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 tiny chip that is inserted into the side of your phone. This is holds your identification number (phone number) and personal information. This is what connects your identity to the phone network.

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

A SIM card contains everything that is needed for your phone to actually work and do what it is made to do. A SIM card gives your phone identity, it number, which we use to communicate.

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

Two factor authentication is when your online account asks you to identify yourself over text, which then grants access to your account.

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

The two-factor authentication related to your phone because that is where you receive the text message, which asks you to make sure that it is you who is logging on to the account.

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

Your online account asks for your phone number. This links your SIM card to your account. So when logging in you have to respond to the text message you got from the company which then grants you access to your account.

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

Data related to finances and a you banking can be taken. The hackers can steal credit card numbers and access bank accounts, gaining a lot of your financial information.

* 1. Social Media

Through your SIM card criminals can get access to your multiple social media accounts. Using your social media they can get personal information like your full name, address, date of birth, pictures and much more. They can also use these platforms putting out inappropriate and secret content, pretending to be you. If this happens you yourself can get into much trouble.

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

These criminals send out emails and messages that look like legitimate health insures or credit card companies. Through this they ask you to give your personal information. Here people usually give away their full name, date of birth, address and phone number. These criminals also go through all your social media accounts and collect whatever information they find helpful.

* 1. Create False Identity

They then pretend being you in front of your cellphone service. They answer the security questions all correctly and accurately using personal information that they have collected.

* 1. Requesting a new SIM card

When requesting a SIM card they will usual tell the cell provider that they have lost it. After answering all the security questions they will request the server to mail them a new SIM card.

1. What are some signs of SIM swap fraud?

If you phone randomly stops working. Calls and texts will not go through. Behavioral changes in the behavioral analysis technology can detect a SIM swap. Some institutions call the user and ask if they have gotten a new SIM card, fi not they alert them that someone may be impersonating them.

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

Some general methods include, carriers offer putting a PIN or passcode on your account, using a authentication app instead of a SIM card and keep your phone numbers away from your account. Also use something safer to secure your important accounts such as your bank account.

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

fido

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

Fido informs its users of the fraud. They have a section about it on their site. They tell their users to not trust anyone that calls them pretending to be a fido worker They have links to other websites which further inform you on the topic and tell you what to do if you have become a victim (link to the Royal Canadian Mounted Police site).