

## Home network security scrutinised

**Home computer users who leave default passwords on network hardware unchanged could be at risk from attack say security experts.**

Researchers created an attack that surreptitiously redirects a user to nefarious sites once they have visited a booby-trapped webpage.

The attack works by re-writing the address book in network hardware to point victims to the scam sites.

About 50% of users leave default passwords unchanged, suggests research.

The theoretical attack was explored in a paper written by researchers from the University of Indiana and security firm Symantec.

In the paper the authors detail how to compromise the routers many people use to share broadband connections between machines in their home.

" This potential threat could affect up to 50% of all home broadband users," said Dr Zulfikar Ramzan of security firm Symantec.

"We're trying to get the word out there and tell people that the only thing they need to do to protect themselves from this very grave threat is change their home router password."

Making changes to a routers set-up requires the use of an administrative password, but the researchers said informal studies suggest that about half of router owners never change the default.

"Most people don't know their router even comes with a password," said Mr Ramzan.

"As a result, most routers still use their factory default settings with easily guessed passwords such as "admin" or "password".

**Fortunately, this attack is easy to defend against**  
Zulfikar Ramzan

Their paper shows how a booby-trapped webpage could use these default passwords and JavaScript - a technology enabled on 95% of computers - to change a router's DNS settings.

The Domain Name System (DNS) turns the web names that humans use into the numeric form that computers prefer. By compromising the router malicious hackers could make it direct people to fake address books.

### Phish Pharming

These fake DNS servers could redirect users to counterfeit banking, e-mail, or government sites which then collect sensitive details like account numbers, usernames, and passwords.

Phishing attacks, where users believe they are on a legitimate site when actually connected to a bogus one, are not new. However, these schemes are usually limited to individual pages.

This method would let hackers do wholesale phishing, called pharming, by redirecting every web address to illegitimate servers that either collect information or attempt to install malicious software.

"Fortunately, this attack is easy to defend against," one of the paper's authors, Zulfikar Ramzan, said on his blog.

"There is an easy fix - you just change your router password and you're all set," said Dr Ramzan.

The security team said they had contacted all of the main router suppliers about the potential attack.

So far only Cisco has issued customer guidelines in response, directing customers to information about changing their passwords.

Story from BBC NEWS:

<http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/6367691.stm>

Published: 2007/02/16 12:44:45 GMT

© BBC MMVII