Mr A B Sample
Sample House
Sample Street
Sample Town
Sample County
AB1 1AB

18-Jul-13

Your Virgin Media account number: 20 - 999999999
Our Reference: VMIS-OPENDNS-F999999999

Dear Mr Sample

This is a message from the Internet Security Team at Virgin Media.

We receive a number of reports from external organisations that alert us to internet security issues and your internet connection has been listed in one of these reports. Don't worry, this is no cause for alarm but please take a few minutes to read this letter and take the appropriate action.

So what’s the issue?

We believe a device connected to your home network may have an Open Domain Name Service (DNS) Resolver. This could be your Virgin Media SuperHub, third party home router and or any device connected to your home network which allows the DNS settings to be open, such as a PC, web-server, mail-server, game-host server, webcam or home entertainment system. The device may have been misconfigured by you, someone in your household or without your knowledge, however if the settings are left open they can be exploited to unwittingly participate in malicious activities, for example a Distributed Denial of Service (DDoS) attack. Essentially this means that one or more of your home devices could be used as part of a collection of computers/devices that are remotely controlled to attack other computer systems.

What is an Open DNS Resolver?

Domain Name System or DNS is like an address book system used by computers connected to the internet. Every time you send an email or browse the web your computer will need to find out where to send your email or where to grab the webpage you want to look at. To do this it contacts a DNS server (also known as a name server), a computer that runs this address book. Usually a DNS server will only communicate with computers that are local to it or have been given permission to communicate with it.

An Open DNS Resolver is a name server that provides "repeated name resolution" for non local clients or users. Essentially it lets any computer system on the internet use it, not just the intended local or authorised users on networks that you control and/or you trust.

How can I fix it?

Here are several online tools that you can use to check for an Open DNS Resolver:

thinkbroadband.com/tools/dnscheck.html *
dns.measurement-factory.com/cgi-bin/openresolvercheck.pl *
https://isc.sans.edu/dnstest.html *
openresolverproject.org/ *

Once you have identified the source of the issue within your home you can get further information on how to resolve the vulnerability from one of the following sites.

team-cymru.org/Services/Resolvers/ *
zytrax.com/books/dns/ch9/close.html *

If you are unable to fix this issue yourself we advise that you seek the advice of someone who will be able to assist you further or go to a local repair/upgrade shop, or a nationwide big chain for a payable service to help secure your connection. Thank you for reviewing this information and we hope any issue you may have is swiftly resolved.

Yours Sincerely

Analyst
Virgin Media

TIP: Want to check this letter is genuine? Please visit virginmedia.com/openresolver

* These links to external sites are provided as a courtesy and we are not responsible for the content of these sites or any problems encountered whilst applying these steps and we are not able to provide any technical support for such problems.