

TWO-STEP VERIFICATION.



Two-step verification

Recently, Hiscox has seen a large number of cyber claims where criminals have hacked into customers' email accounts. This has given them access to personal and confidential information and has also allowed them to send emails from the hacked account. Often they will send emails to the customers of the victim, asking them to make payments to bogus bank accounts.

These attacks can be incredibly costly, not only in terms of the monetary loss, but also because of the time required to handle them and the potential reputational damage they can cause.

Two-step verification (also known as two-factor authentication or multifactor authentication) is a security feature that can prevent many of these incidents by helping to secure the user login processes. In most cases, login security is reliant on a user's password, which can be compromised in a variety of ways. Two-step verification adds a second layer of security, such as a one-time pincode sent to an application or mobile device, making it much harder for hackers to gain unauthorised access to a system or platform.

While two-step verification does not protect against all potential hacks, it remains to be an incredibly important cyber security solution, especially as more and more IT services move to the cloud.

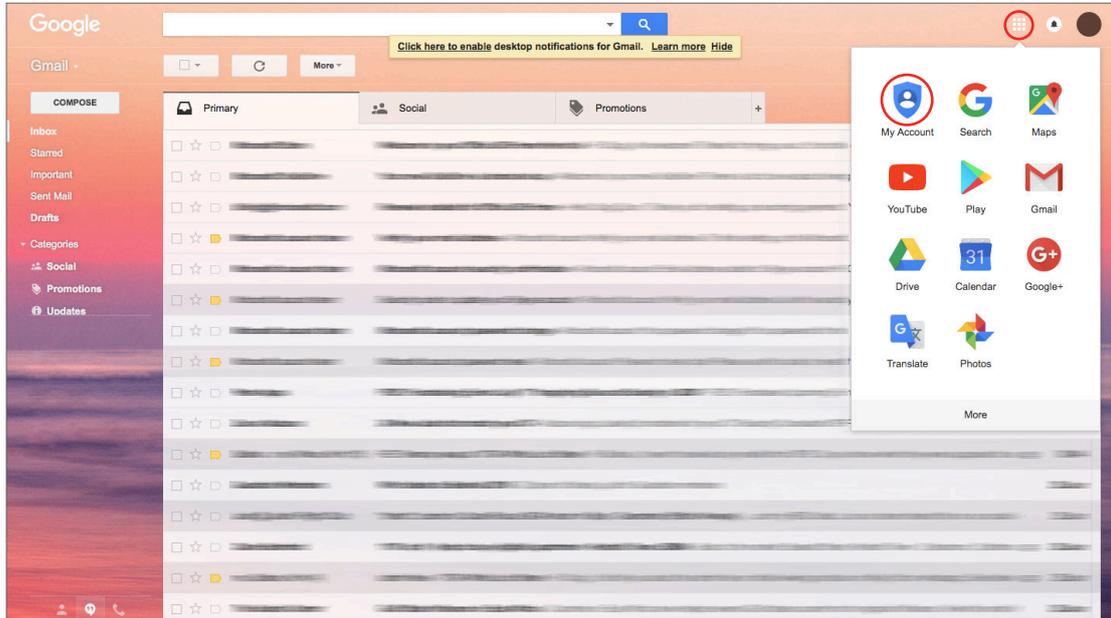
In many instances two-step verification is not turned on by default. This guide provides you with instructions on how to turn on two-step verification for Alphabet's Gsuite (including Gmail) and Microsoft's Office 365.



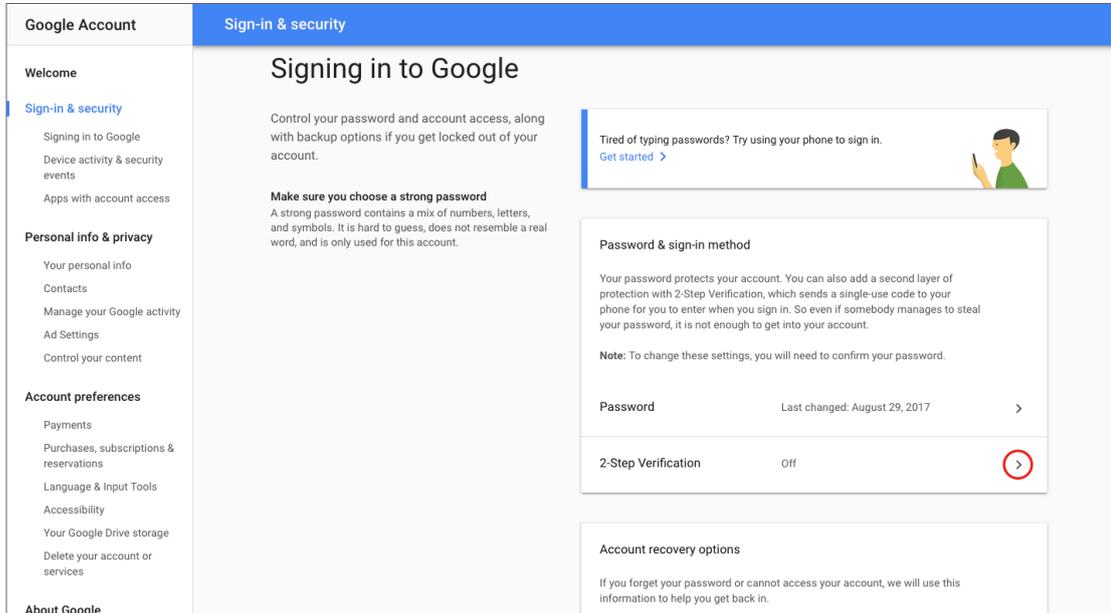
Two-step verification

Gmail/G Suite

1. Click the 3x3 square icon, then click 'My Account'.



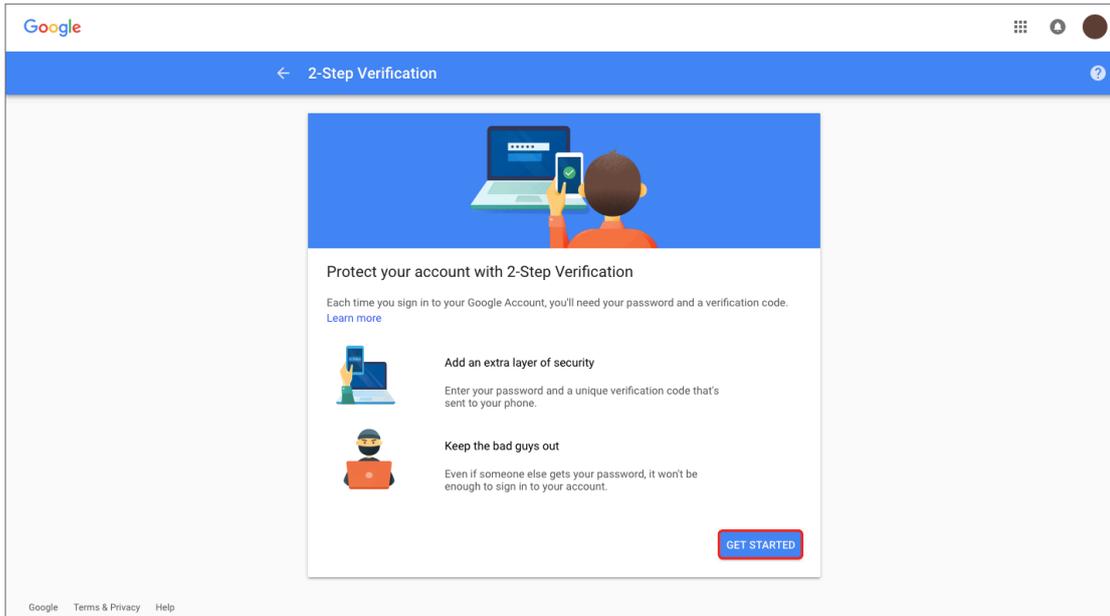
2. This shows that '2-Step Verification' is currently off. Click on the little arrow to set it up.



Two-step verification

Gmail/G Suite

3. Click on 'GET STARTED', you will then be taken to a screen where you can choose how you want to set up two-step verification. Options include either receiving a code via SMS, or getting a 'Google prompt' direct to your phone. Simply follow the steps and you'll be set.



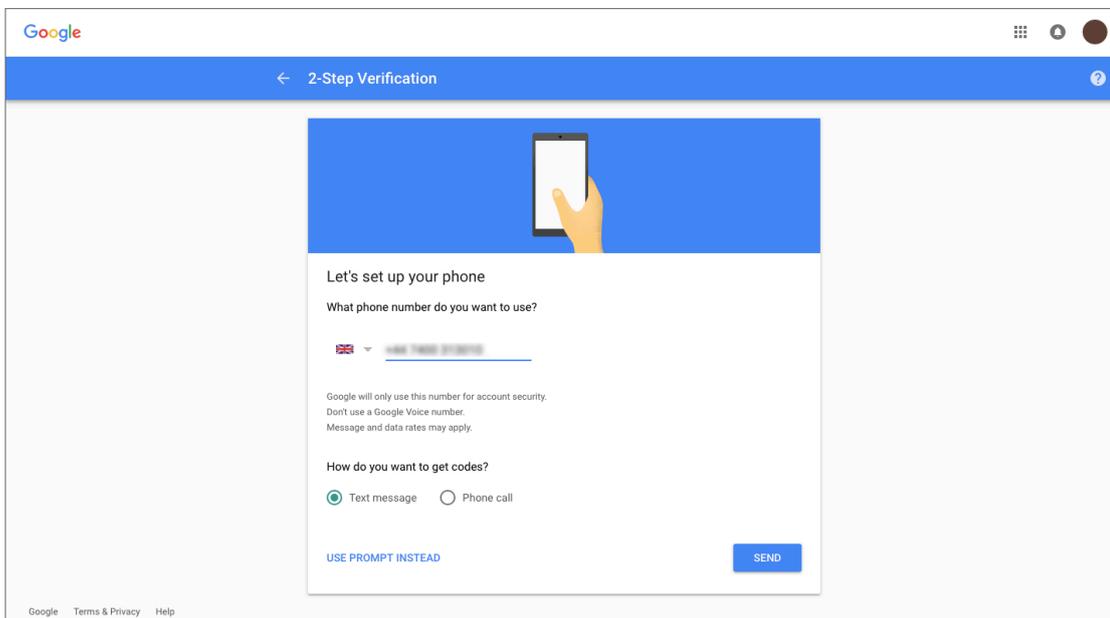
The screenshot shows the Google 2-Step Verification introduction page. At the top, there is a blue header with the Google logo on the left and navigation icons on the right. Below the header, a blue banner features an illustration of a person at a laptop with a smartphone nearby. The main content area is white and contains the following text:

Protect your account with 2-Step Verification

Each time you sign in to your Google Account, you'll need your password and a verification code. [Learn more](#)

- Add an extra layer of security**
Enter your password and a unique verification code that's sent to your phone.
- Keep the bad guys out**
Even if someone else gets your password, it won't be enough to sign in to your account.

A red "GET STARTED" button is located at the bottom right of the main content area. At the bottom of the page, there are links for "Google", "Terms & Privacy", and "Help".



The screenshot shows the Google 2-Step Verification phone setup page. It features a blue header with the Google logo and navigation icons. Below the header, a blue banner shows a hand holding a smartphone. The main content area is white and contains the following text:

Let's set up your phone

What phone number do you want to use?



Google will only use this number for account security. Don't use a Google Voice number. Message and data rates may apply.

How do you want to get codes?

Text message Phone call

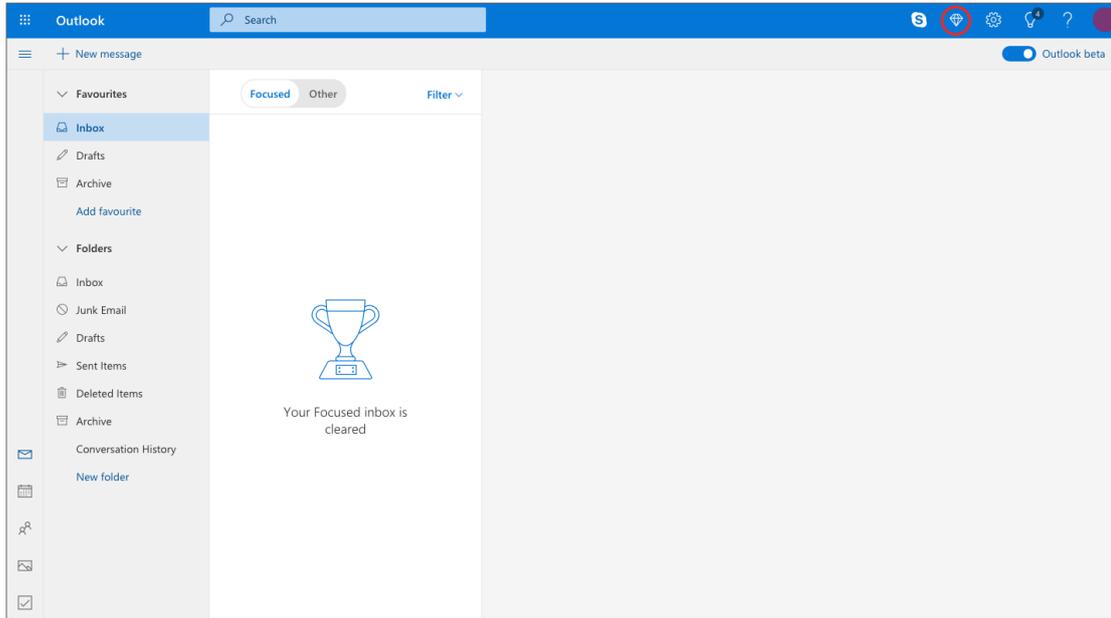
[USE PROMPT INSTEAD](#)

At the bottom of the page, there are links for "Google", "Terms & Privacy", and "Help".

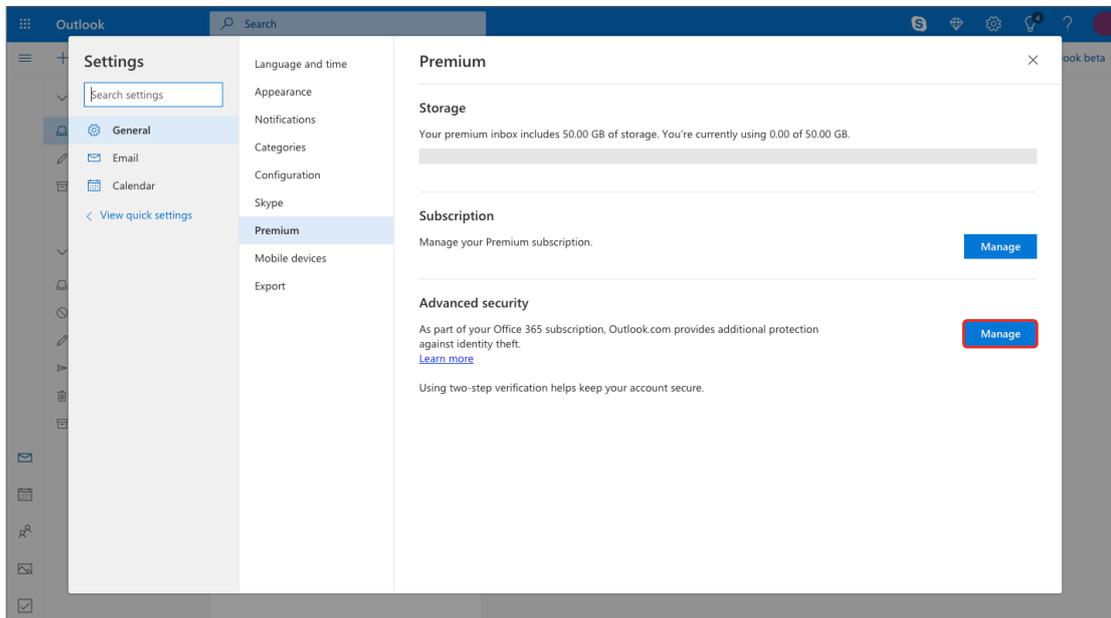
Two-step verification

Office 365

1. Log into your Office 365 account. Click on the diamond icon.



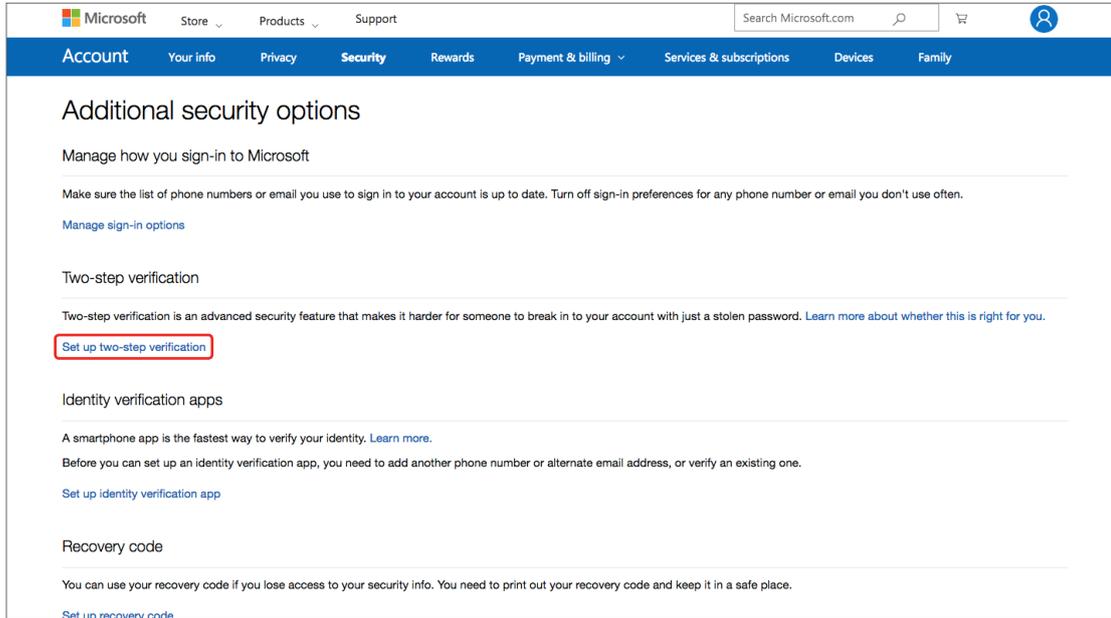
2. This will bring you to the 'Premium' page. Click on 'Manage' next to the 'Advanced security' section.



Two-step verification

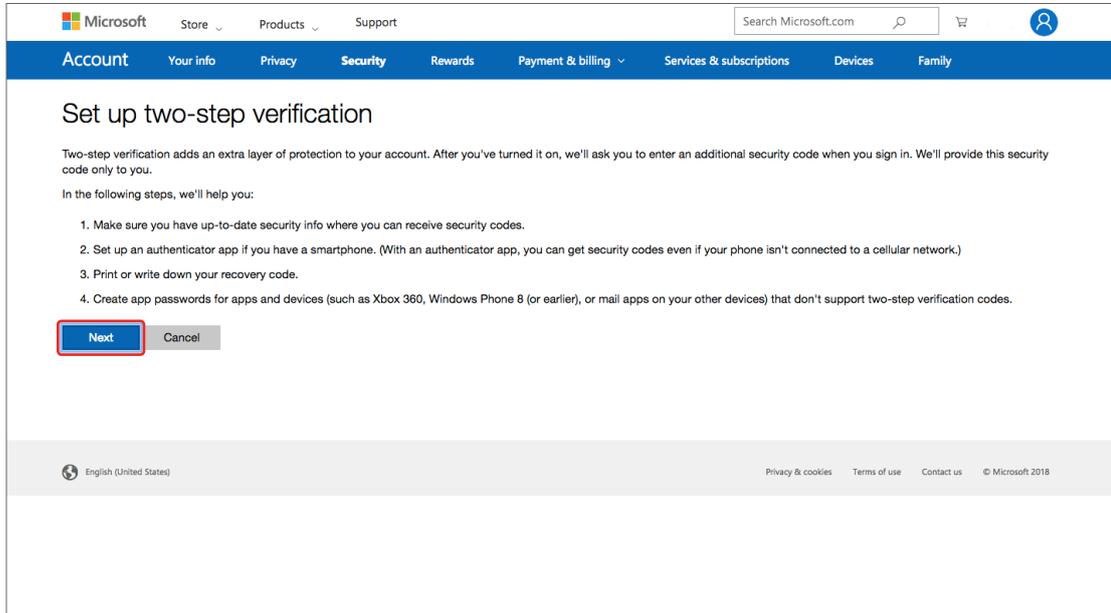
Office 365

3. Click on 'Set up two-step verification'.



The screenshot shows the Microsoft account management interface. At the top, there is a navigation bar with 'Account' selected. Below it, the 'Additional security options' section is visible. Under the 'Two-step verification' heading, the link 'Set up two-step verification' is highlighted with a red rectangular box. Other sections include 'Manage sign-in options', 'Identity verification apps', and 'Recovery code'.

4. Click 'Next'.



The screenshot shows the 'Set up two-step verification' page. It contains a list of four steps to follow. At the bottom of the page, there are two buttons: 'Next' and 'Cancel'. The 'Next' button is highlighted with a red rectangular box. The footer of the page includes the language setting 'English (United States)' and copyright information '© Microsoft 2018'.

Two-step verification

Office 365

5. Choose how you want to receive verification codes and follow the steps to complete the setup.

The screenshot shows the Microsoft account security setup page. The page title is "How else can we verify your identity?". Below the title, there is a question: "To finish setting up, we need one more way to make sure you're you. How would you like to receive a verification code?". Underneath, there is a section titled "Verify my identity with:" followed by a list of options: "An app" (selected), "A phone number", "An alternate email address", "Windows Phone", "Android", "iPhone, iPad or iPod touch", and "Other". At the bottom of the form, there are "Cancel" and "Next" buttons. The page footer includes the language "English (United States)", links for "Privacy & cookies", "Terms of use", and "Contact us", and the copyright notice "© Microsoft 2018".