

Google – Two-Factor Authentication (MFA) management

In connection with the cybersecurity measures required by our government, two-factor authentication (MFA) is now required when you log in to your college Google account.

During your first login, you will be asked to activate MFA. To start the steps, click the « Activate » button.

Step 1: Activate MFA

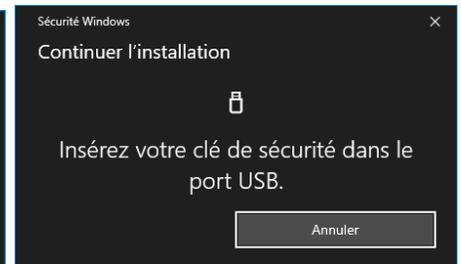
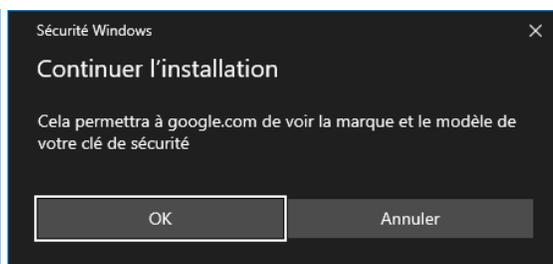
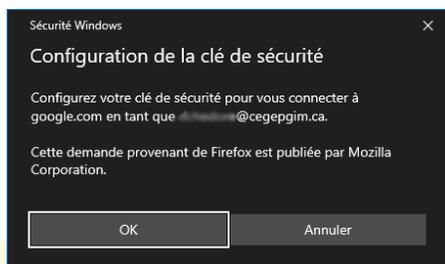
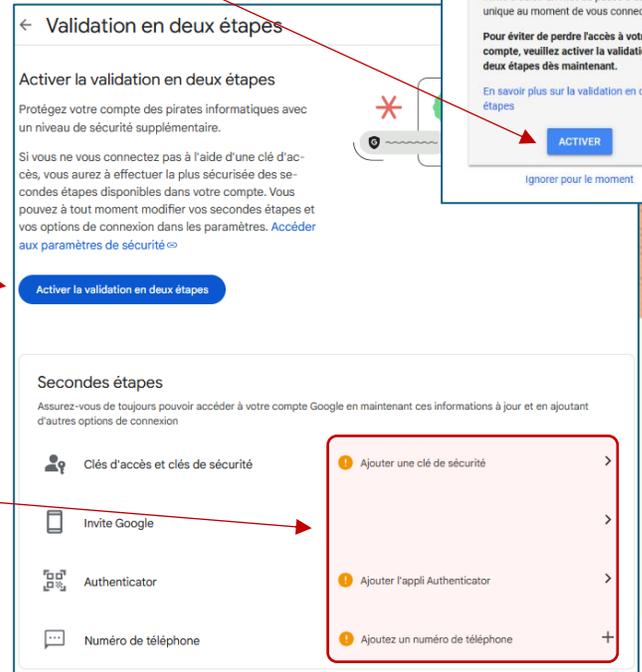
Click on « Activate your Two-factor authentication » button.

Step 2: configure MFA

There are several methods to configure two-factor authentication, and we will explain each of them. To start, choose one from the list in the second step.

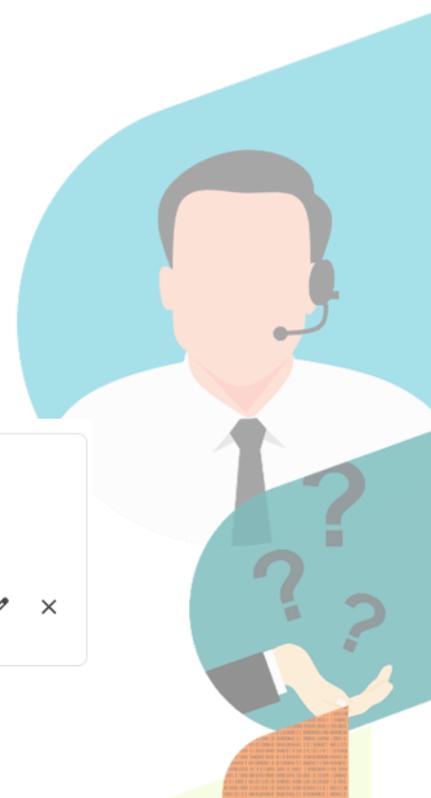
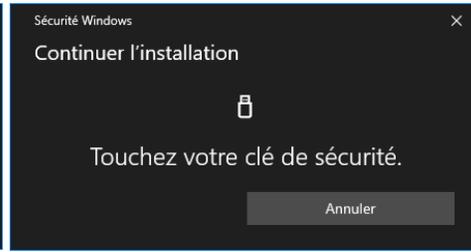
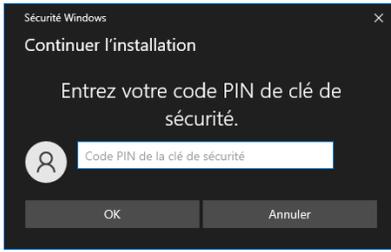
A) Access keys and security key

If you have a security key (USB) provided by the college for Microsoft MFA (M365), it can also be used for Google. To start, connect your security key to your computer and follow the steps below:



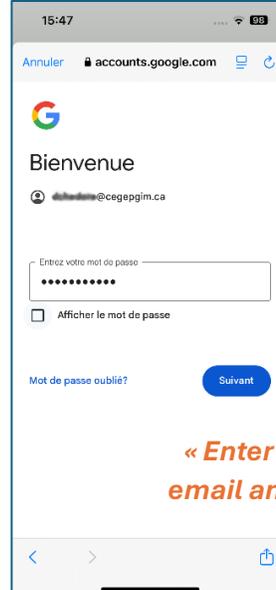
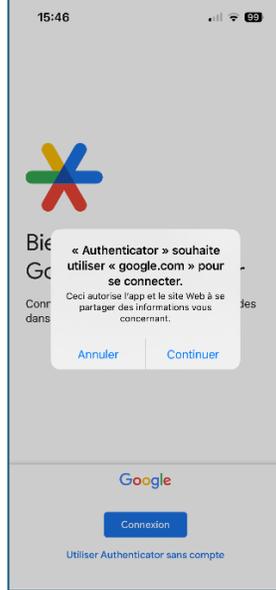
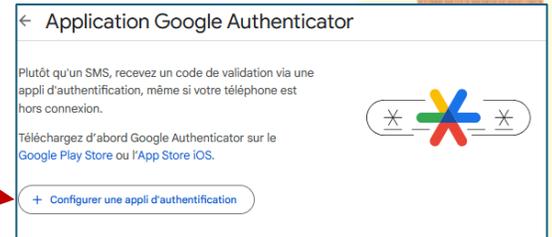
« Enter your Pin number »

« Touch your security key »



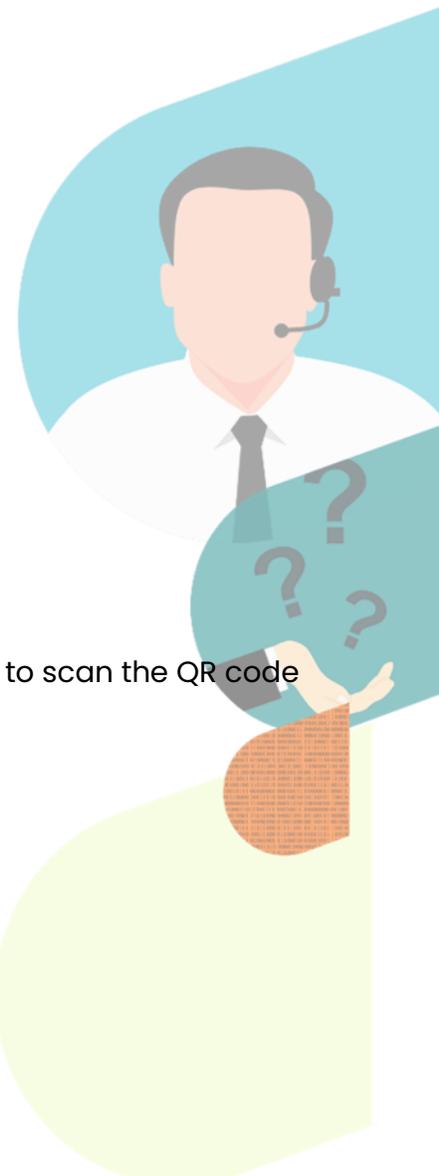
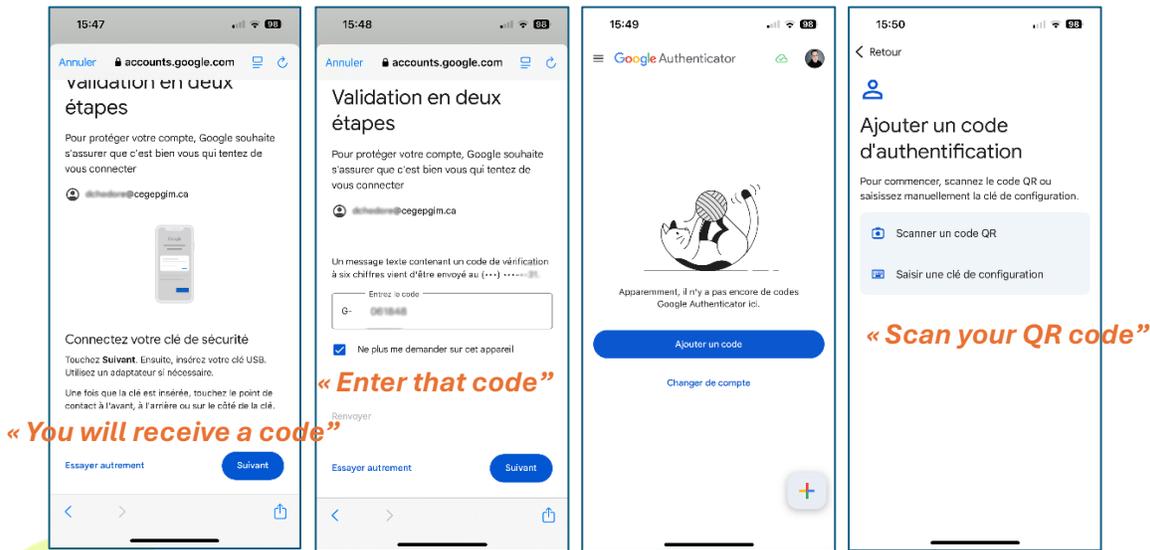
B) Authenticator Application

You can use your own mobile device (Android or Apple (IOS)) via an authentication apps called **Google Authenticator**. Install it on your device and follow the instructions:

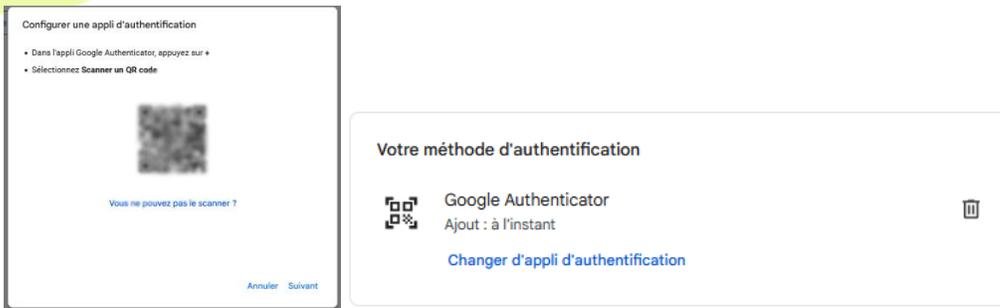


« Enter your google email and password »



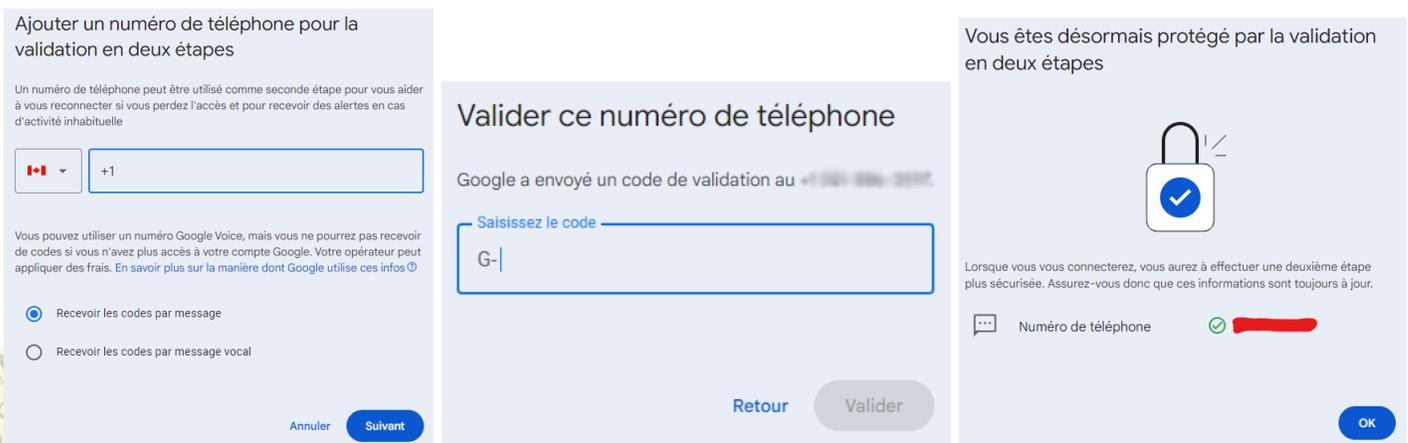


Once the application installed and configured on your mobile, you just need to scan the QR code displayed on your PC/MAC and click next.



C) Phone number

Use your mobile device to receive a SMS code.



« Enter your phone number »

« Enter the received google code via SMS and click on Validate »