# The Problem with Mobile Phones

Mobile phones are basically insecure:

1. Information sent from a mobile phone is vulnerable
2. Information stored on a mobile phone is vulnerable
3. Mobile phones give out information about their location
4. Mobile phones can be used to eavesdrop

Not only can the company that runs your mobile phone network intercept your calls and text messages (if unencrypted), and monitor your location ? many companies also choose, or are required, to share this information with governments if asked.

Here, we'll describe some of vulnerabilities you need to be aware of when using mobile phones of any type, and recommend ways you can stay a bit safer.

## 1. Information sent from a mobile phone is vulnerable

Each mobile phone provider has full access to all text and voice messages sent via its network. Other people who are close to the mobile phone can also tap calls and text messages using inexpensive equipment. The safest practice is to assume that traditional calls and SMS text messages have not been secured against eavesdropping or recording.

See the [Making a Call](umbrella://lesson/making-a-call) and [Sending a Message](umbrella://lesson/sending-a-message) Lessons to learn how to text and talk more securely. The situation can be different when you are using secure communications apps to communicate (whether by voice or text), because these apps can apply end-to-end encryption to protect your communications.

If you absolutely have to communicate sensitive information using regular phone or SMS, try to use an inconspicuous code for sensitive words that you and your contact have agreed on before hand.

## 2. Information stored on a mobile phone is vulnerable

Mobile phones can store all sorts of data: call history, text messages sent and received, address books, photos, video clips, text files. These may reveal your network of contacts, and personal information about you and your colleagues.

Some phones have encryption options available which should be applied. If you have an Android phone this can be done in Settings -> Personal -> Security -> Encryption.

Do not store confidential files and photos on your mobile phone. Move them, as soon as you can, to a safe location, as outlined in the [Backing Up](umbrella://lesson/backing-up) lesson. Frequently erase your phone call records, messages, address book entries, photos, etc. Learn more about safe deleting in the [Deleting lesson](umbrella://lesson/safely-deleting).

Protect your SIM card and additional memory card (if your phone has one), as they may contain sensitive information. For example, make sure that you don?t leave them at the repair shop when your phone is being serviced. Use only trusted phone dealers and repair shops if possible. When selling, handing on or disposing of your phone make sure all information is deleted. Never hand on or sell SIM cards or memory cards ? you should physically destroy them.

When capturing pictures or video it is important to be careful of privacy and safety of those pictured. For example, if you take photos or record video of a sensitive event, it might be dangerous to you or to those who appear in the recordings if your phone fell into the wrong hands. [Guardian Project](https://guardianproject.info/) has created an open-source app called [ObscuraCam](http://lesson/obscuracam) to detect/select faces on photos and blur them. Obscuracam also deletes the original photos and if you have set up a server to upload the captured media, it provides an easy way to upload it.

Metadata such as phone identity and location are also captured on photos and videos. In some instances, such information is really important to have to prove the credibility of images and video so that they could be used as evidence in courts of law. At other times metadata can put you or others at risk. The Guardian Project has made a plugin tool for ObscuraCam called InformaCam that allows you to store a version of the image/video with metadata while also creating a redacted version without any sensitive data that can safely be shared on social media.

## 3. Phones give out information about their location

The greatest privacy threat from mobile phones is the way that they announce your location all day and all night through the signals they broadcast. Every mobile phone automatically and regularly informs the phone service provider where it is at that moment. Only if a phone is switched off or without signal will it be prevented to send out such signals.

If you have a smartphone your location can also be tracked from apps, WI-FI or Bluetooth. Many apps use your GPS location to help them provide services, or just to collect data for their own use. You should only turn on your location when you need it and make sure that you only give location permissions to apps that you trust and that have a good reason to know where you are.

In each case, location tracking is not only about finding where someone is right now. It can also be about answering questions about people's historical activities and also about their beliefs, participation in events, and personal relationships. For example, location tracking could be used to try to find out whether certain people are in a romantic relationship, to find out who attended a particular meeting or who was at a particular protest, or to try and identify a journalist's confidential source.

## 4. Phones can be used to eavesdrop on the owner

If a phone is infected with the right malware it is possible for its microphone or camera to be turned on remotely allowing somebody to hear or see whatever is happening in the same room as the phone. This may happen even when the phone appears to be switched off.

As a result, people having a sensitive meeting or conversation are sometimes told to turn off their phones off and take out the battery. While this will make sure your phone can?t be used to listen in on you, it does have its own disadvantage: if many people at one location all switch off their phones at the same time, it's a sign to the mobile carriers that they all thought something was worth them turning their phones off, such as a sensitive meeting.

An alternative that might give less information away is to leave phones in another room where the phones' microphones wouldn't be able to overhear the conversations. If you know this wouldn?t be possible, try to take the battery out of your phone before you travel to the meeting.

Don?t forget that using a phone in public, or in places that you don't trust, makes you vulnerable to traditional eavesdropping techniques, or to having your phone stolen.

# General Precautions

As is the case with other devices, the first line of defence for the safety of the information on your mobile phone is to physically protect the phone and its SIM card from being taken or tampered with.

* Keep your phone with you at all times and avoid leaving it out in public.
* Always use your phone's security lock codes or Personal Identification Numbers (PINs) and keep them secret. Always change these from the default factory settings.
* Draw or make a mark on the SIM card, additional memory card, battery and phone with something unique and not immediately noticeable to a stranger. Place printed tamper-proof security tape over the joints of the phone if it is easily opened. (Tamper-proof security tape can be bought cheaply and easily over the internet) This will help you easily to identify whether any of these items have been tampered with or replaced.
* If your phone is locked, ask someone you trust about unlocking it. A locked phone poses higher risk as it means all your data is controlled by one operator.
* The 15-digit serial or IMEI (International Mobile Equipment Identity) number helps to identify your phone and can be accessed by keying \*#06# into most phones, by looking behind the battery of your phone or by checking in the phone's settings. Make a note of this number and keep it separate from your phone, as this number could help to trace and prove ownership quickly if it is stolen.
* Consider the advantages and disadvantages of registering your phone with the service provider. If you report your phone stolen, the service provider should then be able to stop further use of your phone. However, registering it means your phone usage is tied to your identity.

# Protection from malware

There are also a number of steps you can take that will help avoid your phone being easily infected with malware. This does not prevent your phone being infected, it just makes it more difficult to infect.

* Keep your software updated to keep your phone secure. There are two types of updates that need to be checked:
  + The phone operating system: For Androids go to: settings -> About phone -> updates -> check for updates
  + Apps you have installed: In Androids, open the Play store app, from the side menu select My Apps.
* Do not accept or install any unknown programmes on your phone, such as ring tones, wallpaper, apps or any others that come from an unexpected source. They may contain malware.
* Connect your phone to a computer only if you are sure it is malware free. Learn about how to check in the [Malware lesson](umbrella://lesson/malware).
* If you don't know or use any of the features and applications on your phone, disable or uninstall them if you can.
* Try to avoid connecting to WiFi access points that don't provide passwords.
* Make sure communication channels like Infrared (IrDA), Bluetooth and Wireless Internet (WiFi) on your phone are switched off and disabled if you are not using them. Use them only in trusted situations and locations. Consider not using Bluetooth, as it is relatively easy to eavesdrop on this form of communication. Instead, transfer data using a cable.
* When setting up your phone, there are a number of settings you can select and apps you can download that will help make your phone more secure. Instructions for set up can be found in the tools section: [Basic Security Setup for Android](umbrella://lesson/android).

# Burner phones

Phones that are used temporarily and then discarded are often referred to as burner phones. People who are trying to avoid surveillance sometimes try to change phones and numbers frequently to make it more difficult to recognise their communications. They will need to use prepaid phones (not associated with a personal credit card or bank account) and ensure that the phones and SIM cards were not registered with their identity; in some countries these steps are straightforward, while in others there may be legal or practical obstacles to obtaining anonymous mobile phone service.

There are a number of limitations to burners hiding your identity.

* First, just swapping SIM cards offers minimal protection, because the network operator knows the history of which SIM cards have been used in which devices, and can track either individually or both together.
* Second, governments have been developing mobile location analysis techniques where location tracking can be used to generate leads or hypotheses about whether multiple devices actually belong to the same person. There are many ways this can be done. For example, an analyst could check whether two devices tended to move together, or whether, even if they were in use at different times, they tended to be carried in the same physical locations.
* A third problem for the successful anonymous use of telephone services is that people's calling patterns tend to be extremely distinctive. For example, you might habitually call your family members and your work colleagues. Even though each of these people receives calls from a wide range of people, you're likely the only person in the world who commonly calls both of them from the same number. So even if you suddenly changed your number, if you then resumed the same patterns in the calls you made or received, it would be straightforward to determine which new number was yours. Remember that this inference isn't made based only on the fact that you called one particular number, but rather on the uniqueness of the combination of all the numbers that you called.

Together, these facts mean that effective use of burner phones to hide from government surveillance requires, at a minimum:

* Not reusing either SIM cards or devices;
* Not carrying different devices together;
* Not creating a physical association between the places where different devices are used;
* And not calling or being called by the same people when using different devices.
* (This isn?t necessarily a complete list; for example, we haven?t considered the risk of physical surveillance of the place where the phone was sold, or the places where it's used, or the possibility of software to recognize a particular person's voice as an automated method for determining who is speaking through a particular phone.)

Swipe right for this lesson's checklist

Go to the Expert lesson for advice on how to root and encrypt your phone.

[Go to Expert Lesson](umbrella://lesson/mobile-phones/2)

### RELATED LESSONS/TOOLS

* [Making a Call Lesson](umbrella://lesson/making-a-call)
* [Sending a Message Lesson](umbrella://lesson/sending-a-message)
* [Backing Up Lesson](umbrella://lesson/backing-up)
* [Safe Deleting Lesson](umbrella://lesson/safely-deleting)
* [Malware Lesson](umbrella://lesson/malware)
* [ObscuraCamTool](umbrella://lesson/obscuracam)
* [Basic Security Setup for Android](umbrella://lesson/android)

### FURTHER READING

* [Security in a Box ? Chapter 10, Use mobile phones as securely as possible](https://securityinabox.org/en/guide/mobile-phones)
* [Security in a Box ? Chapter 11, Use smart phones as securely as possible](https://securityinabox.org/en/guide/smartphones)
* [EFF - The problem with mobile phones](https://ssd.eff.org/en/module/problem-mobile-phones)