Google 2 factor authentication User Guide

Description:	This guide describes how to setup "Two factor authentication" for your Google account.
Updated Date:	March, 2018

Summary

ITSC is pleased to launch "Two factor authentication" for Google account to enhance your protection against unauthorized access to your information. With such option enabled, your information is still protected even when someone manages to obtain your password.

You are highly suggested to enable the option to protect your data and files. The following are what you expect once enable the settings:

1. You will need to have your mobile device around when you login;
2. You will be required to enter one more verification code in addition to your password via text, voice call, or a mobile app;
3. You will be required to enter the verification code per device every login, or has an option of not asking the code every time.

Section 1: What is 2 Factor authentication and why we need it?

2 Factor authentication is an additional security layer you can add to your Google accounts in order to prevent unauthorized access. When you log in Google application, you need to provide not just your password, but also the verify code for it too. That means, unless someone has access to both, they won't be able to access your account.

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

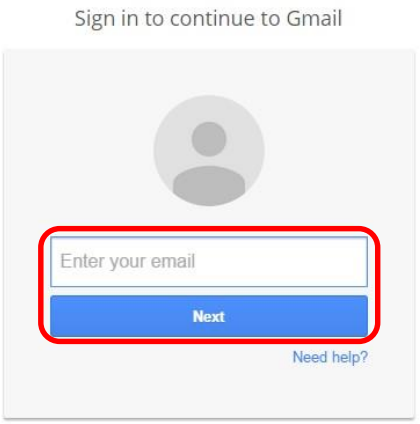
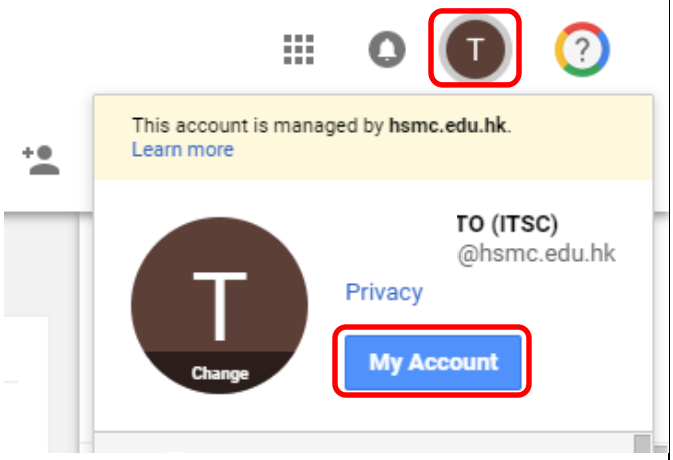
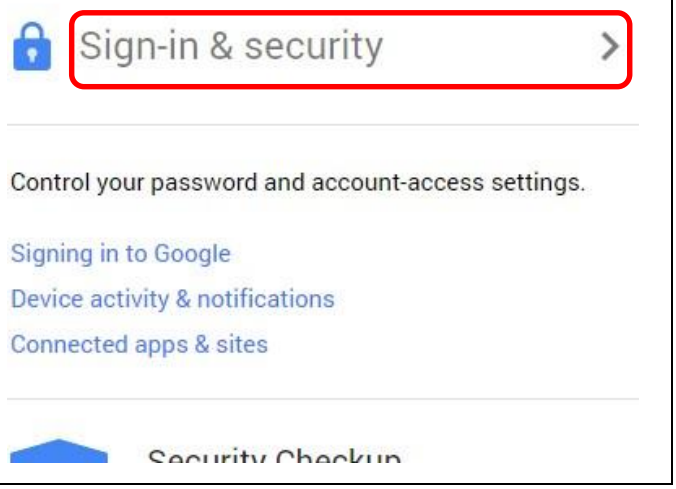
- Using the same password on more than one site;
- Downloading unauthorized software from the Internet;
- Clicking on links in email messages;
- Opening attachments from unknown senders.

When a bad guy steals your password, they could lock you out of your account, and then do some of the following:

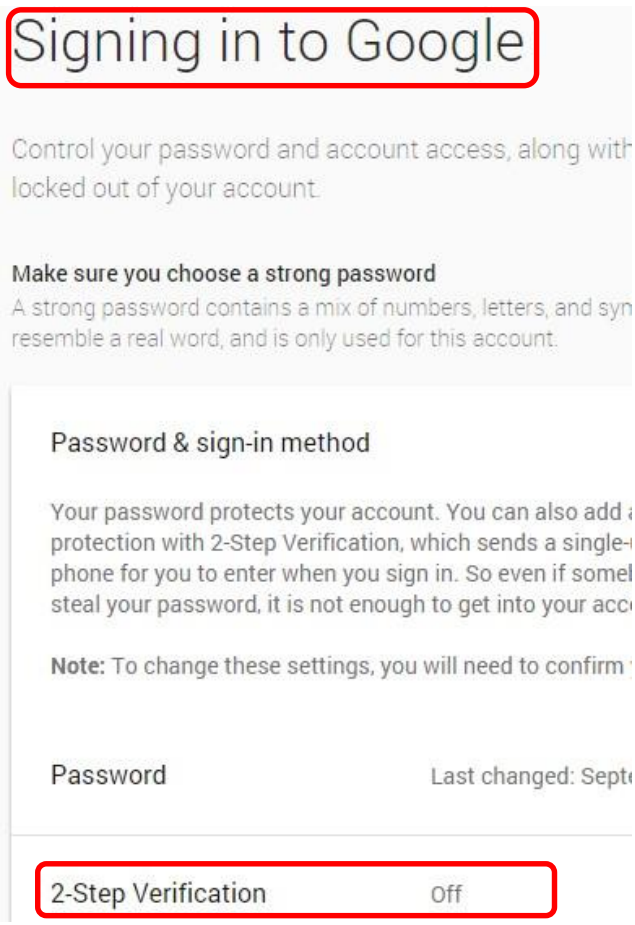
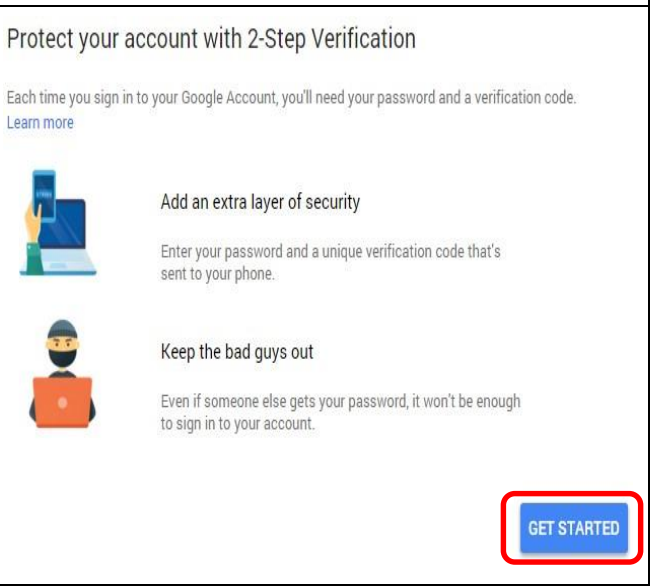
- Go through – or even delete – all of your emails, contacts, photos, etc.
- Pretend to be you and send unwanted or harmful emails to your contacts;
- Use your account to reset the passwords for your other accounts (banking, shopping, etc.)

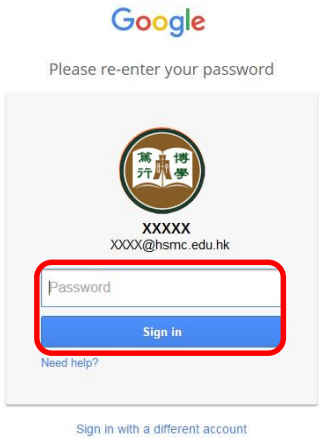
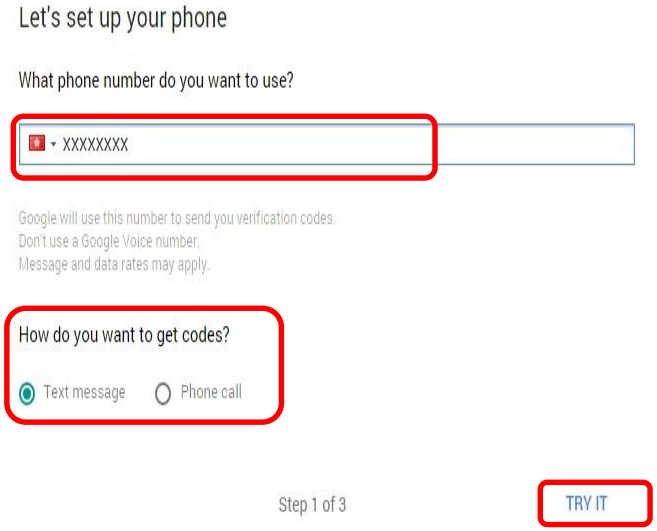
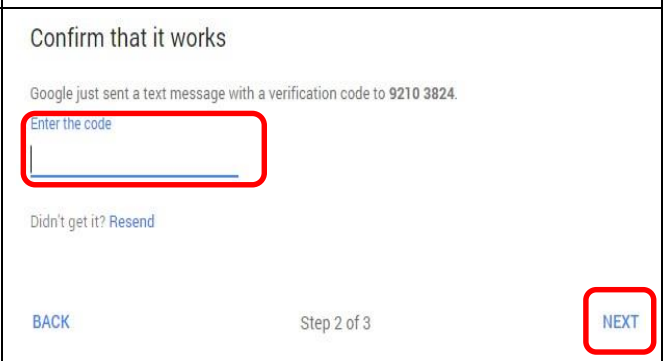
2 Factor authentication can help keeping bad guys out, even if they have your password.

Section 2: How to set up 2 Factor Authentication using SMS?

Steps		Details
1.	Sign in to the Google account.	
2.	Go to My Account. Click icon at upper right hand corner of browser. Then select **My Account**.	
3.	The Page shows several parts of account settings, click **Sign-in & security**.	

2-Step Verification settings

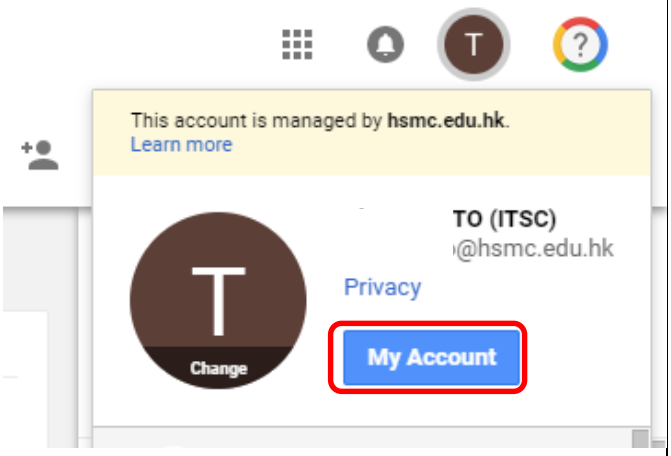
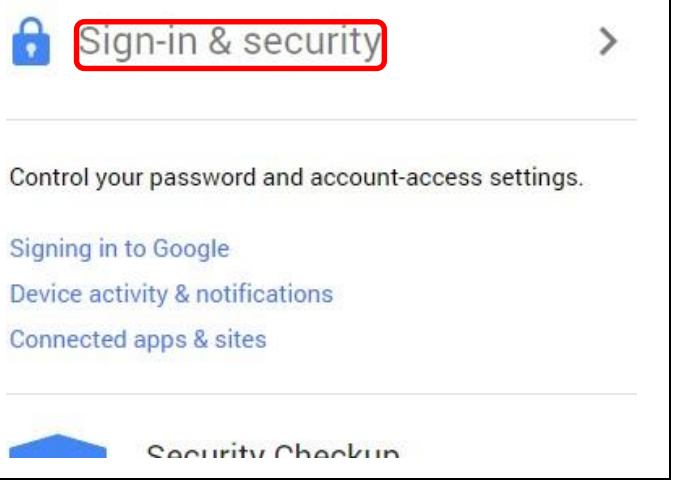
4.	In the middle part of the page, heading with **Signing in to Google**, select **2-Step Verification**.	
5.	It turns to sign-in page with 2-Step verification. Click **GET STARTED**.	

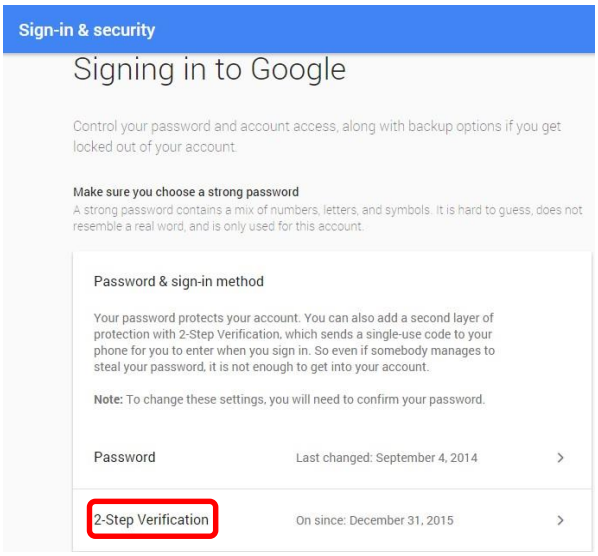
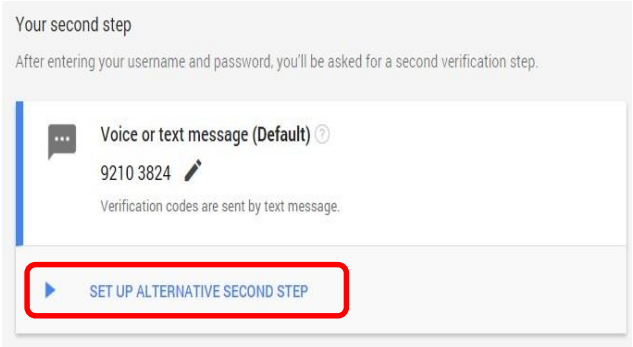
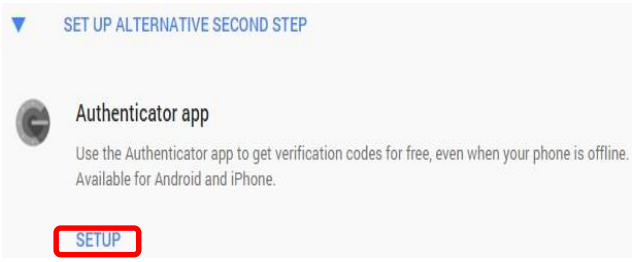
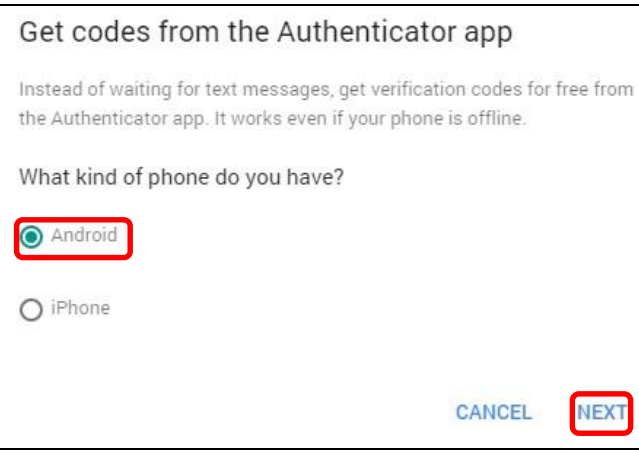
6.	Sign in **Google Account** again to confirm your identity.	
7.	Setup your phone. a. Enter your mobile number. b. Select the way to receive verification code. (i.e. Text message) c. Click **TRY IT**.	
8.	It will send a text message to your mobile. a. Enter verification code. b. Click **NEXT**.	
9.	Click **TURN ON**.	

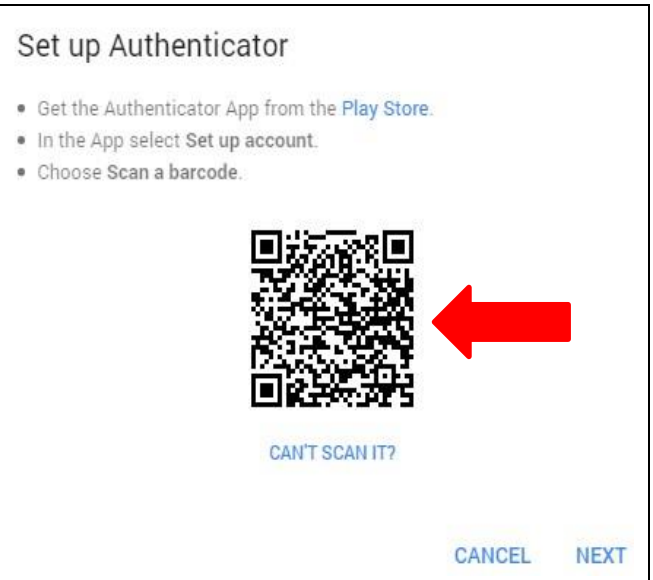
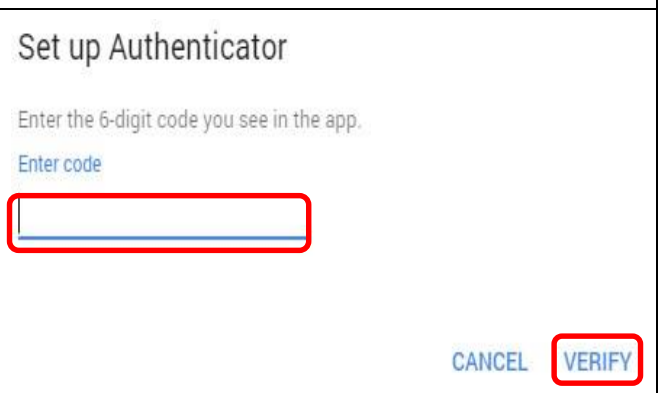
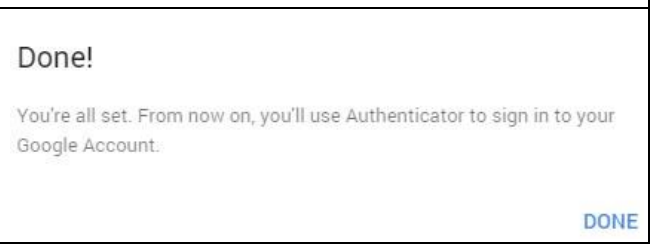
Section 3: Sign in Google Services with 2 Factor Authentication (SMS) enabled

10.	Next time when you sign in Google services (using HSMC account), you will be prompted for the "second factor" in addition to your username and password. **You will get the code via text message (i.e. SMS)**. **Note:** If you want to stop entering the code every time you log in a computer (such as home/office PCs), you can tick "**Don't ask for codes again on this computer**". It will not ask for another 30 days.	

Section 4: How to set up 2 Factor Authentication without SMS access?

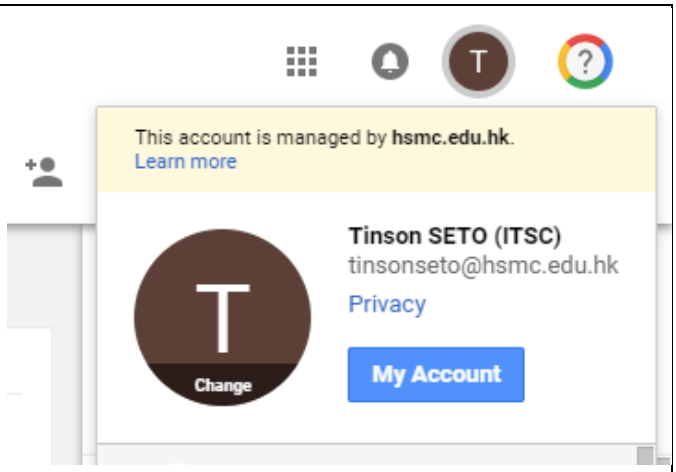
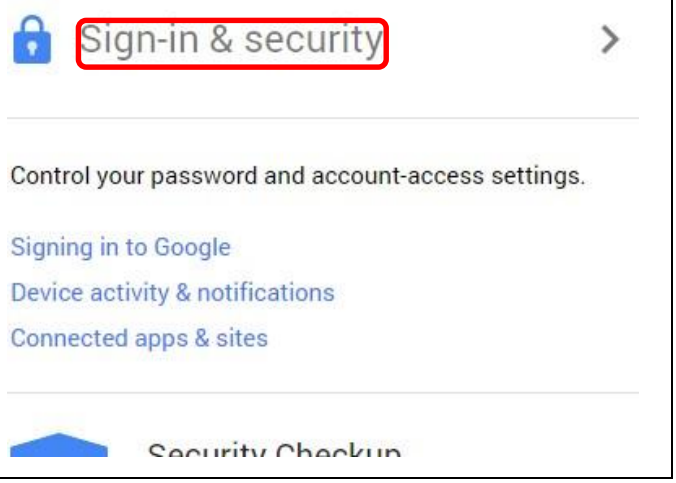
1.	You can download the mobile app (search by "**Google Authenticator**") via App Store (iOS) or Play Store (Android). Install the app.	
2.	Sign in your Google account in your PC. Go to **My Account**.	
3.	Click **Sign-in & security**.	

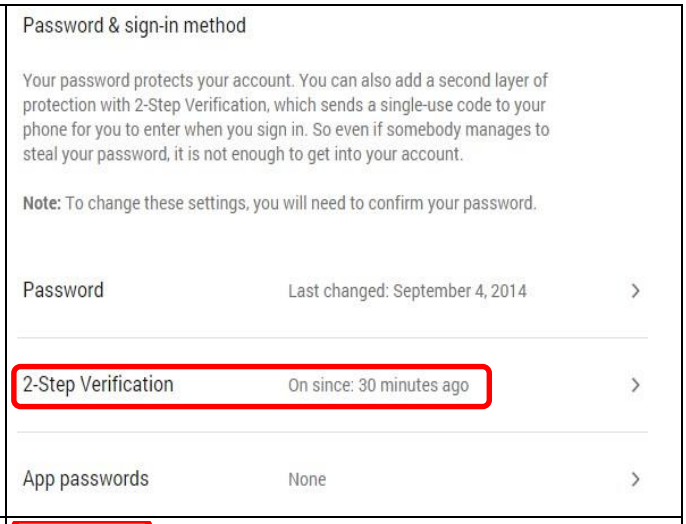
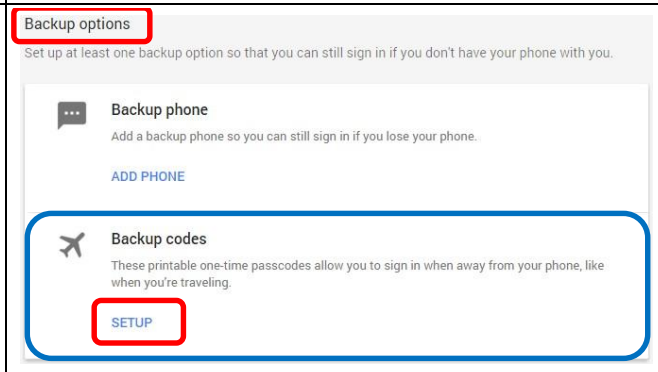
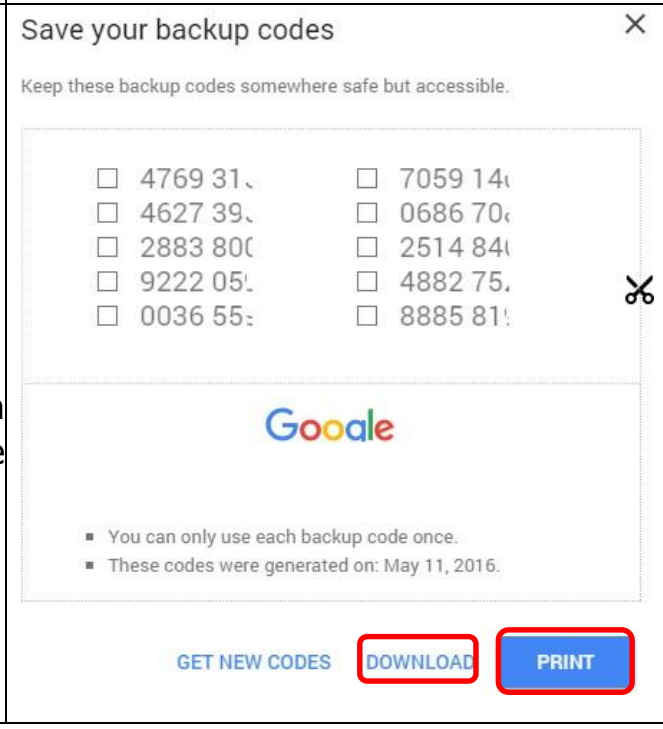
4.	Select **2-Step Verification**.	
5.	In Google 2-Step Verification setting page, you can select "**SET UP ALTERNATIVE SECOND STEP**" to get code via mobile app.	
6.	Under Authenticator app Click **SETUP**.	
7.	Select your mobile OS (currently support Android and iOS), then click **NEXT**.	

8.	On your phone, open the "Google Authenticator" App, tap "+", and then "Scan Barcode". Use your phone's camera to scan the barcode appeared on your PC.	
9.	Enter the 6-digit verification code generated by the Authenticator app. Click **VERIFY**.	
10.	Google Authenticator setup successful.	

11.	Next time when you sign in Google services (using HSMC account), you will be prompted for the "second factor" in addition to your username and password. **Now you can use the mobile app to generate the code.** (if you want skip 2-step on that computer, tick "**Don't ask for codes again on this computer**")	

Section 5: How to set up backup codes in case you have lost your phone?

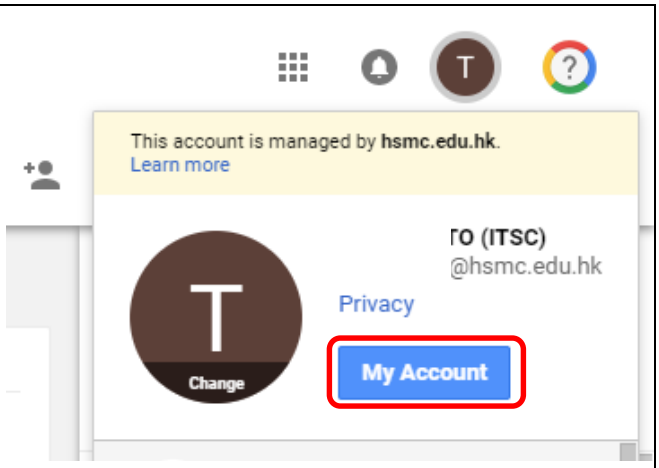
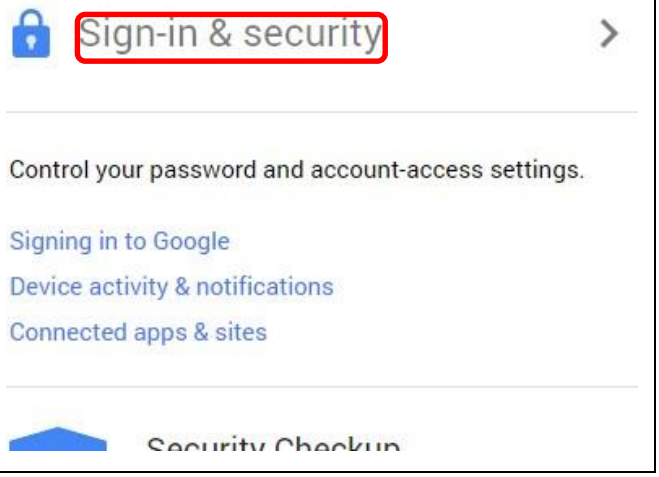
1.	Sign in your Google account. Go to **My Account**.	
2.	Click **Sign-in & security**.	

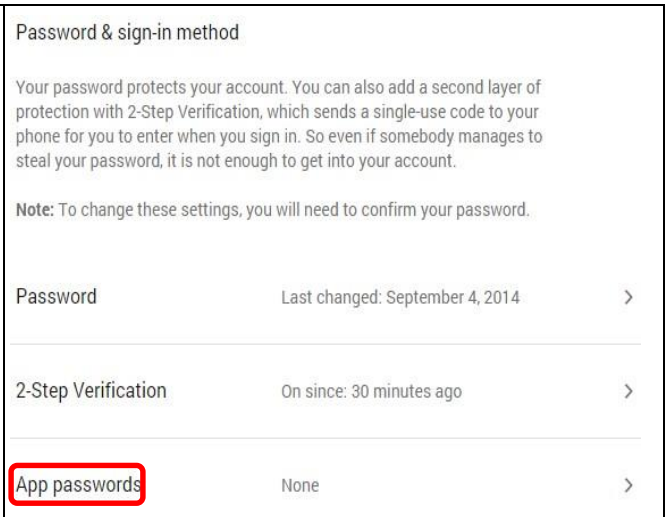
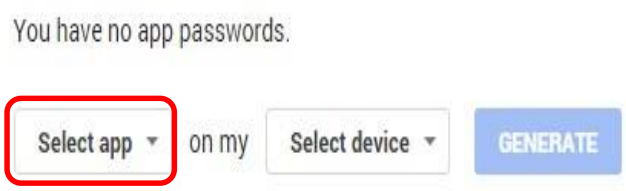
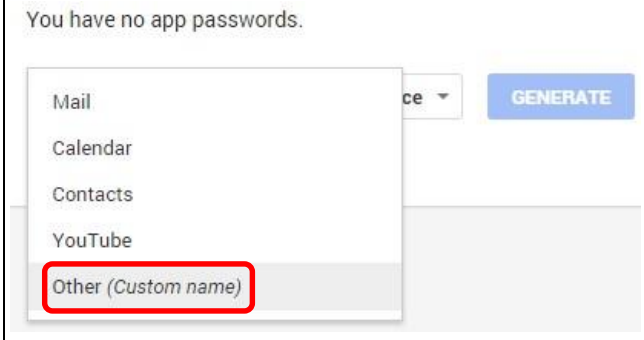
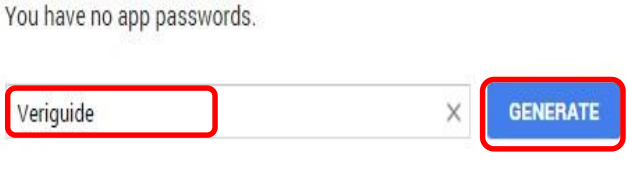
3.	Select **2-Step Verification**	
4.	Under Backup options click **SETUP** in Backup codes session.	
5.	You can **DOWNLOAD** or **PRINT** your backup codes. *Note: Please store the backup codes in a safe place.* The code can be used in case you don't have access to your phone.	

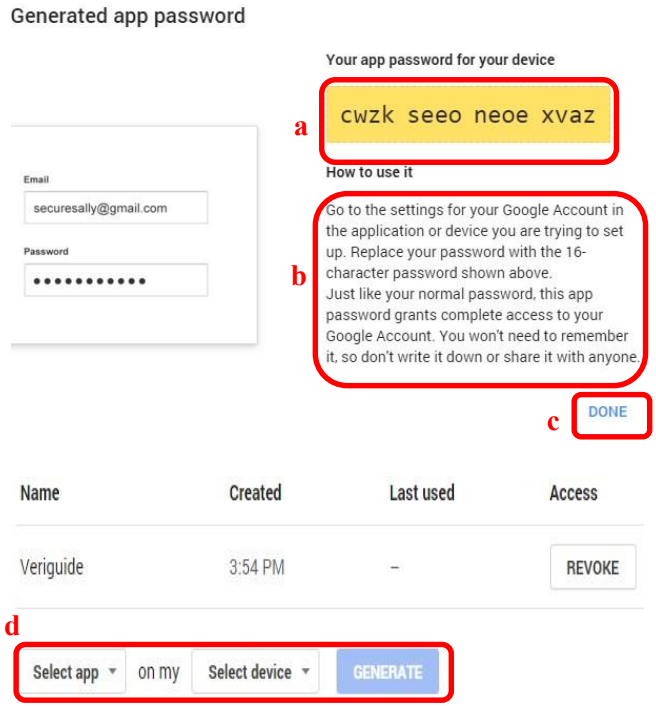
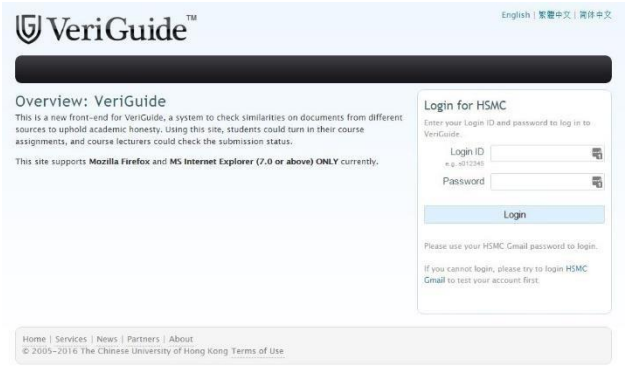
Section 6: My passwords to some applications are invalid once I setup 2 Factor Authentication, what should I do?

The following services require you to provide an "application specific password" when login:

- Veriguide
- Email and calendar applications (such as iPhone/iPad email app, Outlook/Thunderbird on PC, etc.)

1.	Sign in your Google account. Go to **My Account**.	
2.	Click **Sign-in & security**.	

3.	Select **App passwords**.	
4.	Under **Select app** drop down list: Select the appropriate type of application and devices. In this example, we will show how to generate password for VeriGuide.	
5.	Select **Other (Custom name)**	
6.	Type "Veriguide" Click **GENERATE**	

7.	a. A password will be generated. b. Follow the steps given. c. Click **Done**. d. You can repeat the steps for other Apps.	
8.	Use the generated password to login VeriGuide.	

Section 7: How to get help if I have any problem?

Please contact ITSC (3963-5160) or email (itsc@hsmc.edu.hk)