How to get gogo in flight wireless internet for free.

****DISCLAIMER****

Stealing internet is illegal. I do not condone stealing of internet services. This is merely a flaw in their system that I reported to them on August 15, 2013. I take no responsibility for your actions. The information provided is without warranty. Seriously, do not try this at home or in flight.

A little history on the matter. We were on a flight to DEF CON (this is how good stories start) and were in the mood. Rather than be destructive, we set out to see if we could gain internet access while on the plane. In short, we were successful and it was much easier than we imagined.

We were only armed with a rooted Android tablet and two rooted Android phones. You only need one rooted Android device or pretty much any PC. For the sake of this article and from in flight experience, Android was used.

So here goes:

Apps you need for this demonstration:

- DSploit
  http://dsploit.net
- ChangeMac http://code.google.com/p/diewland-quick-code/downloads/detail?name=ChangeMac.v.0.9.apk

However I'm sure there are equivalent apps out there that are also free and readily available.

Warning, these steps are all from memory and are by no means exact.

Part 1:

1. Once you hit 10,000 feet and it's deemed safe for electronics by the pilot, fire up DSploit.
2. Connect to the gogo network and then select the network's subnet mask (the one ending in 0/24)
3. You are going to want to run a MiTM (Man in The Middle) attack, so select that.
4. On the next screen select Session Hijacker. This will hijack the sessions of those who are about to purchase some internets.
5. Give it a few minutes, you'll need to gather a session from someone who just paid. Once you find one that says gogoair.com or similar (I forget what domain is used in flight) you should be good.
6. Note the IP address of the user and then replay their session, it'll show you the "Thanks for paying" page. This gives you the authentication you need. If not, go wait for another session.

When I made it to this point, it would attempt to give me internet but it wasn't 100% working. For the record, replaying their session logs you into their account where you are able to purchase more wifi time without a password or credit card information.

Part 2:

1. So now you've got the session needed and the IP associated with that session. Go back a few pages in DSploit, it'll show you the list of connected devices (Where you selected the 0/24 subnet earlier)
2. Find and match the IP of the user you hijacked the session from, it will also display their mac address. Copy it down
3. Open ChangeMac and spoof your mac address to theirs.
4. You may need to reboot

You should now have internet!

I'd also like to note that you could then continue hijacking sessions and do other things while on that network since AP isolation is disabled. I'll let you use your imagination.
Something else I'd like to point out, you can do all of this without agreeing to the terms of service or even displaying the terms of service.
Disclosure history:

- 8/15 - First contacted vendor notifying them of issue/asked about bug bounty program (Need some cheddar, ya know?)
- 8/21 - Manager of Information Security, Scott, responds asking to know more about the issue described. Tells me there isn't a Bug Bounty Program
- 8/21 - I respond that I am disappointed with the lack of Bug Bounty Program but then fully disclosed the issue and suggested AP isolation.
- 8/26 - I never heard back from Scott. I write back to him that I'd like to talk/post about my findings publicly and would like to make sure things are patched first.
- 9/5 - Still nothing from Scott. I tell him again that I'd like to publish my findings and that I would really like to make sure things are fixed before I go public.
- 9/5 - Scott's auto-responder says that he is out of the office with limited access to email for the day and that he will respond to my E-mail when he returns
- 9/9 - I alert Scott that I'll be disclosing this on the 15th
- 9/9 - Scott responds that he is pushing for a Bug Bounty Program (woo!) and would like to preview what I'm going to publish (this)
- 9/15 – Haven't heard back from Scott, not publishing yet.
- 9/16 – I wrote Scott back asking for his comments before I publish.

I have no idea if this is fixed yet or if they are even fixing it.