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 Subscriber Identity Module (SIM) Card contains information that gives a user access to a specific mobile network. Access to a mobile network allows the user to use communication services like calling and messaging.

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

A SIM card is required for the phone to work because it connects the phone to the mobile network, which is uses to activate the phone and use specific communication services.

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 method of authentication that sends the user a message to confirm their identity when accessing a service.

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

Two factor authentication is related to our phones because when in use, an OTP (One Time Password) is sent as a text message to the user, which is then used by the user to verify their identity.

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

A SIM card is related to two-factor authentication because it is the way that phones receive messages, and these messages are used to verify the user’s identity by two-factor authentication.

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

* Address
* People under your account
* Credit Score
* Transferring Money
  1. **Social Media**
* Twitch Account (from Amazon Prime)
* Snap chat
* Facebook
* Instagram
* Pinterest

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

* Criminals follow your social media accounts to find more information about you.
  1. **Create False Identity**
* They take pictures off of Google, make notes of your information and make your full profile.
  1. **Requesting a new SIM card**
* They make a fake store to describe to the carrier company to describe how you lost your SIM card and will need a new one.

1. **What are some signs of SIM swap fraud?**

Some signs of SIM swap fraud are:

* Your phone is not working.
* No service
* The provider company calls you to confirm the new sim request.

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

Using a service provider that has special protection is a way to prevent SIM swap fraud.

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

I do not hat a carrier.

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

For this question, I will take Bell for example. All phones on the Bell company have to answer special security questions before being able to get a new SIM. The user can change this to be a very difficult to guess question and prevent a SIM swap.