

What is device code phishing, and why are Russian spies so successful at it?

Researchers have uncovered a sustained and ongoing campaign by Russian spies that uses a clever phishing technique to hijack Microsoft 365 accounts belonging to a wide range of targets, researchers warned.

The technique is known as device code phishing. It exploits “device code flow,” a form of authentication formalized in the industry-wide OAuth standard. Authentication through device code flow is designed for logging printers, smart TVs, and similar devices into accounts. These devices typically don’t support browsers, making it difficult to sign in using more standard forms of authentication, such as entering user names, passwords, and two-factor mechanisms.

Rather than authenticating the user directly, the input-constrained device displays an alphabetic or alphanumeric device code along with a link associated with the user account. The user opens the link on a computer or other device that’s easier to sign in with and enters the code. The remote server then sends a token to the input-constrained device that logs it into the account.

Device authorization relies on two paths: one from an app or code running on the input-constrained device seeking permission to log in and the other from the browser of the device the user normally uses for signing in.

A concerted effort

Advisories from both security firm Volexity and Microsoft are warning that threat actors working on behalf of the Russian government have been abusing this flow since at least last August to take over Microsoft 365 accounts. The threat actors masquerade as trusted, high-ranking officials and initiate conversations with a targeted user on a messenger app such as Signal, WhatsApp, and Microsoft Teams. Organizations impersonated include:

<https://arstechnica.com/information-technology/2025/02/russian-spies-use-device-code-phishing-to-hijack-microsoft-accounts/>