Scam-as-a-Service

CASE STUDY: Kali365 takes your tokens

In May 2026, the United States Federal Bureau of Investigation issued a warning. Hackers are making use of a new and dangerous tool: Kali365, a phishing-as-a-service platform that can bypass multi-factor authentication.

Phishing-as-a-service tools like Kali365 are available in back channels like Telegram and on the dark web, ready for purchase and use by anyone. But Kali365 stands out because of its ability to gain persistent access: not only bypassing MFA but maintaining the attacker's connection to your Microsoft 365 account.

Here's how it works. First, the hacker sends you a lure: a phishing email impersonating a specific service, usually something common and work-related, and giving specific instructions. "A document has been shared with you. Go to the verification page and enter this code to view it."

The key is the code that the hacker supplies. The code actually gives the hacker the authorization to access the victim's account. Essentially, the victim is tricked into telling the system, "They're with me. They can come in." And once they're in, the hacker copies the victim's OAuth access and refresh tokens, allowing them to maintain their access.

Now the hacker can access and exploit everything connected to the victim's Microsoft account: email, Teams and more. And from there, the hacker is able to expand their access and compromise more victims.

For the individual employee, the best defense is alertness. Don't trust unexpected document shares or emails instructing you to enter codes that you didn't anticipate. If you suspect phishing, report it!

Phishing Software for Sale

Kali365 isn't the only prebuilt hacking tool or service available. Let's look at some others.

- **Outsider Enterprise**: fake sites and brand impersonation; shutdown announced in June 2026 after about $1.9B in losses.
- **SniperDZ**: phishing domains, templates and affiliate tutorials; busted by Interpol in February 2026.
- **BlueKit**: credential harvesting, session hijacking and 7- to 30-day subscription tiers. Currently active.

What is a login token?

A login token is a cryptographically protected string that acts as a digital access ticket to a system. When you enter your credentials, the server sends the token to your device, allowing your device to stay authorized for about 60 to 90 minutes. Some, like refresh tokens, can keep your session going for days or weeks. However, most users don't realize tokens exist … Which makes token-stealing tools like Kali365 more of a danger.

1. https://www.ic3.gov/PSA/2026/PSA260521 2. https://learn.microsoft.com/en-us/entra/identity-platform/security-tokens