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 for a cellphone is a storage for the users data

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

Without the SIM card you have no mobile network

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

It keeps your password safe and it is a extra layer to security

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

Without this someone can easily get you passwords from your cellphone number.

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

Without this someone can easily get you passwords from your cellphone number.

1. List some of the services criminals can access if they get control of your SIM card.
2. Banking & Financial
3. Social Media
4. Photos
5. And other personal information
6. Explain how criminals can get control of your SIM card.
   1. Collecting Personal Information
   2. Create False Identity
   3. Requesting a new SIM card
   4. Through your phone number
7. What are some signs of SIM swap fraud?
   1. Not having any access to your informations
   2. Your photos or private information being leaked
8. How can you prevent SIM swap fraud?
   1. What are some general methods

Creating a pin that’s not very easy to guess such as your birthday or name or 0000 is too easy to guess for someone.

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

Chatr

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

When checked on the Chatr website the site does not tell you anything about the prevention against the SIM fraud and SIM fraud in general