

This brochure has been developed as part of the **Consumer Education Programme** of the **Communications Commission of Kenya**. It was compiled as a result of a review of material from various sources and presents the current perception of the information available on mobile-phone security, with particular reference to Kenya.

Introduction

The loss or theft of a mobile-phone is a major concern to most users. Not only because a mobile-phone represents a valuable monetary investment, but also because it acts as a repository for potentially sensitive data of a personal as well as a financial nature. Most mobile-phone users store a wide range of data on their phones – either on the phone's internal or external memory (on the handset or on the Subscriber Identity Module or SIM card). The SIM card is typically used for the storage of contacts and short messages while the memory capacity of the handset is typically used for the storage of data relating to personal photos, emails, and calendar items. In both cases, unless access to this data is protected by a PIN number (or by a security device, which is supplied with some models of mobile-phones), it is easily accessible by unauthorized persons.

Data-security

There are two main methods of securing data, they are:

Via the SIM lock

This method requires the user to store data on the SIM card and to use a PIN number (Personal Identification Number) every time the SIM card is inserted in the mobile-phone. PIN numbers are generally 4-digit numbers which are known ONLY to the user of the mobile-phone. By using this method of data security, the user ensures that even if the phone is lost or stolen the data cannot be accessed.

Via the phone lock

Using this data-protection method, the mobile-phone is locked and only by the use of a specific password can it be opened for use. When creating passwords users should note that 8-digit passwords are more secure than 4-digit ones. Users are also advised to use the built-in automatic phone-lock system with which most mobile-phones are now supplied and which activates after a stipulated time lapse of, for instance, 30 seconds. The latter is particularly effective in protecting such sensitive data as that contained in incoming emails – many of which may be of a corporate or business nature.

Safeguarding your mobile-phone

To protect your mobile-phone from theft or abuse:

- Keep it in a safe place and out of sight.
- Only give your number to people you trust.

- Avoid using it in the street. If you need to make a call in a public place be discrete and stand somewhere with optimum all-round vision.
- Use a PIN code to lock your phone.
- When walking alone, put your phone on 'silent' or 'vibrate only' mode so that the ring-tone does not attract attention to you.
- Be alert while walking and texting at the same time.
- Security-mark your phone with a unique code. The best place to put this is beneath the battery.
- Never leave your mobile-phone on a table or seat in a public place such as a cinema, pub, restaurant or nightclub – this invites theft.
- Never leave your phone unattended in your car. If you must leave it in the car put it out of sight and switch it to silent mode – it takes seconds for a thief to smash a car window.
- If you have a Bluetooth or Wi-Fi enabled phone - install anti-virus software.
- Always keep mobile-phones out of the reach of very young children.
- Avoid making easily-identifiable contact entries such as 'mum' or 'dad' so as to protect them from unwelcome calls in the event that the phone is lost or stolen.

Alternative methods of data-protection

There are two major types of mobile-phone technology: GSM (Global System for Mobile Communications) and CDMA (Code Division Multiple Access) – both of which offer different methods of data-protection.

Data-protection and the GSM mobile-phone

Every GSM mobile-phone has a unique 15-digit electronic serial number known as the International Mobile Equipment Identity (IMEI), which is programmed into the handset and is also written under the battery. To access the IMEI number key in ***#06#** and note down the number that appears on the screen. In the event that your mobile-phone is lost or stolen you should immediately contact your network-provider and give them the IMEI number so that they can block your mobile-phone against future use with any SIM card on any Kenyan GSM network. This acts as a powerful deterrent to potential thieves. Should you recover your phone, your network-provider can also unblock it so as to restore the phone to normal use. IMEI numbers are also useful to the police, who can use them to identify lost or stolen phones.

Data-protection and the CDMA mobile-phone

Every CDMA phone has a unique 8-digit electronic identification number, known as an Electronic Serial Number (ESN), which can be found beneath the battery and serves the same function as the IMEI number outlined above.

What to do if your mobile-phone is lost or stolen

If your mobile-phone is lost or stolen you should immediately contact your network-provider, give them your IMEI or ESN number and ask them to block the phone against future use. If you have a GSM mobile-phone your network-provider will block both your SIM card and your IMEI number so that your phone cannot be used on any Kenyan network. You should also report the loss or theft to the police and provide them with the relevant identification number.

Hidden battery power

Some mobile-phones are designed to reserve a measure of battery power for emergency use. This can be activated by keying-in *3370#, at which point the mobile-phone will re-start and display a significant increase in battery power. This reserve is automatically replenished the next time the phone is charged.

Need to know more?

For further information on the above topic or any other aspect of health and safety with regard to communicational equipment, please contact:

Disclaimer: while every attempt has been made to ensure that the information included in this document is accurate, it is intended ONLY as a guideline towards the safe operation of communications equipment and should not be regarded as (or used in lieu of) legal advice. The Communications Commission of Kenya will not, therefore, accept any liability for the consequences of any actions taken, or decisions made upon the information offered. **Acknowledgements:** This brochure was developed as part of the Consumer Education Outreach Programme of the Communications Commission of Kenya, working in partnership with Teknobyte (Kenya).

CONSUMER AFFAIRS DIVISION,
COMMUNICATIONS COMMISSION OF KENYA

P.O. BOX 14448, NAIROBI, 00800

Email: chukuahatua@cck.go.ke

TEL - 020 - 44 55 555, 0714 - 444 555, 0737 - 44 55 55

Mobile Phone Security



Communications
Commission
of Kenya

**CHUKUA
HATUA**
Pata huduma ya
mawasiliano unayostahili