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/>
* <https://krebsonsecurity.com/2015/11/talktalk-script-kids-the-quest-for-og/>

Questions:

1. What is a SIM card?

A sim card is quite simple. It is a smart card inside a mobile phone and it carries an identification number which is unique to the phone and owoner, it stores personal data.

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

It is necessary for activation for one main reason. That is because it allows cellular network known which phones are using it. They need it to communicate with their cell carrier which allows them to also call others, send messages through the server the carrier provides with the sim.

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

It is a type of multi-factor authentication. Meaning it is a method of confirming users’ identity. This means they ask combinations of stuff for example something they know, and something they are. Questions that no one will know the answer to unless you are yourself.

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

It is related your phone because everyone has it. It holds private information people have. Nowadays everything is on individual’s phones. It will be a problem not having it on your phone as direct messages, photos, videos, and many more private things are stored in it. It can harm people’s lives.

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

It is related because without people can get away with identity fraud. With this being said It’s getting increasingly risky to use online services. You store a lot of your personal data in the cloud, and your credit cards are linked to accounts on retail websites. Hackers would love to get at your data, to empty your bank account, or to access your email account, using it for spam and phishing. Phishing is an online way of luring it happens in online games for example RuneScape. It is a MMORPG and people get lured for credit cards resulting in withdrawal of money and thousands of dollars in expenses. It is now moving its way on mobile phones.

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

Some services individuals can go through are your credit cards. Once with the sim card you can put it in your phone recover contacts, messages, and credit cards. Once in contacts or even messages they can harass your peers or private people you may talk to. They also can use your contacts to find out where you live and others harassing them in the future.

1. Explain how criminals can get control of your SIM card.
   1. Banking & Financial

If they know any of your banking information which can lead them into getting into the sim and causing lots of problems. Firstly, they can take stuff out of your account and use it against you. Secondly, use your information against you and do something called identity fraud.

* 1. Social Media

If they can get into your social media they can manipulate individuals into getting your own information and then using it against you pretending to be you for example contacting the companies on your account to than get a new sim and take al of your stuff.

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

Once collecting personal information, they can call your carrier and pretend to be you. Once they are successful of doing this they then steal your identity and all the belongings with it.

* 1. Create False Identity

They then create a false identity manipulating the company and people that it is you and the company easily gives more useful information.

* 1. Requesting a new SIM card

They then request a new SIM card put in a similar phone to that company and can basically get anything of yours.

What are some signs of SIM swap fraud?

Number one is phishing messages and suspicious communications asking for information. The hacker requires the victims bank details with this they can many things. Another is loss of signal. This means your sim not connecting to the server anymore meaning someone is using one claiming to be you. This is a major sign as now they are onto your own sim and can backtrack everything you have done. Lastly, random links on your phone. Never open them as they are known as phishing links and can harm your phone as well as steal information.

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

Using two step authentication and letting the company know if anything suspicious happens shut it down and contact the actual owner thorugh anything for example email, social medias, mail etc.

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

My carrier is Rogers

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

They contact you and shut it down providing individuals with a new SIM or even phone if they hack into your phone which is a positive as the company is trying to do something to stop it. They also try to track it to get the hacker charged although it is har people have been caught before.