Ian Waweru

Lucinda Wittkower

Information literacy

10/31/2021

Ghost in the cloud

I’ve heard many stories before about hacking and they always had to do with international breaches or personal information being extorted. However, after watching an interview with Kevin Mitnick I found his stories to be interesting and entertaining. He was able to do a lot of things without using any high-end technology system to help him. One of the stories he told was about how he was able to hack into McDonald’s. He was able to do this by using a radio signal that was much stronger than the McDonald’s employees’ microphone. He would proceed to interact with the customers and act as an employee for fun. I found this story fascinating and funny because he was only 16 and was able to hack into McDonald’s at his age. I did something like this one time however, it wasn’t as significant or problematic as Kevin’s story. I would connect my phone to a speaker and when my roommates ask for it I would also be connected. So when they turned it on I would still be connected since I had a stronger signal to it than they did. I would play funny videos and other content just so I could their expressions afterward. It’s a similar concept but it’s still different because a McDonald’s microphone probably has a higher frequency. He also demonstrated an attack called the IVR spoofing attack. This attack has to do with how a hacker can achieve banking information after a conversation between a client and their bank. He showed on the screen an application called spy bridge and you can see the call going on between Kevin and his bank. He would proceed to put in his information and his location then continued to complete the call. As he finished up you can see how spy bridges the information he typed in on his phone and his area code. That application he showed is an example of how an attack can occur on your banking account. I found this demonstration to be very informal because it showed me how easy it was to access my information using another system. He said in the video this challenge can be hard to mitigate this type of attack however if I want to protect my information I would go to the bank in person. I believe it’s also better to log in to your bank on a computer because you can trust yourself and the computer safety mechanisms. On the phone, it can be hard to tell who is listening and whom you’re talking to. Overall, it’s important to be aware of what’s going on because the most unlikely can happen based on what I watched.

**SOURCE:**

[**https://www.youtube.com/watch?v=76yrWGzScgI**](https://www.youtube.com/watch?v=76yrWGzScgI)