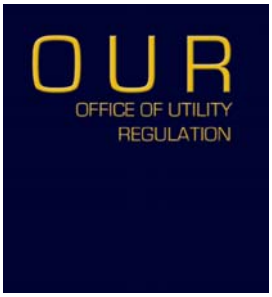

Office of Utility Regulation

Advice to Internet Users on Rogue Diallers and Modem Hi-Jacking

---

Information Notice

Document No: OUR 04/16 **August 2004**

Office of Utility Regulation
Suites B1 & B2, Hirzel Court, St Peter Port, Guernsey, GY1 2NH
Tel: (0)1481 711120, Fax: (0)1481 711140, Web: www.regutil.gg

Rogue Diallers

The Office of Utility Regulation has become aware of an Internet scam which may have reached Guernsey and could affect Guernsey internet users who dial up to the internet over ordinary telephone lines.

The scam, commonly known as "Modem hi-jacking" or "Rogue Dialling", can result in Users unwittingly dialling long distance or premium rate telephone numbers through their modem and potentially running up considerable phone charges.

How can this happen?

When visiting some websites, internet users can unknowingly download software which can then change the settings on the computer for internet dial up, diverting it from dialling the normal Internet Service Provider (ISP) to dialling expensive premium rate, or international numbers instead.

The software can be installed surreptitiously without the user's knowledge or consent and the change of settings may not be noticed until the new number has been used and high phone charges incurred.

How do I know if my PC is affected?

There are some warning signs you can look out for that might alert you that your PC may be affected by rogue diallers, including:

- You are unable to send emails when on line.
- You are online and hear your modem disconnect and dial-up again. (Some rogue diallers mute the dialling noise that your modem makes to hide the fact that the modem has disconnected from your normal ISP and is re-dialling a different number).
- An unfamiliar short-cut icon appears on your desktop.

However, many users do not become aware that they are affected until unexpectedly large phone bills are received. Internet users should check their phone bills and if your bill includes calls to unknown international numbers (starting with 00) or premium rate numbers (starting with 090), then you should check your settings to make sure that your PC modem has not been hi-jacked.

How can I prevent this from happening to my computer?

There are a number of steps that internet users can adopt to protect themselves against this type of scam.

In the first place, you can contact your ISP and ask for advice on any measures you can take to reduce the risk. Your ISP will be best placed to advise you and may be able to recommend filters or monitoring software.

Internet users can take steps themselves to reduce the risk of modem hi-jacking, including:

- Turn off your computer and modem when not in use;
- Always exercise caution when entering any unknown websites or when clicking on popup boxes as this can trigger a software download;
- Regularly check your internet settings are set to dial the correct number to connect you to the internet via your chosen ISP;
- Turn the volume up on your modem so that you can hear if your connection to your ISP is disconnected and another number re-dialled.

Internet users can also contact Cable & Wireless Guernsey and ask to have access to premium rate services and/or international numbers barred from their phone line.

What should I do if I suspect my PC is affected?

If you believe your PC has been affected you should contact your ISP immediately, inform them of the problem and ask for any advice on how to remove the unwanted software.

Who can I complain to?

If you are a victim of a rogue dialler you can register your complaint with ICTIS which is an independent organisation responsible for regulating the content and promotion of all UK phone services charged at a premium rate.

ICTIS contact details are:

Free help line: 0800 500 212
In writing: ICSTIS
Clove Building
4 Maguire Street
London,SE1 2NQ
Email: secretariat@icstis.org.uk

You can also contact your ISP or your telephone service provider (Cable & Wireless Guernsey) and register your complaint.

