X (FORMERLY KNOWN AS TWITTER) SOCIAL MEDIA BREACH 2025

"LARGEST SOCIAL MEDIA BREACH EVER"

BLUF

On March 31, 2025, the social media platform X (formerly Twitter) was hacked, with the breach traced back to January 2025. The hacker, ThinkingOne, combined data from this hack with information from a 2022 breach and distributed over 34 gigabytes of stolen data for free via an online forum. The compromised data included sensitive user details such as names, emails, locations, screen names, and account activity for around 200 million users, affecting high-profile public figures and regular users alike. While the breach is suspected to have been carried out by an insider with internal access, X has not confirmed the hacker's identity, and investigations are ongoing. The leaked information raises significant security concerns, particularly around phishing and social engineering attacks, as well as the potential for privacy violations. In response, X has acknowledged the breach, is strengthening security measures, and advises users to update passwords, enable two-factor authentication, and be cautious of phishing attempts.

WHAT

What Occurred: On March 31, 2025, the social media platform, X (formerly Twitter), was the victim of a data hack, which has subsequently been identified as having been conducted initially in January 2025. Open source reporting identifies a 'data enthusiast', who goes by the hacker name 'ThinkingOne', combined the data from a previous data hack occurring in January 2022, and distributed it for free via an unidentified data breach forum. ThinkingOne identified their decision to distribute the X user data for free after being unsuccessful in their attempts to contact X to return the data as part of their platform 'bug' vulnerability bounty program.

What Data Was Taken: The following stolen user data, totaling more than 34 gigabytes in size, has been identified as being leaked between the combined 2022 / 2025 X data hack:

- **Name**
- **Screen name**
- **Email**
- **Followers**
- **Date of creation (of the account)**
- **ID**
- **Location**
- **Location Description**
- **URL**
- **Time Zone**
- **Language**
- **Followers Count**
- **Friends Count Listed Count**
- **Favorites Count**
- **Statuses Count**
- **Protected**
- **Verified**
- **Default Profile**
- **Default Profile Image**
- **Last Status Create At**
- **Last Status Source**
- **Created At**

What is Being Done: X has acknowledged the 2025 data hack and is investigating with law enforcement. While only publicly available data was affected, privacy concerns remain. X is enhancing security measures, including data protection and encryption, and advising users to review security settings, watch for phishing, and enable two-factor authentication. The investigation continues, with uncertainties about further data exposure or leaks.

WHAT SHOULD USERS DO GOING FORWARD

After the 2025 X data hack, users should take several proactive steps to safeguard their information:

1. **Change Passwords:** Users should immediately update their X account passwords, ensuring they are strong and unique, ideally using a password manager to manage credentials securely.
2. **Enable Two-Factor Authentication (2FA):** Turning on 2FA adds an extra layer of security, requiring a secondary verification method (like a code sent to your phone) to log in.
3. **Be Cautious of Phishing Attempts:** With exposed email addresses, users should be wary of unsolicited emails or direct messages asking for personal information or login credentials.
4. **Review Account Permissions:** Users should review and limit third-party applications connected to their X accounts to minimize the risk of further data exposure.
5. **Monitor Accounts for Suspicious Activity:** Regularly check for unfamiliar logins or posts, and report any suspicious activity to X's support team for investigation.

WHO

Who Was Impacted: The 2025 X data hack impacted **around 200 million users of the social media platform X.** High-profile public figures, celebrities, and everyday users alike were among those whose data was compromised. This hack also raised concerns about the security of millions of accounts, as sensitive information could be exploited by hackers for malicious purposes.

Who Was Responsible: The 2025 X data hack is **suspected to have been perpetrated by an insider, possibly an employee of X.** The hacker, ThinkingOne, asserted that accurately enumerating all Twitter user IDs would be challenging without internal access, suggesting an insider's involvement. **However, X has not officially confirmed the breach's origin or the identity of those responsible, and investigations are ongoing.**

HOW

How Can The Data Be Used: The leaked information poses substantial risks, including increased susceptibility to phishing attacks and social engineering schemes. Attackers could utilize the data to craft convincing fraudulent communications, deceiving users into divulging sensitive information or engaging in harmful actions.

WHY

Why There Should Be Concern: The 2025 X data hack exposed sensitive information from 200 million accounts, including **emails, locations, and user activity**. This increases risks of p**hishing, social engineering, and privacy violations.** Hackers could exploit the data to manipulate users or track their behavior. The breach also **threatens trust in X** and raises concerns about the platform's data security.

SOURCES

- https://www.forbes.com/sites/daveywinder/2025/04/01/hacker-claims-to-have-leaked-200-million-x-user-data-records-for-free/
- https://www.safetydetectives.com/news/x200m-leak-report/
- https://www.dailydot.com/debug/x-data-leak-201-million-users/
- https://mashable.com/article/x-breach-data-leak-what-can-hackers-do?
- https://www.windowscentral.com/software-apps/twitter/elon-musks-x-might-have-a-mole-problem