Choosing an Email App

As with text messaging, there are several different email apps you can use on your smartphone. Most carriers ship their phones with two primary email apps—Email and Gmail. The Email app can be configured to work with a variety of email accounts, including both web-based and traditional IMAP and POP3 accounts. The Gmail app is designed to work exclusively with Google's popular web-based email service. Depending on what types of email accounts you have, you might find yourself working with both of these apps.

There are other email apps available, too, in the Google Play Store. These are all good apps, but don't really offer much more in the way of functionality than what you find with the preinstalled Email and Gmail apps. Still, you might like the way one or the other of these apps work, so they're worth checking out. Some of the more popular ones are listed in the following table.

App	Description	Price
MailDroid	Works with IMAP and POP3 email	Free
Microsoft Outlook	The official Microsoft Outlook app for Android devices; works with Outlook.com, Microsoft Exchange, Office 365, and most web-based email services	Free
my Secure Mail	More secure solution for IMAP and POP3 email	Free
myMail	Works with most web-based email services, as well as IMAP and POP3 services	Free
Yahoo Mail	Works with the Yahoo! Mail web-based email service	Free

>>>Go Further

IMAP, POP3, AND WEB-BASED EMAIL

Web-based email services, such as Gmail and Yahoo! Mail, store your email messages online, and you access them from a designated app or from any web browser on any computer or device. IMAP (Internet Message Access Protocol) and POP3 (Post Office Protocol 3) email services, on the other hand, download all your messages to your designated phone or computer, and thus aren't easily accessible from other devices.

Most corporate and work email is IMAP/POP3, as is (probably) the email assigned to you by your Internet service provider. It's the traditional form of email used for the past several decades.

That said, most users today prefer web-based email for its convenience and usability across multiple devices. Samsung's Email app works with both web-based and IMAP/POP3 email accounts—and with multiple accounts. So if you have a web-based account with Gmail or Yahoo! Mail, as well as an IMAP/POP3 account through work, you can use this one app to access all your messages from both accounts.

It's Not All Good

Dealing with Unwanted Spam

If you're like most people, you get a fair amount of unsolicited, unauthorized, and unwanted email messages in your inbox—in other words, *spam*. These spam messages are the online equivalent of the junk mail you receive in your postal mailbox and are a huge problem.

Although it's probably impossible to do away with 100% of the spam you receive (you can't completely stop junk mail, either), most email apps and services include some sort of spam filtering. In Samsung's Mail app, potential spam messages are identified and sent to a special Spam folder for each account.

You can view the contents of the Spam folder by tapping the Inbox down arrow a scrolling to the Accounts section, selecting an account, and then tapping Spam. It's a good idea to check your Spam folders from time to time; occasionally legitimate messages end up there by mistake.

It's Not All Good

Protecting Yourself from Phishing Attempts

Phishing is a technique used by online scam artists to steal your identity by tricking you into disclosing valuable personal information, such as passwords, credit card numbers, and other financial data, typically via email. If you're not careful, you can mistake a phishing email for a real one—and open yourself up to identity theft.

A phishing scam typically starts with a phony email message that appears to be from a legitimate source, such as your bank, eBay, PayPal, or another official institution. When you click the link in the phishing email, you're taken to a fake website masquerading as the real site, complete with logos and official-looking text. You're encouraged to enter your personal information into the forms on the web page; when you do so, your information is sent to the scammer, and you're now a victim of identity theft. When your data falls into the hands of criminals, it can be used to hack into your online accounts, make unauthorized charges on your credit card, and maybe even drain your bank account.

The best way to guard against phishing scams is to use common sense. That is, you should never click through a link in an email message that asks for any type of personal information—whether that be your bank account number or eBay password. Even if the email looks official, it probably isn't; legitimate institutions and websites never include this kind of link in their official messages. Instead, access your personal information only by using your web browser to go directly to the website in question.

So remember, don't click through suspicious email links, and don't give out your personal information and passwords unless you're sure you're dealing with an official (and not just an official-looking) site!