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?

It’s a card within a mobile phone containing identification number and personal data of the user.

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

Without a SIM card a GSM phone won’t work and won’t connect to the cellular network.

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

A [text-based two-factor authentication](https://www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication) is a method where the user verifies their account’s identity through a text message on their phone.

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

It is related to my phone because I’ll get a verification message if I login into my social media or bank account.

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

The two-factor authentication sends a message to your phone for verification and my SIM card is in my phone. Using two-factor authentication a criminal can use personal information against you and get your SIM card and deny you access into your accounts.

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

* criminals can get a hold of cryptocurrency if the user has it
* can get hold of checking accounts
  1. Social Media
* your photos
* your account and send messages/posts

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

* looking for date of birth and other personal information by snooping around on social media and looking at your account for whatever personal information you leaked out
  1. Create False Identity
* By speaking to phone company using all the information they put together and pretending to be you in the phone
  1. Requesting a new SIM card
* After answering questions like date of birth, passwords, emails and other things, they’ll request a new SIM card to be sent to them or if they live in a remote place they can reprogram a new one
* Then by doing that they’ll have your SIM card with all your personal information and more while the SIM card in your phone will be deemed useless

1. What are some signs of SIM swap fraud?

It’s tough to find signs of SIM card fraud because most victims figure out they’ve been robbed of their SIm card when they try to call or text someone. When the criminal deactivates the SIM none of your calls can go through.

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

Some general methods is to be wary of how much personal information you put about yourself online because that's what criminals use to get a hold of your SIM card. You can also use encrypted apps that aren’t vulnerable to snooping. You should try to avoid services that provide you with SMS (Short Message Service) because its not encrypted which makes it easy to snoop.

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

AT&T

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

It has an extra security feature that’ll ask you for a password during online interaction with other people. It can be turned on if you log on to AT&T’s web dashboard.