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 card which is small in size and it stores personal information of a specific user in Global System for Mobile phones

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

A SIM card is required for your phone to work because it allows it to connect to a mobile network.

1. 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 another piece of security which is in the form of an unsystematic generated code and it is required to be inputted along with a password and username.

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

Two-factor authentication is related to your phone because it is a security code that can only be received on your phone.

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

Two-factor authentication is related to your SIM card because it is a piece of information that gets sent through SMS messaging and that is solely connected to your SIM card.

1. List some of the services criminals can access if they get control of your SIM card.
   1. Banking & Financial

Criminals can send phishing emails to credit card companies and they can fool them into giving personal information about a victim and their credit card number. They can access bank accounts of victims and create a second account so that they can transfer their money to it.

* 1. Social Media

Criminals can access your social media services such as Instagram, Twitter, and LinkedIn.

1. Explain how criminals can get control of your SIM card.
   1. Collecting Personal Information

Criminals can gather personal information from the victim’s social media accounts and through phishing emails.

* 1. Create False Identity

Criminals can create a false identity by going to a bank that a victim has an account registered in and they can create another identical account for money transfer.

* 1. Requesting a new SIM card

Criminals can call phone providers and they can tell them that they lost a SIM card and they can give them personal information about the victim.

1. What are some signs of SIM swap fraud?

Some signs of SIM swap fraud are deactivation of your SIM card, a decrease in deposited bank money, application login changes, and phone number theft.

1. How can you prevent SIM swap fraud?
   1. What are some general methods

Some general methods to prevent SIM swap fraud are to set up a PIN number, not post personal information on social media, and using an authenticator app.

* 1. Who is your Canadian phone company / carrier?

I do not own a phone but the Canadian phone company of my parents’ is Fido.

* 1. What do they offer regarding SIM swap fraud prevention?

Fido does not offer anything regarding SIM swap prevention. One Canadian company that does offer SIM swap prevention is Telus. Telus provides a secondary set of security questions and PINs to make it more difficult for criminals to get their hands on SIM cards that do not belong to them.