TOTAL MEDICAL COMPLIANCE
www.totalmedicalcompliance.com
(888) 862-6742

Cybersecurity & COVID-19

March 31, 2020

Cybercriminals are gaining access to home and small business routers and redirecting victims to fake COVID-19 themed websites that install malware.

A commonly faked website is the World Health Organization's website. When the victim is redirected, they are instructed to download an application that offers the latest updates on COVID-19, which is actually malware.

This then enables the cybercriminal to collect account credentials and payment card information.

Linksys and D-Link routers are the kinds of routers currently being targeted.

If you have one, be careful if navigating to the following sites (watch your browser address bar for redirected site names) and do not download applications from or click pop-ups or advertisement prompts.

- aws.amazon.com
- goo.gl, bit.ly
- washington.edu
- imageshack.us
- ufl.edu, disney.com
- cox.net
- xhamster.com
- pubads.g.doubleclick.net
- tidd.ly
- redditblog.com
- fiddler2.com
- winimage.com

Resources:

- Full article from infoRisktoday.com: Hijacked Routers Steering Users to Malicious COVID-19 Sites
- TMC COVID-19 Resource Page