

# “Hey! Who Used My Gmail?!”

**Joel Anderson**  
**University Information Security**  
**April 2015**



Information Technology

UNIVERSITY OF MINNESOTA

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.



[Help home](#)**Learn more**[Keeping your account secure](#)[Protecting your family's online safety](#)**Last account activity**[Gmail security checklist](#)

## 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 POP<sup>1</sup> client, a mobile device, a third-party application etc. We'll 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.

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.



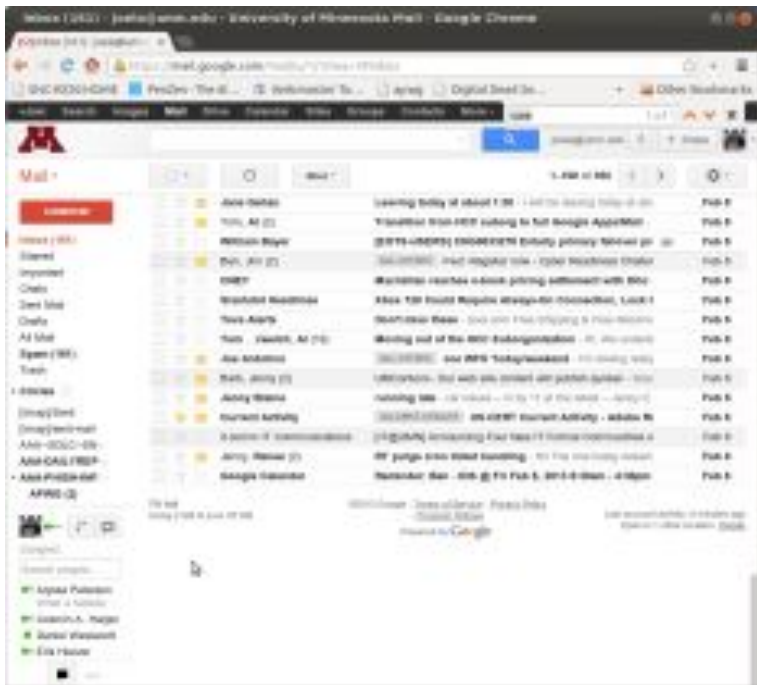
**Great! Where is it??**



Information Technology

---

UNIVERSITY OF MINNESOTA



Down on the bottom right of the screen

# Just log into the Gmail Web interface and check “Account Activity”



click **details**



### Activity on this account

This feature provides information about the last activity on this mail account and any concurrent activity. [Learn more](#)

This account does not seem to be open in any other location. However, there may be sessions that have not been signed out.

[Sign out all other sessions](#)

#### Recent activity:

Access Type [ ? ] (Browser, mobile, POP3, etc.)	Location (IP address) [ ? ]	Date/Time (Displayed in your time zone)
Browser	* United States (MN) (160.94.247.199)	3:07 pm (0 minutes ago)
Mobile	United States (MN) (134.84.45.153)	2:51 pm (16 minutes ago)
Browser	* United States (MN) (160.94.247.199)	1:49 pm (1 hour ago)
Mobile	United States (MN) (134.84.45.153)	1:28 pm (1.5 hours ago)
Browser	* United States (MN) (160.94.247.199)	1:17 pm (1.5 hours ago)
Browser	* United States (MN) (160.94.247.199)	12:00 pm (3 hours ago)
Browser	* United States (MN) (160.94.247.199)	11:05 am (4 hours ago)
Browser	* United States (MN) (160.94.247.199)	10:17 am (4 hours ago)
Browser	* United States (MN) (160.94.247.199)	8:46 am (6 hours ago)
Browser	* United States (MN) (160.94.247.199)	8:22 am (6 hours ago)

**Alert preference:** Show an alert for unusual activity. [change](#)

\* Indicates activity from the current session.

This computer is using IP address 160.94.247.199. (United States (MN))

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?**



Activity information - Google Chrome  
https://mail.google.com/mail/u/1/?ui=2&ik=2c0fd5c7ac&view=ac

### Activity on this account

This feature provides information about the last activity on this mail account and any concurrent activity. [Learn more](#)

This account does not seem to be open in any other location. However, there may be sessions that have not been signed out.

[Sign out all other sessions](#)

Recent activity:

Access Type [ ? ] (Browser, mobile, POP3, etc.)	Location (IP address) [ ? ]	Date/Time (Displayed in your time zone)
Browser	* United States (MN) (160.94.247.199)	3:07 pm (0 minutes ago)
Mobile	United States (MN) (134.84.45.153)	2:51 pm (16 minutes ago)
Browser	* United States (MN) (160.94.247.199)	1:49 pm (1 hour ago)
Mobile	United States (MN) (134.84.45.153)	1:28 pm (1.5 hours ago)
Browser	* United States (MN) (160.94.247.199)	1:17 pm (1.5 hours ago)
Browser	* United States (MN) (160.94.247.199)	12:00 pm (3 hours ago)
Browser	* United States (MN) (160.94.247.199)	11:05 am (4 hours ago)
Browser	* United States (MN) (160.94.247.199)	10:17 am (4 hours ago)
Browser	* United States (MN) (160.94.247.199)	8:46 am (6 hours ago)
Browser	* United States (MN) (160.94.247.199)	8:22 am (6 hours ago)

**Alert preference:** Show an alert for unusual activity. [change](#)

\* Indicates activity from the current session.  
This computer is using IP address 160.94.247.199. (United States (MN))

DON'T miss this - it will let you terminate ALL other sessions, even non-active ones.

This account does not seem to be open in any other location. However, there may be sessions that have not been signed out.

[Sign out all other sessions](#)





## ***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).



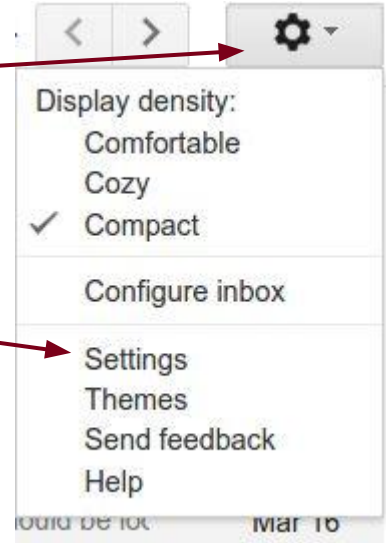
Tampering with your account  
doesn't require staying logged  
into your account!

***Wait, what?!***



Intruders in your email account may use the “settings” options to change or add filters to your account. This may be done by intruders to delete official notices or to have copies of your mail sent to the intruder’s own account.

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:

## Settings

[General](#) [Labels](#) [Inbox](#) [Accounts](#) [Filters](#) [Forwarding and POP/IMAP](#) [Chat](#) [Labs](#) [Offline](#)

The following filters are applied to all incoming mail:

[edit](#) [delete](#)

Be sure to delete any entries 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!* If you find forwarding has been added to your account - REMOVE IT!**

Settings

General Labels Inbox Accounts Filters Forwarding and POP/IMAP Chat Labs Offline



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://my-account.umn.edu/selfservice>
- Reset 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://my-account.umn.edu/selfservice> to make sure your settings (eg. self-service secrets) haven't been changed.

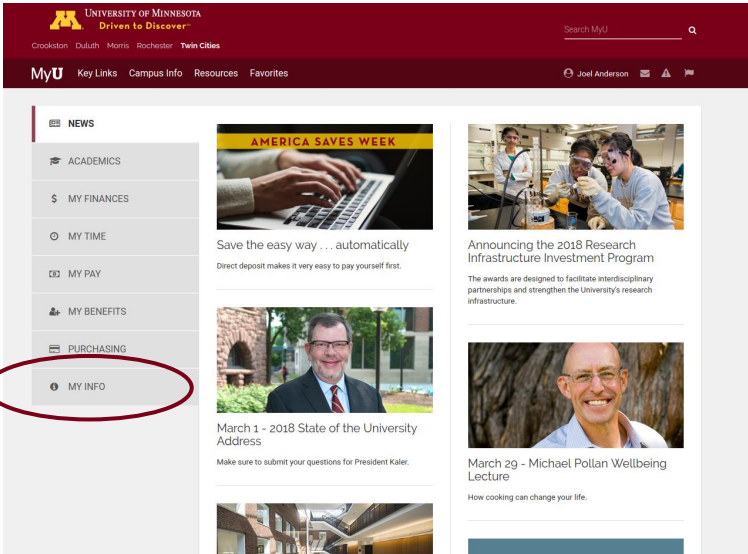
Verify that your PeopleSoft settings, such as direct deposit routing information, have not been modified.

If you discover anything changed, report it immediately to [abuse@umn.edu](mailto:abuse@umn.edu) for guidance.



Also...

***Phishers sometimes change your name to match the spam they intend to send from your account, check to make sure your name is correct!***



The image shows a screenshot of the MyU portal. The top navigation bar is dark red with the University of Minnesota logo and the slogan "Driven to Discover". Below the navigation bar, there is a sidebar menu on the left with the following items: NEWS, ACADEMICS, MY FINANCES, MY TIME, MY PAY, MY BENEFITS, PURCHASING, and MY INFO. The "MY INFO" item is circled in red, and a red arrow points to it from the left. The main content area displays several news items, including "AMERICA SAVES WEEK", "Announcing the 2018 Research Infrastructure Investment Program", "March 1 - 2018 State of the University Address", and "March 29 - Michael Pollan Wellbeing Lecture".

<https://myu.umn.edu>



Information Technology  
UNIVERSITY OF MINNESOTA



***Finally -***

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

contact [abuse@umn.edu](mailto:abuse@umn.edu)



Information Technology

UNIVERSITY OF MINNESOTA