

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 Internet security and privacy, with particular reference to Kenya.

Introduction

When using the Internet, it is imperative to ensure the security and privacy of ALL of the user's data. Information on how to do this is offered below.

Securing the wireless network

Wireless devices broadcast via radio waves, which are sent out by a transmitter. This means that any receiver within range (and tuned to the transmission frequency) will receive the signal. Thus, when personal information is to be transmitted, it must be guarded against unauthorised access (usually referred to as 'eavesdropping'). There are a number of security/privacy risks inherent in wireless communication, as outlined below:

Risks related to the use of Bluetooth devices

Bluetooth devices communicate using short-range wireless signals and operate on a frequency band between 2.4 GHz to 2.4835 GHz, achieving speeds of up to 1 Mbps. They can be used to link a mobile phone to a headset, a keyboard or a mouse to a computer and a laptop to a printer, among others. The use of Bluetooth technology presents the following security/privacy threats:

- **Blue snarfing**, which is the unauthorized access to personal data, such as; calendars, contact lists, emails, text messages, pictures or videos
- **Blue bugging**, which allows an unauthorized person to take control of another person's phone – allowing them to listen in to conversations, make calls and send messages
- **Blue jacking**, which is the sending of unsolicited messages, via the Bluetooth technology, to other Bluetooth-enabled devices

In order to protect themselves against such risks, Bluetooth users are advised to ensure that all such devices are protected by passwords, and that all Bluetooth functions are turned off when not in use.

Mobile phones and safety and security

Because they can be used for voice transmission, as wireless modems and as web browsers, mobile phones can be accessed by unauthorized persons to obtain personal data.

Data storage on mobile phones

Most mobile phone users store a wide range of data on their phones, using either the phone's internal or external memory or in the Subscriber Identity Module(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 personal or other data such as photos, emails, and calendar items. In both cases, unless access to this data is protected by a PIN (Personal Identification Number) number (or by a security device, which is supplied with some models of mobile-phones), it is easily accessible by unauthorized persons.

Mobile phone data security

There are two main methods of securing data on a mobile phone, they are:

Via the SIM lock

This method requires the user to store data in the SIM card and to use a PIN number every time the SIM card is inserted into the mobile phone. PIN numbers are generally 4-digit code 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 specific password can it be opened for use. When devising passwords users should note that 8-digit codes are more secure than 4-digit codes.

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 emails – many of which may be of a corporate or business nature.

Protecting the mobile phone by means of accessing the IMEI number

Consumers can guarantee the safety and security of their mobile phones by ensuring that they know the IMEI (International Mobile Equipment Identity) number, which is a unique identification code that can be used by the service provider to block the phone against future use (via the SIM card and on ANY network. It can also be used by the Police in the recovery of stolen goods. Consumers are advised to use the IMEI number, which is a powerful deterrent to potential thieves. Should the phone be recovered, the network-provider can also unblock so as to restore the phone to normal use.

How to access the IMEI (International Mobile Equipment Identification number)

To access the IMEI (International Mobile Equipment Identification number) the user should key in * # 0 6 # and note down the 15-digit number that appears on the screen.

Wireless Fidelity (Wi-Fi)

Wireless Fidelity (Wi-Fi) is wireless data network, which allows Wi-Fi enabled devices (such as PCs or mobile phones) to connect to the Internet – at such time as they are in the vicinity of the wireless data network. Offering low-cost implementation and high-access use, WiFi areas are sometimes termed 'hot spots' and are typically deployed in public areas – such as airports, universities, bookstores, coffee shops, offices and hotels. In the interests of security and safety, users of Wi-Fi are advised to encrypt all data before transmission. Small organizations are also advised to consider the use of **WiFi Protected Areas**, while the larger organizations are advised to consider the use of **Virtual Private Networks (VPN)**

Securing wireless networks

Any device within a wireless network can serve as an illicit entry point to the entire network if it is not properly protected. It is therefore vital to secure the entire network rather than to secure specific devices. Users wishing to secure their wireless network are advised to:

- Encrypt all data during transmission
- Use antivirus and anti 'spy ware' software as well as firewalls
- Turn off identifier broadcasting. Change the identifier of the router from the default
- Change the router pre-set password
- Allow only specific computers to access the network
- Turn off the wireless network when it is not in use.

Identity theft

Identity theft is the theft of a person's name, PIN number, ID card number, credit card number or other personal data. The usual means by which identity theft is accomplished is by 'Phishing', whereby a fraudulent but credible e-mail is sent to the victim – soliciting all such personal data as is required. Once this personal data is obtained, it can be used to access funds, run up accounts or to facilitate a broad range of fraudulent practices. There are a number of indications that identity theft has been perpetrated. They are as follows:

- The appearance of invoices or proof of purchase regarding items that the user did not purchase
- Calls from debt collection agencies relating to same
- Apparent redirection of utility bills and other important correspondence
- The erosion of the user's credit rating.

What to do if you become a victim of identity theft

- Place a fraud alert on your credit reports
- Close any accounts that have been accessed
- File a police report
- Notify the relevant regulatory authority.

'Spam scams'

Most people are resigned to the fact that they receive 'spam' (unsolicited 'junk' mail). Such mail can, however, prove a serious security risk. Some spam messages, for instance, request the provision of personal data – which can lead to identity theft, as outlined above. Others invite entry to websites – which can, in themselves, offer a wide range of personal and security risks; yet others are designed to perpetrate a specific 'scam', which has been deliberately designed to defraud the victim of his/her money.

Some common 'spam scams'

The 419: conmen claiming to be connected with former government officials in 'Nigeria' or another such country offer to transfer funds to the victim's bank account given that certain fees are paid in advance. Official-looking documents may follow but eventually the victim will be asked to send funds to cover such things as; transaction and transfer costs, attorney's fees. Victims are also often asked to send a blank letterhead or bank access codes.

The Work-at-Home Scam: the victim receives an advertisement offering steady 'work-at-home' income for minimal labour (envelope-stuffing, craft assembly work). The victim will then be required to work in advance of payment – which may not follow. Funds may also be requested to 'facilitate' such payment.

Foreign Lotteries: the victim will receive an email offering enticing odds in a foreign lottery, or a message that they have

won a foreign lottery. Payment will, however be requested before the victim can assess these winnings.

Check overpayment: a so-called buyer of a service or item that is offered by the victim will offer to pay them with a cashier's, personal, or corporate cheque. When it arrives, the cheque will be made out for MORE than was owed – supposedly 'by mistake'. The victim will be asked to bank the cheque but to be so kind as to return the overpayment in the interim. Typically all such cheques are counterfeit.

Pay-in-Advance credit: the victim will be advised that they have 'pre-qualified' for low-interest loan or credit card. Such loans or credit cards rarely exist and a 'processing fee' is always required from the victim in advance.

Investment schemes: the victim receives an email offering an investment, which promises unusually high yields and NO risk. The victim is usually pressurized into signing a contract for an investment scheme which rarely performs as promised – if at all.

To avoid becoming a victim of 'spam scam'

- Protect your personal information
- Know who you are dealing with
- NEVER act impulsively
- Obtain all promises, guarantees or agreements in writing first.
- Disregard any offer that asks you to pay for anything in advance
- Consider the use of a 'spam filter'

How to respond to such scams

The best way to respond to all such scams is NOT to respond, never to send funds, never to volunteer ANY personal or financial information and to remember that things which sound 'too good to be true' generally are.

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).



Communications
Commission
of Kenya

Internet security and privacy

**CHUKUA
HATUA**
Pata huduma ya
mawasiliano unayostahili

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