SECURITY INSIGHTS:

The Device Code Phishing

Genady Vishnevetsky, Chief Info Security Officer, Stewart Title Guaranty Company

Device code phishing has emerged as a concerning tactic that exploits users' familiarity with authentication processes, often leading them to unknowingly enter valid device codes and link a hacker's device to their accounts.

Device codes, which are alphanumeric or numeric, authenticate accounts on devices lacking standard login interfaces, such as IoT gadgets like Roku or Apple TV, as well as streaming apps like Netflix or Hulu, and various cloud applications. This method ensures that authentication is specific to a particular device by presenting a code for the user to enter on a computer, eliminating the need for text input.

Threat actors can take advantage of applications or services by generating a device code on their own devices. They deceive victims into inputting this compromised device code on the legitimate authentication page of the service. Once a victim navigates to the authentication page and enters the code, they must verify their identity using their credentials and multifactor authentication (MFA). If successful, the service provider issues an access token. However, an attacker can steal these tokens, granting them unauthorized access to the victim's account and allowing them to move laterally to other linked services without requiring a password.

This type of deception frequently manifests through emails that seem to be from IT support, invitations for Microsoft Teams meetings, or other communications labeled as "urgent." Such tactics aim to manipulate users into providing unauthorized access to their accounts.

Device code phishing is particularly troubling because it does not rely on malicious links or attachments. Instead, victims are lured into entering their device codes and login credentials on what appears to be a legitimate authentication page, making the attack more difficult to detect. This method exploits user habits, as many individuals are accustomed to authentication prompts from collaboration tools like Microsoft Teams. Consequently, they are less likely to question these requests, which significantly heightens the chances of a successful attack.

TAKEAWAYS:

- **Never enter codes you didn't ask for. I**f a site or message gives you a code, but you weren't trying to log in, ignore it. Don't go to the website or enter the code.
- **Use two-factor authentication.** This adds an extra layer of protection. Even if someone tries to log in, they'll still need a second code (usually sent to your phone).
- **Be skeptical of login prompts.** If you get a message urging you to "verify your account" or "reconnect your service," slow down. Double-check that it came from a trusted source.