

Forum:[Hack Forums](#)

Thread: [How can you bypass a fake ap asking for credentials](#)

ColorMeEvil - October 15, 2016, 10:11 am

Let's say there was a hacker in your area who set up a unsecured open AP asking for your Time Warner credentials when you try to connect to the Internet.

Is there any way to bypass the credentials page, and just use the internet?

Also in the same vein, if someone were to use fluxion on your network and you were aware of it, what could you do?

pomwtin - October 15, 2016, 11:31 am

(Oct 15, 2016 10:11 AM)ColorMeEvil Wrote: [\[CITE\]](#) Let's say there was a hacker in your area who set up a unsecured open AP asking for your Time Warner credentials when you try to connect to the Internet.

Is there any way to bypass the credentials page, and just use the internet?

Also in the same vein, if someone were to use fluxion on your network and you were aware of it, what could you do?

What makes you think rogue AP will have working WAN connection? It could just shut down after credentials were verified...

It depends on how rogue AP would be made, there are several ways of limiting what "user" is able to do.

If AP is simple and really basic- using only DNS spoofing and indeed has WAN access, then you could just type IP into url bar :P (just a basic example)

You could perform deauth attack on it, try to overload it somehow, connect to it and try to hack the hacker :P, etc...

Some APs have this option, and all they do is inform administrator and perform deauth attack on rogue AP (but what if fake AP uses encrypted management frames??)

Novoo - October 17, 2016, 4:16 am

Find the asshole (just go where the signal is strongest) and beat him up

rewtus - October 18, 2016, 7:07 am

Currently the only cure against fluxion is to change the channel as it's not following it automatically due to a limitation in the design, but that will resolve it until the attacker follows it along on the new channel manually. The only complete solution is to stop using wireless and resort to a wired connection in case you're not able to find and beat him as suggested above. :)

Deus Ex Machina - October 18, 2016, 12:03 pm

(Oct 15, 2016 10:11 AM)ColorMeEvil Wrote: [\[CITE\]](#) Let's say there was a hacker in your area who set up a unsecured open AP asking for your Time Warner credentials when you try to connect to the Internet.

Is there any way to bypass the credentials page, and just use the internet?

Also in the same vein, if someone were to use fluxion on your network and you were aware of it, what could you do?

Never have tried this for ISP APs, but on airlines and hotels you can spoof a client's MAC address and get access to bypass the login...although you end up dropping packets because the AP doesn't know which one of the two identical MAC addresses to send packets too.

rewtus - *October 19, 2016, 5:05 am*

Also is the captive portal only for traffic running on port 80? I have seen places where they catch only plain http traffic only and it flows freely on all of the others ports, so you can go around it by using a SSH tunnel or VPN. The easiest way to spot such access points of for example if you have skype running and it's able to connect when you associated to the AP.