

Forum:[Hack Forums](#)

Thread: [Instagram Data Breach](#)

SocialSolutions - March 6, 2026, 8:28 am

Reports surfaced on January 10, 2026, confirming that a significant database containing user information is circulating on dark web forums. Security researchers, including teams from Malwarebytes, identified a threat actor known as "Solonik" as the source of the leak on BreachForums. While social media is currently flooded with panic regarding "hacked" accounts, the situation is technically a data scrape rather than a system-wide breach.

What actually happened

The leaked database contains the personal information of approximately 17.5 million Instagram users. Although the data appeared publicly this week, forensic analysis suggests the information was likely collected - or "scraped" - from Instagram's servers throughout 2024.

Scraping usually happens when bad actors exploit a loophole in an API (the software that allows apps to talk to each other) to pull public data in bulk. Meta has denied that their internal passwords or systems were compromised, stating that the data was collected from publicly viewable fields.

The password reset storm

The most visible symptom of this leak for the average user is a sudden flood of password reset emails. Since the leaked database includes millions of valid email addresses, hackers are using automated bots to spam the "Forgot Password" function.

This creates a chaotic situation where you might wake up to a dozen legitimate emails from security@mail.instagram.com. The attackers are banking on two outcomes:

You panic and click a fake link sent in a follow-up phishing email that looks like it came from Instagram.

You get annoyed by the notifications and accidentally approve a login request.

If you are receiving these emails but cannot find any successful login attempts in your activity log, your account has likely not been breached. The hackers are simply knocking on the door because they know the address.

What data was compromised

While passwords were not included in the Solonik dump, the leak exposes specific personal identifiers that can be used for targeted social engineering or identity fraud.

The compromised data fields include:

Email addresses and phone numbers.

Instagram usernames and real names.

Profile bio descriptions.

Partial physical addresses (primarily for business or creator accounts).

Steps to secure your account

The primary risk right now is not a direct login by a hacker, but rather you falling for a scam that utilizes this leaked info. You need to close the avenues that allow attackers to use this data against you.

Switch to an authentication app Because phone numbers were part of this leak, SMS-based two-factor authentication is less secure. Attackers can potentially swap SIM cards or intercept texts. Go to your settings and enable an authenticator app like Google Authenticator or Duo. This ensures that even if someone has your password and phone number, they cannot generate the login code.

Verify official communication Scammers will send fake emails pretending to be Instagram support, claiming your account is at risk of deletion due to this leak. Instagram has a built-in log of every real email they send you. You can find this in the app under Settings > Security > Emails from Instagram. If the email you received does not appear in that internal list, it is a phishing attempt.

Check connected apps Since this data was scraped via API abuse, it is possible the leak originated through a third-party service, such as those apps that track follower counts or analyze engagement. Revoke access to any third-party app you do not recognize or actively use in the "Website Permissions" section of your settings.

Ignore the reset emails If you receive a password reset link you did not request, do not click it. If you are concerned about your account security, navigate to the Instagram app or website independently to change your credentials. Never follow a link delivered to your inbox during a security event like this.

andrew11 - August 17, 2026, 9:25 am

This is a fake news. kindly ignore this