Home internet connections hacked – here's how to protect yourself

May 4 2018, by Sandeep Nair Narayanan, Anupam Joshi And Sudip Mittal

Credit: Peter Olexa from Pexels

In late April, the top federal cybersecurity agency, US-CERT, announced that Russian hackers had attacked internet-connected devices

throughout the U.S., including network routers in private homes. Most people set them up – or had their internet service provider set them up – and haven't thought much about them since. But it's the gateway to the internet for every device on your home network, including Wi-Fi connected ones. That makes it a potential target for anyone who wants to attack you, or, more likely, use your internet connection to attack someone else.

As graduate students and faculty doing research in cybersecurity, we know that hackers can take control of many routers, because manufacturers haven't set them up securely. Router administrative passwords often are preset at the factory to default values that are widely known, like "admin" or "password." By scanning the internet for older routers and guessing their passwords with specialized software, hackers can take control of routers and other devices. Then they can install malicious programs or modify the existing software running the device.

Once an attacker takes control

There's a wide range of damage that a hacker can do once your router has been hijacked. Even though most people browse the web using securely encrypted communications, the directions themselves that let one computer connect to another are often not secure. When you want to connect to, say, theconversation.com, your computer sends a request to a domain name server – a sort of internet traffic director – for instructions on how to connect to that website. That request goes to the router, which either responds directly or passes it to another domain name server outside your home. That request, and the response, are not usually encrypted.

A hacker could take advantage of that and intercept your computer's request, to track the sites you visit. An attacker could also attempt to alter the reply, redirecting your computer to a fake website designed to

steal your login information or even gain access to your financial data, online photos, videos, chats and browsing history.

In addition, a hacker can use your router and other internet devices in your home to send out large amounts of nuisance internet traffic as part of what are called distributed denial of service attacks, like the October 2016 attack that affected major internet sites like Quora, Twitter, Netflix and Visa.

Has your router been hacked?

An expert with complex technical tools may be able to discover whether your router has been hacked, but it's not something a regular person is likely to be able to figure out. Fortunately, you don't need to know that to kick out unauthorized users and make your network safe.

The first step is to try to connect to your home router. If you bought the router, check the manual for the web address to enter into your browser and the default login and password information. If your internet provider supplied the router, contact their support department to find out what to do.

If you're not able to login, then consider resetting your router – though be sure to check with your internet provider to find out any settings you'll need to configure to reconnect after you reset it. When your reset router restarts, connect to it and set a strong administrative password. The next step US-CERT suggests is to disable older types of internet communications, protocols like telnet, SNMP, TFTP and SMI that are often unencrypted or have other security flaws. Your router's manual or online instructions should detail how to do that.

After securing your router, it's important to keep it protected. Hackers are very persistent and are always looking to find more flaws in routers

and other systems. Hardware manufacturers know this and regularly issue updates to plug security holes. So you should check regularly and install any updates that come out. Some manufacturers have smartphone apps that can manage their routers, which can make updating easier, or even automate the process.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Home internet connections hacked – here's how to protect yourself (2018, May 4) retrieved 18 September 2024 from https://phys.org/news/2018-05-home-internet-hacked.html