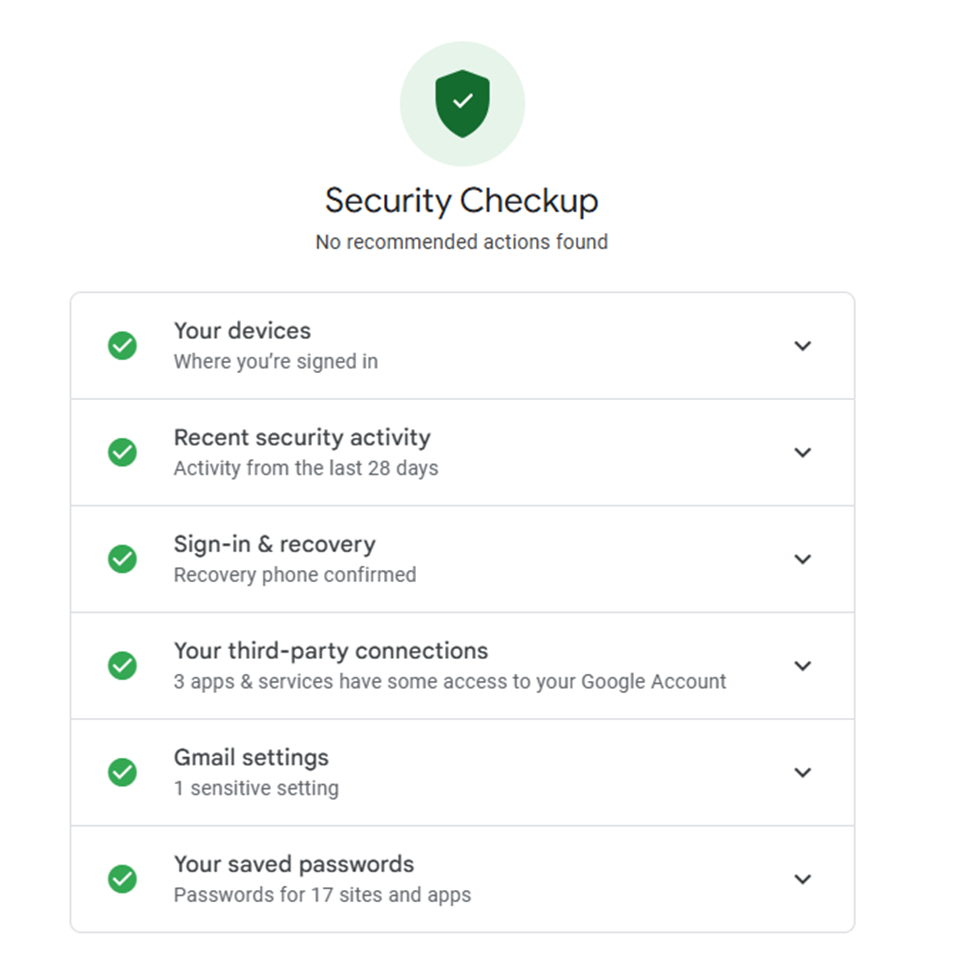
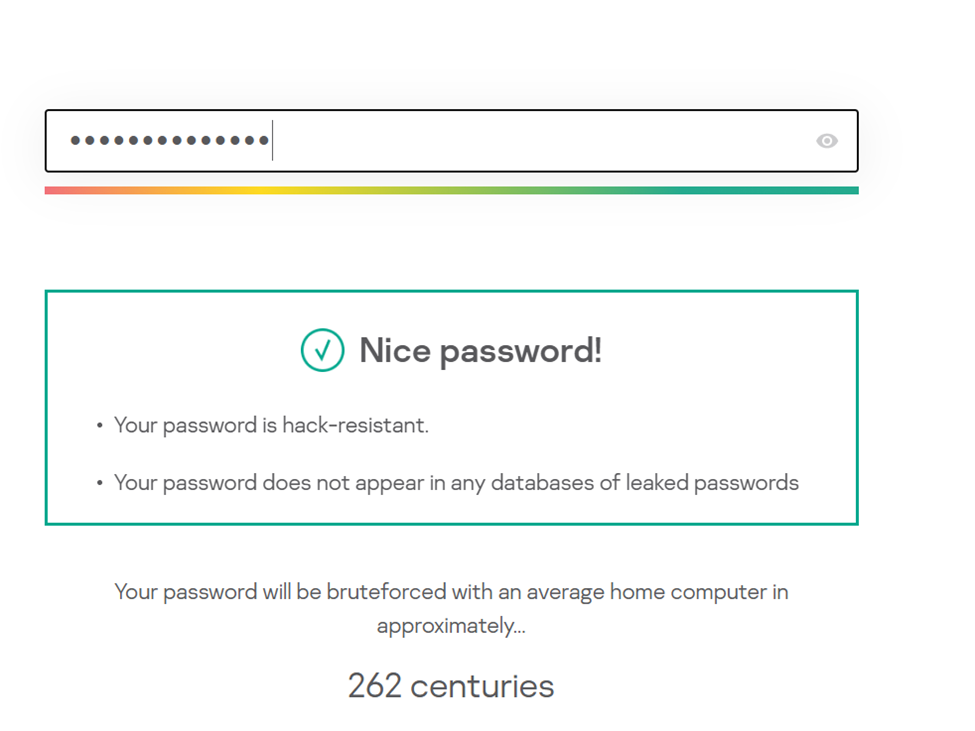
***Evaluating Email Security: Confidentiality, Integrity, and Availability***

**1. Confidentiality Analysis**

**Password Settings:** My Gmail password is quite complex and unique, as it includes a strong combination of uppercase and lowercase letters, numbers, and symbols. The password has no connection to my personal data and is not similar to any of the other passwords I use.



**- Two-Step Authentication (2FA):** My Gmail account has two-step authentication, which is linked to my personal phone number. In addition to two-step authentication, my account also has an extra email account, which serves as a backup.



**2. Integrity Analysis**

* **Protection Against Viruses and Malicious Attachments:** Attachments in the Gmail messages I send and receive are automatically scanned for virus detection by Google's security system.
* **Protection Against Cyber Attacks:** My email service, Gmail, is highly protected against cyber attacks as it uses a hundred variables to detect suspicious activities. An example of this is the two-step verification system or the Advanced Protection Program.

**- Identifying and Blocking Spam and Phishing Messages:** Emails received in the spam section have always been reported and then deleted, as have phishing emails.

**3. Availability Analysis**

* **Account and Message Accessibility:** My email service guarantees constant access to my account and messages. Additionally, there is an option to recover the account in case of password loss.
* **Backup Copies of Messages and Data:** In case of a threat, my Gmail account has regular backups made to another email address.

**4. Preparing Conclusions**

* **Conclusions on Email Security:**

Considering the analysis conducted on my Gmail account, it is highly secured against threats as the password is complex and unique, and two-factor authentication (2FA) is activated.