

2 Factor Authentication

to secure your login



Secure your Personal eMail accounts Gmail , Hotmail & Dropbox with 2-Factor Authentication

Two-step verification is an additional security which is now enabled on Personal Email Accounts, Social Media etc e.g.: Gmail, Dropbox etc where you can secure your information and data from unauthorized access.

It's important that only you have the ability to access your account details, update your password, access the data you store and keep up to date.

Why you need it

It's easier for someone to steal your password.

Any of these common actions could put you at risk of having your password stolen:

- Using the same password for more than one site
- Downloading software from the Internet
- Clicking on links in email messages

2-Step Verification can help to keep bad guys out, even if they have your password.

How it Works



- 1) Install Google Authenticator App from Play store or Apple Stores on your mobile and follow instruction
- 2) Open your Gmail, Hotmail → Go to Account Settings → enable 2-Factor Authentication.
- 3) And follow instruction to enable it on your Mobile and your respective account

Note

- You can always enable/ Disable 2-Factor Authentication from respective account whenever required
- The Google Authenticator app for Android, iPhone, or BlackBerry can generate verification codes even when you are offline on your mobile device or without 2G/3G data connectivity.

Signing in to your account will work bit differently

1. Whenever you sign in to Google/ any other account which supports two factor authentication, you need to enter your password as usual.
2. You'll be asked for the security code from your two factor authenticator app.