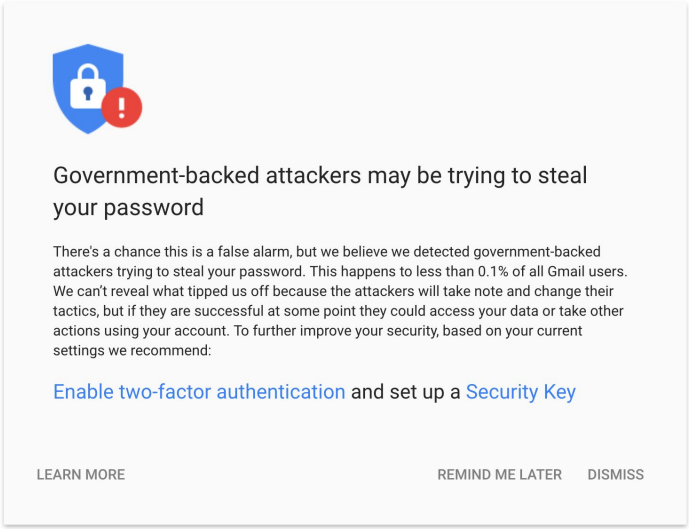
Security and disinformation in the U.S. 2016 election: Steps against phishing and hacking

Criminals and state actors sometimes use “phishing” attacks that trick users into entering account details and passwords into fake pages. These attacks are looking for access to a user’s email, social network, or other online account. As has been reported, government-backed actors attempted spear-phishing attacks—sophisticated efforts to compromise very specific targets—ahead of the 2016 U.S. election.

- Our improving technology tools have let us significantly decrease the volume of phishing emails that get through. With automated protections, account security (like security keys), and specialized attack warnings, Gmail is the most secure email service today: Fighting phishing with smarter protections.

- We recently launched Advanced Protection, offering our strongest security features for users that are at particularly high risk of attack, as well as new protections in Chrome.

- When we detect that a user’s account has been targeted by a government-backed attacker, we show a warning that includes proactive steps they can take to increase their security. The warnings look like this:



- During the 2016 election, we sent thousands of these warnings to users in the U.S., in relation to many government-backed attackers We have sent similar warnings around the time of recent elections in France, Germany, and the Netherlands.

- We will continue to provide more information and specifics to government authorities about phishing and hacking attempts, in accord with our standard protocols for cooperation with law enforcement.

Published October 30, 2017