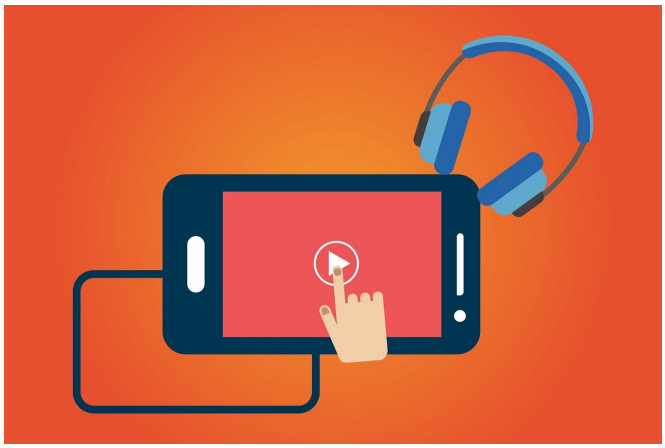
Scammers are creating Netflix lookalikes to target people staying at home, study finds

6 April 2020, by Dalvin Brown, Usa Today



Credit: CC0 Public Domain

Scammers are focusing more attention on people looking to stream content from Netflix during what has quickly become the stay-at-home era.

Researchers at the cybersecurity security firm Check Point recently released a study noting a substantial rise in the number of cyberattacks performed by websites posing as the streaming giant in the wake of the ongoing coronavirus crisis.

Over the past two weeks, more than 30,103 new coronavirus-related domains were registered, of which almost 3,000 were malicious or questionable and under investigation, researchers said.

Phishing attacks by Netflix look-a-likes doubled, and many of the websites offer payment options to steal user data and payment information.

"As the number of physical casualties increase, so is the number of cyberattacks relating to the virus," said Omer Dembinsky, data manager of threat intelligence at Check Point. "Clearly, hackers are shifting their resources away from targeting businesses ... and towards activities that can reach us directly in our homes."

On average, over 2,600 coronavirus-related cyber attacks occur each day, the researchers said. And bad actors aren't just targeting people looking for TV shows and movies.

Zoom, which has become a household name as people conduct more remote meetings and video chats, is also a favorite among hackers.

Check Point Research saw a recent spike in the number of "Zoom"-related domains registered and spotted malicious "Zoom" files targeting remote workers. Over 1,700 new "Zoom" websites were registered since the coronavirus pandemic started, 25% of which were registered over the past week.

Security researchers are also warning of the new trend of "Zoombombing," where people crash public meetings with curse words, obscenities and worse.

So what can I do to stop it?

Following common-sense safety practices can protect your data and financials from hackers using look-a-like websites:

1. Watch for spelling errors in emails or websites.

2. Look out for files received via email from unknown senders, and be warry if they prompt for a certain action you would not usually do.

3. Make sure you do not reuse passwords between different applications and accounts.

APA citation: Scammers are creating Netflix lookalikes to target people staying at home, study finds (2020, April 6) retrieved 19 August 2022 from https://techxplore.com/news/2020-04-scammers-netflix-lookalikes-people-home.html