

Forum:[Hack Forums](#)

Thread: [What can be done with people connected to your wifi?](#)

jessepinkman420 - August 7, 2022, 11:31 pm

Hey, I am wondering about the power one would have if he were to, for example, create a WiFi network called 'Starbucks Guest' in a Starbucks and have people connect to it. Apart from DNS spoofing, what could be done?

BiNBo - August 8, 2022, 5:27 am

Well, there's definitely a lot of vulnerability that can be created from this type of setup no doubt. Anybody connecting to your network could be at risk of a variety of attacks. Malware distribution, Man In The Middle attacks, etc. You could leverage the situation to some pretty extreme degrees. Did your imagination have any specific questions regarding what might be possible?

jessepinkman420 - August 8, 2022, 5:56 am

(Aug 8, 2022 05:27 AM)BiNBo Wrote: [\[CITE\]](#) Well, there's definitely a lot of vulnerability that can be created from this type of setup no doubt. Anybody connecting to your network could be at risk of a variety of attacks. Malware distribution, Man In The Middle attacks, etc. You could leverage the situation to some pretty extreme degrees. Did your imagination have any specific questions regarding what might be possible?

How would one go about distributing malware through devices connected to the wifi? I didn't even know that was possible. I myself have no idea what can be done other than DNS spoofing (maybe). I was hoping to get a better idea of what's possible

johnhoea - September 7, 2022, 6:48 pm

depends on your skills , there could be done anything from sniffing credentials to opening a camera to having full control of the device , depends on your skills

DramaKing - September 11, 2022, 12:52 pm

(Aug 8, 2022 05:56 AM)jessepinkman420 Wrote: [\[CITE\]](#) How would one go about distributing malware through devices connected to the wifi? I didn't even know that was possible. I myself have no idea what can be done other than DNS spoofing (maybe). I was hoping to get a better idea of what's possible

I guess one could use drive-by downloads on a captive portal, though it would be plenty obvious. There's also SSL stripping and HSTS hijacking for packet sniffing.