Desmond Hughes

Purdue University Global

IT262 Certified Ethical Hacking I

Cheryl Waters

August 22, 2022

If my friend lost his job and doesn’t have cable TV and he doesn’t have Internet access, I would encourage him to find another way to get the things he needs instead of me breaking the law. I would not use my ethical hacking skills to hack the neighbor’s wireless signal to gain access to the internet. Even though he needs the internet to search for a job, I would tell him there are a couple of different resources to look for jobs. He could go to the library, and take advantage of their free internet. My friend could also go to restaurants like McDonalds or even Starbucks, who also have free internet. He can also go to jobs and ask for an application if they offer them, and even go to open interviews. I would not help my friend hack into the neighbor’s wireless network so that, he can look for a job. There are many opportunities to get a job.

I wouldn’t help my friend, because it isn’t the right thing to do, and it can lead to getting in trouble and catching charges, which will be on my record. With it being on my record, future jobs will do background checks and notice them. I could lose my current profession if I get caught, especially if it deals with ethical hacking. If the manager see I use my skills for other than work and for illegal purposes, it won’t look good on my part. Performing that hack may ruin my life.

If I did say yes, I would have to be very carful not to get caught, because if I do then I will have to face the consequences. There are multiple ways I can hide myself and keep my identity safe from being figured out. One thing I can do is not use Windows. Instead, I could use other open-source operating systems, for example Tails or Whonix. Another thing I can do to not get identified is not to connect directly to the Internet. I can hide myself and stop myself from being tracked down by hiding my IP address using VPN and TOR, which blocks trackers. VPN creates an encrypted private tunnel, and TOR is a network that nodes routes of your traffic. Another thing I can do is not use my real email. That way it will be harder to trace back to me, and it will be more anonymous. Another thing I can do is not use public Wi-Fi. Using public Wi-Fi, it can be traced back to you. There are multiple ways to backup my steps so that I won’t be discovered. The answer will still be no I still wouldn’t hack the neighbor’s wireless network.

Hacking someone’s wireless network is considered to be unauthorized access of a computer network. That is when someone gains access to a computer network, system, application, and data without permission. Doing that is violating the owner of that wireless networks personal space. You must have consent when using someone else's wireless connection. There are three primary objectives that are used to prevent unauthorize access, Confidentiality, Integrity, Availability. Confidentiality meaning protecting sensitive information from being access. Integrity meaning protecting information from being changed or destroyed. Availability protecting information from disruption. All fifty states have computer crime laws that addresses unauthorized access and computer trespassing. In result of being caught you will get a citation, which varies depending on the state you are in.

Computer Crime Statutes. (2022). Retrieved 23 August 2022, from https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx

Ian Sutherland - Thriller Author. (2022). Retrieved 23 August 2022, from https://ianhsutherland.com/5-ways-computer-hackers-remain-anonymous/

Unauthorized Access: Prevention Best Practices | Egnyte. (2022). Retrieved 23 August 2022, from https://www.egnyte.com/guides/governance/unauthorized-access