



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.

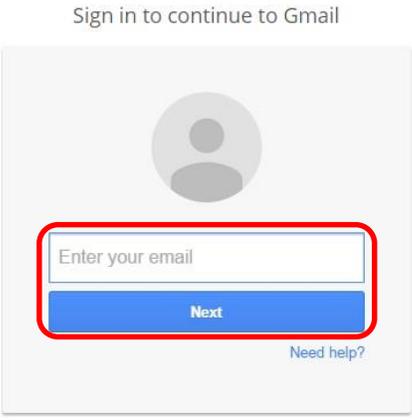
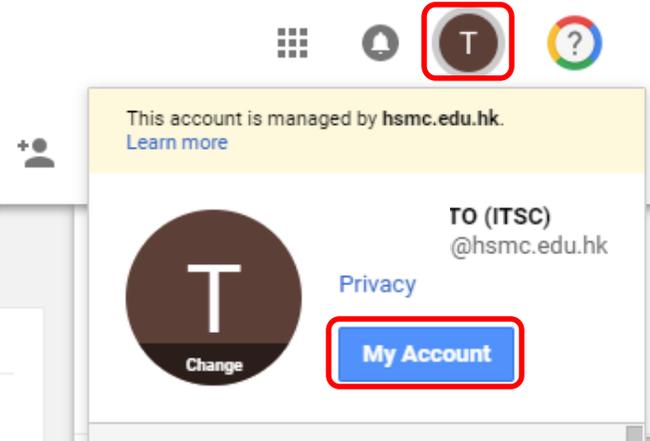
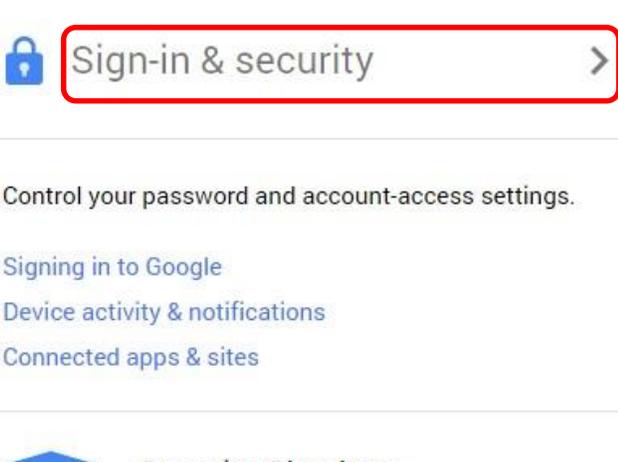
When a bad guy steals your password, they could lock you out of your account, and then do some of the following:

- 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.

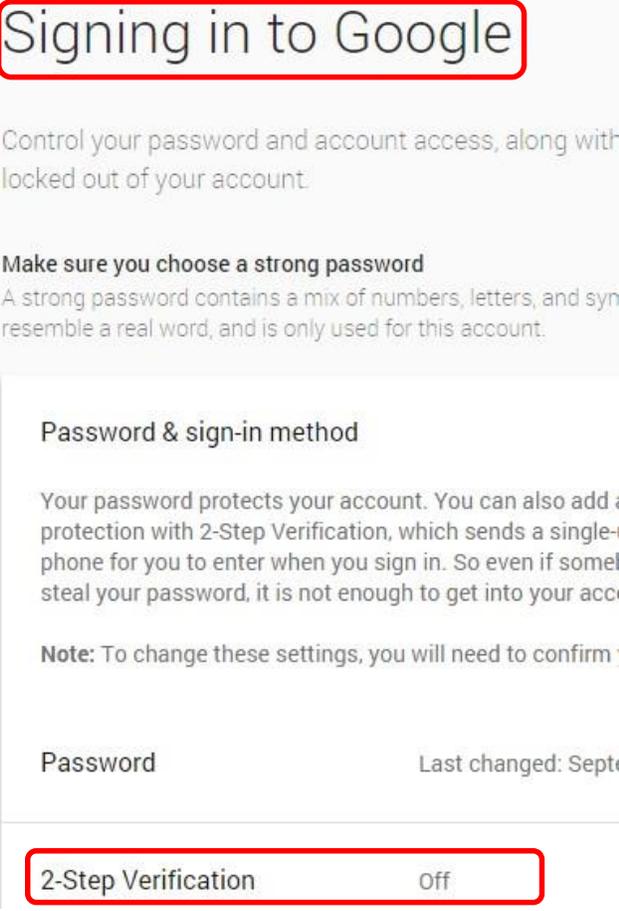
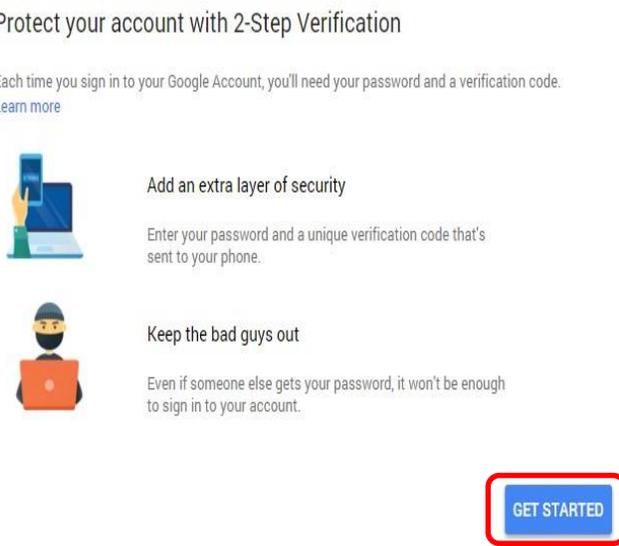


Section 2: How to set up 2 Factor Authentication using SMS?

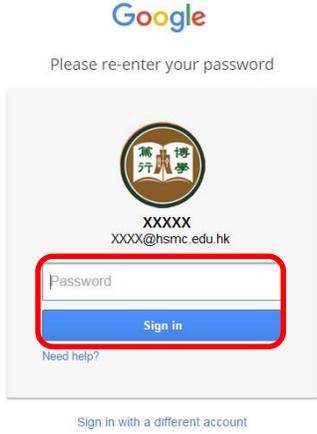
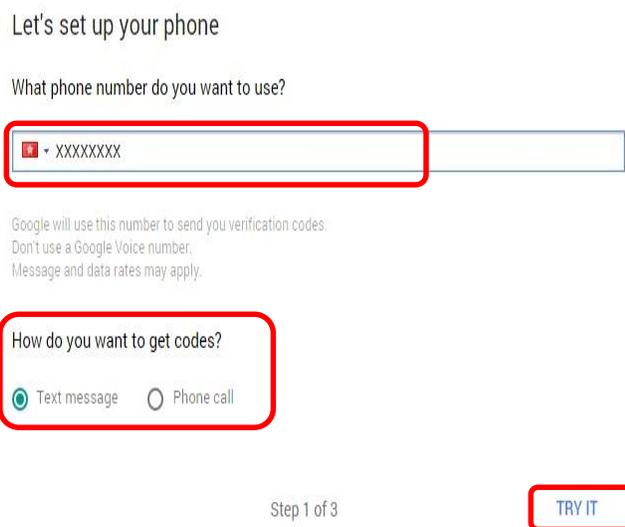
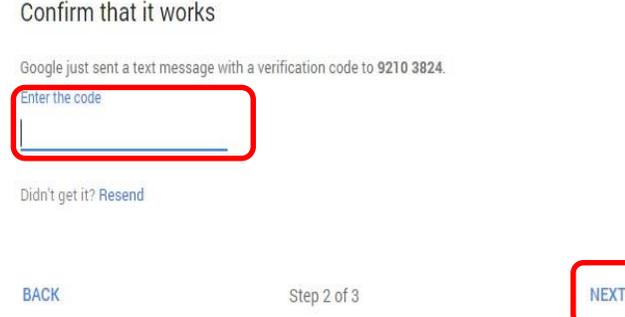
Steps	Details
1. Sign in to the Google account.	 A screenshot of the Google sign-in page. At the top, it says "Sign in to continue to Gmail". Below this is a large grey circle representing a profile picture. Underneath is a text input field labeled "Enter your email" and a blue button labeled "Next". A red box highlights the "Enter your email" field and the "Next" button. There is a "Need help?" link at the bottom right.
2. Go to My Account. Click icon at upper right hand corner of browser. Then select My Account .	 A screenshot of the Google account management page. At the top right, there are icons for a grid, a bell, a profile picture (a circle with the letter 'T'), and a help icon. A red box highlights the profile picture icon. Below these icons is a yellow banner that says "This account is managed by hsmc.edu.hk" with a "Learn more" link. Underneath is a profile card for "TO (ITSC) @hsmc.edu.hk" with a "Privacy" link and a "Change" link. A blue button labeled "My Account" is highlighted with a red box.
3. The Page shows several parts of account settings, click Sign-in & security .	 A screenshot of the Google account settings page. At the top, there is a blue lock icon followed by the text "Sign-in & security" and a right-pointing arrow. A red box highlights this entire section. Below this, there is a heading "Control your password and account-access settings." followed by several links: "Signing in to Google", "Device activity & notifications", and "Connected apps & sites". At the bottom, there is a blue house icon and the text "Security Checkup".



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.	 <p>The screenshot shows the Google sign-in interface. At the top, it says "Please re-enter your password". Below this is a card with the Hang Seng Management College logo, the name "XXXXX", and the email address "XXXX@hsmc.edu.hk". A red box highlights the "Password" input field and the "Sign in" button. There are also links for "Need help?" and "Sign in with a different account".</p>
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 .	 <p>The screenshot shows the "Let's set up your phone" screen. It asks "What phone number do you want to use?". A red box highlights the phone number input field containing "XXXXXXXX". Below this, it asks "How do you want to get codes?" with two radio button options: "Text message" (selected) and "Phone call". A red box highlights these options. At the bottom right, there is a "TRY IT" button. The page is labeled "Step 1 of 3".</p>
8.	It will send a text message to your mobile. a. Enter verification code. b. Click NEXT .	 <p>The screenshot shows the "Confirm that it works" screen. It states "Google just sent a text message with a verification code to 9210 3824." Below this is an "Enter the code" input field, which is highlighted with a red box. There is a "Resend" link for "Didn't get it?". At the bottom left is a "BACK" button, and at the bottom right is a "NEXT" button. The page is labeled "Step 2 of 3".</p>
9.	Click TURN ON .	 <p>The screenshot shows the "It worked! Turn on 2-Step Verification?" screen. It asks "Now that you've seen how it works, do you want to turn on 2-Step Verification for your Google Account liamwong@hsmc.edu.hk?". At the bottom left is a "BACK" button, and at the bottom right is a "TURN ON" button. The page is labeled "Step 3 of 3".</p>

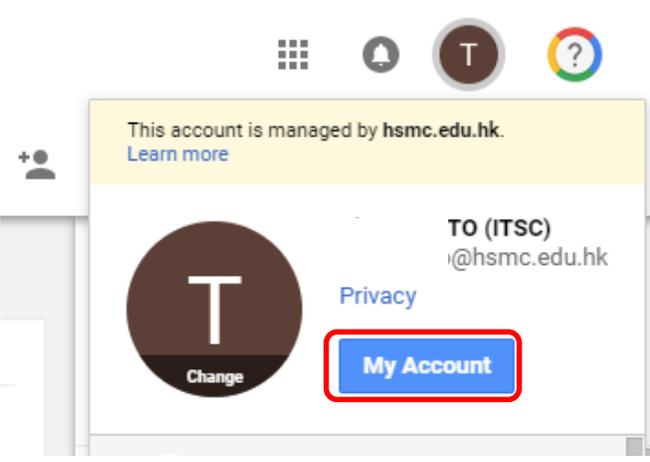
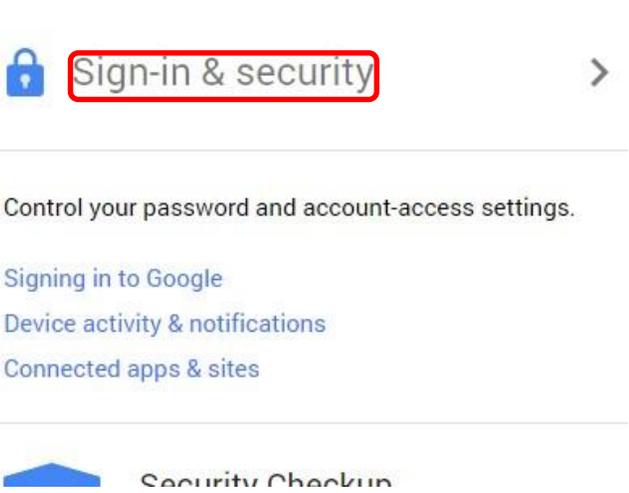


Section 3: Sign in Google Services with 2 Factor Authentication (SMS) enabled

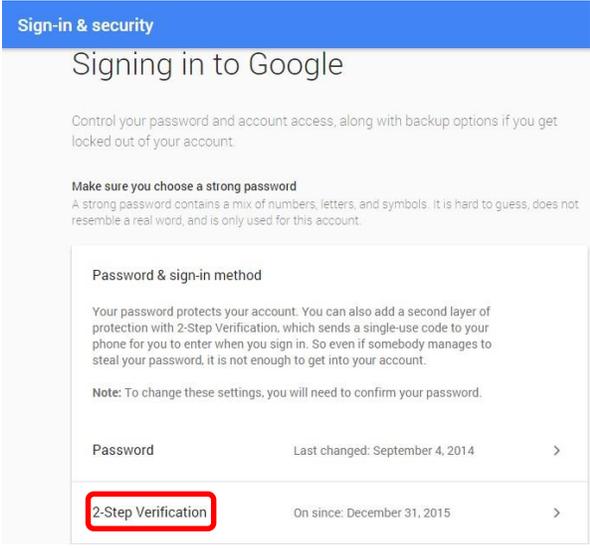
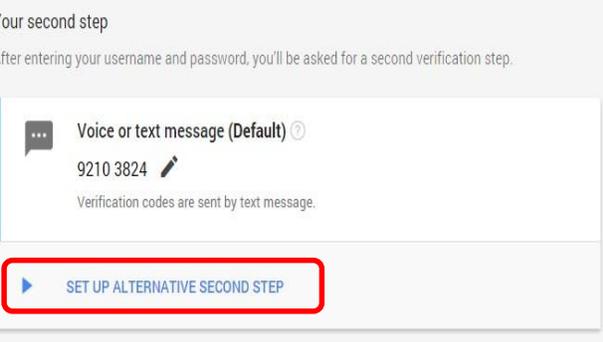
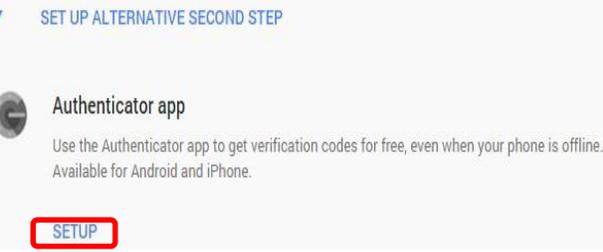
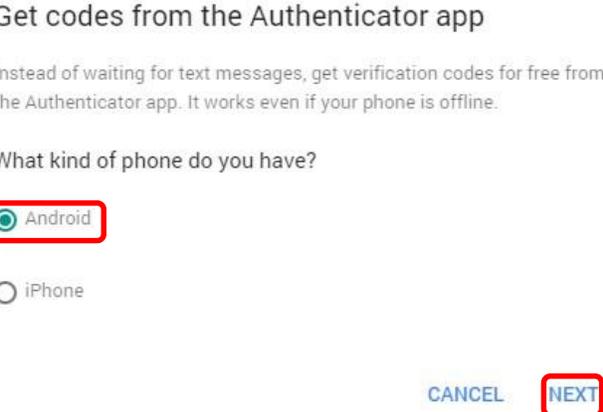
<p>10. Next time when you sign in Google services (using HSMC account), you will be prompted for the “second factor” in addition to your username and password.</p> <p>You will get the code via text message (i.e. SMS).</p> <p>Note: If you want to stop entering the code every time you log in a computer (such as home/office PCs), you can tick “Don’t ask for codes again on this computer”.</p> <p>It will not ask for another 30 days.</p>	 <p>The screenshot shows a Google sign-in interface. At the top is a blue circular profile picture placeholder. Below it, the text 'XXXX XXXX' and the email address 'xxxx@hsmc.edu.hk' are displayed. A red box highlights a password input field containing six dots and a blue 'Sign in' button below it. A 'Need help?' link is visible at the bottom left of the sign-in area.</p> <p style="text-align: center;"></p>  <p>The screenshot shows the '2-step Verification' screen. It features a smartphone icon with a green notification bubble. The text reads: 'A text message with your code has been sent to: **** *'. A red box highlights an input field containing 'XXXXXX '. Below the input field is a blue 'Verify' button. At the bottom, there is a checkbox labeled 'Don't ask for codes again on this computer'.</p>
--	--



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

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



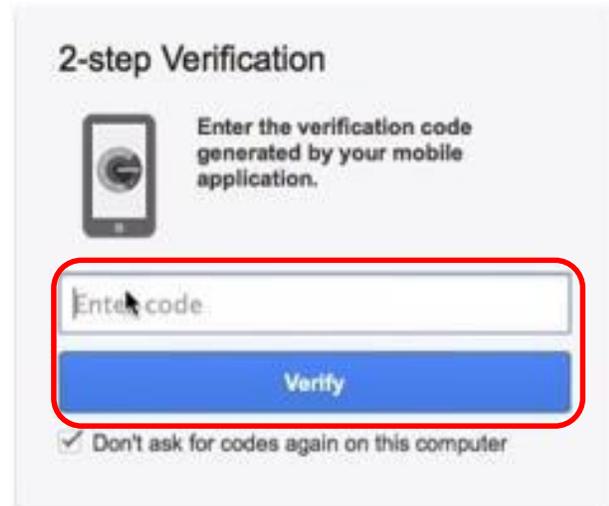
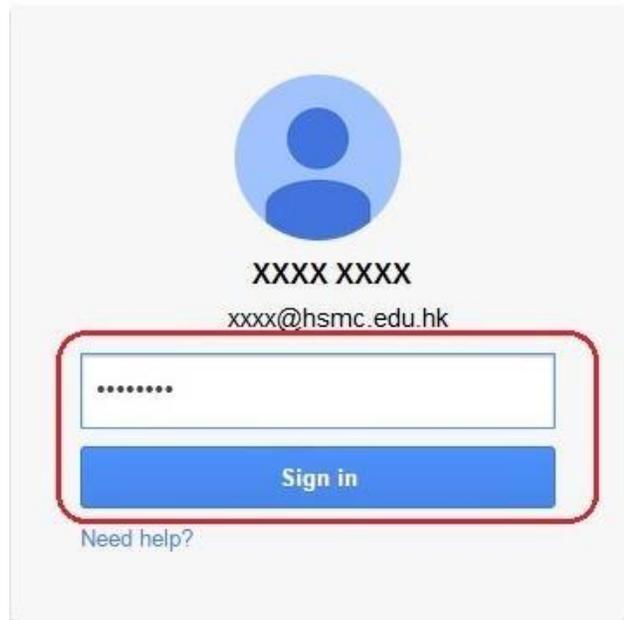
4.	Select 2-Step Verification.	 <p>Sign-in & security</p> <h3>Signing in to Google</h3> <p>Control your password and account access, along with backup options if you get locked out of your account.</p> <p>Make sure you choose a strong password A strong password contains a mix of numbers, letters, and symbols. It is hard to guess, does not resemble a real word, and is only used for this account.</p> <p>Password & sign-in method</p> <p>Your password protects your account. You can also add a second layer of protection with 2-Step Verification, which sends a single-use code to your phone for you to enter when you sign in. So even if somebody manages to steal your password, it is not enough to get into your account.</p> <p>Note: To change these settings, you will need to confirm your password.</p> <p>Password Last changed: September 4, 2014 ></p> <p>2-Step Verification On since: December 31, 2015 ></p>
5.	In Google 2-Step Verification setting page, you can select “SET UP ALTERNATIVE SECOND STEP” to get code via mobile app.	 <p>Your second step</p> <p>After entering your username and password, you'll be asked for a second verification step.</p> <p>Voice or text message (Default) ⓘ 9210 3824 ✎ Verification codes are sent by text message.</p> <p>SET UP ALTERNATIVE SECOND STEP</p>
6.	Under Authenticator app Click SETUP .	 <p>SET UP ALTERNATIVE SECOND STEP</p> <p>Authenticator app Use the Authenticator app to get verification codes for free, even when your phone is offline. Available for Android and iPhone.</p> <p>SETUP</p>
7.	Select your mobile OS (currently support Android and iOS), then click NEXT .	 <p>Get codes from the Authenticator app</p> <p>Instead of waiting for text messages, get verification codes for free from the Authenticator app. It works even if your phone is offline.</p> <p>What kind of phone do you have?</p> <p><input checked="" type="radio"/> Android</p> <p><input type="radio"/> iPhone</p> <p>CANCEL NEXT</p>

<p>8.</p>	<p>On your phone, open the "Google Authenticator" App, tap "+", and then "Scan Barcode".</p> <p>Use your phone's camera to scan the barcode appeared on your PC.</p>	<p>Set up Authenticator</p> <ul style="list-style-type: none"> • Get the Authenticator App from the Play Store. • In the App select Set up account. • Choose Scan a barcode. 
<p>9.</p>	<p>Enter the 6-digit verification code generated by the Authenticator app.</p> <p>Click VERIFY.</p>	<p>Set up Authenticator</p> <p>Enter the 6-digit code you see in the app.</p> <p>Enter code</p> <input data-bbox="779 1060 1079 1123" type="text"/> <p>CANCEL VERIFY</p>
<p>10.</p>	<p>Google Authenticator setup successful.</p>	<p>Done!</p> <p>You're all set. From now on, you'll use Authenticator to sign in to your Google Account.</p> <p>DONE</p>

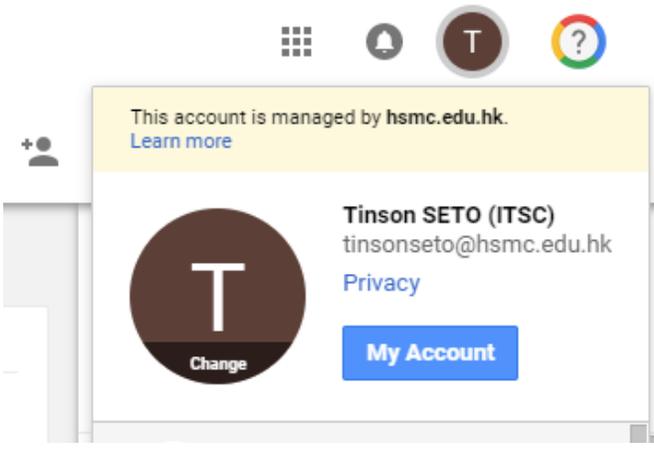
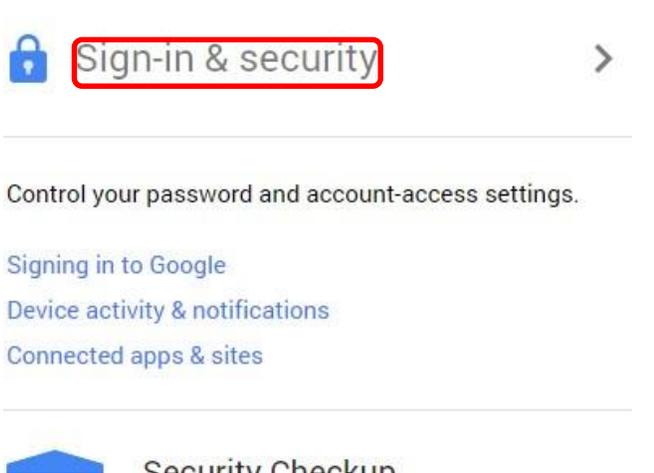
11. Next time when you sign in Google services (using HSMC account), you will be prompted for the "second factor" in addition to your username and password.

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?

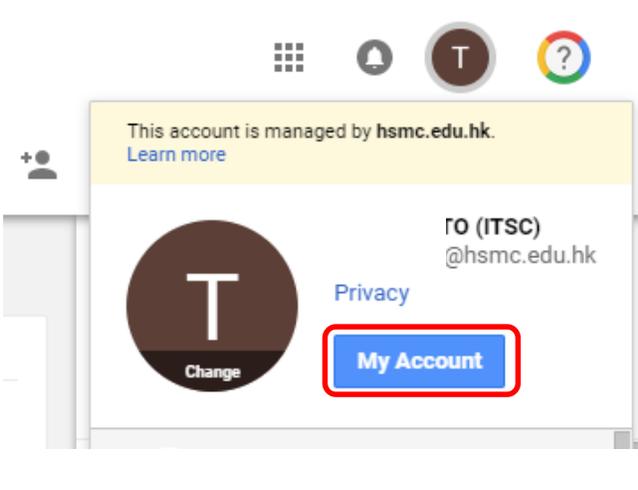
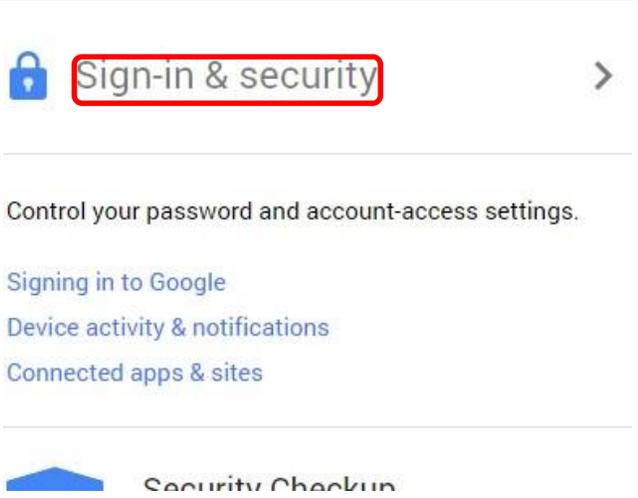
<p>1. Sign in your Google account.</p> <p>Go to My Account.</p>	 A screenshot of a mobile device showing the Google account management interface. At the top, there are icons for the app drawer, notifications, the user's profile (a circle with the letter 'T'), and a help icon (a circle with a question mark). Below these is a yellow banner that reads "This account is managed by hsmc.edu.hk" with a "Learn more" link. Underneath the banner is a profile card for "Tinson SETO (ITSC)" with the email address "tinsonseto@hsmc.edu.hk" and a "Privacy" link. A large circular profile picture with the letter 'T' is shown, with a "Change" button below it. To the right of the profile picture is a blue button labeled "My Account".
<p>2. Click Sign-in & security.</p>	 A screenshot of the "Sign-in & security" settings page on a mobile device. The title "Sign-in & security" is at the top, with a blue padlock icon to its left and a right-pointing chevron icon to its right. Below the title is a horizontal line, followed by the text "Control your password and account-access settings." Below this are three menu items: "Signing in to Google", "Device activity & notifications", and "Connected apps & sites". At the bottom of the page, there is a blue arrow icon pointing right and the text "Security Checkup".

<p>3. Select 2-Step Verification</p>	<p>Password & sign-in method</p> <p>Your password protects your account. You can also add a second layer of protection with 2-Step Verification, which sends a single-use code to your phone for you to enter when you sign in. So even if somebody manages to steal your password, it is not enough to get into your account.</p> <p>Note: To change these settings, you will need to confirm your password.</p> <p>Password Last changed: September 4, 2014 ></p> <p>2-Step Verification On since: 30 minutes ago ></p> <p>App passwords None ></p>										
<p>4. Under Backup options click SETUP in Backup codes session.</p>	<p>Backup options</p> <p>Set up at least one backup option so that you can still sign in if you don't have your phone with you.</p> <p>Backup phone Add a backup phone so you can still sign in if you lose your phone. ADD PHONE</p> <p>Backup codes These printable one-time passcodes allow you to sign in when away from your phone, like when you're traveling. SETUP</p>										
<p>5. You can DOWNLOAD or PRINT your backup codes.</p> <p><i>Note: Please store the backup codes in a safe place.</i></p> <p>The code can be used in case you don't have access to your phone.</p>	<p>Save your backup codes</p> <p>Keep these backup codes somewhere safe but accessible.</p> <table border="0"> <tr> <td><input type="checkbox"/> 4769 31</td> <td><input type="checkbox"/> 7059 14</td> </tr> <tr> <td><input type="checkbox"/> 4627 39</td> <td><input type="checkbox"/> 0686 70</td> </tr> <tr> <td><input type="checkbox"/> 2883 80</td> <td><input type="checkbox"/> 2514 84</td> </tr> <tr> <td><input type="checkbox"/> 9222 05</td> <td><input type="checkbox"/> 4882 75</td> </tr> <tr> <td><input type="checkbox"/> 0036 55</td> <td><input type="checkbox"/> 8885 81</td> </tr> </table> <p>Google</p> <ul style="list-style-type: none"> You can only use each backup code once. These codes were generated on: May 11, 2016. <p>GET NEW CODES DOWNLOAD PRINT</p>	<input type="checkbox"/> 4769 31	<input type="checkbox"/> 7059 14	<input type="checkbox"/> 4627 39	<input type="checkbox"/> 0686 70	<input type="checkbox"/> 2883 80	<input type="checkbox"/> 2514 84	<input type="checkbox"/> 9222 05	<input type="checkbox"/> 4882 75	<input type="checkbox"/> 0036 55	<input type="checkbox"/> 8885 81
<input type="checkbox"/> 4769 31	<input type="checkbox"/> 7059 14										
<input type="checkbox"/> 4627 39	<input type="checkbox"/> 0686 70										
<input type="checkbox"/> 2883 80	<input type="checkbox"/> 2514 84										
<input type="checkbox"/> 9222 05	<input type="checkbox"/> 4882 75										
<input type="checkbox"/> 0036 55	<input type="checkbox"/> 8885 81										

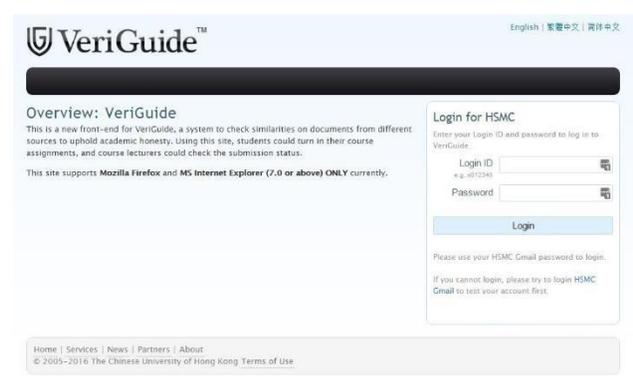
Section 6: My passwords to some applications are invalid once I setup 2 Factor Authentication, what should I do?

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 .	 A screenshot of a Google account management page. At the top, it says "This account is managed by hsmc.edu.hk." Below that is a profile picture of a brown circle with a white 'T' and the text "ro (ITSC) @hsmc.edu.hk". There are links for "Privacy" and "My Account". The "My Account" button is highlighted with a red rectangle.
2.	Click Sign-in & security .	 A screenshot of the "Sign-in & security" page in a Google account. The title "Sign-in & security" is highlighted with a red rectangle. Below the title, there is a description: "Control your password and account-access settings." and several links: "Signing in to Google", "Device activity & notifications", and "Connected apps & sites". At the bottom, there is a "Security Checkup" link.

3.	<p>Select App passwords.</p>	<p>Password & sign-in method</p> <p>Your password protects your account. You can also add a second layer of protection with 2-Step Verification, which sends a single-use code to your phone for you to enter when you sign in. So even if somebody manages to steal your password, it is not enough to get into your account.</p> <p>Note: To change these settings, you will need to confirm your password.</p> <p>Password Last changed: September 4, 2014 ></p> <hr/> <p>2-Step Verification On since: 30 minutes ago ></p> <hr/> <p>App passwords None ></p>
4.	<p>Under Select app drop down list:</p> <p>Select the appropriate type of application and devices.</p> <p>In this example, we will show how to generate password for VeriGuide.</p>	<p>You have no app passwords.</p> <p>Select app ▼ on my Select device ▼ GENERATE</p>
5.	<p>Select Other (Custom name)</p>	<p>You have no app passwords.</p> <p>Mail ▼ GENERATE</p> <p>Calendar</p> <p>Contacts</p> <p>YouTube</p> <p>Other (Custom name)</p>
6.	<p>Type "Veriguide"</p> <p>Click GENERATE</p>	<p>You have no app passwords.</p> <p>Veriguide X GENERATE</p>

<p>7.</p>	<p>a. A password will be generated.</p> <p>b. Follow the steps given.</p> <p>c. Click Done.</p> <p>d. You can repeat the steps for other Apps.</p>	<p>Generated app password</p> <p>Your app password for your device</p> <p>a cwzk seeo neoe xvaz</p> <p>How to use it</p> <p>b Go to the settings for your Google Account in the application or device you are trying to set up. Replace your password with the 16-character password shown above. Just like your normal password, this app password grants complete access to your Google Account. You won't need to remember it, so don't write it down or share it with anyone.</p> <p>c DONE</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Created</th> <th>Last used</th> <th>Access</th> </tr> </thead> <tbody> <tr> <td>Veriguide</td> <td>3:54 PM</td> <td>-</td> <td>REVOKE</td> </tr> </tbody> </table> <p>d</p> <p>Select app ▾ on my Select device ▾ GENERATE</p>	Name	Created	Last used	Access	Veriguide	3:54 PM	-	REVOKE
Name	Created	Last used	Access							
Veriguide	3:54 PM	-	REVOKE							
<p>8.</p>	<p>Use the generated password to login VeriGuide.</p>									

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

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