

## **KEEPING YOUR GMAIL ACCOUNT SECURE:**

If you are using your Google account and getting maximum benefit from Gmail, Contacts and Drive, you want to make sure your account is secure and hasn't been tampered with. These are some of the things you can do to assure your account is secure.


**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 client, a mobile device, a third-party application etc. It will 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.

Check your Alert Preferences so you will be notified for unusual activity on your account.

There is a box at the top where you can sign out all other sessions. This will sign you out of your google account on **all** devices that you own. If your account is ever compromised or if you lose a mobile device, be sure you sign out of all other sessions and change the password immediately on your account. You will then have to sign in to each device again with your new password.

**SECURE PASSWORDS AND RECOVERY OPTIONS:** Use unique passwords for your account, especially important accounts like email, online banking and brokerage accounts. Passwords should be a mixture of letters, numbers and symbols. The longer your password is, the harder it is for someone to guess.

Click the **gear icon**  in the upper right, and select **Settings**.  
Click on the **Accounts Tab**.

Under **Change account settings**, you can change your password and recovery options. Your recovery email address can be used to send you an email to reset your password if you get locked out or challenge an account hijacker. Your recovery email address should be a different email address from the account you are working in.

You can also check on "Other Google Account Settings" from this location. It is important to review these settings under the categories of Personal Info, Security, Language, Data Tools, Account History and Help. You might be surprised at who you may have inadvertently granted access to your account.

**COMPROMISED GMAIL ACCOUNT:** Your account may have been compromised if you have experienced any of the following issues:

The people in your contact list have received suspicious messages from your address.

Contacts or mail have gone missing.

You've received a warning about suspicious activity from your Last Account Activity.

If your account has been compromised you must immediately change your password and review the websites that you have granted access.

### **KEEPING YOUR ACCOUNT SECURE: These are Google's recommendations:**

Google takes account security very seriously. To ensure that your computer and account remain safe, we strongly recommend following these steps regularly:

1. **Check for viruses and malware.** Run a scan on your computer with a trusted anti-virus software. If the scan detects any suspicious programs or applications, remove them immediately
2. **Regularly update your account recovery options.** Make sure to update your account recovery options to check that they are always up-to-date.
3. **Enroll in 2-step verification.** 2-step verification adds an extra layer of security to your account by requiring you to sign in with something you know (your password) and something you have (a code sent to your phone).
4. **Perform regular operating system and browser updates.** Whether you use Windows or Mac OS, we recommend enabling your automatic update setting, and updating when you get a notification. To check for browser updates in Internet Explorer, select the **Tools** tab and click **Windows Update**. In Firefox, just click the **Help** tab and select **Check for Updates**. Note that Google automatically updates to a newer version when one is released.
5. **Never use your Google Account password on another website.** If you enter your password in an external website and it's compromised, someone could try to sign in to your Google Account with the same information.
6. **Protect your password.** Never enter your password after following a link in an email from an untrusted site. Always go directly to [mail.google.com](mailto:mail.google.com) or [www.google.com/accounts/Login](http://www.google.com/accounts/Login). Also, never send your password via email. Google will never email you to ask for your password or other sensitive information.
7. Always sign out of your account when you're using a public computer. Just click Sign Out in the top right corner of the screen when you're done using your Google account.