

## Computer 'Cold Calling' Scam - Advice

Callers offering to update your virus protection on your computer.

Gardai have become aware of a scam involving fraudulent calls being made to members of the public.

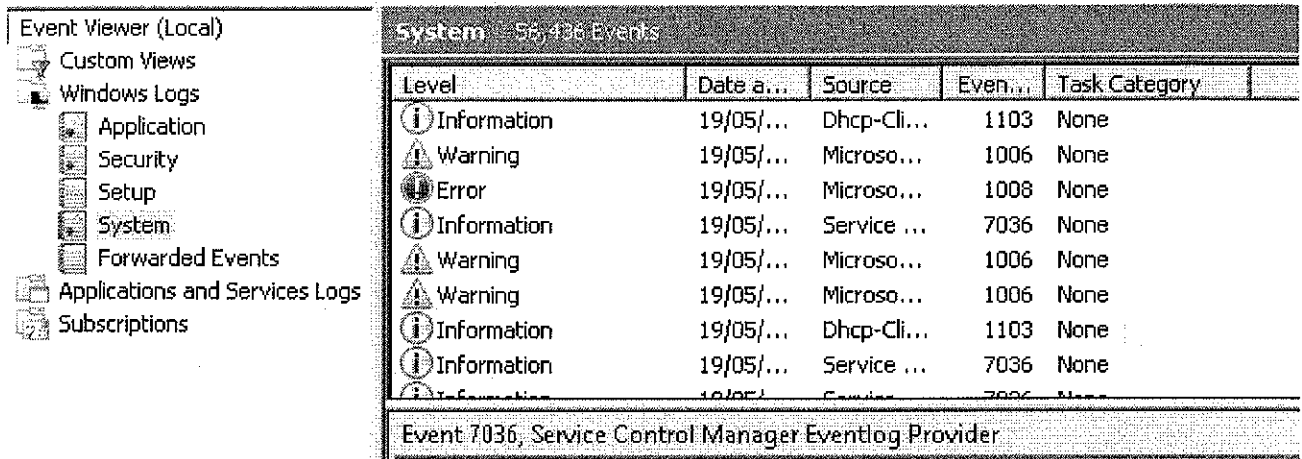
### The Scenario works like this:

You the owner of a computer receive an un-invited call from a call centre abroad. The number calling may appear to be from an Irish number and the caller may use your name.

The caller asks if you have a PC in the house. The caller then claims that they are calling on behalf of well known computer companies and will check your computer for problems.

The caller then asks you to look at the Windows Event Log. They then try to persuade you that any alerts recorded there are as a result of virus activity and that it urgently needs to be fixed.

The caller then talks you through granting them remote access to the PC. This allows them full control of the computer. They then run a scan and charge a sum of money for the service. They will take payment by credit card, and may charge a further amount for an extended service.



The screenshot shows the Windows Event Viewer interface. On the left, the 'System' log is selected under 'Windows Logs'. The main pane displays a list of events with columns for Level, Date and Time, Source, Event ID, and Task Category. The events listed include Information, Warning, and Error messages from various system components like Dhcp-Client, Microsoft Windows, and Service Control Manager.

Level	Date and Time	Source	Event ID	Task Category
Information	19/05/...	Dhcp-Cl...	1103	None
Warning	19/05/...	Microso...	1006	None
Error	19/05/...	Microso...	1008	None
Information	19/05/...	Service ...	7036	None
Warning	19/05/...	Microso...	1006	None
Warning	19/05/...	Microso...	1006	None
Information	19/05/...	Dhcp-Cl...	1103	None
Information	19/05/...	Service ...	7036	None
Information	19/05/...	Service ...	7036	None

Event 7036, Service Control Manager Eventlog Provider

*A sample of what a Windows event log may look like. Errors and warnings are common and may not necessarily indicate virus activity.*

## **Ramifications:**

The owner of the PC:

1. Has granted full control of their PC to someone they don't know.
2. May also have given their credit card details to someone they don't know.
3. May be exposed to potential loss of personal data and/or financial loss.

## **Advice to those who MAY be subjected to this scam**

- If members of the public require a service to be performed on their computers they should seek out a reputable company to provide it.

## **Advice to those who HAVE BEEN subjected to this scam**

- Any members of the public who may have given full PC access to a cold-caller should have the computer inspected by a reputable service centre.
- Any members of the public who have given credit card details to a cold-caller should contact their financial institution for advice.

## **General Advice**

- Be extremely sceptical of any un-invited call received and do not rely on phoning back the number to verify authenticity.
- If you have any suspicions regarding the call contact your local Garda Station.
- Additional Crime prevention advice relating to computer fraud can be found on the Garda Website [www.garda.ie](http://www.garda.ie)