All About Apps
We’ll cover...

● What’s an app?
● What are app permissions?
● What do companies gain by getting your permission?
● Typical permissions requested by apps
● How to check up on apps already on your phone
● App safety tips
What’s an “app?”

- A mobile application, also referred to as a mobile app or simply an app, is a software application designed to run on a mobile device such as a phone, tablet, or watch.

- Every program on your phone is an app!
What are app permissions?

- The purpose of a *permission* is to protect the privacy of a user.

- Apps must request permission to access sensitive user data (such as contacts and text messages), as well as certain system features (such as camera and internet).

- Depending on the feature, the system might grant the permission automatically or might prompt the user to approve the request.
Why do apps need to access data on our devices?

- **Functionality** – e.g. access to the camera is required by Snapchat; Google Maps requires location data
- **Security** – e.g. personal data is required to confirm the user’s identity
- **Data mining** – information on the app’s users is mined in order to facilitate ongoing product optimisation, or for marketing purposes (not always a good thing…)

**Permissions by themselves are harmless and in THEORY provide users a good mobile experience...**
When does access cross the line?

- Some apps ask for a host of permissions to access data and functions they don’t require

- The key lies in identifying the purpose of the app and questioning what seem to be unnecessary requests

- If an app is free, it’s important to ask how the developers are making their money (Ads? Premium service upgrade?)

- If it’s difficult to figure how an app you use is making money, it is highly likely that you as a user are its source of monetization
Typical permissions requested by apps

Modify, delete and read storage: Gives an app permission to access the storage on your device in order to save and edit files.

Full network access: Most apps require some kind of Internet access, whether it's for software updates, syncing or retrieving data from online resources.

Read and send text messages: This permission can also be used to automatically scan your incoming texts for authorization codes. Make sure that if an app is asking for this, it has a clear use for it.

Read your contacts: The ability to share content with your friends in some way is often the underlying purpose.
**iPhone/iPad:** Go to Settings, scroll down to your apps, then click on an app to review allowed access.
How to check apps already on your phone: Android

Android smartphones and tablets: Go to Settings-->Apps, then tap the app you want to check. Then, scroll down the app’s information screen towards the Permissions section and read about the permission groups the app has.
Follow these tips to stay safe:

- **Research the app and its developer** — A web search can reveal important info.

- **Read the reviews** — Users’ comments can provide valuable insights.

- **Understand permissions and access rights** — Understand the risks before you grant access to device data, features, and functionality.

- **Avoid risky apps** — Do not download childish apps, risqué apps, and those that deliver illegal or pirated content.
Mobile Device Makeover

Thursday, October 3
10-10:30am
2-2:30pm

Coming up next…

- Treat devices like cash
- Use a lock on every device
- Back up your data
- Keep private conversations private
- Make trusted connections