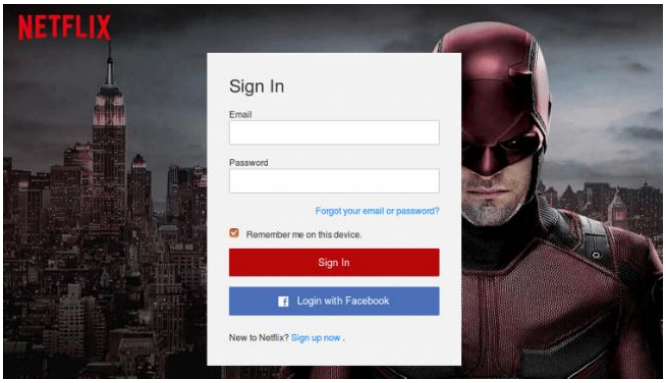
Security and Risk online: Netflix Users Targeted with yet another sophisticated Phishing Scam

If you have a Netflix account you might be at risk of falling prey to a new phishing scam that targets Netflix users through emails. These emails contain a fake login screen of Netflix and ask for the login information. If the user enters the login information, the scammers ask for the credit card details.



This particular campaign has been discovered by FireEye Labs. The company maintains that this phishing campaign is aimed at obtaining personal and financial information of Netflix's customers. The scammers have used some

different tactics of malware and encryption, which make this campaign different from other phishing scams. These tactics help the campaign prevent detection from spam stopping applications and phishing filters and easily deceives and trap innocent users. FireEye researchers also state that the domains they identified to be used in this campaign are not active anymore, which means that the scammers also keep changing domains to prevent their origins from being traced.

More: Netflix Users Targeted with Phishing, Malware Scams Stealing Credit Card Data

According to FireEye Labs' Mohammed Mohsin Dalla, "the phishing websites we observed were no longer active." While the Aroostook County Sheriff's Office in Maine released a summation asking Netflix users in the US to be cautious while opening and viewing emails that ask for Netflix credentials.

The scam involves sending emails to Netflix users asking them to update their membership information by firstly entering their login details. In this regard, scammers have created a genuine-looking, but fake, Netflix login page where the option to log in via Facebook is also available. Once entered, the request for more information continues as the users are asked to enter a home address and then fill a form in which their credit card information is required. After the user has provided all the information, their real Netflix profile page appears.

This scam is unique in various respects; such as it uses pages that were on web servers and were infected to host this campaign, the pages looked genuine and the information from the victims was encrypted using AES encryption, which is why it was difficult to detect this scam and lastly, the hacked pages were IP-filtered and would show in a hand-in internet security like Google. Such services will receive a 404 error. The attackers obtain the information through a PHP-based email system.

More: Cover Your Cams: Webcam of This Couple Got Hacked While Watching Netflix

If you receive an email where a sender is asking you to download a file or click on a link we recommend simply ignoring and deleting that email. Never download/click on any file that comes from an unknown sender. Happy browsing.