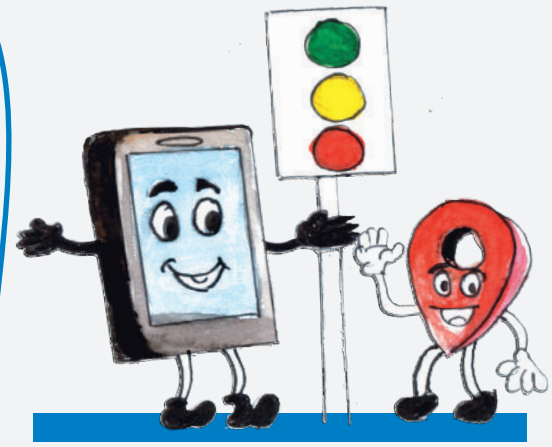
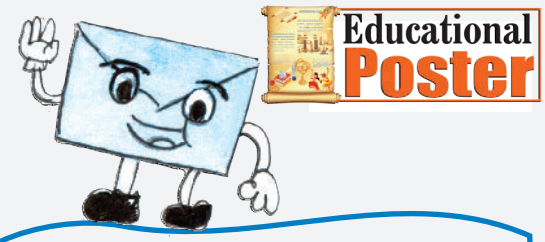
Illustrations: Akshita Rathore, AIS MV, X C

Making A Newspaper Contest AIS MV 2025-26

What really happens upon tapping 'install'? It's like inviting unknown guests to your house, letting them wander about some rooms, and leaving a few doors unlocked. So, Nandini Rastogi, AIS MV, XII D, brings to you a guide to unravel the verbosity of 'Terms & Conditions'.

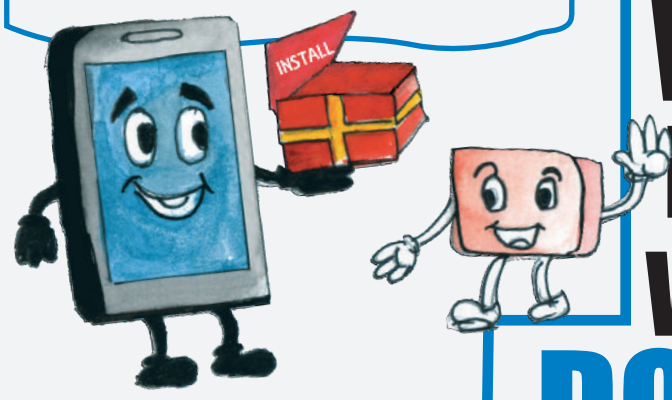
WHAT HAPPENS WHEN YOU DOWNLOAD AN APP?





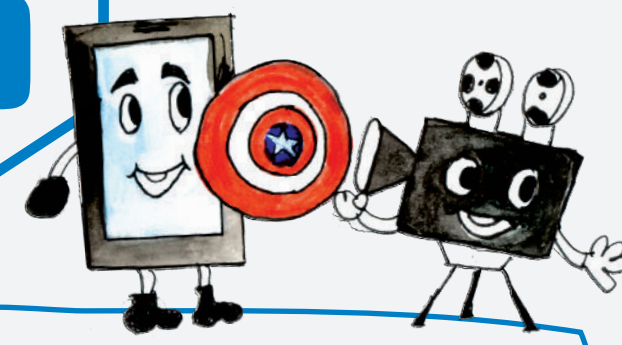
1 Behind the install button

What you do: Tap 'install' and a new icon is added to your home screen.
What really happens: The app has now become a part of your phone's storage, bringing with it all files necessary to run the app in the form of codes and scripts.
Why it matters: The app connects to your device's location, camera, microphone, and more. Its access is neither specified nor controlled. Most media and messaging apps keep running in the background.



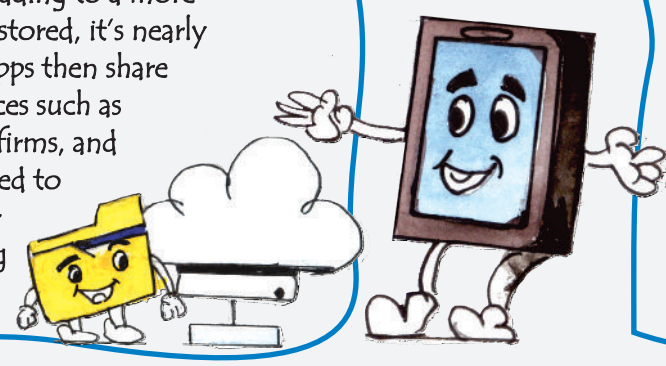
2 Tap to agree… to what?

What you do: Tap 'Allow' on access to camera, location, contacts et cetera.
What really happens: The app gets access to your contacts, call logs, files — confidential or not, and even your real time movements — both digital and physical.
Why it matters: Once these permissions are granted, the app will have unrestricted access to your data. Even when you select 'Allow only while using the app' the app still collects and stores data in the background. And the catch is, some of these permissions are non-negotiable; meaning that unless you grant them, the app won't work.



3 The data domino effect

What you do: Open the app and start using it.
What really happens: The app will also connect to internet servers and communicate with other softwares through Application Programming Interface (API).
Why it matters: The servers store your data for various purposes, making it accessible to authorised users i.e. the apps, leading to a more efficient user experience. Once stored, it's nearly impossible to erase this data. Apps then share your data with third party sources such as advertising networks, analytics firms, and cloud services, which is combined to create your digital profile. Your data may now be resold starting a whole new chain of data use.



4 Outsmarting the app trap

What you do: Review app settings and permissions.
What really happens: Limits apps' access to data.
Why it matters: By taking small, cautious steps such as granting limited permissions, using privacy tools, and curtailing background activity you ensure that your guest has access only to the information it needs. By proactively protecting your data you reduce risk of identity theft and unauthorised access.

Page editor: Akshita Rathore, AIS Mayur Vihar, X C