

archive.org

DECLARATION OF MINA CHING

1. I am a Records Request Processor at the Internet Archive. I make this declaration of my own personal knowledge.

2. The Internet Archive is a website that provides access to a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public. The Internet Archive has partnered with and receives support from various institutions, including the Library of Congress.

3. The Internet Archive has created a service known as the Wayback Machine. The Wayback Machine makes it possible to browse more than 450 billion pages stored in the Internet Archive's web archive. Visitors to the Wayback Machine can search archives by URL (i.e., a website address). If archived records for a URL are available, the visitor will be presented with a display of available dates. The visitor may select one of those dates, and begin browsing an archived version of the Web. Links on archived files in the Wayback Machine point to other archived files (whether HTML pages or other file types), if any are found for the URL indicated by a given link. For instance, the Wayback Machine is designed such that when a visitor clicks on a hyperlink on an archived page that points to another URL, the visitor will be served the archived file found for the hyperlink's URL with the closest available date to the initial file containing the hyperlink.

4. The archived data made viewable and browseable by the Wayback Machine is obtained by use of web archiving software that automatically stores copies of files available via the Internet, each file preserved as it existed at a particular point in time.

5. The Internet Archive assigns a URL on its site to the archived files in the format http://web.archive.org/web/[Year in yyyy][Month in mm][Day in dd][Time code in hh:mm:ss]/[Archived URL] aka an "extended URL". Thus, the extended URL http://web.archive.org/web/19970126045828/http://www.archive.org/ would be the URL for the record of the Internet Archive home page HTML file (http://www.archive.org/) archived on January 26, 1997 at 4:58 a.m. and 28 seconds (1997/01/26 at 04:58:28). The date indicated by an extended URL applies to a preserved instance of a file for a given URL, but not necessarily to any other files linked therein. Thus, in the case of a page constituted by a primary HTML file and other separate files (e.g., files with images, audio, multimedia, design elements, or other embedded content) linked within that primary HTML file, the primary HTML file and the other files will each have their own respective extended URLs and may not have been archived on the same dates.



archive.org

6. Attached hereto as Exhibit A are true and accurate copies of browser screenshots of the Internet Archive's records of the archived files for the URLs and the dates specified in the attached coversheet of each screenshot.

7. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

DATE: August 30, 2025

Mina Ching

EXHIBIT A

https://web.archive.org/web/20110210192241/https://googleblog.blogspot.com/2011/02/advanced-sign-in-security-for-your.html

INTERNET ARCHIVE Wayback Machine https://googleblog.blogspot.com/2011/02/advanced-sign-in-security-for-your.html Go JAN FEB MAR 10 2010 2011 2012 662 captures 10 Feb 2011 – 28 About this capture
Share Report Abuse Next Blog» Create Blog Sign In

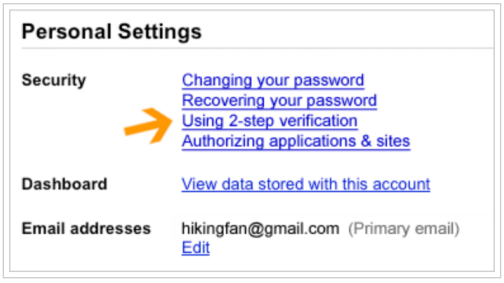
Advanced sign-in security for your Google account

2/10/2011 08:30:00 AM
(Cross-posted on the Gmail Blog)

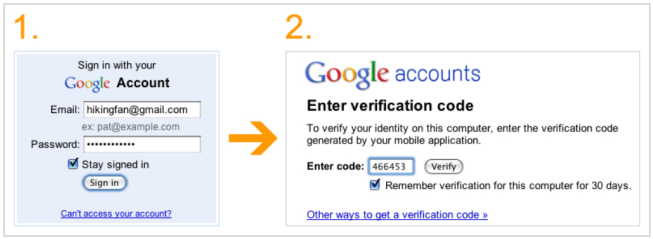
Has anyone you know ever lost control of an email account and inadvertently sent spam—or worse—to their friends and family? There are plenty of examples (like the classic "Mugged in London" scam) that demonstrate why it's important to take steps to help secure your activities online. Your Gmail account, your photos, your private documents—if you reuse the same password on multiple sites and one of those sites gets hacked, or your password is conned out of you directly through a phishing scam, it can be used to access some of your most closely-held information.

Most of us are used to entrusting our information to a password, but we know that some of you are looking for something stronger. As we announced to our Google Apps customers a few months ago, we've developed an advanced opt-in security feature called *2-step verification* that makes your Google Account significantly more secure by helping to verify that you're the real owner of your account. Now it's time to offer the same advanced protection to all of our users.

2-step verification requires two independent factors for authentication, much like you might see on your banking website: your password, plus a code obtained using your phone. Over the next few days, you'll see a new link on your Account Settings page that looks like this:



Take your time to carefully set up 2-step verification—we expect it may take up to 15 minutes to enroll. A user-friendly set-up wizard will guide you through the process, including setting up a backup phone and creating backup codes in case you lose access to your primary phone. Once you enable 2-step verification, you'll see an extra page that prompts you for a code when you sign in to your account. After entering your password, Google will call you with the code, send you an SMS message or give you the choice to generate the code for yourself using a mobile application on your Android, BlackBerry or iPhone device. The choice is up to you. When you enter this code after correctly submitting your password we'll have a pretty good idea that the person signing in is actually you.



It's an extra step, but it's one that significantly improves the security of your Google Account because it requires the powerful combination of both something you *know*—your username and password—and something that only you should *have*—your phone. A hacker would need access to both of these factors to gain access to your account. If you like, you can always choose a "Remember verification for this computer for 30 days" option, and you won't need to re-enter a code for another 30 days. You can also set up one-time *application-specific passwords* to sign in to your account from non-browser based applications that are designed to only ask for a password, and cannot prompt for the code.

To learn more about 2-step verification and get started, visit our Help Center. And for more about staying safe online, see our ongoing security blog series or visit http://www.staysafeonline.org/. Be safe!

Posted by Nishit Shah, Product Manager, Google Security

Permalink

Share:

Labels: apps, security

Search This Blog
Search
powered by Google
Site Feed
Google
534K readers BY FEEDBURNER
Make Google your homepage

Blog Archive
Blog Archive

Labels
accessibility (28)
acquisition (17)
ads (89)
Africa (2)
Android (1)
apps (348)
April 1 (3)
Asia (10)
books + book search (41)
developers (97)
diversity (10)
education (65)
enterprise (73)
Europe (25)
faster web (14)
free expression (44)
gadgets (5)
Geo (79)
Google Apps highlights (26)
Google at 10 (14)
google.org (46)
googlenew (3)
googlers and culture (159)
green (56)
healthcare (21)
India (11)
innovation (14)
Latin America (7)
Mac (2)
measurement (9)
mobile (92)
online safety (13)
open source (10)
personalization (69)
photos (29)
policy and issues (119)
politics (51)
privacy (58)
recipe (8)
recruiting and hiring (30)
research (5)
scholarships (25)
search (390)
search quality (17)
search stories (8)
security (22)
small business (11)
This Week in Search (48)
user experience and usability (34)

Links to this post

Create a Link

Newer Post | Home | Older Post

video (92)
yourgooglestories (5)
youtube highlights (9)

More blogs from Google

Visit our directory for more information about Google blogs.

Follow Google on Twitter

Visit our Twitter directory for more information.

Sign up to get our posts via email. No more than one message per day.

Subscribe

Delivered by FeedBurner

Recent posts from our blogs

Advanced sign-in security for your Google account
Gmail Blog

Poznajcie nowych moderatorów forum Google dla webmasterów
Google Blog-Polska

Beste fremgangsmåter for klikk for å ringe: nyttige tips for optimalisering av mobilkampanjene dine
Inside AdWords - Norge

Finzione e realtà su AdSense. Parte VI: contenuto generato dagli utenti
AdSense Blog-Italiano

More “I do”s, less “to-do”s: wedding planning simplified
The Official Google Blog

We Love Feedback

Do you want to comment on a post? Send us some email.

Google Blog is powered by Blogger. Start your own weblog.

Copyright © 2011 Google Inc. All rights reserved.
Privacy Policy | Terms of Service