Before we proceed, we need to learn how to **protect our privacy**. This challenge is to emphasize the importance of protecting your secrets so that it is not being exposed to the public.

WHAT is Privacy Protection?

As you proceed to next the challenge, you'll start to use API secrets, username, and password. Privacy protection is a practice **NOT** to publish your keys to the internet.

WHY is that important?

Whoever has your secrets can use your public keys to access your account and manipulate it. For example, you do not want to have your Twitter account hijacked and have undesired images or sensitive issues posted.

Example cases:

Case I (2015) : Holloway's Twitter

Looking at the posts above, Holloway ***accidentally posted his Twitter API keys onto Github*** back in 2015. Later, someone swiped his Github repository and posted on his behalf. His Twitter account could have been abused for e-marketing purposes, like quoting a website.

He was lucky and reset the keys in time. In the future, he began to use **environment variables** to protect his keys from being published to remote repositories.

Case II (Jan 2016): Ian's AWS

Ian was performing a learning on AWS S3 server for image hosting. He wasn't aware that he needed to protect his API keys and ***committed the latest codes with his AWS API keys to Github***.

One day later, he received the above email and was charged for over **USD$2k**.

Thanks to AWS awesome services and negotiation, these heavy charges were lifted over time.

From his experience, he **strongly** emphasized that the Figaro gem is very important.

Without it, his AWS account can be abused for cloud mining.

HOW often do we make this mistake?

Very often. Very easy. Almost not realizing until you're a victim.

Example:

When we use action-mailer for sending emails, after reading through documentation and some trial and errors, the end result from configuration code in `config/development.rb` looks something like this:

```
config.action_mailer.delivery_method = :smtp
config.action_mailer.default_url_options = { host: 'localhost:3000' }
config.action_mailer.perform_deliveries = true
config.action_mailer.raise_delivery_errors = true
config.action_mailer.smtp_settings = {
  address:              "smtp.gmail.com",
  port:                 587,
  domain:               "gmail.com",
  user_name:            "test@gmail.com",
  password:             "bracalula",
  authentication:       :plain,
  enable_starttls_auto:  true
}
```

Can you see that the **user_name** and **password** are being exposed? Without careful refactoring, `git commit` can publish them onto a public Github repository.

IMPORTANT NOTE:

As long as you push to the Github public repository, regardless of branches, you're exposed.

How to Prevent?

There are 2 ways of doing things but in this challenge, we're going to use the Figaro gem. We're going to use it in your PairBnB app to ensure that your secrets will not be exposed.

Go through the Figaro gem documentation. From the documentation, you'll see :

1. Include the Figaro gem in your **gemfile** and run `bundle install`
    - `gem "figaro"`
2. Install Figaro into your app by running the Figaro installation command
    - `bundle exec figaro install`
3. Check the files
    - Check if you have an **application.yml** file - this is where you will be storing your secret keys.
    - **IMPORTANT**: Check if **.gitignore** file includes `config/application.yml` - this will ensure that your **application.yml**is **NOT** tracked by git!
4. Commit the changes as "installed Figaro Gem".

Once done, have your partner or peers review the code.