

Keeping our users secure

Archived: 2026-04-05 16:46:24 UTC

As you may have read, there's been a recent uptick in large-scale security attacks aimed at U.S. technology and media companies. Within the last two weeks, the [New York Times](#) and [Wall Street Journal](#) have chronicled breaches of their systems, and Apple and Mozilla have turned off Java by default in their browsers.

This week, we detected unusual access patterns that led to us identifying unauthorized access attempts to Twitter user data. We discovered one live attack and were able to shut it down in process moments later. However, our investigation has thus far indicated that the attackers may have had access to limited user information – usernames, email addresses, [session tokens](#) and [encrypted/salted](#) versions of passwords – for approximately 250,000 users.

As a precautionary security measure, we have reset passwords and revoked session tokens for these accounts. If your account was one of them, you will have recently received (or will shortly) an email from us at the address associated with your Twitter account notifying you that you will need to create a new password. Your old password will not work when you try to log in to Twitter.

Though only a very small percentage of our users were potentially affected by this attack, we encourage all users to take this opportunity to ensure that they are following good password hygiene, on Twitter and elsewhere on the Internet. Make sure you use a strong password – at least 10 (but more is better) characters and a mixture of upper- and lowercase letters, numbers, and symbols – that you are not using for any other accounts or sites. Using the same password for multiple online accounts significantly increases your odds of being compromised. If you are not using good password hygiene, take a moment now to [change your Twitter passwords](#). For more information about making your Twitter and other Internet accounts more secure, read our [Help Center documentation](#) or the [FTC's guide on passwords](#).

We also echo the [advisory](#) from the U.S. Department of Homeland Security and security experts to encourage users to disable Java on their computers in their browsers. For instructions on how to disable Java, read [this recent Slate article](#).

This attack was not the work of amateurs, and we do not believe it was an isolated incident. The attackers were extremely sophisticated, and we believe other companies and organizations have also been recently similarly attacked. For that reason we felt that it was important to publicize this attack while we still gather information, and we are helping government and federal law enforcement in their effort to find and prosecute these attackers to make the Internet safer for all users.

Updated 4:47pm: Corrected detail on disabling Java in penultimate paragraph.

Posted by Bob Lord ([@boblord](#))
Director of Information Security

Source: https://blog.twitter.com/official/en_us/a/2013/keeping-our-users-secure.html