I was not able to read the Medium article. I did find another article regarding multi-factor authentication <https://www.cybersecuritydive.com/news/multifactor-authentication-weaknesses/633399/>. This article posits that MFA is only as strong as the weakest point: “it would be somewhat pointless to use email-based MFA if your email itself does not have MFA,” Sounil Yu, CISO and head of research at JupiterOne.

Multi-factor authentication was the first thing I searched for due to Greg (NPR article) and Matthew (ZDNet article) both mentioning non-SMS based MFA. Matthew’s article in particular I found lackluster. He mentioned removing personal data from Google Drive but still uses it for photos. From photos, people can create ridiculous videos like this: <https://www.youtube.com/watch?v=EF-y4zUZps0>. They can also use photos for more malicious means as well.

Within my network, I protect myself by keeping my credit accounts frozen. All my passwords were created by several algorithms that I subsequently sliced, diced, and mashed together adding a sprinkle of my own within them. Those passwords are kept on a sheet of paper in my house.

I try to avoid cross dependencies, such as relying on my phone number to open or access other accounts. The one exception is Venmo, which I have tied to a credit card instead of bank account. Theoretically, I should better in a better position to stop a payment from a credit card than recover money that was withdrawn from a bank account.

The other big weakness associated with my phone isn’t from my phone itself – it’s from my smartwatch. It doesn’t automatically connect to my phone unless I have Bluetooth on to update my health records and fitness results. That should make it slightly better than being constantly connected and communicating with my phone.

Outside of those two apps, I don’t believe anything is specifically tied to my phone/phone number. I attempt to avoid giving away as much contact information as possible when setting up accounts.

When it comes to the IoT (internet of things), I only use the smart watch. I don’t want a smart refrigerator, smart laundry, or anything else that requires an internet connection. Speaking of “smart” items, there was temporary outroar of Netflix’s crackdown on password sharing - Netflix customer service representatives were telling Tesla owners to purchase an additional account for their Tesla. <https://www.notateslaapp.com/news/1202/netflix-s-new-password-sharing-policy-won-t-affect-your-tesla>

I could strengthen the security of the network by changing the default IP address, changing the router password, adding encryption methods, using a VPN, creating a “guest” network, turning off universal plug and play features. <https://consumer.ftc.gov/articles/how-secure-your-home-wi-fi-network> I could also install additional firewall and cyber security protections on my phone.

Strengthening all of my accounts, with various passwords and answers to security questions, is the best way to prevent someone from accessing an account using publicly identifiable information. When it comes to cell phone usage, acting like a drug dealer would likely lead to the best results security wise. Get some burner phones and go through them periodically. Keep the apps on the phone separate by grouping so general communication is held on one phone and apps with sensitive information is on another phone.

There isn’t a great way to avoid being a victim without dedicating a massive amount of time to protecting oneself. The best thing to do is to minimize potential loss by partitioning accounts and providing random answers to questions and new passwords for each account.