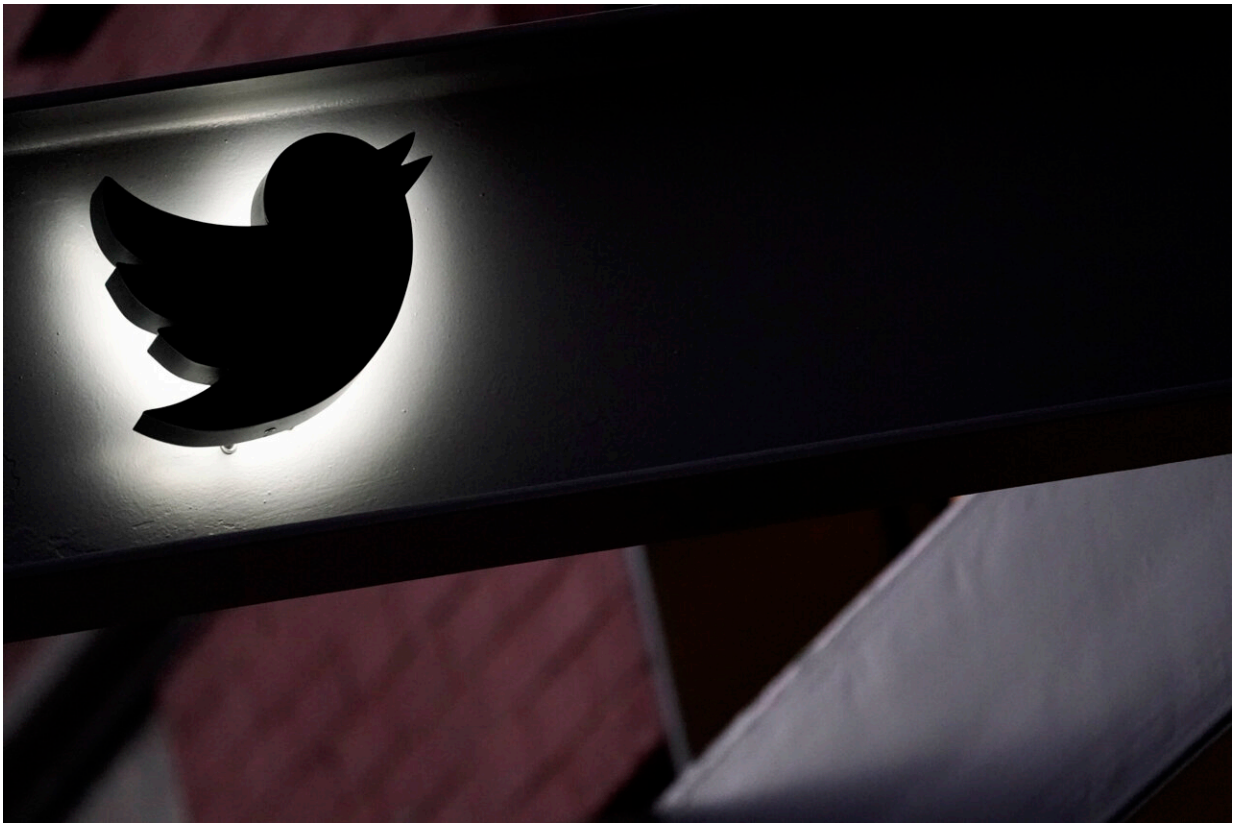
Twitter leak exposes 235 million email addresses from hack

January 6 2023, by Barbara Ortutay



The Twitter logo is seen on the awning of the building that houses the Twitter office in New York, Wednesday, Oct. 26, 2022. Personal emails linked to 235 million Twitter accounts hacked some time ago have been exposed according to Israeli security researcher Alon Gal, Friday, Jan. 6, 2023. Credit: AP Photo/Mary Altaffer, File

Personal emails linked to 235 million Twitter accounts hacked some time ago have been exposed according to Israeli security researcher Alon Gal—making millions vulnerable to having their accounts compromised or identities exposed if they have used the site anonymously to criticize oppressive governments, for instance.

Gal, who is the co-founder and chief technology officer at cybersecurity firm Hudson Rock, wrote in a LinkedIn post this week that the leak "will unfortunately lead to a lot of hacking, targeted phishing, and doxxing."

While account passwords were not leaked, malicious hackers could use the email addresses to try to reset people's passwords, or guess them if they are commonly used or reused with other accounts. That's especially a risk if if the accounts are not protected by two-factor authentication, which adds a second layer of security to password-protected accounts by having users enter an auto-generated code to log in.

People who use Twitter anonymously should have a Twitter-dedicated email address that does not disclose who they are and is used solely for Twitter, experts say.

Though the hack appears to have taken place before Elon Musk took over Twitter, the news of the leaked emails adds another headache for the billionaire, whose first couple months as head of Twitter have been chaotic, to say the least.

Twitter did not immediately respond to a message for comment on the hack.

News of the breach could put the company in trouble with the Federal Trade Commission. The San Francisco company signed a consent agreement with the agency in 2011 that required it to address serious data-security lapses.

Twitter paid a $150 million penalty last May, several months before Musk's takeover, for violating the consent order. An updated version established new procedures requiring the company to implement an enhanced privacy-protection program as well as beefing up information security.

In November, a group of Democratic lawmakers asked federal regulators to investigate any possible violations by the platform of consumer-protection laws or of its data-security commitments.

The FTC said at the time it is "tracking recent developments at Twitter with deep concern," though no formal investigation has been announced. But experts and current and former Twitter employees have been warning of serious security risks flowing from the drastically reduced staff and deepening disorder within the company.

In August, Twitter's former head of security filed a whistleblower complaint alleging that the company misled regulators about its poor cybersecurity defenses and its negligence in attempting to root out fake accounts that spread disinformation.

Among Peiter Zatko's most serious accusations is that Twitter violated the terms of the 2011 FTC settlement by falsely claiming that it had put stronger measures in place to protect the security and privacy of its users.