

Mobile phone security

[Technology](#), [Mobile Phone](#)



This fact sheet has been developed for the Consumer Education Program by the Communications Commission of Kenya. It was compiled by studying material from various authoritative sources and adopting what is universally acceptable and relevant to the Kenya situation. The fact sheet is intended to enable Consumers have a good understanding of the issues discussed and hence empower them when making decisions regarding CIT products and services. Introduction One of the biggest threats that a mobile phone user faces today is loss or theft of the phone.

Not only is the mobile valued as a physical device, the phone may contain personal and financial data stored in the handset or in the phone's subscriber identity module (SIM card). While a stolen SIM can be barred by a mobile network once the theft has been reported it is a bit harder to bar the handset from being used with different SIM card. Unless the user had protected his personal information with a PIN prior to the theft or loss of the phone, this data can be accessed by unauthorized persons. Mobile phone users normally store a wide range of information on their phones.

This information can either be stored in the phone's internal or external memory (depending on the make and model of the phone) or in the SIM card. The SIM card is used mainly to store contacts and short messages while the phone's memory is used to store information such as personal photos, emails, and calendar items. In order to prevent unauthorized persons from using the phone and further gaining access to the stored information, some mobile phones have security features which the user can activate. This fact sheet has been developed to address security of the information stored and what to do should you lose the phone.

<https://assignbuster.com/mobile-phone-security/>

Securing the information stored. There are at least two methods one can use to secure the information stored on a mobile phone. These are: a) SIMI lock

This method takes advantage of the SIMI card as a storage element to secure private information associated with the subscriber. The subscriber uses a PIN number which is mostly a four digit code which should only be known to him and is always prompted by the mobile phone every time the SIMI card is inserted into the phone. It is an effective method since even if the subscriber loses the SIMI card the other person cannot access any information stored on it.

Phone lock Mobile phone security This method takes advantage of a password to lock the mobile phone such that access to the phone's functions can only be permitted upon input of the correct password. An eight-digit code is more secure than a four-digit code. Most phones also have an inbuilt an automatic phone lock system which kicks in after a stipulated time period e. G. 30 seconds when activated which is mostly used as a keypad lock and subscribers are advised to take advantage of this features to enhance the security setting AT tenet phones. N more nana el n a evolves Delve capable AT achieving emails, security especially of corporate email with sensitive internal and external data has become a major concern. This means that mobile handsets hold data which previously only resided in computers. Since this method is more effective and protects more information than the first, subscribers are advised to always lock their phones especially if they hold any sensitive information. Safeguarding your Handset Some of the ways to keep your mobile safe include: ; ; ; Keep your phone safe and out of sight.

Only give your number to your friends and people you trust. Avoid using your phone in the street. If you need to call someone in a public place, be discrete and be somewhere where you can see what is happening around you. Use a PIN code to lock your phone. If you're walking alone put your phone on silent or vibrate mode so your ring tone doesn't draw attention to you. Be alert while walking and texting at the same time. Security-mark your phone with a unique code. The best place is underneath the battery.

Many mobile phones are stolen in public places such as cinemas, pubs and nightclubs, especially when they are left on a bar, table or on a seat, so don't leave your phone in such places unattended. Don't leave your phone unattended in a car - if you must, put it out of sight and turn it off or switch to silent mode. It takes seconds for a thief to smash a window and enter a car. For a Bluetooth or Wi-Fi enabled phone install antivirus software to help guard against harmful programs or viruses. For the sake of the safety of very young children; always keep the phone out of their reach.

Avoid making easily identifiable entries in the phone e. G. 'mum' or 'dad' for the security of such persons should the phone be lost. There are other methods of securing your phone that are dependent on the technology that the phone is based on. The two main technologies used for the provision of mobile services are GSM (Global System for Mobile Communications) and CDMA (Code Division Multiple Access). Phones based on these two technologies connect to their respective networks differently, so the security features differ slightly. Mobile phone security Your GSM Phone's Unique Equipment Identification Number Each GSM mobile phone has a unique

electronic serial number called the MIME (International Mobile Equipment Identification) number, which can be identified by the GSM network. It is a 15-digit number programmed into the handset and also written is at the back of the handset, under the battery. On most GSM handsets, it can be accessed by dialing a special key sequence using the keypad, when the phone is switched on.

Upon purchase of a mobile handset, users are advised to record their MIME number for use in case the mobile phone is lost or stolen. Your mobile phone service provider can liaise with the police regarding a lost or stolen handset and, if found, your handset will be identified using the MIME. Thieves are deterred from stealing mobile phones by MIME blocking. Blocking an MIME on a mobile phone network prevents a GSM mobile phone from being used with any SIM on any Kenya GSM network. Mobile carriers are able to block the use of customers' lost or stolen mobile phones and unblock recovered mobile phones on their network.

They have also agreed to exchange their lists of blocked and unblocked MIME numbers with other mobile carriers so these can also be processed (blocked/unblocked) on all mobile networks. The CDMA phone unique electronic identification number CDMA phones also have a unique electronic identification number, the Electronic Serial Number (ESN). This number can be found on the back of the CDMA handset under the battery and usually has eight digits, combining letters and numbers. Users are advised to record this number for identification purposes in case the phone is lost or stolen.

Hidden battery power Some mobile phones are designed to reserve battery power. If the cell battery is very low and the user is expecting an important call or is confronted by an emergency situation, and doesn't have a charger at that moment, one can activate this reserve battery power. To activate, press the keys *3370#, the cell phone will restart with this reserve and the instrument will show a significant increase in battery power. This reserve will get replenished the next time one charges their cell phone.

However it should be noted that this only works on some phones. What to do if one's mobile handset is lost or stolen If the user's mobile phone is lost or stolen, the user is advised to contact their mobile phone service provider immediately to suspend service and prevent unauthorized calls being made and billed to the user. If one has a GSM mobile phone, the provider will 3 Mobile phone security block the subscriber's SIMI card and MIME number to prevent heir phone from being used on all Kenya mobile networks.