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?

* SIM stands for subscriber identity module or subscriber identification module.
* A SIM card is a small smart card made up of embedded contacts and semiconductors
* SIM card is what provides your phone an identity. That is where you get your phone number from.

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

It gives the phone a phone number.

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 when websites uses verification from your phone to log in. It sends you a text asking if you want to login.

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

Two factor authentication uses your phone to login. That

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

Your SIM card is where your phone gets its texts and calls. It is basically the identity of the phone and so the two factor authentication contacts your phone through the SIM card. If the SIM card is taken then the two factor authentication contacts the SIM card, giving whoever stole it access.

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

a. Banking & Financial

Virtual currency traders, Bitcoin.

b. Social Media

Email, iMessage, Messenger, Twitter, LinkedIn, etc.

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

a. Collecting Personal Information

Through your SIM card the criminal could go through your contacts and gather information about where you live, your age, etc. They can also get this information from checking your accounts on social media or other websites.

b. Create False Identity

They could get access to all your accounts. By doing this they can act as you on these websites and text and act normally but also post private information or pictures on the internet, under your name. They can also use your money if you have your passwords online.

c. Requesting a new SIM card

One reason it’s so easy because you can easily call your phone provider and ask for another SIM card, which they will send to the criminals location and you wouldn’t even know about it until you ask. They ask simple and easy questions that anyone can get answers to quite easily by doing some further research.

8. What are some signs of SIM swap fraud?

If there are posts of things you didn’t post or if your friends are getting texts from you that you didn’t send. If there is any fishy business revolving your accounts and random actions that say you did it but you really didn’t do it. This means someone else may be doing it under your name.

9. How can you prevent SIM swap fraud?

a. What are some general methods

Not give two factor authentication access. This makes it so the hacker doesn’t have access to all your accounts and login information so even if they have the SIM, they can’t do much. Be wary of where you put all your information on your accounts. Sometimes it’s better to keep your accounts private and not give all your personal information away.

b. Who is your Canadian phone company / carrier?

Fido and Rogers

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

There isn’t much on what they do to makes sure SIM swap doesn’t happen too often, but it does talk on identity theft which will be taken really seriously. If they talk on their consequences of the identity theft and fraud, people will be more scared to do it in the first place.