INTERNATIONAL

News of :- 22-01-2018 04:36 PM

Less than 10% of Gmail users enable two-factor authentication: Google

San Francisco, Jan 21 (IANS) Despite the growth of sophisticated cyber threats globally, Google has said that less than 10 per cent of active Gmail users have enabled two-factor authentication making the remaining 90 per cent more vulnerable to cyber attacks.

According to Google engineers, compromised passwords are the top way hackers gain access to accounts and all users -- especially those in the enterprises -- should implement two-factor authentication immediately.

"Further, only 12 per cent of Americans use a password manager to protect their accounts," US-based news website Techrepublic quoted Google engineer Grzegorz Milka as saying in a presentation at the Usenix Enigma 2018 security conference in California late on Saturday.

Two-factor authentication is one of the most effective ways to protect online accounts given that compromised passwords are the top way attackers gain access to accounts.

In the enterprise, if a hacker can break into the email of even one employee, it gives them not only access to company data but also ammunition for future phishing attacks -- making it even more important for firms to ensure all employees have enabled two-factor authentication and gone through cybersecurity training.

The feature, which Google calls 2-step verification, requires using a second step-often a single-use key or password-along with the account password to verify a user's identity and allow them into their account.

With Google, the second step can come in the form of a text message, a phone popup, through a Google Authenticator app or from a number of printed single-use codes.

Google first rolled out its two-factor authentication feature back in 2011, yet users have failed to adopt the safety measure in large numbers. The feature adds a few seconds to the login time but is claimed to be the best option to stay away from cyber attacks.

Milka said that Google did not make two-factor authentication mandatory for all users due to usability.

"It's about how many people would we drive out if we force them to use additional security," he was quoted as saying.

Google has made a number of other efforts to improve security for its users.

In January 2017, the company announced new layers of enterprise-grade security controls for "G Suite" to give users more control and visibility over sensitive information.

In October last year, it rolled out the "Advanced Protection Programme" that offers better defenses against phishing, accidental data sharing and fraudulent account access for executives and professionals in fields where confidential information is shared online.
