

7 July 2010

By: Lucian Constantin, Security News Editor



Facebook scam tells users to paste malicious JavaScript into their browsers

[Facebook Users Tricked into Loading Malicious Code in Their Browsers](#)

Unwatchable video used as lure

Security researchers from AVG warn of an ongoing Facebook scam which asks users to paste malicious JavaScript into their browser's address bar. Users are lured onto pages that claims to contain a video 99% of people can't watch until the end.

The rogue Facebook profile pages are called "99% of people can't watch this video more than 25 seconds" and display a picture of a girl using her palms to covering her face. Users who land on these scam pages are encouraged to click on the "Video Here!" tab, where a fake video player is displayed.

Underneath the video player image there is a message which reads: "Copy the code below, paste it into your browser's address bar and press enter to load this video..Plz wait 7-8 secs for processing!!!" A text box below it contains obfuscated JavaScript code, which if pasted into the browser, automatically "Likes" the page and posts a rogue status update on the victim's profile, promoting it.

"It's not clear what the payload is at this point, because we're still figuring it out, but it's probably one of the sites that wants to charge you \$9.95 a month automatically to your mobile phone account," Roger Thompson, chief research officer at AVG, [writes](#) on his blog. He also points out that the particular page he analyzed was "liked" by almost 600,000 users.

We were not able to locate that particular page ourselves, probably because it was already deleted by Facebook's security team. However we did find many identical ones which are still live at the moment and so far have been liked by thousands of users.

The "copy this code in your address bar" trick is not new. Just last week we [reported](#) on an Orkut phishing scam that tricked users into loading malicious JavaScript into their browsers by promising a free mobile credit recharge code.

You can follow the editor on Twitter [@lconstantin](#)