Ensuring your information is safe online

By Posted by Eric Grosse, Engineering Director, Google Security Team

Published: 2011-06-01 · Archived: 2026-04-06 01:13:32 UTC

The Internet has been an amazing force for good in the world—opening up communications, boosting economic growth and promoting free expression. But like all technologies, it can also be used for bad things. Today, despite the efforts of Internet companies and the security community, identity theft, fraud and the hijacking of people's email accounts are common problems online. Bad actors take advantage of the fact that most people aren't that tech savvy—hijacking accounts by using malware and phishing scams that trick users into sharing their passwords, or by using passwords obtained by hacking other websites. Most account hijackings are not very targeted; they are designed to steal identities, acquire financial data or send spam. But some attacks are targeted at specific individuals. Through the strength of our cloud-based security and abuse detection systems*, we recently uncovered a campaign to collect user passwords, likely through phishing. This campaign, which appears to originate from Jinan, China, affected what seem to be the personal Gmail accounts of hundreds of users including, among others, senior U.S. government officials, Chinese political activists, officials in several Asian countries (predominantly South Korea), military personnel and journalists. The goal of this effort seems to have been to monitor the contents of these users' emails, with the perpetrators apparently using stolen passwords to change peoples' forwarding and delegation settings. (Gmail enables you to forward your emails automatically, as well as grant others access to your account.) Google detected and has disrupted this campaign to take users' passwords and monitor their emails. We have notified victims and secured their accounts. In addition, we have notified relevant government authorities. It's important to stress that our internal systems have not been affected—these account hijackings were not the result of a security problem with Gmail itself. But we believe that being open about these security issues helps users better protect their information online. Here are some ways to improve your security when using Google products:

- Enable 2-step verification. This Gmail feature uses a phone and second password on sign-in, and it protected some accounts from this attack. So check out this video on setting up 2-step verification.

- Use a strong password for Google that you do not use on any other site. Here's a video to help.
- Enter your password only into a proper sign-in prompt on a https://www.google.com domain. We will never ask you to email your password or enter it into a form that appears within an email message. Here's a video with more advice.
- Check your Gmail settings for suspicious forwarding addresses ("Forwarding and POP/IMAP" tab, Fig. 1) or delegated accounts ("Accounts" tab, Fig. 2).

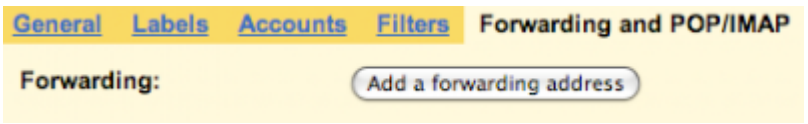

Fig. 1

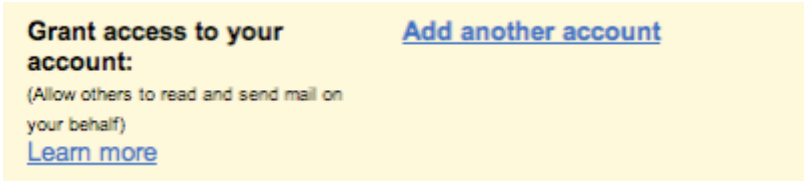

Fig. 2

- Watch for the red warnings about suspicious account activity that may appear on top of your Gmail inbox.
- Review the security features offered by the Chrome browser. If you don't already use Chrome, consider switching your browser to Chrome.
- Explore other security recommendations and a video with tips on how to stay safe across the web.

Please spend ten minutes today taking steps to improve your online security so that you can experience all that the Internet offers—while also protecting your data. *We also relied on user reports and this external report to uncover the campaign described.
