

LIVE Weekly Training

Ghost Phone & Tablet

Class #6

App Stores, Text Messaging, and Printing/Scanning

Introduction

I'm going to try to keep this to just 60 minutes. The content we're going to cover today includes:

1. App stores - How to install and uninstall apps and the different ways to get applications
2. Text messaging - Clearing up confusion about messaging and why some features work differently
3. Printing and scanning - Quick tips for these functions

I'll be sharing the screen of a Pixel device (I think this is a Pixel 6). I'll try to address questions in the chat as we go along.

App Stores

F-Droid

What really is F-Droid? There's a team of developers that manage this app store. People who create and develop apps can submit them to go into the F-Droid app store. Mostly all of the apps that people submit here are from independent developers, though there are some larger teams and companies. They're all open source.

A key question people ask is: "Is this app safe?" The answer is you have to do your own due diligence. If the app is something we have installed on the device already (the list of all the other apps that you see here on the device), we have vetted them to the best of our knowledge. We believe those apps are safe, which is why we put them on the phone. Just because something is in F-Droid or just because you hear something is "open source" does not mean that it's necessarily safe.

Think of it this way: It's like going to a car dealership. The dealer says, "Hey, check out this car." You're looking at the car and think it looks good. You trust the dealership, but it's wise to take it for a test drive. It's wise to open up the hood, look, and bring someone with you (hopefully someone who knows what they're looking at) who can check the engine and kick the tires.

Checking App Safety

When evaluating an app, look at:

1. **Permissions:** On the bottom, you'll see something that says "permissions." The ideal scenario is "no permissions." This means when you open the app (like Open Sudoku), it's not going to ask you for access to your contacts, access to your WiFi - it doesn't need anything. It's just going to run independently.
2. **Updates:** Look for versions and when the app was last updated. For example, if you see it was updated January 26, 2025 - that's pretty recent. You know the team of developers working on this app are doing constant updates.
3. **Website:** Many apps have websites where you can learn more about the developers and verify that the company is legitimate.

App Example: Quick SMS vs. QK SMS

One of the apps you probably have on your phone right now is Quick SMS. Previously we used QK SMS, but the team at QK SMS retired the project, and a new team of developers (including some from the old project) started Quick SMS. On all new devices we're pushing out Quick SMS, which is a better alternative to the stock

messaging app with more functionality.

Checking App Info and Permissions

If you want to see an app's permissions:

- Hard press an app
- Go to "App Info"
- There you can turn notifications on/off
- You can change what permissions it has
- You can access storage and cache settings (useful if you want to clear data)

GitHub

GitHub is a repository - think of it like a massive library. If you're a developer or team with an application to share, you can put it into GitHub. For example, I have open here Antenna Pod, which is one of the apps on your device.

Through GitHub, you can:

- Look at the whole project
- See all the code
- Learn about the app and the team
- Get all kinds of information

For open source projects, it's almost guaranteed they'll have a page in GitHub. You can search for the project or app and find it.

Aurora Store

Aurora works similarly to the Android app store. When you open it, don't click "Google" for login (unless you want Google to know what applications you're downloading). Click "anonymous" instead.

With Aurora, you can see app permissions, data safety information, and privacy details. For example, looking at Snapchat:

- 71 permissions (compared to Sudoku with zero)
- Collects app info, performance data, location, device IDs, contacts, financial info, web browsing history, personal info, audio messages
- Uses Google Firebase (which is bad news - it likely needs Google Play Services and feeds Google a lot of info)

Downloading Apps Directly from Websites

You can also download apps directly from websites if it's a trusted application. For example, with Meetin (an alternative web conferencing application for business):

1. Go to their website
2. Click download
3. Your browser will warn "it might be harmful" - this is a standard warning
4. Choose to download anyway if you trust the source
5. Install from your downloads

Note that apps downloaded this way may need to be updated through their original source rather than through an app store.

App Updates

To check for updates:

- In F-Droid, go to the "Updates" tab on the bottom
- In Aurora Store, also go to "Updates"

It's good to update your apps regularly, and uninstall apps you don't use (if they're not stock apps).

Sandboxing Apps

If you're worried about an app requesting information you don't want to share, you have options:

1. **Permission Control:** Hard press the app, go to App Info, go to Permissions, and turn off permissions it doesn't need. For example, if Aurora Store wants access to sensors, you can turn it off if you don't think it needs that.
2. **Create a Separate User Account:** This is like partitioning the device so you have two totally separate Graphene OS installs going on at the same time. Apps in different user accounts can't talk to each other.
3. **Set Up Private Spaces:** Go to Settings > Security and Privacy > Private Space. This further sandboxes applications and prevents them from accessing anything else on your device.

Text Messaging

With text messages, especially with iPhone, understand that Apple controls the entire experience. All text messages clear through Apple servers. If you're going iPhone to iPhone using iMessage, what you're seeing is on the Apple server, which is why they can send much larger files.

If you're not using iPhone and iMessage, or not using Google messaging, you're limited by the traditional text messaging service controlled by carriers (Verizon, AT&T, T-Mobile), which restrict how large of a file you can send/receive.

This is why many people say "I can't send/receive videos like I used to with my iPhone." The workaround is to get friends and family to use a different service like Signal, Telegram, or Session.

Quick SMS or QK SMS won't make that experience any different - they're just interfaces for managing text messages, not services with servers in the cloud.

Printing and Scanning

If you have a printer or scanner and want to print from your phone:

1. Download the app for your printer brand (HP, Brother, Canon, etc.)
2. Make sure your printer and phone are on the same WiFi network

For scanning, remember that a scanner is just taking a picture of a document. You can simply:

1. Use your phone camera to take pictures of documents
2. Take multiple pictures for multiple pages
3. If needed, use apps to convert images to PDF

This approach can save a lot of time and frustration.

Affiliate Program

Our affiliate program is now live. If you want to promote what we're doing:

- You can make 10% on laptops, 15% on phones, and up to 40% on training and support services
- To join, log into your account on the website and go to the affiliate section
- You can track links, conversions, commissions, etc.
- For those with large audiences, we can work on creating discount codes