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 cellphone SIM card stores user data in GSM (Global System for Mobile) phones.**

2. 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**

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

4. 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. And it is a way of making sure that the user of the account is actually them.**

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

**It is related to SIM cards because 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.**

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

a. Banking & Financial

**- Bank Accounts**

**- Credit Cards**

**- Banking Information**

**- Financial Provider**

b. Social Media

**- Social Media Identity**

**- Social Media Accounts**

**- Personal Information**

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

a. Collecting Personal Information

**- All the data 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**

b. 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**

c. Requesting a new SIM card

**- Criminals can call the SIM provider, pretend that they are the actual user and request for a new SIM card, even with prepared answers to the security questions because all the user’s information is stored on the card**

8. What are some signs of SIM swap fraud?

**- Users can be compromised when trying to place a call or a text**

**- Messages and calls won’t go through**

**- Some institutions call customers to determine whether they got a new SIM card or alert them that someone is potentially impersonating them**

9. How can you prevent SIM swap fraud?

a. What are some general methods

-  **Setting a PIN**

**- Providing passcodes when establishing service**

b. Who is your Canadian phone company / carrier?

**I do not have a cell phone carrier**

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

**- Setting Pin numbers**

**- Passcodes**

**- Certain application softwares can provide extra layers for two-step authentication**