

## Introduction

Premium Rate Services (PRS) offer either information or entertainment and are charged at a 'Premium' (higher than conventional rates) cost. PRS are typically accessed via the SMS (short messaging service) on a variety of media including; landline telephones, fax, internet, mobile-phones or TV. PRS offer access to such services as: **Entertainment:** competitions, phone-chat services, horoscopes, interactive

TV games, charitable fund-raising, TV voting (e.g. as used for Tusker Project Fame, Big Brother), ring-tone and logo downloads. **Information:** Directory Enquiry Service, technical help-lines (for such things as IT problems), adult entertainment, weather or traffic updates, sports or global news.

## PRS numbers

PRS numbers provide a means by which Premium Rate Services may be accessed. They are typically prefixed by **0900** or **091** on fixed line networks (or, when accessed by mobile-phone, by a three-, four- or five-digit number).

## Toll-free numbers

Toll-free numbers (typically prefixed by 800 or 888) allow callers to make FREE calls and are typically used by organizations that wish to make it easy for users to contact them and, therefore, pay for the calls themselves.

## Regulation of the PRS service

PRS services are regulated by The Communications Commission of Kenya (CCK), which is responsible for investigating all complaints and taking action against organizations that breach the terms and conditions of their licences.

## PRS 'scams' (fraudulent deceptions)

A number of 'scams' can be perpetrated using the PRS service. The prime scam relates to the reverse-charge SMS service which, when activated, results in the user being charged for all incoming SMS calls. To activate the reverse-charge SMS service, the user must send a pre-specified message or make a call to a specific number (usually a 3, 4, or 5-digit number).



## How the reverse-charge SMS scam works

The user will receive an SMS message offering an inducement for them to call a certain (PRS) number (to claim a prize, or receive news of a loved one). Thereafter the operator of the scam can send unlimited (PRS) messages.

## How to safeguard yourself against fraudulent scams

- Never reply to text-messages from unknown sources.
- Should you be approached by someone asking to use your mobile-phone in an 'emergency' direct them to a public phone. In case of a serious emergency YOU should dial 999 or 112 on their behalf.
- Ask your Service Provider for details on availability and procedures for PRS call-barring.
- Report the scam to the network operator IMMEDIATELY.

## Internet 'Dialer' scams

If you are using a dial-up Internet connection to access a certain PRS, you may be asked to download software known as a 'dialer'. If fraudulently configured/designed, it may temporarily disconnect the dial-up connection and connects the user to a PRS

number. Whilst many of these 'dialers' are perfectly legitimate some, known as 'rogue dialers', automatically connect the user's computer to a PRS - to which it remains connected until such time as the user manually disconnects it and re-connects to their usual provider.

## Protection against PRS scams

- Install (and update) firewalls, anti-virus protection and anti-'pop-up' software.
- Check the dial-up setting on your computer regularly. When using broadband - disconnect the dial-up modem. Before downloading PRS content ALWAYS read the terms and conditions.
- Do not allow children to open e-mails from unknown sources.
- Ask your Service Provider to bar your equipment from dialing PRS numbers.

## How to react to a PRS scam

Contact your Service Provider immediately. In the event that you feel your complaint has not been properly handled, contact CCK (see details below).