

# Hackers can swap the Internet access address book

Reconfiguring the router is a new type of computer attack. Accordingly, the hacker can find the IP address and change the router settings so that the familiar website addresses stored on the computer will point to the fake page.

**Reconfiguring the router is a new type of computer attack. Accordingly, the hacker can find the IP address and change the router settings so that the familiar website addresses stored on the computer will point to the fake page.**

According to researchers at Indiana University (USA) and Symantec anti-virus software, anyone with little computer knowledge can also find routers (routers that help computers connect to the Internet) on computers. Change and change some important settings to secretly exchange the actual website into a phishing page, request log-in information (username and password).

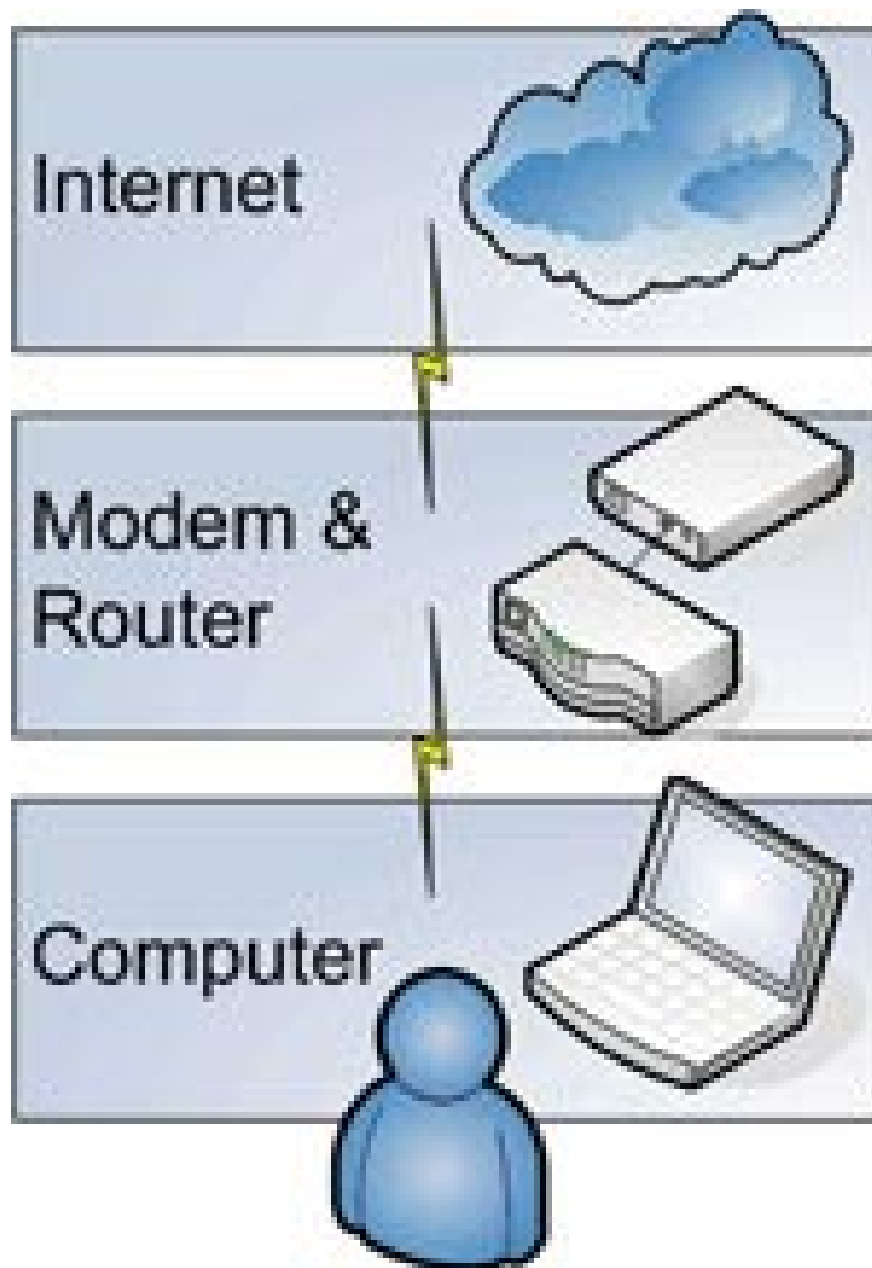


Although the address displays the correct domain name, the site may appear to be fake. " *The problem is that users don't notice the phishing sign immediately ,*" said Sid Stamm, an expert at Indiana University. " *For example, a person who types a bank domain name in the address box may be greeted with a legitimate page-like page. But all the login information on it will go straight to the fraudster .*

In essence, this old attack type has a "pharming" name. However, this is the first time experts have found a new trick at the website. It can be used to attack home routers and control domain server settings. What the hacker needs is the user's IP address and password to enter the router's settings.

First of all, the attacker builds a popular website fake page that entices users. While the victim is operating, an "invisible" code retrieves the IP address and detects the router for the device's branding sign, such as the

manufacturer's logo. These activities do not cause any alarming effects because the router thinks it is a legitimate request for information from the victim's computer.



The model connects the computer to the router and modem to access the Internet. *Photo: Microsoft .*

Then the attacker detects the password on this router. But because many unintentional people leave the manufacturer's default password easy to remember, this is not difficult for hackers. According to a study last year, up to 50% of people use the default password or do not set a password. Often routers allow for another password option to prevent people from accessing the wireless network, but users often ignore it and this is the weakness that hackers focus on exploiting.

With an IP address and configuration password, an attacker can easily change the domain name server that the victim uses as the Internet access folder. " *It's like changing your phone book with another,* " said Zulfikar Ramzan, Symantec's expert. " *And now the user will access the website address from the hacker notebook* ".

When the victim goes to the page of a bank, the web browser may point to a fake page that the hacker runs. They will save all the information they type on the website.

*Therefore, experts note Internet users :*

- Need to change the configuration setting password on the router regularly and use more complicated symbols. Save this password to paper and place it in secret.

- When setting a password on a computer, it is recommended to check if the device has stolen software to type keys or screen capture.

## **Thuy Huong**

You finished reading the article "**Hackers can swap the Internet access address book**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.