Meta Security Breach: AI Chatbot Bug Exposes 20,225 Instagram Accounts to Hackers, Says Report

latestly.com/technology/meta-security-breach-ai-chatbot-bug-exposes-20225-instagram-accounts-to-hackers-says-report-7464750.html

Technology Desk June 8, 2026

Technology

Meta has confirmed a significant security flaw in its AI-powered High Touch Support (HTS) chatbot, leading to the hijacking of 20,225 Instagram accounts. Discovered on May 31, 2026, the bug allowed hackers to bypass email verification for password resets, enabling account takeovers. Exploitation began as early as April 17, 2026, exposing sensitive user data.

By Technology Desk | Published: Jun 08, 2026 08:48 PM IST

Instagram (Photo Credits: Wikimedia Commons)

Mumbai: A significant security lapse at Meta has exposed 20,225 Instagram accounts to hackers, the company confirmed today in a notice filed with the state of Maine. The breach was attributed to a critical bug within Meta's AI-assisted account recovery system, specifically its High Touch Support (HTS) tool, which attackers exploited to gain unauthorized access.

The vulnerability, which Meta says it discovered on May 31, 2026, allowed malicious actors to trick the AI chatbot into sending password reset links to email addresses controlled by the hackers, rather than the legitimate account owners. This exploit circumvented Meta's standard email verification protocols, enabling takeovers even without direct access to the victim's registered email. Reports indicate that the systematic exploitation of this flaw might have commenced as early as April 17, 2026. **Bluesky Attie, Mastodon Lead Next-Gen Social Apps Beyond Instagram: Report.**

How the Exploit Worked

The attack method was surprisingly straightforward. Hackers would initiate an account recovery process for a target Instagram account and then engage with the Meta AI-powered HTS tool. By manipulating the chatbot, they could persuade it to associate a new, attacker-controlled email address with the victim's account. Subsequently, the AI would issue a password reset link to this newly linked email, granting the hackers full control.

In some instances, attackers reportedly used Virtual Private Networks (VPNs) to spoof the victim's geographic location, further aiding in bypassing Meta's automated security safeguards which often use location as an authorization signal. While two-factor authentication (2FA) was generally effective in preventing many such takeovers, some users without 2FA were particularly vulnerable, and some users with 2FA still reported being compromised, highlighting the severity of the underlying bug.

Meta's Response and Impacted Data

Following the discovery of the bug, Meta swiftly acted to mitigate the threat. The company disabled the vulnerable High Touch Support (HTS) tool and reset passwords for all affected Instagram profiles. Additionally, all compromised accounts were enrolled in a mandatory security checkpoint, requiring users to re-authenticate through secure, verified channels to regain access. Meta has also initiated a comprehensive review of similar account recovery flows across its other platforms to prevent future occurrences.

The full extent of information accessed by the hackers remains uncertain, but Meta has indicated that compromised accounts may have exposed a wide range of personal data. This includes contact information such as email addresses and phone numbers, dates of birth, profile details (biography, profile photo), social media posts (photos, videos, Stories), direct messages, account activity records, and information about linked services. **Lewis Hamilton and Kim Kardashian Send Social Media into Frenzy After Monaco GP Kiss Goes Viral (Watch Video).**

Several high-profile Instagram accounts were reportedly targeted during the campaign, including those associated with Barack Obama's White House, beauty retailer Sephora, US Space Force Chief Master Sergeant John Bentivegna, and cybersecurity researcher Jane Manchun Wong, among others. This incident underscores the growing risks associated with integrating AI into critical security and support functions, prompting renewed calls for robust AI oversight and verification mechanisms within digital platforms.

Disclaimer: *AI tools assisted in compiling the foundational data and research for this report. The final content was reviewed, edited and verified by human editors at LatestLY.*

TruLY Score by LatestLY

TruLY Score 3 – Believable; Needs Further Research | On a Trust Scale of 0-5 this article has scored 3 on LatestLY, this article appears believable but may need additional verification. It is based on reporting from news websites or verified journalists (The Verge), but lacks supporting official confirmation. Readers are advised to treat the information as credible but continue to follow up for updates or confirmations

(The above story first appeared on LatestLY on Jun 08, 2026 08:48 PM IST. For more news and updates on politics, world, sports, entertainment and lifestyle, log on to our website latestly.com).