

What should I do if I fall victim to a dialler program?

When you receive your phone bill, you should pay the charges that you agree with (uncontested charges) and contact your service provider outlining the charges that you believe are associated with a dialler program.

What has ComReg done?

We published an initial consumer guide about modem hijacking in April 2004. After talking to phone companies and ISPs and consulting the public, we directed them to take specific steps.

- ISPs must recommend free or low-cost hardware and, or, software to their users.
- Phone companies must prevent direct-dial access to specific country codes but can “unblock” specific numbers if satisfied that the number does not present a risk.
- Phone companies cannot charge for any direct-dial calls to the listed destinations unless they are to ‘unblocked’ numbers.

These measures are temporary and the destinations to which they apply will change from time to time. They only protect against dialling specific countries.

How can I contact ComReg?

By phone (LoCall): **1890 229 668**
(9.00am to 5.30pm) Monday to Friday

By fax: **(01) 804 9671**

By email: consumerline@comreg.ie

Our websites are:

www.comreg.ie / www.askcomreg.ie / www.callcosts.ie

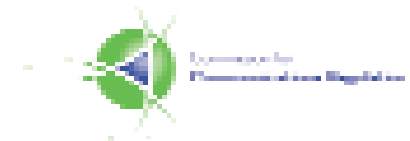
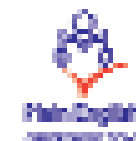
By post: **ComReg Consumer Team, Irish Life Centre
Block DEF, Lower Abbey Street, Dublin 1**

Modem Hijacking Scams Using Dialler Programs



Legal Disclaimer: We prepared this document from a variety of sources. While we took reasonable care to prepare it, we do not accept any responsibility for any loss or damage anyone may suffer by using any of this information.

August 2007



A guide to modem hijacking scam using dialler programs

We want to let phone users know about the risk of having your internet (dial-up modem) settings changed without you knowing or giving your consent. When this happens you could unintentionally build up phone charges at rates of up to €5 per minute. The normal rate varies between 1c and 5c per minute.

In this guide, we:

- explain the issues regarding dialler programs; and
- tell you the steps to take to prevent being affected by rogue dialler programs.

What are dialler programs?

A number of websites use dialler programs instead of credit cards to collect payments. This method is a way of charging you for content through your normal phone bill – similar to other premium rate services.

If you access websites offering content in this way, you will be asked to download a piece of software known as an 'internet dialler'. This software will change the settings of the modem connecting your computer and phone line, making the connection costs more expensive than usual.

Dialler programs are generally used by web servers located outside Ireland and the cost of calling the country where they are located is very high.

So what is the issue?

The problem arises when consumers do not know that they have downloaded a dialler program or are unaware of what the dialler program does.

Rogue sites may not make clear that you are installing software on your computer or that the dial up settings for your internet access will be permanently changed. They may even mute the dialling noises that your modem makes to hide the fact that the modem has disconnected from your normal ISP and is dialling a different number.

Essentially, these providers are hijacking your modem settings – taking them over and changing them for their own benefit. You may become aware of the hijacking or a hijacking attempt while accessing the internet, but often consumers only realise that they have fallen victim when they receive a phone bill with high call charges to international or premium rate numbers.

Typical signs of modem hijacking

- You hear your modem disconnect and dial up again.
- Your internet speed becomes much slower than normal. There may be other reasons for this, but when checking, always start by looking at your dial-up settings and properties.
- You receive an unexpectedly high phone bill, which lists unknown and high-cost international phone numbers.
- You see an unfamiliar short-cut icon on your desktop.
- You are online but cannot send emails.

What you can do to tackle modem hijacking

- Check your internet settings regularly to see that the phone number your computer is dialling to connect to the internet is the correct one. For most Irish ISPs (Internet Service Providers) the phone number will start with 189X, for example 1890 or 1891.
- Be cautious when clicking on popup boxes (extra windows that appear). If in doubt about viewing the content, always click 'No' or use the 'Esc' (Escape) key to close the window.
- Exercise similar caution if you are re-directed to an unexpected web page.
- Turn up the volume on your modem so you can hear whether your modem has disconnected and is attempting to re-dial.
- If you notice any connections or icons on your desktop that are unfamiliar, investigate them and delete if they are not valid programs. You will also need to uninstall the underlying programs; simply deleting the icons will not be enough.
- Turn off your computer and modem when not in use.
- Set up password protection for access to your computer and the internet.
- Bar access to premium rate or international numbers, but consult your telecom supplier about whether this affects voice calls.
- Install protective software and update it regularly. Your ISP should recommend software to help you deal with the problem.
- Consult your ISP's help pages or its technical support for information or help with solving the problem.