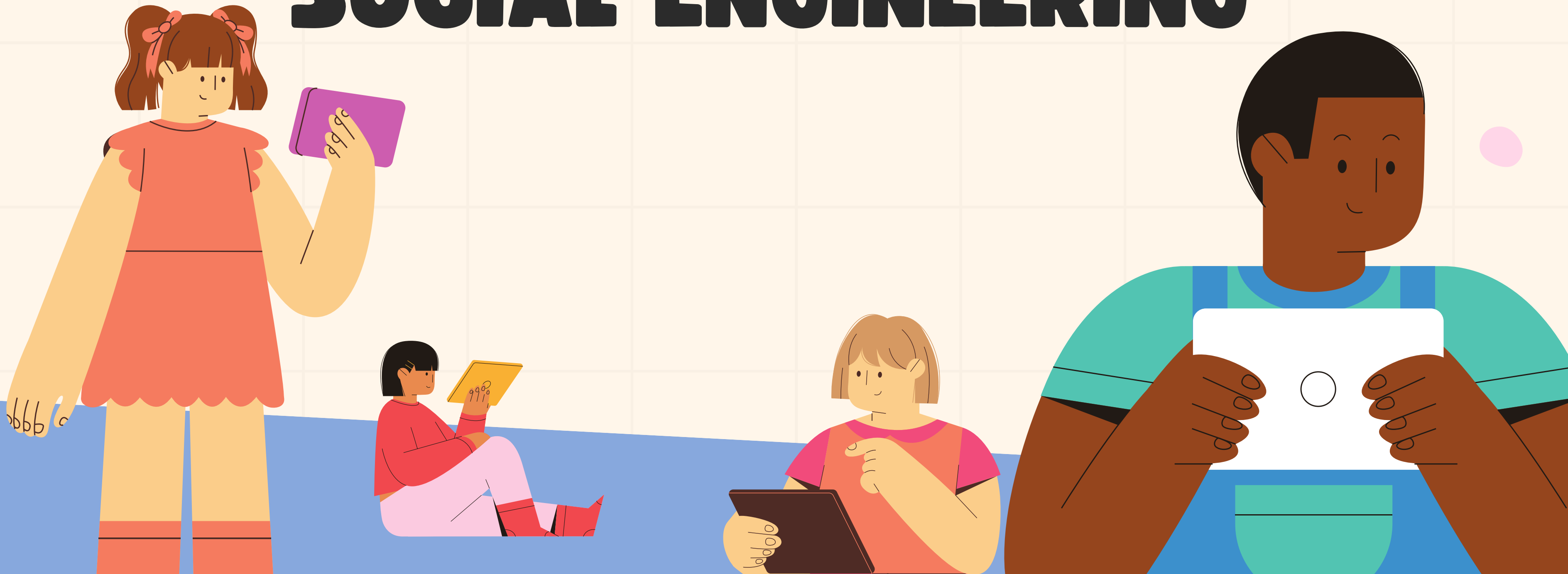
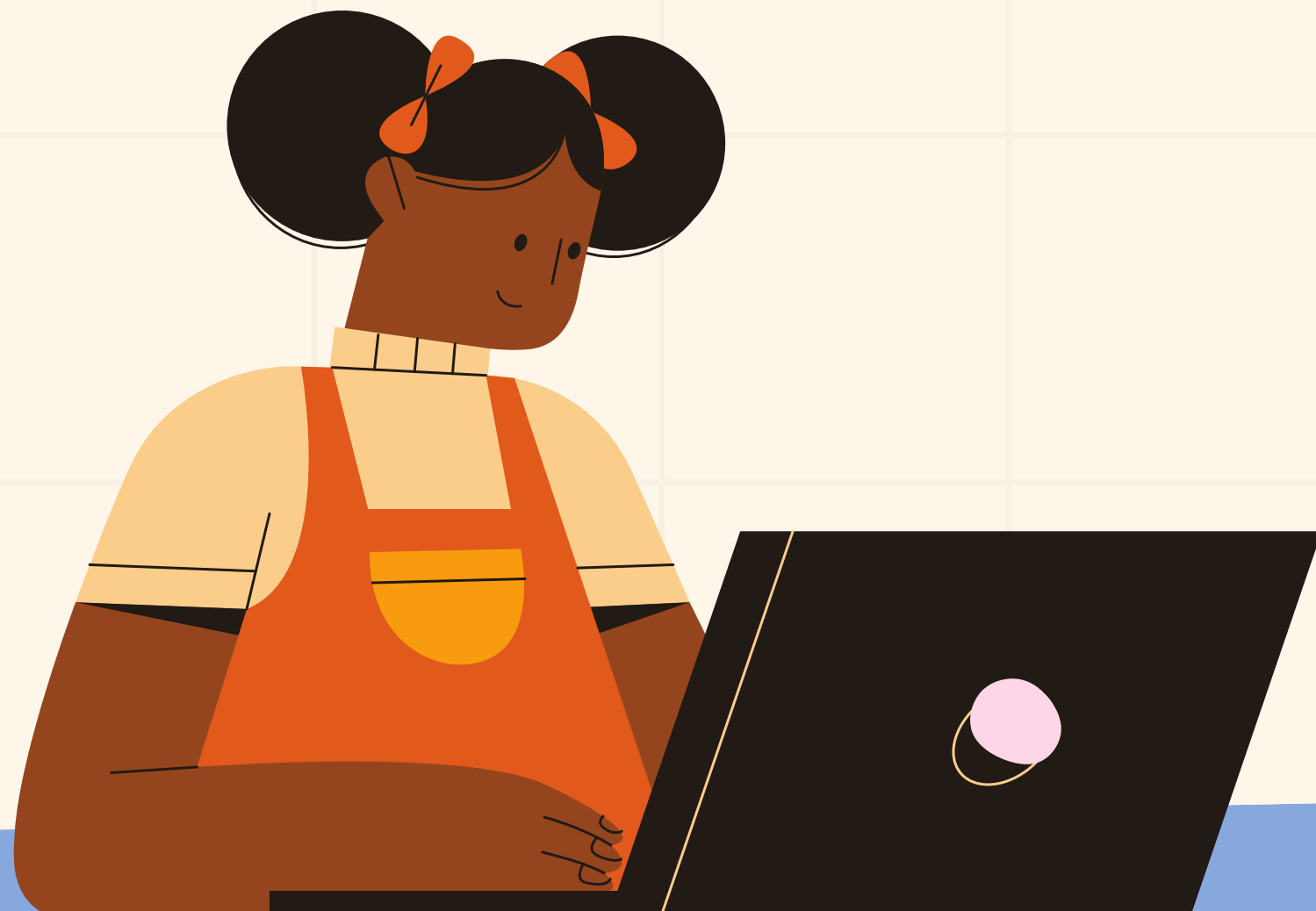


INTRODUCTION TO SOCIAL ENGINEERING



WHAT IS SOCIAL ENGINEERING?



- Imagine someone tries to trick you into sharing personal information, like your password, address, or phone number, without you realizing it. This is called social engineering.
- In the world of the internet, bad people (called "hackers") use social engineering to manipulate and fool others into giving away sensitive information. They might pretend to be someone you trust, like a friend, teacher, or even a company, to get you to share details that you shouldn't.

WHY IS SOCIAL ENGINEERING DANGEROUS?

Social engineering can lead to a lot of problems like:

- Someone stealing your personal information.**
- Losing money or your identity.**
- Someone taking control of your online account**

WHAT IS SOCIAL ENGINEERING AND HOW DOES IT WORK?

- Social Engineering is when someone tricks you into giving away personal information or access to something you own.
- The person using social engineering doesn't use fancy technology—they rely on tricking or manipulating you to get what they want.



HOW DOES SOCIAL ENGINEERING WORK?

Social engineers know how to make you feel comfortable or trusting.

They may seem friendly, use fear tactics, or pretend to be someone you know

They often ask for personal information, such as your password, phone number, or address.



Hey! I can't log into my account, can you send me the password?"

1

REAL-WORLD EXAMPLE

- Imagine you get a message from "your friend" saying they've locked themselves out of their account and need your help with the password.
- But guess what? It's not your friend! It's someone trying to trick you.



WHY DO PEOPLE USE SOCIAL ENGINEERING?

- Hackers use social engineering because it's easier than breaking into a computer system.
- People are often the weakest link in security—hackers know how to trick us into giving away information.

