

Mobile Phone Security



Introduction

The loss or theft of a mobile-phone is a major concern to most users. Not only because a mobile-phone is valuable, but because it acts as a storage medium for data, which is typically stored on the handset or on the Subscriber Identity Module or SIM card. In both cases, unless access to this data is protected by a PIN number (or by a security device), 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.

Via the phone lock

Using this data-protection method, the mobile-phone is locked and only by the use of 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.

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.
- Use a PIN code to lock your phone.
- When walking alone, put your phone on 'silent' or 'vibrate only' mode.
- Be alert while walking and texting at the same time.
- Security-mark your phone with a unique code.
- Never leave your mobile-phone unattended in a public place or in your car.
- 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.

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.

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.