“Hey! Who Used My Gmail?!”

Joel Anderson
University Information Security
April 2015
The other day, I spoke on the phone to someone worried about her email account – it seemed clear that it had been borrowed – probably by a phisher.
Which raises the question –

How can you tell if someone else has used (IS using!) your account?

Happily, Gmail gives you a tool to answer that question, the “Last Account Activity” control.
Last account activity

What is ‘Last account activity’?

Last account activity shows you information about recent activity in your mail. Recent activity includes any time that your mail was accessed using a regular web browser, a POP3 client, a mobile device, a third-party application etc. We list the IP address that accessed your mail, the associated location, as well as the time and date.

To see your account activity, click the Details link next to the Last account activity line at the bottom of any Gmail page.

How to understand this data

Access type

If you're concerned about unauthorized access to your mail, you'll be able to use the data in the 'Access type' column to find out if and when someone accessed your mail. For instance, if the column shows any POP access, but you don't use POP to collect your mail, it may be a sign that your account has been compromised.

Location (IP address)

In this column we list the last 10 IP addresses your mail was accessed from, and the associated locations.
Great! Where is it??
Just log into the Gmail Web interface and check “Account Activity”

Down on the bottom right of the screen

Click details
You'll see type of access, IP address (and geographic location*), and when it occurred.

* my caller appeared to be using her account in Maryland... ...when she was in Minnesota?
DON'T miss this - it will let you terminate ALL other sessions, even non-active ones.
One caveat:

Sometimes this activity log can be misleading.

For example, if you access your mail from a cellphone, your “location” may be tied to the location of your wireless provider. It may appear the mail is being accessed from far away when it really IS your access. Check the time and see if it matches a time you were using your account (sometimes you can double check by using your mobile device and then revisiting the activity log to find where the access was seen).
Tampering with your account doesn’t require staying logged into your account!

Wait, what?!
Intruders in your email account may use the “settings” options to change or add filters to your account - deleting official notices or sending copies of mail to their own accounts.

Examine your email account’s settings - click on the “gear” icon in the upper right of your inbox display, and choose “Settings.”
On the “Filters” tab, you can review filters that you (or some intruder) may have set:

Be sure to delete any entry that have been added without your knowledge. You can also review filters by choosing “edit.”
Don’t forget to check “Forwarding” as well. Intruders can add a forward that copies all your mail to some other address - *don’t let them.*

From “Settings” click on the Forwarding tab to review current settings for your account.
So - if someone suspects their account is compromised:

• Go to https://www.umn.edu/myaccount,
• Change your Internet Password
• Go to http://gmail.umn.edu
• Select the Last Account Activity control and
• Click “Sign Out All Other Sessions”

Note: “Sign Out” will expire session cookies – a session from a hijacked session may not be active or show up in the activity list – the “Sign Out” button will close those sessions as well.
And, **don't forget**: 

*Phishers sometimes alter account settings.*

Check [https://www.umn.edu/myaccount](https://www.umn.edu/myaccount) to make sure your settings (eg. forwarding, self-service secrets) haven't been changed.

Verify that your PeopleSoft settings, such as direct deposit routing information, have not been modified.

If you discover anything changed, report it immediately to abuse@umn.edu for guidance.
Also...

Phishers sometimes give you a nom de spam check to make sure your name is correct!

https://hrss.umn.edu
Finally -

If you have any questions, or suspicions about your account and whether it has been compromised –

contact abuse@umn.edu