Fake OpenAI, SpaceX and Anthropic event invitations used to steal Microsoft and Google logins



Attackers are sending fake event invitations that use the names of OpenAI, SpaceX and Anthropic to lure employees. Two phishing-as-a-service platforms are used to capture Microsoft and Google credentials and authentication sessions.

- Fake event invitations branded as OpenAI, SpaceX and Anthropic are targeting employees.
- Two different phishing-as-a-service platforms are behind the campaigns.
- The goal is to steal Microsoft and Google account credentials.
- Authentication sessions are also targeted, not only passwords.
- Well-known technology brands are being used as the lure.

What was reported

According to BleepingComputer, attackers are sending invitations to supposed events linked to OpenAI, SpaceX and Anthropic in order to draw employees into phishing attacks. The campaigns rely on two different phishing-as-a-service platforms, which give attackers ready-made infrastructure for this type of fraud.

The objective is to steal Microsoft and Google account credentials as well as authentication sessions. Targeting sessions matters because a stolen session can give access to an account even when the password alone would not be enough.

Why it matters

The lure is an invitation from a prominent technology brand, which is the kind of message staff may be curious about and open during working hours. Corporate Microsoft and Google accounts typically give access to email, documents and other business services, so a single compromised account can have wide consequences for a regulated institution.

The source excerpt does not provide further detail on the scale of the campaigns, the victims or the specific platforms, so organisations should treat this as an indicator of current attacker technique rather than a confirmed threat to any one sector.

What to do next

The practical response is a combination of user awareness, stronger sign-in controls and readiness to respond quickly if an account is suspected to be exposed. The actions below are a sensible starting point.

What to do now

1. Alert staff that unsolicited invitations to events from well-known technology firms may be phishing, and ask them to report rather than click.
2. Review Microsoft and Google sign-in protections, favouring phishing-resistant multi-factor authentication where available.
3. Confirm you can quickly revoke active sessions and reset credentials for a suspected compromised account.
4. Monitor for unusual sign-in activity and new session or token use on Microsoft and Google accounts.
5. Add event-invitation lures to your next phishing awareness exercise.