How to know if Facebook, Instagram, Google and other social networks have been hacked

If you think you are being targeted, or worse, the account has been hacked, how do you know who has someone holding your account?

Hackers often target profiles of wealthy politicians or investors. But practically anyone can become a target. An attacker may be a partner or a cyber criminal who wants to attack the victim's bank account.

If you think you are the target, or worse, the account has been hacked, how do you know if someone is holding your account?

It is really a difficult question to answer, because online services offer different types of data and they are often not easily found. Today, **TipsMake.com** will guide you to read the basic steps to see if there are any traces of penetration in your online account, such as Gmail, email from Microsoft, Facebook and Twitter, or not.

Warning : Sometimes, users cannot receive a clear answer about whether an account has been hacked. If in doubt, you should seek advice from an expert, such as a friend who works for IT or a company's technical advice line. In addition, the scope of this guide covers only online services. If hackers get into the computer, all of these services can be compromised and the techniques described here will not be able to help detect anything.

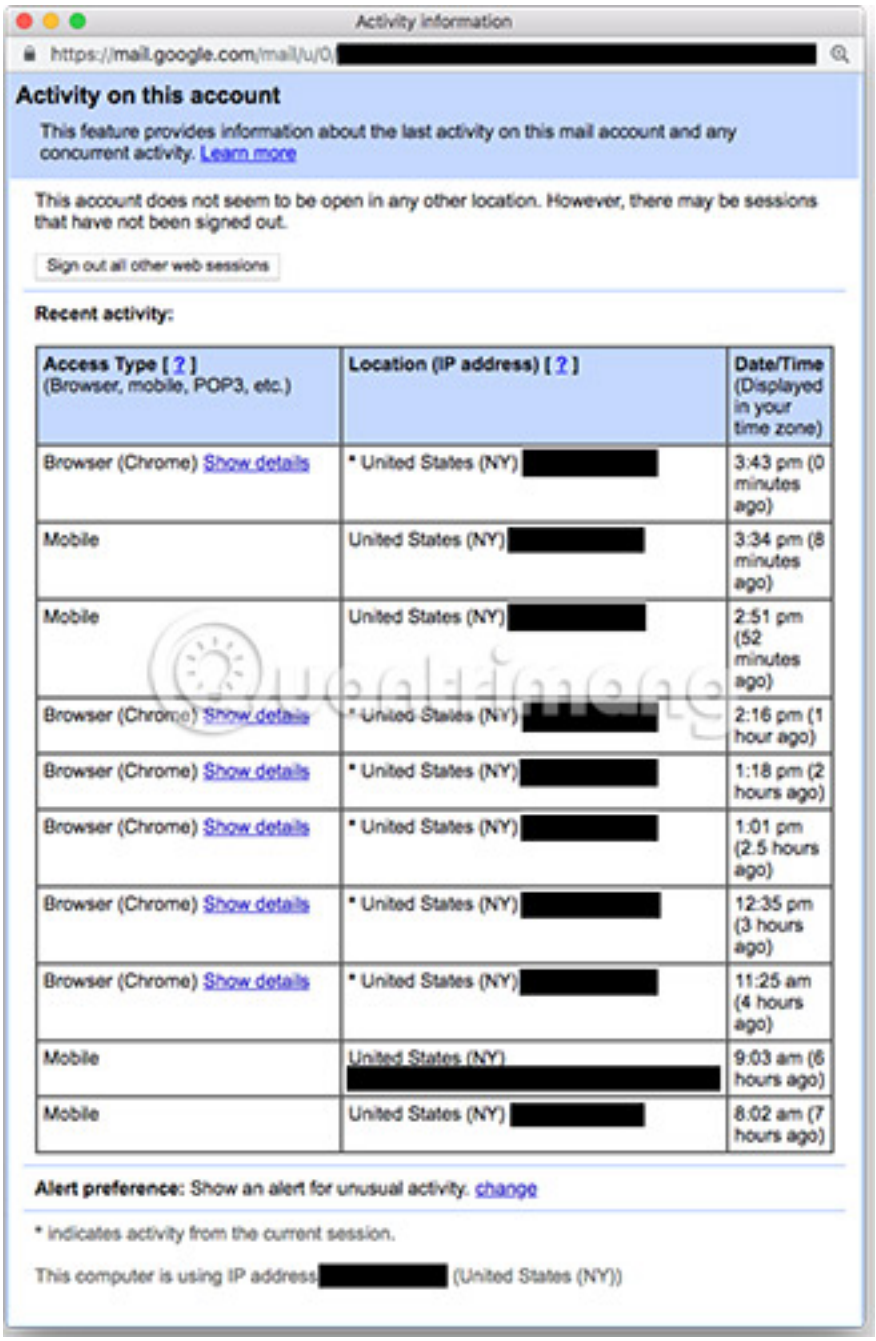
Check if the account has been hacked

1. Gmail
2. Microsoft Outlook
3. Yahoo
4. Facebook
5. Twitter
6. Instagram
7. Steam

Gmail

The first thing to do if you suspect someone has hacked into your Gmail account is to log into Gmail and check ' **Last Account Activity** '. This option is located in the bottom right corner of the Gmail main interface.

A window that looks like this will appear:



Do you recognize the devices and IP addresses listed here? If the answer is no, and you see a place that looks very strange (such as this place is in another country that you have never been to), that could be a sign that someone has logged in to the account. Your Gmail. In that case, click on the ' **Sign out all other web sessions** ' option. This option will force anyone (except you) to log out of your account and change your password immediately.

Next, visit the Google account security dashboard, perform a security check and complete the steps. Please review which applications have access to information on your account. Do you recognize those applications? If not, revoke the access rights. Here, users can also see if there are any security measures, as well as check the

two-factor authentication settings for Gmail.

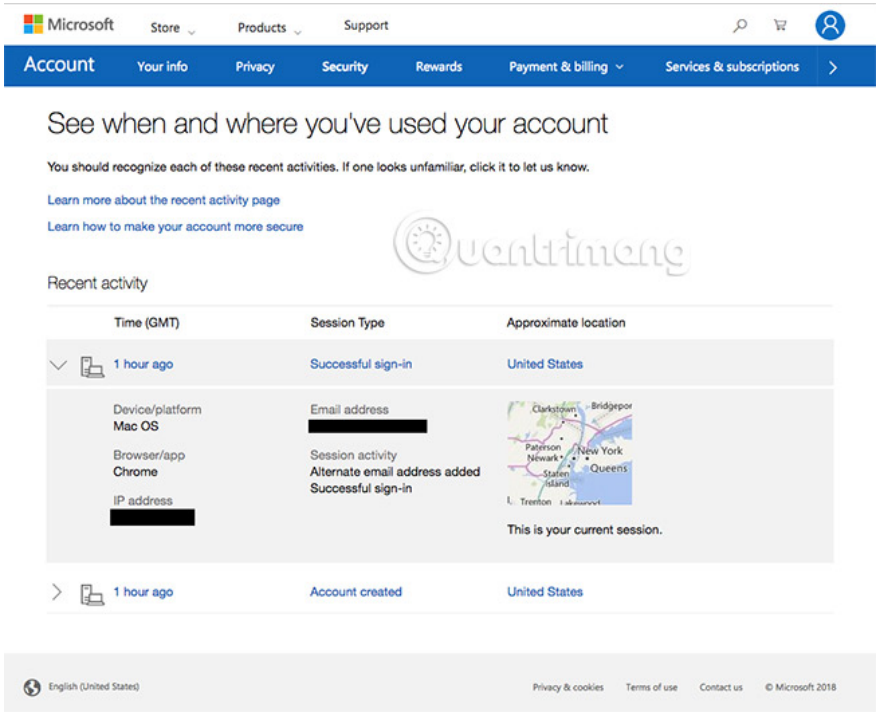
Finally, check to see if hackers have added any filters, email redirects or forwarding settings to stealthily steal your email and hide the fact that they did it. Don't forget to check the trash to see if any forwarding emails have been deleted by hackers.

If you find anything suspicious, change your Gmail password immediately.

Microsoft Outlook

'Giant' email service Microsoft provides the same mechanism as Google. Visit **https://account.microsoft.com/security** and click **Review Activity** to view recent logins and other activities.

This option will take the user to a page that looks like this:

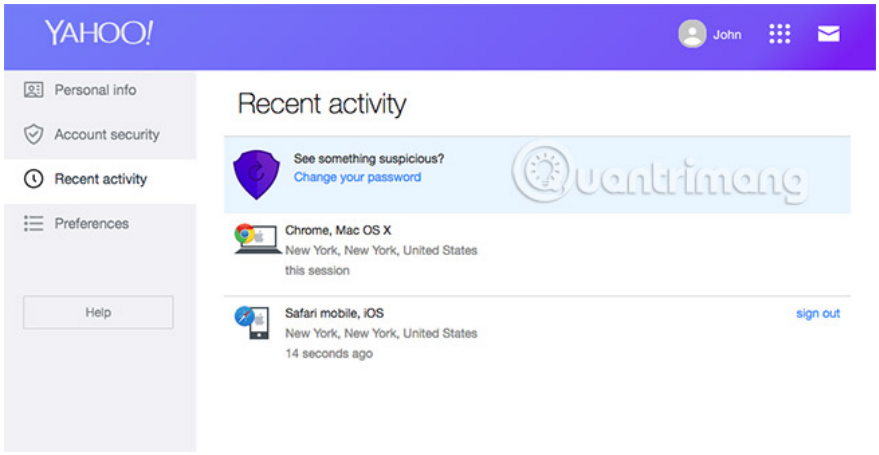


If you see anything suspicious, go back to the main **Security** page and then click the **Change Password** option **.**

Yahoo

Like Google and Microsoft, Yahoo gives users the ability to view some information about the device and which IP address was used to log into the account.

To see this data, visit **https://login.yahoo.com/account/activity.**



If you click on the individual devices displayed in the test list, you can see more information about the IP address, time and location of the login in the last 30 days.

Yahoo also has a site that helps users identify legitimate Yahoo sites, requests and contact information to help users discover fake pages.

If anything unusual happens on the **Recent activity** page **,** change the password immediately.

Facebook

This social network has a series of tools to help users find out if something unusual is happening or not. Visit the Security and Login page of Facebook **(https://www.facebook.com/sinstall?tab=securance).** Here, users can see the logged-in place, a feature similar to Gmail.

If moving to the device name section, its IP address will be displayed.

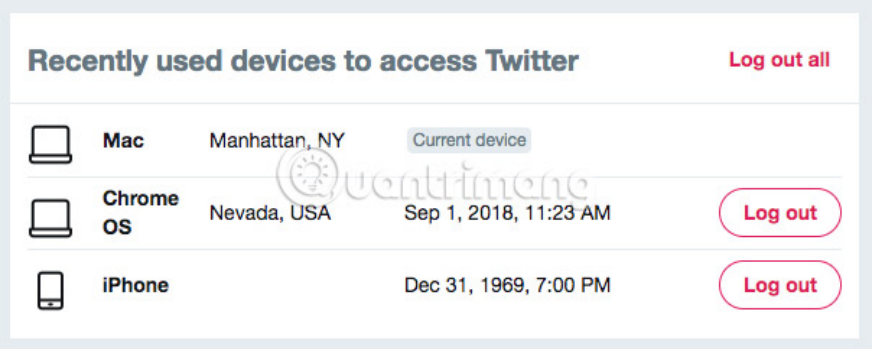
Users should enable ' **Get alerts about unrecognized logins** ' settings, let Facebook alert if someone signs in from your IP address or new location to your account.

If you think someone has broken into your account, check out the **App passwords and Authorized Logins section** to see if there's anything suspicious or not. If yes, delete it. If you think something is wrong, change your Facebook password immediately. That also helps log out any hacker.

Further reference: How to know your Facebook has been hacked

Twitter

This blog service has no details to find out if your account has been hacked. If you're still worried, visit **https://twitter.com/sinstall/simes** and see which device has been used to access your account. Unfortunately, this option does not display the IP address.

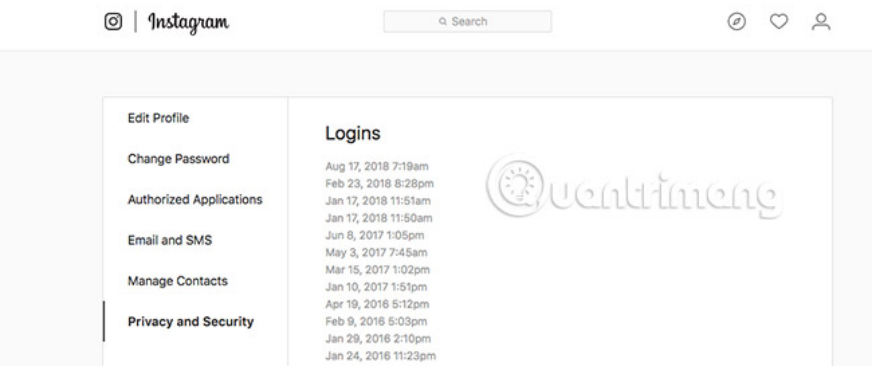


Again, if you see anything suspicious, log out and then change the password. Also, take a moment to review the applications that have access to your Twitter account here.

Instagram

This photo sharing social network has a feature to check previous logins, but the data types displayed are quite limited. All the user can see is the date and time of login, no location, no IP address.

To check, visit **https://www.instagram.com/accounts/access_tool/** and click **View All under Activity, Logins** .



If using the mobile application, click the **Hamburger** menu in the top right corner, then select **Settings** in the lower right corner, scroll down to the **Privacy and Security section** and click **Account Data.** Then continue scrolling down and clicking **All under Activity, Logins** .

If you see a suspicious login (which is a little hard to identify), change your password immediately.

Steam

This video player platform does not allow users to see which computers or IP addresses are logged in. But if you are worried about hacked hackers, go to **https://store.steampowered.com/account/,** click **Manage Steam Guard** in **Account Security,** then click **'Deauthorize all other devices'.**

This will force anyone else to log in to your account. After that, change your password immediately.

See more:

1. Google instructs how to handle when a website is hacked
2. How to identify a link is safe?
3. How to get back Facebook is hacked and lose registration email
4. How to retrieve a hacked Facebook account

You finished reading the article "**How to know if Facebook, Instagram, Google and other social networks have been hacked**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.