools.





Once validated, the attacker displays a device code that has been generated from a legitimate Microsoft authentication request. The victim is instructed to enter this code into a Microsoft login page, which appears genuine and includes Microsoft branding and standard authentication prompts.





After the code is submitted, Microsoft completes the authentication process and issues an authenticated session to the attacker's device. From this point, the attacker can access the victim's Microsoft 365 data using standard session-based access without requiring further credentials or interaction from the victim.

How To Stop Modern Phishing Attacks

Preventing AiTM and device code phishing attacks requires a combination of user awareness and technical controls working together. From a human perspective, users need to understand that unexpected login prompts, approval requests, or authentication codes should always be treated with caution. They should never enter a device code unless they have intentionally initiated a sign-in process themselves. Most successful attacks rely on urgency and confusion, so encouraging staff to pause and report anything unusual remains one of the most effective defences.

However, as attackers increasingly use AI to create more convincing phishing emails, it is becoming harder for users to reliably spot these threats on their own. This makes technical controls essential to reduce the likelihood of compromise.

Organisations using Microsoft 365 can significantly improve their security posture by moving to Microsoft 365 Business Premium, which includes Entra ID P1 and enables Conditional Access policies beyond the basic security controls found in lower-tier plans. Conditional Access allows administrators to define how and where users can sign in, such as restricting access from unfamiliar locations, requiring stronger authentication for risky sign-ins, or blocking access from unmanaged devices. It also allows organisations to disable high-risk authentication methods such as device code flow entirely. This reduces the value of stolen sessions and limits unauthorised access attempts.

Alongside this, browser-based security tools and endpoint protection can help detect and block fake Microsoft login pages before users interact with them. Email security solutions are also increasingly using AI-driven detection and behavioural analysis to identify and block phishing attempts before they reach the user.

While these attacks are designed to bypass MFA, enforcing phishing-resistant authentication is still critical in preventing other attacks that exploit weaker methods. Authentication apps and hardware security keys are now recommended by the UK's National Cyber Security Centre, rather than legacy methods such as SMS.

Conclusion

AiTM and device code phishing attacks are effective because they exploit trust in legitimate Microsoft sign-in processes rather than obvious fake websites. As a result, traditional email filtering and password policies alone are not enough to protect accounts. A layered approach that combines user awareness, Conditional Access controls, and targeted restrictions on authentication methods is now essential to reduce risk.

If you want to strengthen your organisation's Microsoft 365 security posture and reduce the risk of account compromise, contact ANother IT to discuss upgrading your security and your business.