Read the following articles:

· <https://www.digitaltrends.com/mobile/sim-swap-fraud-explained/>

· <https://www.itworldcanada.com/article/warning-protect-your-mobile-phone-numbers-from-being-hijacked/396018>

· <https://www.wired.com/story/sim-swap-attack-defend-phone/>

Questions:

1. What is a SIM card?

A sim card is a smart card inside a mobile phone that stores and carries out your personal information.

2. Why is a SIM card required for your phone to work?

A SIM card is required for your phone to work because without a SIM card, yo u can’t connect to a mobile phone network and if you are not connected to a mobile phone network than you would not be able to make phone calls, and message people on the go because you don’t have data.

3. What is “[text-based two-factor authentication](https://www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication)” ?

Text-based two-factor authentication is a method of confirming users and identities by using a combination of two different factors such as something they know or something they have.

4. How is two-factor authentication related to your phone?

Two-factor authentication is related to my phone such as an Iphone because it asks you for your password, touch ID, and security questions, just Incase if someone has your phone, that person would have to go through everything to access your personal information. This would make it really difficult for someone that is trying to break in or access your personal information.

5. How is two-factor authentication related to your SIM card?

It’s related to a SIM because a SIM has a password or security question that only you would know and your phone/carrier company. This makes it’s more secure and harder for a hacker to steal information.

6. List some of the services criminals can access if they get control of your SIM card.

a. Banking & Financial

b. Social Media

If criminals get control of your SIM card, they can access your social media such as Instagram, Twitter, Snapchat, and Facebook. They can access your contacts, photos, and text messages.

They can only access your banking/financial information only if you fully saved it on your phone.

7. Explain how criminals can get control of your SIM card.

a. Collecting Personal Information

b. Create False Identity

c. Requesting a new SIM card

They can get your SIM card by physically hurting you and taking it by hand. They can follow you around to get your personal information, and when they have your information they can try hacking you.

8. What are some signs of SIM swap fraud?

Some signs of SIM swap fraud is mostly by text messages and phone calls. Once the perpetrators deactivate a SIM, messages and calls won’t go through and this is how you know that you have been targeted and your information is comprimised.

9. How can you prevent SIM swap fraud?

a. What are some general methods

b. Who is your Canadian phone company / carrier?

c. What do they offer regarding SIM swap fraud prevention?

Do not share your personal information with strangers. You can talk to your phone company/carrier service and maybe ask for a secret password when everytime you want to access your personal information so by this, your account information will be really secure and it would be really hard for someone to steal it.