

Systems and Software

Broadband Routers – Default Passwords

Overview

Broadband Routers provide the connection between the computer and the internet. They convert the signals that computers understand into a format suitable for transmission down a cable or BT telephone line.

This document highlights the importance of changing the default passwords.

The default username and password of the majority of routers is admin/admin or tech/tech.

Why Change the Password

Three of the main security risks in not changing your password are

- 1) Wireless routers attacked over wireless interface (Wifi)
- 2) Drive-by Pharming
- 3) People making changes

Wireless routers attacked over wireless interface (Wifi)

Wireless routers are susceptible to attack from people over the wireless interface. A network enabled computer or laptop can hack into the router and change the security settings, allowing the hacker free access to the internet and potentially the contents of any hard drives in the PCs connected to the router.

Drive-by Pharming

The technology behind drive-by Pharming is quite complex, but luckily the solution is simple. Only buy routers from reputable suppliers (not eBay) and change the password in the router.

If the broadband router is compromised, the cyber criminals are able to monitor all transactions, including accesses to bank accounts. The user can be re-directed to fake web sites that look identical to the real ones. The user logs in as normal, and now the cyber criminal has all the details they need to empty the account.

With the conventional Phishing and Pharming attacks, the web address in the browser will be different in some small way. With a compromised router, the address will be identical to the real one. There is no way to tell the difference.

For more details on Phishing see

http://www.helpaccountants.co.uk/members/documents/Software_and_Systems_Security_Phishing_SS005.pdf

For the technology minded reader, the drive-by Pharming works by the user visiting a web site that contains malicious code. The user does not need to click on any links or icons, the code runs as the page is opened. This is where the term drive-by originates.

The user will be completely unaware that anything has happened. The malicious code silently logs into the router with the default username password, and changes the DNS router settings to point to a false server. The server can choose to give the user a false sense of security by only re-directing bank account web sites, all other web sites (www.bbc.co.uk etc) would be unaffected.

People Making Changes

This is not a problem in a small office at home, but in larger companies technically minded people may unknowingly make a change that allows external access to the hard disks on all of the PCs connected to the network. They may also be enabling network ports to allow the pirating of music and films. The owner of the network connection may be held liable not the employee who may have since left.

How to Change the Password

The broadband router will come with an installation guide. The manufacturer's web site should have an on-line version of the installation guide if it has been lost.

If a guide cannot be found, the following section describes the usual steps.

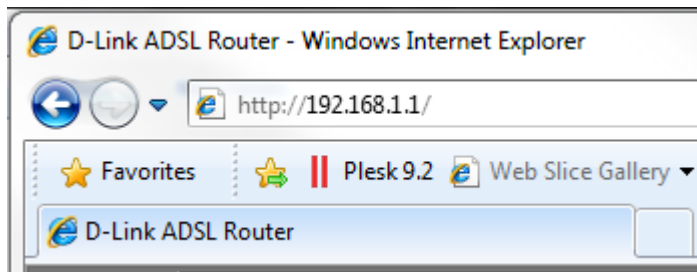
The password can be changed by logging into the router. This is typically done by connecting the box to a PC via a console connection or via one of the Ethernet ports on the back. Hopefully the router has already been configured to not allow setup changes over the wireless network, as this is a big security risk.

Typically, the Internet browser (IE or Firefox) is used as the interface application rather than an application that is installed on the PC. The router is accessed by typing the address <http://192.168.0.1> into the address bar. I.e. where the address <http://www.helpaccountants.co.uk> is normally entered.

Note that there is no **www** in the address for the router.

Examples for the popular browsers are shown below.

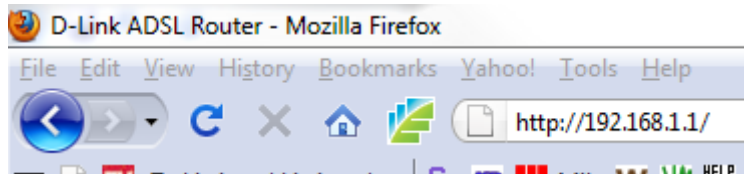
Internet Explorer:



Chrome:



Firefox:



The admin password should be supplied in the literature. It is not unusual for the username and password to be set as the default admin admin or tech tech.

Change the password to something that cannot be easily broken. I.e. mixture of letters and numbers. Record the password somewhere secure and then reboot the router.

For more details on how to increase the security of the PCs connected to the network, see

[www.helpaccountants.co.uk/members/documents/Software and Systems Safe PC Setup SS016.pdf](http://www.helpaccountants.co.uk/members/documents/Software_and_Systems_Safe_PC_Setup_SS016.pdf)