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 stores user data in GSM (Global System for Mobile) phones.

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

They’re mainly used to authenticate cellphone subscriptions, without a SIM card, GSM phones are not able to tap into any mobile network. Without a sim card you are unable to make phone calls, have data or text message.

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 a way of securing someone’s identity via text messages when they have signed up for a certain account via text messages

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

Two factor authentication is related to phones because lots of people sign up with social media accounts, banking, and other online accounts.

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

SIM cards are what people use to be able to access and have certain things. In addition, it is related to SIM cards because someone can swap another person’s SIM card and pretend like it is the user of the account and then access all their important information such as their banking or social media accounts.

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

* Bank Accounts
* Credit Cards
* Banking Information
* Financial Provider
  1. Social Media
* Social Media Identity
* Social Media Accounts
* Personal Information

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

What the user input into their phone will be compromised because if someone has your SIM card, then they can access a user’s personal information through the SIM card

* 1. Create False Identity

If a person has a user’s SIM card then they can create a fake identity using the identity of the SIM card and all the data that is stored on it

* 1. Requesting a new SIM card

For requesting a new SIM card the person needs to know the persons information, for example the person’s name, date of birth and etc.

1. What are some signs of SIM swap fraud?

* Messages and calls won’t go through
* Users can be compromised when trying to place a call or a text

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

* Providing passcodes when establishing service
  1. Who is your Canadian phone company / carrier?

Bell

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

Passwords

Setting pin numbers