



# WARNING: MOBILE PHONE FRAUD

Mobile phone fraud involves a variety of scams that either persuade you to buy phone-related products/services that turn out to be substandard or non-existent; or to make phone calls or texts to premium services by accident; or to unknowingly sign up to expensive subscription services.

## MISSED CALL SCAMS

Your phone registers a missed call. You don't recognise the number so you call it back. Most of the time the call will be perfectly above board, but you may be redirected to a premium rate service which can cost up to £15 per call.

## RECORDED MESSAGE SCAMS

The number you're asked to call back may be a recorded message telling you that you've won a prize, and giving you another number to call to 'claim' it. But this second number may be a premium rate one. Also, your prize may be nothing more than a ring tone subscription - which can also be a fraud.

If you have been affected by this report it to Action Fraud by calling 0300 123 2040 or visiting [www.actionfraud.police.uk](http://www.actionfraud.police.uk)

**ActionFraud**  
Report Fraud & Internet Crime  
[actionfraud.police.uk](http://www.actionfraud.police.uk)

## PROTECT YOURSELF AND YOUR MOBILE OR SMART DEVICE FROM FRAUD

1. Most phone service providers have their own security policies in place to help protect your data; examples include a secret question or a personal PIN for your account. It's always worth checking what they have and make sure you sign up to use them
2. Set up a password or passcode on your phone or tablet and keep it locked when you're not using it. Your user guide will tell you how to do this.
3. Never store personal details like passwords or PIN numbers in texts or emails that are accessible through your phone or tablet.
4. If your phone is stolen, tell your provider straight away – they can blacklist and deactivate it remotely. You should then change any passwords for online accounts you access through your phone as soon as possible (for example online banking).
5. Never allow application or files to be installed from unknown sources particularly on smartphones/tablets (e.g. Android apps outside of Android Market™)

